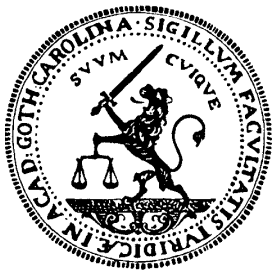


JURIDISKA FAKULTETEN
vid Lunds universitet

Christer Pettersson

Elektronisk signatur jämförd med en traditionell namnteckning

Examensarbete
20 poäng

Handledare
Eva Lindell-Frantz

Ämnesområde
Civilrätt

Höstterminen 2001

Innehåll

Sammanfattning

Electronic signatures allow software at the end of an electronic transaction to confirm the identity of the party initiating the transaction and to verify the integrity of the information received. The use of an electronic signature will begin a new era in the transition from old-fashioned pen-on-paper signatures to those that can be electronically created and stored.
The Electronic Signatures Act, granted e-signatures the same legal standing as traditional ones, went into effect in the beginning of this year 2001. There is also an EU-directive, currently being finalised in Community institutions, that will facilitate the cross-border use of electronic signatures by laying down basic common requirements to be incorporated into national law. The Electronic Signatures Act does not dictate that any particular technology to be used, leaving those choices to the marketplace. Now the parties to an electronic contract, agreement, or record have the ability to establish their own procedures and requirements when using or accepting electronic records and documents. Regardless of the method selected by users of electronic signatures, each document will retain the same legal effect, validity and enforceability of the traditional signature. Regarding the admissibility of evidence, the Act provides that in a judicial proceeding, a record or signature may not be excluded solely because it is in an electronic format. Under the terms of the legislation, consumers can choose to sign their contracts with a pen or a click.
Electronic signatures can guarantee the identity of the parties as well as the identity and confidentiality of messages and the directive gives the Member states the legal framework to work within. This approach is designed to accommodate the dynamism of electronic signature technology where certificates and certification service providers are required. The directive does not cover the legal recognition related to the conclusion and validity of contracts or other non-contractual formalities requiring signatures. Therefore the directive does not harmonise national rules on contract law or other non-contractual formalities requiring signatures. This means that the various legislative bodies need to take into account the evolution of technology and maintain a readiness to implement new legislation as the need arises rather than responding years to late. This can be made by standardisation procedures and harmonisation laws. However, the new Act contains numerous exceptions and restrictions, which may limit the law’s impact.
Many hope this new law will accelerate the speed of transacting business, consumer confidence, and advance the general development and progress of the Internet. But it will be a good alternative to try to understand the legal problems behind some contractual solutions. Electronic signatures could mean cost savings and convenience for consumers, but questions about security, liability, fraud and contracts have to be worked out.

Förord

Med visshet om att examensuppsatsen utgör det sista kunskapsprovet under juristutbildningen är det lämpligt att tacka dem som har bidragit till att det har varit en utvecklande och lärorik tid i Lund.
Speciellt vill jag tacka min handledare Eva Lindell-Frantz för att med ett stort mått av flexibilitet och kunskap har kunnat bidra till en givande uppsatsperiod. Dessutom vill jag tacka Hans Goldbeck-Löwe för hjälp med korrekturläsning.
Alla andra väljer jag att tacka med det favoritcitat som finns på en minnessten i Lund och som kan leda till eftertanke. "Lär er betänka huru få era dagar äro, för att ni må undfå att visa hjärtan"

Förkortningar

CA	Certification Authority
Ds	Departementsskrivelsen
EDI	Electronic Data Interchange
EU	Europeiska Unionen
ES	Elektronisk Signatur
HD	Högsta Domstolen
NJA	Nytt juridiskt arkiv
PKI	Public Key Infrastructure

1 Inledning

1.1 Introduktion

Under senare år har behovet av instrument för säkrare elektronisk handel ökat. Den traditionella namnteckningen behöver kompletteras med en elektronisk signatur för att fungera som ett avgörande bevis på att ett avtal har kommit till stånd. Elektronisk identifiering i kombination med elektroniska signaturer gör det möjligt att veta vem som är motpart i ett avtal slutet över nätet.
Med elektronisk signatur skall det bli möjligt att fullgöra sin avtalsskyldighet, undertecknande av en begäran om sjukpenning eller lämna in en deklaration över Internet. För att elektroniska signaturer ska kunna användas över nationsgränserna är det angeläget att uppnå en harmonisering av reglerna på området. Till följd av detta arbete att lyckas med harmoniseringen kom EU-kommissionen därför med ett direktiv om elektroniska signaturer. EU-kommissionen har gett den legala rätten för att elektroniska signaturer skall få samma juridiska status som namnunderskrifter. I Sverige har riksdagen antagit Lag (2000:832) om kvalificerade elektroniska signaturer med ikraftträdande 1 januari 2001.
Syftet med EU-direktivet och den svenska lagen är att underlätta användandet av elektroniska namnteckningar införa bestämmelser om säkra tekniska lösningar, framställa elektroniska signaturer, skapa kvalificerade certifikat samt utfärda sådana certifikat. EU-direktivet om elektroniska signaturer och motsvarande lagstiftning i Sverige har skapat en möjlighet att uppnå säkra elektroniska affärer över Internet.

1.2 Syfte

Uppsatsen bygger på en teoretisk teknisk och juridisk analys av gällande rätt angående elektroniska signaturer. Syftet är att göra en traditionellt rättsdogmatisk uppsats där en studie av olika förarbeten och doktrin skall leda fram till en deskription av gällande rätt angående ramverket för elektroniska signaturer. Uppsatsen behandlar även den teknik som krävs för att en elektronisk signatur skall fungera.
Uppsatsens andra stora del kommer att vara av analyserande karaktär för att kunna besvara frågan om den traditionella signaturens grundläggande funktioner uppfylls av en elektronisk signatur. Syftet är att bedöma hur avtalsrätt i allmänhet och hur en elektronisk signatur i synnerhet är tillämpbar i en elektronisk miljö. I relation till ovanstående bör även en internationell utveckling bedömas, om än översiktligt, för att den elektroniska handeln, som utgör den digitala signaturens hemvist, idag inte längre är någon nationell företeelse utan en global företeelse som kommer att kräva globala lösningar.

1.3 Frågeställningar

Nedanstående frågeställningar kommer att behandlas i denna uppsats**.**

1. Hur fungerar en elektronisk signatur?
2. Vilka strukturer för hantering av certifikat finns det?
3. Vilket krav kommer det att ställas på den tekniska lösningen? Kommer det att krävas hårda certifikat?
4. Kan en elektronisk signatur uppfylla en traditionell namntecknings funktioner? De funktioner som skall undersökas är[1]

- Identifiering
- Äkthetsfunktionen
- Bevisfunktionen
- Avslutsfunktionen/viljefunktionen
- Varningsfunktionen

5. Vilket bevisvärde får den elektroniska signaturen?
6. Hur pass väl anpassade är de grundläggande avtalsformerna; realavtal, konsensualavtal och formalavtal för avtalsrätt i en elektronisk miljö och hur skall förklaringsmisstag och motivvillfarelse bedömas i motsvarande miljö?

1.4 Avgränsningar

Det förefaller sig naturligt att avgränsa uppsatsen inom den tekniska beskrivningen, men det är av största vikt för en jurist att det ges möjlighet att sätta sig in i de tekniska bakgrundsfakta som finns runt ett rättsproblem. Jag har valt att låta den traditionellt begränsade metodbeskrivningen få större utrymme för att kunna förstå de texter som innehåller både tekniska och juridiska termer men utan någon straff, skadestånds eller IP-rättslig fokusering.
Det tillkommer även en avgränsning i det att jag inte diskuterar begreppet dokument och hur det sätts in i elektroniska miljöer samt heller inte gör någon djuplodande analys av vilket bevisvärde ett elektroniskt dokument kommer att få. Givetvis finns det med delar om detta i uppsatsen, men det huvudsakliga målet är inte att fokusera på detta. Det finns inte heller någon intention att göra en internationell jämförelse, utan det är fråga om att behandla den elektroniska signaturens rättsverkningar utifrån svensk rätt i relation till EU-direktivet.

[1] Teletrustrapport 4/1991“ Informationssäkerhet och digital signering”

1.5 Material

Jag har arbetat med olika juridiska källor och teknisk litteratur. De juridiska arbeten jag arbetat med är främst offentligt material i form av förarbeten till lagen om elektroniska signaturer. Det är viktig att inleda med att ställa sig den principiella frågan på vilket sätt förarbeten till lagen kan utnyttjas som underlag för lagtolkning.[2] Min åsikt är att de är ett tolkningsunderlag för en möjlighet att förstå den problematik som kommer att uppstå kring användandet av olika avtalsformer och de funktioner som en signatur kan besitta. Just i frågan om en signaturs funktioner har jag i mitt utredningsarbete funnit att doktrinförfattare hänvisar till varandra och att det därför kan vara svårt att avgöra av som är en primärkälla. Jag väljer att konsekvent ange den refererade källan utan att kommentera författarens primärkälla.
I en kommentar om de olika rättskällornas inbördes hierarki hänvisar jag till den ordning som Strömholm anger, att lagen är det uttryckliga tolkningsunderlaget och har högsta rang följt av förarbetsuttalanden och praxis.[3] Det är i detta sammanhang viktigt att nämna att rättskällehierarkin saknar en väsentlig del i mitt fall, nämligen viktiga prejudikat och praxisutveckling eftersom det inte finns någon praxis på området. Noterbart är dessutom att värdet på EU-direktivets förarbeten är begränsat.
Den juridiska argumentationen är i behov av att inte bara vara uppbyggd på åsikter utan även materiella argument. Detta får till följd att det även är nödvändigt att beakta värdefulla delar i den doktrin som finns på området när det saknas heltäckande förståelse ifrån lag, förarbeten och praxis.[4]
Flera institutioner har en utredande funktion på det studerade rättsområdet, men lagstiftningsrätten är förbehållen riksdagen. Näringsdepartementet har utrett delar om elektroniska signaturers juridiska status och hur man bygger upp en PKI-struktur. Utrikesdepartementet har analyserat frågor kring export och import av krypteringsteknologi. IT-kommissionen, som är underställd näringsdepartementet, för en öppen debatt om olika typer av exporthinder och nyckeldeponering. Avslutningsvis driver Statskontoret frågan om en elektronisk signatur ur ett säkerhetsperspektiv med hänsyn till statens behov av säkerhet och PKI-tjänster.

[2] Strömholm Stig ,Rätt, Rättskällor och Rättstillämpning, 1996, s.367

[3] Aa, s.321

[4] Aa, s.509 ff

1.6 Definitioner

Många termer verkar ha en allmänspråklig betydelse men har i själva verket en specifik juridisk-teknisk innebörd. Juridiska texter är ofta termtäta med ordrika meningar och komplicerad satsbyggnad. Detta innebär att det är av stort värde med beskrivning av definitioner för att bidra till större klarhet och enkelhet.[5]
Ordens makt över tanken kan lätt locka till felaktiga slutsatser när traditionella termer används i en ny elektronisk miljö och det kräver en defintionsbeskrivning i ett flertal avsnitt i uppsatsen. Det som genomgående har varit ett problem är det faktum att det inte har varit någon konsekvent användning av begreppen digital signatur och elektronisk signatur. Signatur är en egenhändigt skriven namnteckning för att intyga tillförlitlighet och äkthet och den tekniska utvecklingen har medfört att den kan utföras i digital form.[6]
En mycket bra definitionsbeskrivning, för att klargöra skillnaderna mellan en digital signatur och en elektronisk signatur, är hur dessa begrepp beskrivs i en ganska nyutkommen bok.[7] Digital signatur är en teknisk metod för att med kryptering och ett nyckelpar, bestående av en publik och en privat nyckel, kunna identifiera avsändare av information. Begreppet elektronisk signatur är däremot den lösning som skall vara en ersättning för en juridiskt bindande namnteckning. Tyvärr förväxlas ofta dessa begrepp.[8]
Enligt advokatfirman Lagerlöf & Leman är det endast signaturer baserade på asymmetriska öppna nyckelsystem som skall benämnas digitala signaturer, medan begreppet elektronisk signatur bör inrymma alla tänkbara varianter, från de kryptografiskt skyddade till att skriva under med sitt namn i ett word-dokument.[9]
EU-kommissionen har fastslagit att termen elektroniska signaturer skall användas för att terminologin i medlemsstaternas lagstiftningar skall vara så teknikneutral som möjligt. Kommissionens val när det gäller användandet av ordet elektronisk har dock fått en hel del kritik från remissinstanserna eftersom digitala signaturer redan är ett etablerat begrepp i alla medlemsstater.[10]
Emellertid förefaller det som om begreppet elektronisk signatur har en korrekt betydelse och kommer sålunda att användas i hela uppsatsen.

---

[5] Jensen Ulf, Rylander Staffan, Att skriva juridik, 1995, s 10
[6] Stora Svenska Ordboken, 1998, s 1068
[7] Halvarsson Andreas, Morin Tommy, Elektroniska signaturer - E-Affärer utan elände med identifiering, signering och kryptering, 2000, kap 1-2 innehåller föredömliga historiska genomgångar och en omfattande definitionskatalog.
[8] Halvarsson Andreas, Morin Tommy, Elektroniska signaturer - E-Affärer utan elände med identifiering, signering och kryptering, 2000, s 19-20
[9] Elektronisk dokumenthantering - En rättslig problemorientering, Riksarkivet/ Lagerlöf & Leman, s 23. Lagerlöf & Leman kan genom sin långa erfarenhet på området anses vara en källa med hög validitet.
[10] http://www.leksell-data.se/98edis4/signaturer.html

1.7 Disposition

Uppsatsen inleds med en genomgång av metodval och en diskussion kring hur den komparativa metoden kan angripa rättsområden som präglas av en stark koppling till tekniska lösningar.
Detta avsnitt följs av en beskrivning av de tekniska lösningarna för att ge läsaren en insikt i hur en elektronisk signatur fungerar och hur omfattande regleringen är kring det tekniska och juridiska ramverk som omger signaturen.
I uppsatsens fjärde och femte kapitel görs en rättsdogmatisk undersökning av vad som är gällande rätt vid användning av elektroniska signaturer. Dessa delar innehåller även en komparativ jämförelse för att bedöma hur implementeringen har genomförts. Till detta kommer även en kortare internationell utblick för att läsaren skall få insikt i hur långt framme EU är i sitt arbete att skapa grunden för en ökad avtalsmöjlighet via nätet. Avslutningskapitlen 6-7 innehåller de analyserande delarna där det bedöms om den elektroniska signaturen uppfyller den traditionella signaturens fem grundläggande funktioner och hur avtalsrätten fungerar i en elektronisk miljö.[11]
För att lättare skilja mellan refererade källor och egna åsikter avslutas varje kapitel med ett diskussionsavsnitt i kombination med kommentarer från olika ståndpunkter i doktrinen.

[11] Teletrustrapport 4/1991“ Informationssäkerhet och digital signering”

2 Metod

2.1 Metod

Metodologiska frågor är av stor betydelse för att få klarhet i hur det analytiska arbetssättet skall läggas upp för att ta sig an ett rättsproblem som behöver klargöras och belysas. Tyvärr förbises det ofta från den inledande argumentationen av varför man väljer att använda en viss metod. Genom att klargöra valet av metod och genom att sätta in rättsfrågorna i sitt sammanhang går det att få svar på om den elektroniska signaturen uppfyller den traditionella namnteckningens grundläggande funktioner. Till detta kommer den intressanta debatten om hur metodvalet kan göras för att få en rimlig anpassning till rättsproblem starkt bundna till tekniska ramverk och tekniska krav.

2.2 Metodval

Enligt Bogdans resonemang inskränker sig ofta analyserna i komparativ rätt till att jämföra lösningen av en viss rättsfråga och till ett begränsat antal länder.[12] Jag vill istället fokusera på olika avtalsformer samt bedöma hur signaturens grundläggande funktioner kan uppfyllas. Inget bör direkt innebära att den komparativa metoden skall inskränkas till att jämföra ett rättsproblem i olika länder utan metoden skall även kunna utgöra en juridisk arbetsform för att jämföra olika avtalssituationer i en elektronisk miljö.
I princip handlar den komparativa metoden om hur olika rättsfrågor kan besvaras genom att ställa jämförbara element i form av olika avtalsformers anpassning till en elektronisk signatur mot varandra, jämföra signaturens funktioner samt fastställa likheter och skillnader mellan EU-direktivet och hur implementeringen har skett genom den svenska lagen.
Resultatet av den komparativa metoden kan bli en bättre förståelse av den egna rättsordningen genom ett de lege lata arbete. Metoden klargör hur rättsregler och rättsinstitut fungerar i det svenska rättssystemet och resultatet kan användas för att göra en de lege ferenda inriktning med mål att uppnå bästa möjliga och rationellt effektiva lagstiftningsarbete. Men det gäller att hela tiden vara kritisk mot det material som skall studeras.[13]
Den komparativa metoden är inte på något sätt extensivt anpassad för ett fastställt antal områden där den passar utan kan med ett gott resultat användas inom ett stort antal vetenskapliga inriktningar i sitt enskilda sammanhang eller med en utmärkande tvärvetenskaplig karaktär.[14]

[12] Bogdan, Komparativ rättskunskap, 1993, s 19
[13] Aa, s 30-33
[14] Aa, s 40

EU-harmoniseringen strävar efter att direktiven skall få en klar och tydlig inkorporering i den nationella rättsordningen men det kan uppstå problem om inte detaljfrågor ses i sitt sammanhang i den övergripande rättsordning.[15] Genom att använda den komparativa metoden i tolkningen av implementeringsproceduren från direktiv till lagtext går det att få klarhet i de fel och brister som kan finnas i detaljfrågor.
Helt klart ingår det som en viktig och avslutande del inom det komparativa arbetet att försöka förklara likheter och skillnader av det som har framkommit vid jämförelsen. ”En likhet betyder ju att det inte föreligger skillnader, medan en skillnad inte är något annat än en brist på likhet.” Både likheter och skillnader styrs i olika riktningar av samma påverkande faktorer. En rimlig lösning på detta moment 22 problem blir att koncentrera sig på hur pass väl den elektroniska signaturen uppfyller den traditionella signaturens liknande och grundläggande funktioner.[16]

2.3 Metodologisk diskussion för teknikrelaterade rättsproblem

Uppsatsens frågeställningar bör vara ett tungt vägande skäl för att styra valet av metod för att uppnå bästa möjliga och genomarbetade resultat och slutsatser. Fördelen med den komparativa metoden är att den har ett teknikneutralt angreppssätt på rättsregler oavsett om de är rent juridiskt baserade eller i sammanhang med tekniska lösningar.
Den nya generationens jurister menar att lagstiftarna måste ta den tekniska utvecklingen på allvar och upprätthålla en beredskap för att införa ny lagstiftning i takt med att problemen uppstår inom teknikrelaterade rättsområden innan det är för sent.[17]
Ett sätt att vara aktiv är att bevaka tendenser hos rättstillämparna och utvecklingen av sedvänjor och handelsbruk. För att en sedvänja skall beaktas krävs att det är fråga om en spridning inom relevanta handelsområden samt att det har skett under en beaktansvärd tidsperiod. Sedvänjan skall även utgöra en bindande bestämmelse för avtalsparterna och ha en ofrånkomlig påverkan på det berörda rättsområdet. Det blir helt enkelt lättare att uppnå en aktuell lagstiftningsutveckling om sedvänjorna kan omsättas i legitim lagstiftning.[18]
Vissa jurister är kritiska till den metod och de förarbeten som har använts för att uppnå ett underlag för att skapa ny fungerande lagstiftning.[19] Åsikten är att utredningarna håller en alltför låg klass där det även saknas standardiserande lösningar som hade kunnat vägleda lagstiftaren. Problemet

[15] Aa, s 52
[16] Aa, s 71
[17] Plöen The concept of “Urkund” and Information technology, s 145 artikel i Essays on Legal information management.
[18] Strömholm, Aa, s. 239
[19] Wahlgren, Om framtida rättsproblem, 1998, s 9-20, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik, 1998, Jure AB, Stockholm

är enligt Wahlgren att det är svårt att ta ett steget från befintliga företeelser till att beakta icke realiserade framtida rättsproblem som faktorer för att utmärka rättsproblem i behov av regleringar. Utvecklingen styrs i två riktningar där rättsutvecklingen kan ha påverkat möjligheten att använda tekniken på ett effektivt sätt, alternativt att komplexiteten i sig har hindrat möjligheten till rättsutveckling. Teknikens svårtillgänglighet och begreppsproblematik har medfört att utredningarna inte har kunnat medföra en anpassad och föränderlig lagstiftning. Men det är på gott och ont att den befintliga regleringen inte ändras så snabbt utan att ledord som förutsebarhet och rättssäkerhet talar för en avvaktande hållning till accelererande teknisk utveckling[20] Förklaringen till att det är så svårt för lagstiftaren att skapa nya rättsregler är att många av de tekniska begrepp som har uppdagats under senare tid helt enkelt saknar en juridisk motsvarighet. "Det går inte att applicera befintliga rättsregler på nya tekniska företeelser." [21]
Hultmark väger för och nackdelar mot att få till en effektiv utveckling för elektroniska signaturer med sådana kommentarer som att domarna vid tolkningen av regler kring de elektroniska signaturerna bör avvakta. Utvecklingen får inte hindras av att domarna beaktar en felaktig doktrin som skall vägleda den samhälleliga rättsutvecklingen som är i behov av en reglering. Men det är inte givet att en påskyndad lagstiftningsprocess kan bidra till en positiv utveckling för signaturer som ett ex på anpassning till ett tekniskt relaterat rättsproblem. Det är svårt att uppnå en teknikneutral lagstiftning och att den på samma gång kan vägleda i praktiska tillämpningsfall utan att vara alltför generell. Dessutom innebär det att om lagstiftningen knyts upp till en gällande teknisk standard så kan det i sig innebära en blockering av alternativt bättre fungerande tekniska lösningar. Lösningen kan enligt Hultmark vara att skapa en ramlagstiftning som kan fyllas ut med självreglering inom tekniskt komplicerade och anknytande rättsregler.[22]
Det huvudsakliga kravet på att det komparativa arbetet skall kunna göras inom tekniskt relevant och anknuten rättsreglering är att det finns ett nationellt och en gemensam typ av egenskaper, alternativt någon form av formellt gemensamt drag i avtalsformerna och regleringarna. Min bedömning blir att den komparativa metoden helt klart kan användas i jämförelsen mellan signaturens funktioner, hur olika avtalsformer fungerar samt hur implementeringen har gått tillväga av EU-direktivet till svensk lag.

[20] Wahlgren, Om framtida rättsproblem, 1998, s 9-20, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik, 1998, Jure AB, Stockholm
[21] Westman, Informationsteknikens påverkan på den rättsliga regleringen, 1998, s80-81, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik, 1998, Jure AB, Stockholm
[22] Hultmark, Digital signatur - internationella utvecklingstendenser, 1998, s 163-65, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik, 1998, Jure AB, Stockholm

3 Teknik

3.1 Teknisk genomgång

Avsikten med detta kapitel är att beskriva hur en elektronisk signatur fungerar.
Det finns redan idag elektroniska signaturer. Den som exempelvis gör sina bankaffärer över Internet använder sig av en kod som fungerar som en signatur. Men dessa signaturer görs i slutna system, man måste med andra ord komma in i bankens system innan man kan använda sig av dess tjänster. Koden har kunden fått av banken som vet att just den kunden har den avsedda koden. Men hur gör den som vill beställa en vara eller en tjänst via ett öppet system, t.ex. genom ett e-handelsföretags hemsida och hur kan handlaren veta att beställningen är äkta, det vill säga att den som beställer också är den som kommer att betala?
Ramverket för att en elektronisk signatur skall fungera är ganska omfattande med PKI-struktur, kryptering, CA, ansvarsfrågor och det har skapats tekniska utvecklingar som smarta kort för att underlätta för den elektroniska signaturen att få ett genomslag i den elektroniska handeln. Nedan följer en beskrivning av teknik, elektronisk signatur, och bakomliggande ramverk med en avslutande teknikdiskussion.

3.2 Hur fungerar en elektronisk signatur

Signering innebär att man kan identifiera avsändaren samt att man kan avgöra att informationen inte är förändrad på vägen från avsändaren. En grundläggande del i elektroniska signaturer är asymmetriska krypton. I ett asymmetriskt krypto har sändare och mottagare olika nycklar till skillnad mot ett symmetriskt krypto där sändare och mottagare har samma nyckel. I det asymmetriska kryptot är den ena nyckeln privat och måste hållas hemlig, medan den andra, publika, skall vara tillgänglig för alla.[23]

Principen för en elektronisk signering är följande.[24]

1. Avsändaren beräknar kontrollsumma

> En programvara beräknar med en känd formel en kontrollsumma utifrån den information som ska signeras. Det fungerar ungefär på samma sätt som sista siffran i personnumret som är framräknad utifrån de nio första.

[23] Användning av ID-kort - EID, SEIS-rapport 1998, s 16-20
[24] Alpman, Digitala signaturer på väg, Ny Teknik 2001:5, s 17

2. Avsändaren krypterar kontrollsumman med privat nyckel

Kontrollsumman krypteras sedan med avsändarens privata, hemliga, nyckel. Den krypterade informationen, checksumman, bifogas originalinformationen som inte är krypterad. Denna bilaga är en elektronisk signatur.

3. Information och signatur publiceras eller överförs

Nu kan informationen och signaturen distribueras tillsammans.

4. Mottagaren dekrypterar bilagan med kontrollsumma

En mottagare som vill säkerställa informationen kan dekryptera bilagan med avsändarens publika nyckel. Då får man fram en kontrollsumma.

5. Mottagaren beräknar ny kontrollsumma

Mottagaren beräknar en ny kontrollsumma utifrån informationen, givetvis med samma formel som avsändaren använde.

6. Kontrollsummorna jämförs

Den nya kontrollsumman jämförs med den man fått fram genom att dekryptera bilagan till informationen. Om dessa två värden stämmer överens har man kommit fram till två slutsatser. Den första är att avsändaren är den man tror det är (förutsatt att man kan lita på att den nyckel man använt är rätt nyckel) och den andra att informationen inte förändrats. Om värdena inte stämmer överens är antingen informationen förändrad eller avsändaren inte den han utger sig för att vara.

3.3 PKI, Public Key Infrastructure[25]

Public Key Infrastructure, PKI, är en kombination av teknik och regelverk som gör det möjligt att genom certifikat skydda kommunikation över öppna nätverk, t.ex. affärstransaktioner på Internet. PKI möjliggör elektroniska signaturer och elektronisk identifiering med certifikat och asymmetriska krypton. Det viktigaste i en PKI är det regelverk som styr verksamheten i de organisationer som utför olika funktioner. Begreppet PKI står för hela den infrastruktur som ska stödja användningen av elektroniska signaturer. I en PKI ingår en rad olika funktioner, t.ex.

- Certifiering, skapande av certifikat
- Verifiering, kontroll av certifikat
- Funktioner för att tillverka privata/publika nyckelpar
- Revokering, återtagande av certifikat

[25] Användning av ID-kort - EID, SEIS-rapport 1998, s 9-10

3.4 Kryptering

I princip finns det fem skyddsvärda områden som utnyttjar krypteringsteknik och dessa är:[26]

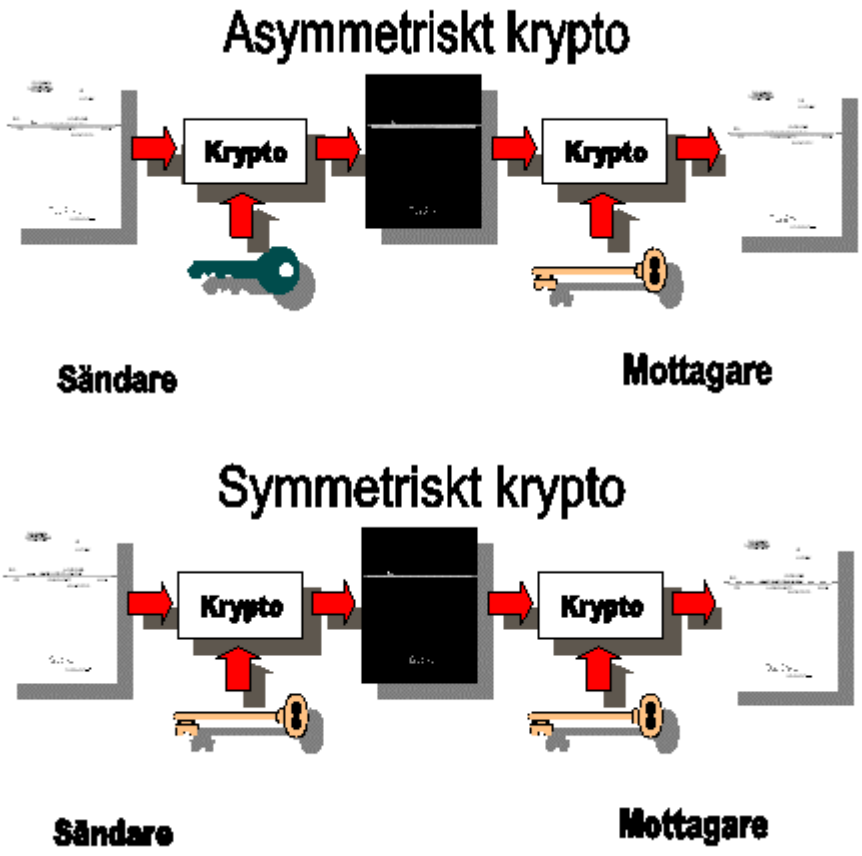
- Äkthetsbevis
  - skydd mot att den som skickar ett meddelande inte är någon annan än den han uppger sig vara
- Insynsskydd
  - skydd mot att ett meddelande kan läsas av obehöriga
- Förändringsskydd
  - skydd mot förändring av innehållet i ett meddelande
- Elektronisk signatur
- Skydd mot förnekande
  - skydd mot förnekande av ursprung och mottagning av meddelande. Tekniken kan bevisa att det var du som skickade meddelandet eller att du mottagit det.

Kryptering kan användas för identifikation för att avgöra vem man kommunicerar med. Man kan med hjälp av krypteringsteknologi skapa en elektronisk signatur, en namnteckning på ett elektroniskt dokument. Dessutom kan man använda samma teknologi för att kontrollera att dokumentet inte förändrats, att dess integritet har upprätthållits. Men när krypteringen utförs av datorer kan den också tas bort med datorer. Därför är nyckelns längd avgörande. Ju längre nyckellängd, desto längre tid tar det att beräkna värdet innan det går att få fram skyddad information. Kryptot är i princip en matematisk algoritm som kan bidra till att intrångsgöraren kan komma över de privata nycklarna.[27] Ett bra exempel för att visa på krypteringens fördelar är säker e-post.
Om person X får brev från Y och Y har krypterat brevet med sin privata nyckel kan X tack vare nyckelhanteringen vara säker på att brevet kommer från Y. Brevet är dock inte skyddat för läsning av andra eftersom vem som helst kan få tag på en publik nyckel.
Om Y dessutom krypterar brevet med X publika nyckel, kan bara X läsa brevet med hjälp av sin egen privata nyckel. Då har man dels säkrat meddelandet för obehörig läsning, dels säkerställt avsändarens identitet.

[26] Salomonowitz Sascha, Essays on Legal Information Management, IRI-rapport 1996:2, s 149-150
[27] Aversten Daniel, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s17

3.4.1 Asymmetrisk kryptering[28]

Asymmetrisk kryptering baseras på två olika nycklar. Den ena kallas hemlig (ofta också "privat" från engelska "private key") och den andra öppen (ofta också "publik" från engelska "public key"). Kryptering med den ena nyckeln kan endast dekrypteras med den andra, och därför kan den s.k. öppna nyckeln, göras fritt tillgänglig.
Eftersom nycklarna är beroende av varandra kan man vara säker på att information man kan dekryptera med den ena nyckeln är krypterad med den andra. Omvänt kan man också vara säker på att om man krypterar information med en nyckel, kan den bara dekrypteras med den andra. Asymmetrisk kryptering används bl.a. för elektroniska signaturer och identifiering.



29

3.4.2 Symmetrisk kryptering[30]

För rak kryptering, eller symmetrisk kryptering, använder man samma nyckel för kryptering och dekryptering. Det gör att både sändare och

[28] Statskontoret skrift 1999:17, Strukturer för hantering av certifikat och krytonycklar i Sverige, bilaga 1, s 3-4
[29] Egen skiss
[30] Aversten Daniel, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s16

mottagare måste ha samma nyckel. Rak kryptering används ofta vid kryptering av ett meddelande där hastigheten är viktig. Kryptoformeln är enklare och det gör att det går åt mindre datorkraft för att kryptera och dekryptera information.
Ett problem är överföring av den gemensamma nyckeln. Eftersom nyckeln måste hållas hemlig för att garantera säkerheten måste den överföras mellan avsändare och mottagare på ett säkert sätt över ett nätverk, till exempel på diskett för att inte någon obehörig skall kunna utnyttja den. En symmetrisk kryptering är alltid snabbare och enklare för datorn att jobba med än asymmetrisk. Samma sak gäller tyvärr också för den som ska knäcka koden.

3.5 CA, Certificate Authority

En organisation som utfärdar certifikat kallas *certificate authority*, CA. En CA är en instans som tillhandahåller tjänster för hantering av certifikat och kryptonycklar för områden som signering, identifiering och konfidentialitet. Posten och Telia är bolag som erbjuder CA-tjänster. Det viktiga är att företaget som utför tjänsterna har förtroende hos användarna för att de skall kunna lita på sina elektroniska signaturer.[31]

3.5.1 Interna och externa CA

En CA kan vara en intern funktion i ett företag. Banker kan t.ex. ha en egen CA-tjänst för signering av nycklar tillhörande kunder som vill använda Internet-tjänster. Ett företag kan utfärda certifikat för nycklar som anställda ska använda i tjänsten. Det går även att anlita en extern CA, ett företag med certifieringstjänster. Det används främst för webbservercertifikat och för e-post. Ett diskuterat alternativ är att låta tillsynen över CAs styras av ackrediterade certifieringsorgan som kontrollerar att en aktör är seriös. Det ackrediterade organet certifierar CAn enligt en viss standard och det krävs att ackrediteringen har skett ifrån ett ackrediteringsorgan. I Sverige är det SWEDAC som ackrediterar.[32] Ett argument som talar emot ett certifieringsorgan är att CAs certifikat måste erkännas av EU-länderna för att fungera och det låter inte rimligt att ett erkännande skulle komma för alla privata organisationers certifikat.[33]

---

[31] Statskontoret skrift 1999:17, Strukturer för hantering av certifikat och krytonycklar i Sverige, s 4

[32] Statskontoret skrift 1999:17, Strukturer för hantering av certifikat och krytonycklar i Sverige, s 5

[33] Noterbart är det enligt 11 kap 6§ regeringsformen krävs stöd i lag om en myndighet anlitar en CA-tjänst som drivs i privaträttslig regi och om den tjänsten på något sätt fyller en funktion av att få karaktären av att ha en förvaltningsuppgift med inslag av myndighetsutövning. Det är lätt att någon myndighet förbiser detta grundlagskrav när det utkontrakterar sin verksamhet i form av olika ramavtal till privaträttsliga subjekt som tillhandahåller tjänster som även medborgarna tar del av. Källa Elektronisk dokumenthantering - En rättslig problemorientering, Riksarkivet/ Lagerlöf & Leman, s 38

Den riktning som Statskontoret förespråkade var att skapa en s.k. toppnod, en myndighet med yttersta övervakningsansvar, som får ett övergripande ansvar för att identifiera de organisationer som erbjuder certifikattjänster och skapa förtroende för de certifikat som cirkulerar.[34] Denna lösning blev också det som tillämpades i och med det att Post och telestyrelsen utsågs till toppnod.[35]

3.5.2 Certifiering - kopplingen mellan verkligheten och nyckeln[36]

Certifiering är en lösning för att koppla en person eller en organisation till ett nyckelpar och därmed binda innehavaren till sina rättshandlingar om inget oförutsett inträffar i hanteringen eller kontrollen av nyckelparet. Andra viktiga delar i certifieringen är verifiering och återkallande av certifikaten.

Certifiering
Certifieringen utförs av en CA. Certifikatet ett bevis på en koppling mellan ett nyckelpar och en person, ett företag eller ett datorsystem. Certifikat är alltid tidsbegränsade då de upphör att gälla. Då bör användaren byta ut sina nycklar och certifiera ett nytt nyckelpar.
Verifiering
Om en användare presenterar ett certifikat med en publik nyckel kan mottagaren vilja verifiera att certifieringen fortfarande är giltig, ungefär som man kontrollerar kreditkort vid användning.
Återkallande, Revokering
Om en CA av något skäl vill återkalla en certifiering bör denna information spridas snabbt, så att inga mottagare accepterar användning av nycklarna. Det kan t.ex. vara en anställd som har slutat och inte längre får använda tjänsteverktygen som behörig att kommunicera som företrädare för företaget.

3.5.3 CAs Ansvarsroll

En användares certifikat är utfärdat av en CA som med sin egen nyckel signerat själva certifikatet. Genom denna certifiering har mottagaren en möjlighet att avgöra om det är rätt nyckel man erhållit. Någonstans måste en mottagare av certifikat för en användare hitta en stark länk, ett certifikat utfärdat av en CA-tjänst man litar på. När det är fråga om nättransaktioner som ska utföras på kort tid har man inte tid att utföra en sådan omfattande kontroll. Även om man löser problemet med tiden så hamnar man i nästa fälla, vilket är omfattningen av all kontroll. Därför är det svårt att tro att ett

[34] Statskontoret skrift 1999:17, Strukturer för hantering av certifikat och krytonycklar i Sverige, s 2
[35] Se bilaga C
[36] Aversten Daniel, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s 23

enda nationellt system skulle fungera. Ingen har ett sådant system i funktion och att satsa på ett sådant utan praktisk erfarenhet verkar väldigt riskabelt. Än mindre är det troligt att ett sammanhängande internationellt CA-system, en enda PKI, tas i bruk. Det lär bli många parallella system av olika karaktär och med olika applikationsområden. Därför växer nu flera olika CA-system upp, som fungerar tillsammans, men i olika tillämpningsområden och i olika nischer.[37]

Digitala certifikat för identifiering av användare vid olika typer av elektroniska avtal är antingen hårda, skyddade på ett smart kort, eller mjuka, lagrade direkt på hårdisken. Mjuka certifikat har ansetts vara för osäkra, riskerna är att en intrångsgörare kan komma åt certifikatet och utnyttja det för egen vinning. Det kommer nu lösningar från företag som har utvecklat teknik för att göra mjuka certifikat säkrare. Det handlar om att gömma det fungerande certifikatet från obehöriga på hårddisken och om någon försöker att använda de tusentals privata nycklar som finns så loggas man ut efter tre felaktiga försök.[38] Det innebär i princip att ett mjukt certifikat kan upprätthålla samma säkerthetsnivå som ett hårt och att det blir billigare men som kravet är i lagstiftningen så skall hårda certifikat användas för att ett signerat avtal med en elektronisk signatur skall vara giltig. Men det ger ändå en indikation på att tekniken hela tiden utvecklas och sätter press på att lagstiftaren måste anpassa sig.

Möjligheten att lagra privata nycklar på filer gör att man uppnår samma säkerhetsfunktion som på ett smart kort. Huvudskillnaden är att man lagrar nyckeln på en fil och låter en applikation byta ut kortets funktion tillsammans med filen. Negativt blir att filerna har lägre insynsskydd är korten och att filerna kan kopieras. Positivt blir att applikationen ersätter så att det inte behövs någon kortläsare samt att det blir billigare.[39]

Lösningen för att skydda mottagaren som litar på certifikaten har medfört att det har tagits med ett skadeståndsansvar i de fall då certifikaten anses vara kvalificerade. En utfärdare blir skadeståndsskyldig om certifikaten inte uppfyller lagens kriterier. Det har införts ett presumtionsansvar i Lagen om kvalificerade elektroniska signaturer 14 § vilket innebär att en utfärdare blir skadeståndsskyldig om kraven i 14§ inte är uppfyllda och utfärdaren inte kan visa att det inte beror på vårdslöshet från honom. Dock är det oklart i vad man lagen kan tillampas för att bedöma ansvar för utfärdande av certifikat som ej omfattas av lagen. Den frågan kommer säkerligen lösas i framtida praxis. Risken är dock att utfärdare gör förbehåll i sina certifikat vilket leder till att de inte anses som kvalificerade.[40] Det går till på så sätt att CA begränsar sin skadeståndsskyldighet genom ett avtal eller klausul med bindande verkan eller begränsar ansvaret mot förlitande part genom att ta med en s.k. recommended reliance limits i certifikatet.[41]

---

[37] Användning av ID-kort - EID, SEIS-rapport 1998, s 13-14

[38] Computer Sweden nyhetsbrev 2000-09-08, Ricknäs Mikael, Arcot öppnar för mjuka certifikat.

[39] Säkerhet med elektronisk identifiering. Statskontoret 1999:30, s 17

[40] Examensuppsats Juridiska fakulteten vid Lunds Universitet, Made Erik, Ansvarsfrågor mellan certifikatutfärdare och mottagare vid elektroniska signaturer, s1, vt 2000

[41] Aversten Daniel, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s 91

Angående nyckelinnehavarens ansvar mot förlitande part bör det inte ske något undantag ifrån huvudregeln att part ej blir bunden av att någon har förfalskat underskriften. Dock bör det ställas krav på nyckelinnehavaren att vara aktsam och om det sker ett vårdslöst borttappande av det smarta kortet så kan det leda till skadeståndsskyldighet.[42]
Förhållanden som inte omfattas av lagens särskilda skadeståndsansvar får istället bedömas i enlighet med allmänna skadeståndsrättsliga principer och i förarbetena till Lagen om kvalificerade elektroniska signaturer 14-15 §§ så anges det att rena förmögenhetsskador bör ersattas.[43]

3.5.4 Certifieringspolicy

En CA verifierar koppling mellan en publik nyckel och en fysisk eller juridisk person. Hur verifiering sker, vilka rutiner man har och hur man hanterar nycklar beskrivs i en certifieringspolicy, certificate policy statement. Certifikatet är basen, själva kopplingen, mellan ett nyckelpar som kan användas för säker e-post, kryptering eller identifiering, och en juridisk person. På certifikatet finns det uppgifter omfattande namn och adressuppgifter och andra nödvändiga administrativa data. Till detta läggs den publika nyckeln som tillhör användaren. CAn uppger egna administrativa data, bland annat hur man kan nå CA för kontroll av intyget, hur länge intyget är giltigt och hänvisning till servrar. En typ av tjänst är utfärdande av certifikat för webbservrar, certifikat som intygar att en nyckel som en viss server använder verkligen hör till den servern och till ett specifikt företag. Genom att upprätta certifikatpolicy och praxis, s.k. Certification Practice Statement, för utfärdande av certifikat kan det visa vilken grad av trovärdighet som certifikaten bör ha enligt de rutiner som anges samt hur de skall tillämpas inom ramen för den angivna och avsedda policyn. Detta kan ta sig uttryck som att ange regler för utlämning och förvaring av den privata nyckeln, PIN-hantering, låsning, öppning och aktivering.[44]
En certifieringspolicy skall reglera det som berör trovärdigheten för certifikatets innehåll och tillförlitlighet. Det viktiga är att certifikatet kopplar ihop rätt persons identitet med hans privata nyckel och att det ges bestämmelser för att skydda den privata nyckeln.[45]

[42] Aversten Daniel, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s91
[43] Proposition 1999/2000:117 Lag om kvalificerade elektroniska signaturer, m.m. s 75
[44] Elektronisk dokumenthantering - En rättslig problemorientering, Riksarkivet/ Lagerlöf & Leman, s 26-27
[45] Användning av ID-kort - EID, SEIS-rapport 1998, s 9

3.6 Elektronisk handel[46]

Elektronisk handel och elektroniska affärer är ett mycket omfattande område där tilltron är stor till att en elektronisk signatur skall kunna lyfta e-handeln. Önskemål finns för att skapa en standard för elektroniska affärer som kan fungera via Internet på ett säkert sätt. Elektronisk handel omfattar många saker som konfidentialitet, integritet och identifikation. Den infrastruktur och de standarder som tas fram på Internet för elektroniska affärer bygger på att uppfylla de här principerna, men redan idag utan alla lösningar för säkerhet på plats har mängden transaktioner som görs över Internet ökat dramatiskt. Det är de stora elektroniska affärssystemen som är drivmotorn idag och de har löst transaktionens giltighet med att en tredje part stämplar dokumentet och loggar när dokumentet signeras, avsänds och mottas så att transaktionen inte kan avvisas av någon av de avtalsslutande parterna.
Men det är ett steg kvar till att få samma genomslag för konsumenthandel via nätet och nyckeln till en rejäl ökning kan vara en fungerande elektronisk signatur. Debattörer menar att de traditionellt inriktade internetportalerna kommer att omvandlas och även utvecklas till internetbaserade finans och kreditinstitut där behovet av en signaturlösning kommer att vara stor.

3.7 Smarta kort[47]

Smarta kort, s.k. aktiva kort, innehåller intelligens i form av ett chip och en mikroprocessor. Mikroprocessorn gör att man kan programmera kortet där processorns minneskapacitet avgör hur många funktioner som får plats. Det smarta kortets minne nås bara via mikroprocessorn och detta ger hög säkerhet. Kortet innebär en funktionell säkerhet för att använda en elektronisk signatur genom att användarens privata kryptonycklar skapas och lagras på det smarta kortet, där funktionen elektroniskt ID-kort dominerar. Samtliga operationer som utförs med de privata nycklarna sker direkt på det smarta kortet, där det måste öppnas med en personlig PIN-kod.[48]
Fördelarna är helt enkelt att de är bättre skyddade mot kopiering. De kan innehålla en hemlighet som inte kan läsas ut ur kortet, men lätt kontrolleras att den stämmer. Detta bidrar starkt till att det smarta kortet kommer att utgöra och säkerställa en elektronisk identitet som gör det möjligt att skapa giltiga avtal. Nackdelarna är att det är svårt att få till en gemensam standard och att uppnå en kompatibilitet mellan olika länder. Dessutom finns det integritetsaspekter genom att det är lättare att koppla ihop inköp som görs med en elektronisk signatur krypterad med det smarta kortet än att följa en individ som handlar via en dators IP-nummer.

---

[46] Digital kråka lyfter e-handeln, Precht Elisabeth, Svenska Dagbladets näringslivsdel, s 15,16/5 2000
[47] Smarta kort - den smartaste lösningen?, Höynä Ulla-Karin, Teldok info nr 17, utgiven i maj 1997 av Teldok
[48] PIN, Personal Identification Number

Fördelarna med det smarta kortet överväger. Ett tungt vägande skäl att den elektroniska signaturen ligger på det smarta kortet och inte på någon hårddisk. Det smarta kortet klassas som ett hårt certifikat vilket innebär att det är näst intill omöjligt att komma åt den privata nyckeln om signaturer krypteras med asymmetrisk metod. Dock ställs det i relation till kontokort ett krav på att hålla en noggrann koll över sin PIN-kod.
Telia har gett sina 25000 anställda ett smart kort med elektronisk signatur för att de skall kunna skicka säker e-post, logga in och identifiera sig själva med sitt kort. Ledningen för Telia anser att genom att låta storföretag använda sig av smarta kort med signaturer skall tekniken få genomslag i samhället och att det då blir en kommersiellt gångbar produkt med lönsamma kringtjänster.[49]

3.8 Det elektroniska ID-kortet

Det elektroniska ID-kortet är personligt och varje användare har, i kortet, ett unikt nyckelpar. Nyckelparet består av en hemlig nyckel lagrad på kortet och en kompletterande, publik, allmänt åtkomlig nyckel. För att kunna skapa elektroniska signaturer krävs en asymmetrisk krypteringsalgoritm som använder sig av dessa båda nycklar. Detta medför att den publika nyckeln kan användas för verifiering av signaturer samt kryptering av meddelanden till nyckelinnehavaren. Den privata nyckeln kan användas för signering och dekryptering av meddelanden. Signering blir ett nödvändigt krav för att i efterhand kunna avgöra äktheten i en påstådd viljeyttring.[50]
Utvecklingen har tagit fart i Finland där man under år 2000 har gett invånarna en möjlighet att få elektroniska ID-kort med elektroniska signaturer och det har fått ett stort genomslag tack vare att det har introducerats flera tjänster på kortet förutom en signatur och identifieringsfunktionen.[51]

3.9 Teknisk diskussion

Mycket arbete läggs ner i EU och i svenska myndigheter på att anpassa lagar och regler för att göra den elektroniska signaturen säker och legalt giltig. Frågorna är många, problemen omfattande och lösningarna är svåra att ta fram. I princip är det intressant att undersöka vad det finns för riskområden, hur analogiresonemang kan föras i förhållande till kontokortsanvändning och knyta ihop dessa resonemang.

[49] Computer Sweden nyhetsbrev 2000-12-04, Hultkvist Jesper, 25000 Teliaanställda får digitala signaturer.
[50] Rapport angående elektronisk identifiering med elektroniskt identitetskort, red Ankarberg, Rikspolisstyrelsen, 2000
[51] Computer Sweden nyhetsbrev 2000-02-21, Ricknäs Mickael, Succé för elektroniska ID-kort i Finland

3.9.1 Riskområden

Användningen av Internet och elektroniska signaturer för kommunikation och avtalsslutande medför en del risker inom ett antal områden på grund av den elektroniska informationens karaktär av att vara mindre respektfull och att invanda fysiska kännetecken saknas. Det bidrar till risker genom att hela signeringsförfarandet kan ske på ett anonymt sätt och att avtalshastigheten är hög.[52]
Winberg menar att det finns sex olika aspekter som måste säkras vid användning i en elektronisk miljö och dessa är:[53]

- Dataintegritet - att skydda informationen som överförs eller lagras.
- Autenticitet - att försäkra sig om att ett meddelande verkligen kommer ifrån den rätta avsändaren och det kan ske med hjälp av någon form av identifikation genom något fysiskt kännetecken som en signatur eller ett lösenord.
- Icke-förnekande av ursprung eller mottagande - att bevisa att köparen inte skall kunna förneka att han beställt en vara eller att säljaren skall kunna förneka emottagen betalning.
- Konfidentialitet eller insynsskydd - att hålla informationen hemlig för utomstående med hjälp av kryptografi eller annan teknisk lösning.
- Duplikatskydd - att förhindra att samma information används mer än en gång. Det kan lösas med hjälp av tidstämpling och detta framgår tydligast i de fall då användandet av elektroniska pengar skall ske.
- Tillgänglighet - att garantera åtkomsten till den elektroniska signaturen och datasystem.

Dessa tekniska säkerhetsaspekter bör åtgärdas för att se till att datorkommunikation med elektroniska dokument blir en säker metod för att utbyta viljeförklaringar och för att avtal i en elektronisk miljö skall vara rättsligt giltiga. Det är i detta sammanhang av vikt att det ges ett straffrättsligt skydd.
Trots ett stort behov av ett straffrättsligt preventivt skydd har det inte hänt särskilt mycket. Av utredningen SOU 1992:110 framgår att det krävs lagändringar för att ge elektroniska dokument och elektroniska signaturer ett likvärdigt straffrättsligt skydd som deras traditionella pappersbaserade motsvarigheter men att detta ej har genomförts och lagstiftningsförändringar låter fortfarande vänta på sig.[54]

[52] Winberg, Elektroniska betalningssystem på Internet, IRI-Rapport 1997:3, Stockholms Universitet s 42-43
[53] Winberg, Aa, 49-52
[54] SOU 1992:110 Information och den Nya Informationsteknologin - Straff och processrättsliga frågor mm, s 230, 268

3.9.2 Analogiresonemang

Ett sätt att bedöma omfattningen av skyddet för den elektroniska signaturen, PIN-koden och den privata nyckeln är att göra ett analogiresonemang med kontokort och kortnummer.
Huvudregeln enligt Lag (1977:981) om konsumentkredit är att kreditföretaget står för risken att någon obehörigt har utnyttjat kontonummret. Kraven som ställs på en kontokortinnehavare idag är enligt praxis till 34§ 1 st 3p att kortet måste spärras direkt och att man står svarslös mot kreditföretaget om man på något sätt genom grov oaktsamhet har tappat bort kortet och kontonummren. Enligt ansvariga på kreditföretagen anses det att vara grovt oaktsam om man har lämnat ifrån sig kortet i en garderob men att man skyddas om det har försvunnit i hemmet.[55]
Det gäller likväl som med kontokort att hålla koll på sin privata nyckel för att inte det skall leda till man genom oaktsamhet tappar bort nyckeln och PIN-koden. Huvudregeln som bör bli snarlik för elektroniska signaturer är att man inte kan tvingas betala för något som man inte har beställt och att det är motparten som har bevisbördan för att man verkligen har beställt varan som man enligt kontoutdraget har betalat för. Råden blir dock att hela tiden kontrollera sitt kontoutdrag så att inte någon har fått tillgång till den privata nyckel och sätter igång att handla med den.[56]
Vårdslösheten från en nyckelinnehavares sida kan bestå i att inte förvarat sin privata nyckel eller PIN-koden på ett betryggande sätt, eller att inte ha spärrat nyckeln genom att anmäla till CA att den blivit stulen. Uppfylls dessa krav är en elektronisk signatur lika betryggande för en konsument som ett kreditkort.

3.9.3 Olika ståndpunkter i doktrinen

Det har nu kommit fram förklaringar om varför rättsliga problem uppstår vid användningen av IT. Det finns förespråkare som menar att lagstiftaren inte hänger med i utvecklingen och att gällande lagstiftning blir ett hinder mot att på ett bra sätt kunna utnyttja teknologins möjligheter. Det som delvis skapar rättsproblem i sammanhang med IT-användning är den anonymisering som här sker då olika avtal skall slutas. Det tar sig uttryck som att avtalsparterna aldrig möts öga mot öga och att det blir allt svårare att avgöra vad som krävs för att en handling skall vara fullbordad med rättsverkan. Lagstiftaren får ett krav på sig att skapa en rättsmiljö som individen förstår för att kunna hantera anonymiseringen. Individen får inte gömma sig bakom argumentet att man inte förstod att man ingick ett avtal bara för att det skedde via Internet.[57]

[55] Sydsvenskan 21/ 2000 C2 Delen.
[56] Aftonbladets IT-bilaga nr 10 28/5 2001, s 15
[57] Benno, Elektronisk handel - rättsliga aspekter, 1997, Transaktionens anonymisering och dess påverkan på rättsliga problemställningar, s50-53

Lösningen enligt artikelförfattaren är att bedöma hur den aktuella rättsregeln påverkas av anonymisering och därefter förändra den i riktning mot att den även kan fungera i nya avtalsrättsliga elektroniska miljöer. Men det får inte ske genom att via lagstiftningsvägen ta hjälp av allmänt hållna målparagrafer och generalklausuler för det leder knappast till ett kvalitativt resultat. Dock går det att uppnå en flexibilitet genom att skapa regleringslösningar för att sedan låta lagen ta vid. Enligt Benno blir då den kodifierade rätten mer dynamisk och anpassad för att motverka anonymisering och motverka rättsproblem som uppstår vid IT-användning.[58] Ett viktigt tillvägagångssätt är att lagstiftaren, som vissa författare har gjort, tar de juridiska aspekterna som utgångspunkt för att definiera krav på tekniken och i denna typ av tillämpningar verkligen bedömer hur pass dynamisk tekniken är och att juridiken då kan utvecklas fritt om lagen görs teknikneutral.[59] Dock är inte den tekniska utvecklingen på något sätt förutsägbar utan lösningar som biometriteknik i form av fingeridentifiering kan delvis ersätta den elektroniska signaturen och dess PIN-kod.[60] Det som kan ske är att med biometriteknik kunna använda tumavtryck istället för PIN-koden och via den vägen komma in i sitt smarta kort och kunna använda sin elektroniska signatur.[61]

[58] Aa, s 68-75
[59] Teletrustrapport 4/1991“ Informationssäkerhet och digital signering” s 27
[60] Precise Biometrics Årsrapport 2000
[61] Computer Sweden nyhetsbrev 2000-09-15, Åsblom Joel, E-signaturer snart i var mans hand.

4 EU-direktivet

4.1 Direktivet[62]

EU-direktivet om elektroniska signaturer 1999/93/EG föreskriver att varje medlemsstat i sin egen lagstiftning ska ha implementerat direktivet senast den 19 juli 2001. Huvudinnebörden i direktivet är ett legalt godkännande att elektroniska signaturer skall uppfylla de rättsliga kraven på samma sätt som signaturer skrivna på papper förutsatt att signatur, certifikat och tillhandahållare av tjänster uppfyller de krav som framställs och att elektroniska signaturer kan godtas som bevis vid rättsliga förfaranden. Medlemsstaterna skall även säkerställa att en tillhandahållare av certifikattjänster är ansvarig för skada som åsamkats en person som har rimlig anledning att förlita sig på uppgifterna samt att direktivet inte tar ställning till vilken teknik som används för att skapa elektroniska signaturer. Det finns anledning att analysera hur direktivet har implementerats genom svensk lag samt att göra en internationell utblick där implementering av EU-direktiv genom standardiseringar har blivit en alltmer vanligt förekommande lösning.

4.1.1 Direktivets utgångspunkt[63]

Direktivets förarbeten redovisas i den rapport som skapades "Ensuring Security and Trust in Electronic Communication - Towards a European Framework for Digital Signatures and Encryption". Denna rapport gick ut på remiss till berörda branschorgan inom krypteringsindustrin och till ett expertmöte som hölls i Köpenhamn. De flesta remissinstanser var eniga om att göra direktivet så teknikneutralt som möjligt.[64] Vidare fick kommissionen stöd från en kommitté som var sammansatt av representanter ifrån alla medlemsstater för att få största möjliga uppbackning ifrån medlemsstater och branschorganisationer.[65]

4.1.2 Direktivets innebörd

Det bedömdes som nödvändigt att införa en gemensam rättslig ram för elektroniska signaturer inom unionen för att utnyttja de möjligheter som elektronisk kommunikation och handel gav. De viktigaste artiklarna i direktivet är artiklarna 1 och 5 (se bilaga B). I artikel 1 fastslås direktivets

[62] Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer 1999/93/EG
[63] I princip så har inte EU-förarbeten något större värde som en rättskälla men det finns dock fog for att nämna utgångspunkten.
[64] Kelleher, Murray, IT Law in the European Union, 1999, s 100
[65] Aa, s 106

tillämpningsområde, i artikel 5 regleras rättsverkan av elektroniska signaturer.
Texten till direktivet är tämligen allmänt formulerad för att kunna omfatta en framtida utveckling. De specifika tekniska krav som ställs på certifieringen är bl.a. därför inte så detaljerad. En av de grundläggande principerna i direktivet är att det inte skall göras någon skillnad mellan elektroniska signaturer och handskrivna signaturer. En elektronisk signatur skall inte förklaras ogiltig endast på grund av att den är elektronisk. Enligt direktivet skall elektroniska signaturer jämställas med handskrivna under förutsättning att vissa krav är uppfyllda. Det måste röra sig om en s.k. avancerad elektronisk signatur. Det innebär att den skall vara unikt knuten till en specifik signatur, att den indentifierar undertecknaren samt är skapad genom åtgärder som undertecknaren ensam kan kontrollera. Ett ytterligare krav som ställs på den elektroniska signaturen, är att den måste baseras på ett avancerat certifikat och slutligen måste den skapas av en säker signaturanordning.
Direktivet har inte till syfte att harmonisera nationell avtalslagstiftning. Speciella formkrav i nationell lagstiftning, med anledning av slutande av avtal, har därför företräde framför reglerna om den rättsliga effekten av elektroniska signaturer enligt direktivet. Direktivet hindrar sålunda inte att parterna, inom ramarna för nationell lagstiftning, kommer överens om på vilka grunder elektroniska signaturer skall godkännas.

4.1.3 Direktivets tillämpningsområde

Enligt artikel 1 syftar direktivet till att underlätta användning av elektroniska signaturer samt till att bidra till deras rättsliga erkännande. Vidare sägs i artikel 1 att direktivet inte skall gälla frågor med avseende på ingående av och giltighet av avtal, eller andra rättsliga förpliktelser för vilka formkrav uppställs i nationell rätt eller gemenskapsrätt. Det innebär att bestämmelsen om elektroniska signaturers rättsverkningar inte skall vara tillämpliga på sådana fall där det i lag uppställs formkrav.

4.1.4 Rättsverkan av elektronisk signatur

I artikel 5 fastställs vad gäller rättsverkan av elektronisk signatur att en s.k. avancerad elektronisk signatur skall tillerkännas samma rättsliga status i förhållande till elektroniska dokument som en handskriven namnteckning har i förhållande till pappersdokument. Det stadgas i artikel 5 att avancerade elektroniska signaturer även skall kunna användas som bevis vid rättsliga förfaranden. I artikel 5 2 p fastslås att övriga typer av elektroniska signaturer inte skall få diskrimineras ur rättslig synvinkel enbart därför att de är i elektronisk form, eller för att de inte baseras på kvalificerade certifikat.

4.2 Hur påverkade direktivet svensk rätt?[66]

Rättsverkningarna av lagen om kvalificerade elektroniska signaturer blev ganska stora då en elektronisk signatur skulle jämställas med en traditionell namnteckning. Dock har inte direktivet haft någon större påverkan på frågan om rättsverkan av elektroniska signaturer i de fall det uppställdes formkrav i nationell rätt. Det fastslogs att en elektronisk signatur skall fungera som bevis vid rättsliga förfaranden i alla medlemsstater. Detta innebar inte någon påverkan på svensk rätt eftersom det finns rättsliga principer om fri bevisprövning och bevisvärdering, vilket innebär att elektroniska signaturer kan godtas som bevis vid rättsliga förfaranden.
Det är vid en jämförelse lätt att finna hur EG-rätten skall samverka med den nationella rätten vid implementeringar. Gemenskapsrätten har emellertid företräde mot nationell lagstiftning det gäller även nationella grundlagar. Det innebär att de EU rättsliga reglerna går före de svenska. Det har fastslagits i flera vägledande rättsfall från EG-domstolen att de nationella staterna har en skyldighet att tolka nationell rätt i ljuset av ett direktiv.[67]
De elektroniska signaturer som nämns i direktivet specificeras på så sätt att den högsta nivån är kvalificerade elektroniska signaturer, som juridiskt kan jämställas med egenhändig namnteckning. En sådan signatur är knuten till en undertecknare och gör det möjligt att identifiera denne. För att skapa sådana signaturer krävs en infrastruktur med certifikat och olika nycklar till krypterad information.
För Sveriges del handlar det inte om några egentliga förändringar eftersom underskriften redan fungerar som bevis. Hur avtal tecknas och genomförs är upp till avtalsparterna. Ofta finns det en överenskommelse mellan parterna eller den bransch som parterna ingår i. Sedvänjan kan exempelvis innebära att för ett avtal skall vara bindande krävs en underskrift på ett traditionellt brev eller via fax. Det är alltså inte lagtexten som bestämmer avtalets riktighet, utan det fastställda förfarandet.[68] Den stora skillnaden vad gäller frågan om rättsverkan är att efter införandet av lagen har en kvalificerad elektronisk signatur nu fått samma rättsverkan som en traditionell namnteckning.

[66] Proposition 1999/2000:117, s 26-32
[67] Strömholm Aa s 326-28
[68] Kolla bilaga i 1998:14 bilaga med uppräkningar av författningar med krav på underskrift.

4.3 Internationell vision

4.3.1 USA

EUs gemensamma regler för elektroniska signaturer är även viktigt för den globala e-handeln. Nästa steg, efter införandet av direktivet och de nationella lagarna inom EU, är att finna gemensamma lösningar med världen utanför EU. I USA arbetade man länge med att skapa motsvarande lagstiftning.[69]
Femtio amerikanska delstater har antagit lagar om elektroniska signaturer. Problemet är att olika stater godkänner olika kategorier: Somliga stater godkänner alla typer av e-signaturer - PIN, normal text, inscannade signaturer etc, medan andra endast accepterar elektroniska signaturer. Den amerikanska regeringen ville ha gemensamma regler som gäller i alla stater. Men eftersom varken USA eller EU har bundit sig för någon specifik teknisk lösning finns det goda utsikter att samma elektroniska signaturer skall komma att fungera på båda sidorna av Atlanten.[70]
Den amerikanska utvecklingen tog fart på allvar då kongressen bestämde att den 1/10 2000 skall elektroniska dokument underskrivna med en elektronisk signatur vara lika bindande som med en traditionell namnteckning. Denna lag som kallas e-Sign Act kan bidra till en internationell utveckling, men flera områden t.ex. familjerätt och arv omfattas inte. [71]

4.3.2 Harmoniseringsregleringar

FN har insett att det krävs en global reglering för elektroniska signaturer och har arbetat fram ett ramverk. Det är kommissionen för internationell handel, UNICITRAL, som har försökt skapa en harmonisering för att inte hindra den globala handeln.[72] På nationell nivå valde man att reglera den elektroniska signaturen på olika sätt innan EU-direktivet trädde i kraft och blev bindande för medlemsstaterna. I Tyskland var man tidigt ute med lagreglering. Det riktades en hel del kritik mot att lagen skulle skapa en lösning som skulle hindra utvecklingen, att regleringen skulle bli alltför tekniskt specifik och att lagen snabbt skulle bli inaktuell på grund av den tekniska utvecklingen. Vissa förespråkare menade att det var marknaden som skall ge stöd till utvecklingen och inte lagstiftaren. Dock hann man aldrig att se några problem uppstå innan direktivet trädde i kraft. I Holland valde man att använda sig av ett självregleringsalternativ. Det byggde på att de allmänna reglerna i sin befintliga form skulle kunna hantera aktuella rättsliga spörsmål

[69] Trendrapport Elektroniska handel, 1999, Sveriges tekniska attachéer, Lundblad Niklas, s 10
[70] Computer Sweden nyhetsbrev 1999-12-05, Lotsson Anders, EU och USA lagstiftar om e-signaturer.
[71] E-sign Act raises the speed limit on the information highway, Cummings Matthew, www.findlaw.com, 2001-03-22
[72] Computer Sweden nyhetsbrev 2000-10-16, Sviden Henrik, FN harmoniserar lagar om digitala signaturer

samt att parterna genom kontraktsreglering själva fick möjlighet att bestämma över ansvarsfördelningen. Rädsla fanns för att om man lät marknaden utveckla den elektroniska signaturen och dess strukturer skulle det bli svårt att överblicka, men den kritiken har kommit lite på skam där den holländska rättsutvecklingen tidigt har haft en god kunskap om nya rättsfenomen och skaffat rationella lösningar till dessa. [73]

4.4 Standardisering

Hänvisning till standarder är en medveten och ofullständig bestämmelse. Det handlar om att en lagbestämmelse får sitt innehåll ifrån en hänvisning till en utomrättslig bedömningsmåttstock som har framkommit inom det specialiserade området. Dock kan det inte vara fråga om någon definitiv rättsregel utan det är omöjligt för lagstiftaren att helt lägga över ansvaret på rättsuppfattningen på någon branschorganisation.[74]
Redan tidigt i det inledande arbetet med att skapa ett direktiv för elektroniska signaturer kontaktades standardiseringorganisationer för att bidra till att standardiseringen. Lösningen som valdes blev att göra direktivet teknikneutralt och tillåta användandet av öppna standarder för att möta de europeiska kraven. Kommissionen vände sig till de Europeiska standardiseringsorganisationerna, och de satte samman EESSI, European Electronic Signature Standardisation Initiative, som har deltagit i utvecklandet av en teknisk standard som skall fylla ut direktivet.[75]
Kravet på en samsyn av tekniken kan vara en välbehövlig väg för att skapa ett ramverk för en elektronisk signatur. Samsynen är något som kan komma till uttryck i form av standarder från branschorganisationer. Det har medfört att standarder har kommit att tillämpas i EG-lagstiftningen. Genom en ny utveckling i form av den s.k. harmoniseringsmetoden hänvisar EU i sina direktiv allt oftare till standarder men utan att dessa blir tvingande. Befogenheten att fylla ut tekniska detaljer i direktiven överlämnas till marknaden och frigör kompetens för EU att ägna sig åt de regulatoriska och rättsliga frågorna.[76] Ett sätt att uppfylla en del av standardiseringsproceduren är att enligt direktivet kan medlemsstaterna införa frivilliga acrediteringssytem som har som mål att höja komptensnivån på tillhandahållandet av certifikattjänster. Lagen (1992:1119) om teknisk kontroll ger möjlighet till frivillig ackreditering av certifieringsorgan och uppfyller det syfte som finns i direktivet.[77]

[73] Hultmark, Digital signatur - internationella utvecklingstendenser, Nordisk årsbok i Rättsinformatik 1998, s 165-66
[74] Strömholm, Aa, s 252
[75] Nytt standardiseringsområde, Elektroniska signaturer, www.sis.se 2000-10-31
[76] ADBJ-seminarium, Elektroniska signaturer - en svensk standard? 1999-10-22, Stockholm
[77] Proposition 1999/2000:117 , s 2

I denna diskussion förespråkar Hultmark en internationell standardiseringsprocess.[78] Möjligheterna till ett större erkännande och genomslag för elektroniska signaturer kan uppnås om det sker en standardisering byggd på frivillig basis, via självreglering. Skall den styras av nationella statliga organ kan det medföra att utvecklingen blir politiserad och trög. Dessutom är det svårt att uppnå en fullständigt teknikneutral lagstiftning där det ges utrymme för ett flertal vägledande praktiska regler och inte alltför generella bestämmelser. Genom att låta vissa tekniska krav fastslås genom standarder går det att låta parterna lösa vissa delar av ansvarsfördelningen via kontraktuell väg. Speciellt kommer det att krävas att CAs blir tvingade att följa de policies som bör upprättas kring utfärdandet av certifikat för att de skall kunna reglera ansvarsfrågan. Ett försök på vägen att åstadkomma en begreppsmässig standardisering är UNICITRAL som har fastslagit i sin modellag om elektronisk handel att en elektronisk signatur inte skall nekas en rättslig effekt bara för att den är i elektronisk form. Denna begreppsstandard framgår under beskrivningsbegreppet funktionell ekvivalens, men det är i princip irrelevant hur vägen till en fungerande elektronisk signatur skall ske, bara målet uppnås att få till ett internationellt uniformt slutresultat som fungerar på effektivaste sätt och motverkar problem.[79]

4.5 Olika ståndpunkter i doktrinen

I valet mellan att låta lagstiftaren styra eller att välja självreglering kan harmoniseringsmetoden med utfyllning av lagregler med standarder vara en bra lösning. Det förekommer allt oftare att juridiska konferenser och seminarier tar upp dessa frågor om valet mellan lagstiftning och självreglering. En sammanfattning av de åsikter som hittills framkommit presenterades vid ett rättssymposium som hölls 23-24 november 2000 på Häringe slott. Symposiet menade att utrymmet för och funktionen av självreglering varierar mellan olika rättsområden och över tiden. Regleringsbehovet styrs av effektivitets, flexibilitets och legitimitetsargument som kan tala både för och emot. En förståelse finns för att det inom vissa rättsområden har varit alltför reglerat genom lagstiftning och för att uppnå önskade förbättrade juridiska lösningar måste behovet av nya regleringsformer utnyttjas för att uppnå resultat. Detta behov kan bland annat tillgodoses genom självreglering eller direktiv som fylls ut med standarder. I princip är det av stort värde att bedöma effektivitetsvinsten totalt sett för hela samhället om man får ett genomslag för elektroniska

[78] Hultmark, Digital signatur - internationella utvecklingstendenser, 1998, s 166-68, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik, 1998, Jure AB, Stockholm

[79] Hultmark, Digital signatur - internationella utvecklingstendenser, 1998, s 166-68, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik, 1998, Jure AB, Stockholm

signaturer och att det sker med minsta möjliga statliga reglering.[80] Ett framtida scenario blir utan tvekan den att berörda aktörer i allt större utsträckning kommer att själva sköta normbildningen i samverkan med statliga institutioner och att det leder till att HD kommer att bedöma dessa samspelsnormer som allmänna rättsprinciper.
Hultmark menar att användningen av elektroniska signaturer borde ha lösts med hjälp av befintliga rättsregler från det allmänna regelverket och inte genom att specialdesigna en lag. Enligt Hultmark finns det en större tillit till det befintliga regelverket, vilket skulle medföra att en lagstiftning inte var nödvändig.[81]
Hon bedömer självregleringsalternativet som lite osäkert för att få ett globalt genomslag där behovet av internationell harmonisering är stort. Enligt henne är viktigt att skapa någon internationell aktiv kodifiering med en minimalistisk reglering och att överlåta standardiseringsprocessen till andra än lagstiftaren i enlighet med de trender som råder för tillfället. Det bör vidare beaktas att regleringen om elektroniska signaturer endast utgör en del i en mycket större process, nämligen globaliseringen och att internationaliseringen i sig kommer att ställa ett ökat krav på de nationella lagarna att de beaktar internationella harmoniseringsaspekter med en tydlig tendens mot uniforma internationella rättsregler.[82]
Vissa förespråkare inom branschen menar dock att vissa branschorgan är fel ute då de försöker att standardisera en idé utan att ha en teknik bakom den.[83]
Motsvarande åsikter framkommer även på det seminarium hos Svenska föreningen för ADB. Det har enligt seminariet uppmärksammats en ny trend som visar sig i att EU försöker harmonisera lagstiftningen med hjälp av standarder. Detta kommer att gå till på så sätt att det i direktiven kommer finnas hänvisningar till standarder satta av marknaden genom datering, vilket innebar att implementeringen av standarder fastställs till ett visst datum. Det positiva var enligt seminariet att viktiga tekniska frågor kunde lyftas bort från politiska organ vilket skapar flexibilitet för att frigöra kompetens hos de statliga organen och påskynda lagstiftningen.[84]

[80] Svensk Jurist Tidning , 3 2001, årgång 86, Josefsson Carl, Lagstiftning eller självreglering?, s 206-218
[81] Hultmark Christina, Digitala signaturer - Internationella utvecklingstendenser, 1998, s 169
[82] Hultmark Christina, Digitala signaturer - Internationella utvecklingstendenser, 1998, s 169
[83] Personligt möte med Lars Sundström, Nexus AB, under våren 2000
[84] Seminarium hos Svenska föreningen för adbj……. www.adbj.se den 1999-10-26,

5 Förarbeten[85]

5.1 Utredningarna

Utredningarna kring elektroniska signaturer har varit många, de har genomgående syftat till att säkerställa att det har funnits tillräckligt med information för att kunna genomföra rätt lagstiftningsåtgärder. För att få en bred bild av vilka utredningarna har varit, vilka remissorgan som har varit inblandade och vilka åsikter de har haft så följer nedan en översiktlig genomgång. Det har funnits ett flertal synpunkter på lagförslaget från olika remissinstanser, bl.a. frågan om definitionsbeskrivningar, formkrav, bevis och ansvarsfrågor.

5.2 Propositionen[86]

5.2.1 Allmänt-Definition

Intressant är den definitionslista som har överförts från direktivet in i den svenska lagen. Bland annat fastställs en kvalificerad elektronisk signatur som en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning. Remissorganen har utan några större kommentarer accepterat att direktivets definitioner även skall tas med i lagen. Utredaren motiverar sitt val med att Sverige visserligen inte är bundet av den terminologi och systematik som anges i direktivet, om det avsedda målet kan uppnås med annan terminologi, direktivet anses utformat på ett sådant sätt att det endast finns ett begränsat utrymme för att avvika från direktivets terminologi, men det bidrar samtidigt också till att den svenska lagstiftarens mål med att skapa enkel och begriplig lagtext försvåras då den tämligen komplicerade verklighet som direktivet beskriver inte kan förenklas alltför mycket.[87] I propositionen resoneras vidare kring Christina Hultmarks slutsatser om att krav på underskrift i författning inte nödvändigtvis bör innebära ett krav på en egenhändigt skriven namnteckning utan att det kan gå lika bra med en elektronisk signatur och att de finner att hon tar stöd i sitt resonemang enligt principen om funktionell ekvivalens som framkommit i UNICITRALS modellag. Utredarna finner att det principiellt skulle fungera men att det finns hinder. Betraktelsesättet som Hultmark uppställer är inte realistiskt och hinder

[85] Detta kapitel kommer att behandla Propositionen 1999/2000:117, Ds 1998:14, Ds 1999:73, IT-Kommissionens arbeten och andra remissorgan. Sou behandlas inte p.g.a att det inte finns någon av värde.
[86] Proposition 1999/2000:117 Lag om kvalificerade elektroniska signaturer, m.m.
[87] Aa, s 6, 37-38

skulle komma ifrån att domstolar och myndigheter inte konsekvent skulle bedöma alla formkrav som tillgodosedda genom en elektronisk signatur.[88]

5.2.2 Formkrav

Det fastställs i propositionen att det inte bör uppställas någon generell regel för att jämställa elektroniska signaturer med traditionella namnteckningar. Det är alltså tillåtet att ha kvar formkrav på nationell nivå som utesluter användning av såväl icke som kvalificerade elektroniska signaturer. Men om det enligt författning eller praxis framkommer att det är tillåtet att uppfylla krav på traditionell egenhändig namnteckning med elektroniska rutiner så måste en kvalificerad elektronisk signatur alltid accepteras och logiskt följer kraven på att det inte får ställas högre krav på en elektronisk signatur än på en kvalificerad elektronisk signatur.[89]
I propositionen finner utredarna vidare att de formkrav som finns i svenska författningar kan ha många syften som att säkra bevis om en åtgärd, om vem som utfört den, om dess innehåll och kunna bevara det på ett säkert sätt under lång tid och att det i sig finns en varningsfunktion genom att avtalsparten blir medveten om att signaturen i sig innebär en rättshandling som kan få betydelsefulla effekter.[90]

5.2.3 Bevis

En underskrift får i regel en stor betydelse i bevishänseende och en av de intressanta frågorna är de bevisbörderegler som skapas av praxis. Det har inte funnits något behov att lagstifta om detta utan det har överlåtits till prejudikat att styra detta. I rättsfallet NJA 1976 s 667 gällde det en situation där en person förnekat att han undertecknat en förvanskad handling. HD menade att om någon gör en sådan invändning får den påstådde fordringsägaren visa att handlingen är äkta, men om gäldenären som i det ovannämnda fallet gör gällande att handlingen är äkta men att den ändrats så är det gäldenären som har bevisbördan. I ett senare fall NJA 1992 s 263 gör HD samma bedömning genom att det bör ligga på kontohavaren att åtminstone göra det antagligt att det föreligger en förfalskning. I utredningarna Ds 1998:14 och i propositionen finner utredarna att det skulle vara farligt att dra några generella slutsatser av detta och skapa några generella bevisbörderegler när det gäller elektroniska signaturer även om det finns en stor rimlig skälighet i HD:s domar och att en analogilösning inte ter sig främmande.[91] Det anges också att direktivet innehåller mer delar om elektroniska signaturers rättsliga verkan än den svenska lagen, där principerna om den fria bevisprövningen och den fria bevisvärderingen bidrar till att den frågan inte får någon central betydelse. Rättsprinciperna är helt enkelt fast förankrade.[92]

[88] Aa, s 17
[89] Aa, s 58
[90] Aa, s 16
[91] Aa, s 17-18
[92] Aa, s 35

5.2.4 Ansvarsfrågor

I huvudsak är det tre olika situationer som upptar diskussion om ansvarsfrågor; undertecknarens ansvar vid obehörig användning, certifikatutfärdarens ansvar gentemot undertecknaren och certifikatutfärdarens ansvar gentemot mottagaren. De ansvarsfrågor som behandlas i utredningen aktualiserar undertecknarens ansvar vid obehörig användning och i lagens förarbeten finner utredaren att det är av betydelse att behandla problemet. Genom att sålunda göra en analogi med obehörig användning av kontokort i enlighet med 34§ i Kkrl så finner utredarna att det skulle vara av vikt att inte ställa för höga krav på konsumenternas ansvar vid obehöriga uttag.[93] I propositionen fastställs det vidare att ett skadeståndsrättsligt presumtionsansvar för den som utfärdar kvalificerade certifikat skall införas till tvingande fördel för den som förlitar sig på certifikatet. Detta har uttryckts i direktivets artikel 6.1 och motsvaras av den svenska lagens 14§. Några remissinstanser var dock kritiska till att det var otydligt ifråga om vilka certifikatutfärdare som omfattades av skadeståndsbestämmelsen och om det endast var de som utfärdar kvalificerade certifikat.[94]

5.3 Ds 1998:14

5.3.1 Allmänt-Definition[95]

Departementspromemorian togs fram efter uppdrag ifrån regeringskansliets bredningsgrupp för elektroniska signaturer och den innehåller beskrivning av den kryptografiska teknik som används och den kringutrustning som finns i form av programvara och hårdvara. Speciellt så uppmärksammades de hot och risker som finns i CAs funktion och uppgifter för att hantera det öppna systemet så att det blir tillförlitligt. Utredningens huvuddelar omfattar de rättsliga aspekterna av elektroniska signaturer och de krav som svensk lagstiftning ställer vad gäller skriftlighet, bevisvärde och jämförande med den traditionella namnteckningens funktioner. Även straff, förvaltnings och processuella frågor togs upp. Utredningens avslutande delar tog med hjälp av en internationell överblick fram olika handlingsvägar för att öppna möjligheten att tillämpa elektroniska signaturer i samhället och den bästa lösningen ansågs vara den form av hybridkaraktär som gör en intresseavvägning mellan avtalsskrivning, lagstiftningsvägen och praxis. Generellt kan sägas att utredningen strävar efter att i första hand skapa ett kunskapsunderlag mer än att leda fram till en ståndpunkt och den innehåller en otroligt bred teknisk genomgång och imponerande komparativ jämförelse mellan ett flertal länders utveckling emot att ge elektroniska signaturer rättsverkan.

---

[93] Aa, s 49
[94] Aa, s 53
[95] Ds 1998:14 s 11-12

5.3.2 Formkrav

I Ds 1998:14 görs bedömningen att för att säkerställa att elektroniska signaturer tillskrivs samma rättsverkan som en traditionell namnteckning vid avtal med formkrav så bör dessa regler ändras i en specifik översyn. En generell regel är inte någon bra lösning, utan översynen bör göras från fall till fall, och för att föregå gjordes det en föredömlig inventering av samtliga rättsregler i den svenska rättsordningen, överenskommelser med främmande makt och EU-bestämmelser vilket finns med Ds bilaga nr 3. Slutsatsen dras i form av en generell regel som innebär att elektroniska signaturer skall godtas i regler med formkrav men att det inte kan bli aktuellt över hela rättsområdet utan en förändring av varje specifikt lagrum.[96]

5.3.3 Bevis

Det fastslås i Ds 1998:14 att någon särskild bevisbörderegel inte bör uppställas vad gäller elektroniska signaturer.[97]

5.3.4 Ansvarsfrågor[98]

Den hotbild som finns i användandet av elektroniska signaturer består av ett flertal situationer:

- En annan person än kortinnehavaren använder kortet och elektroniska signaturer kan därmed skapas av någon obehörig.
- Privata nyckeln kan användas av obehörig.
- Falska smarta kort i omlopp med möjlighet att förfalska innehållet i de certifikat som ligger på kortet och det kan leda till att även falska användbara certifikat finns i omlopp.
- Certifiering kan ske på felaktiga grunder med vilseledande och oriktig information.
- Möjlighet för individen att förneka den elektroniska signaturen. En säker elektronisk signatur skall inte gå att förneka. Kan man få tappa sitt smarta kort med PIN-kod? Svaret finns mer i att vara aktsam och inte förvara kort och kod på samma ställe.
- Tillgänglighetsbrister som innebär att det tar tid innan en revokering görs. Kan en revokering ske direkt så minimeras riskerna.

Enligt utredningen gäller att säkerheten är hög i de applikationer och rutiner som finns både hos CA och användaren för att beivra missbruk av elektroniska signaturer och smarta kort innehållande certifikat. Genom att sätta upp en hotbild kan man framför allt motverka riskerna och även skapa användbara och säkra lösningar.

---

[96] Aa, s 77
[97] Aa, s 185
[98] Aa, s 44-45

5.4 Ds 1999:73

5.4.1 Allmänt-Defintion

I Ds 1999:73 så resonerades det kring målsättningen med direktivet och om det har uppfyllts. Målsättningen vid direktivets utformande var att inte låsa sig vid en viss teknik utan att vara så teknikneutral som möjligt och det har till stora delar uppnåtts.[99] I utredning gjordes den ståndpunkten att det bästa alternativet var att vara återhållsam med lagens tillämpningsområde vid genomförandet av direktivet i svensk rätt och inte överreglera, utan att lagen kan kompletteras i ett senare skede när man ser effekterna på ett tydligare sätt.[100]

5.4.2 Formkrav

När det gäller formkrav förordades att det var av stort värde att studera den avgörande frågan vad det är för syfte som ligger bakom kraven och om de kan uppfyllas med elektroniska signaturer. Det fastslogs att de kvalificerade elektroniska signaturerna har en särställning i de fall det i lag eller annan författning finns formkrav som kan uppfyllas med hjälp av elektroniska signaturer.[101]

5.4.3 Bevis

I utredningen låg fokuseringen på direktivet om ett gemenskapsverk för elektroniska signaturer och genomförandet av det i svensk rätt men även frågan om rätts- och bevisverkan behandlades. Det finns även med en föredömlig översyn av hur långt införandet av elektroniska signaturer har kommit i olika organisationer och myndigheter.[102]

5.4.4 Ansvarsfrågor

I Ds 1999:73 finner man att det framstår som mest lämpligt att stanna vid ett presumtionsansvar för certifikatutfärdaren eftersom certifikatutfärdaren rimligtvis har lättats att föra fram bevisning. Presumtionsansvaret innebar att en utfärdare blir skadeståndsskyldig om kraven i lagen om kvalificerade elektroniska signaturer inte är uppfyllda och utfärdaren inte kan visa att det inte beror på vårdslöshet från honom.[103]

---

[99] Ds 1999:73 s 46
[100] Aa, s 55
[101] Aa, s 89
[102] Aa, s 38-44
[103] Aa, s 82

5.5 IT-kommissionen

IT-kommissionen har i ett flertal rapporter gett sin syn på hur införandet av elektroniska signaturer skall gå till. Dessa rapporter har inte någon lagstiftande karaktär utan har mer en rådgivande funktion. En sammanställning följer.

IT-K 1999-03-22 Organisation för hantering av certifikat och nycklar.

Kommissionen menade att det borde skapas en struktur för hantering av nycklar och certifikat och att regeringen borde utse en myndighet som utövar tillsyn över certifikatutfärdare som ser till att utfärdade föreskrifter följs. De föreslog Patent och registreringsverket som den mest lämpliga övervakaren av CA. Se p 7.3 i kommissionens rapport.

IT-K 1999-04-15 Vikten av användning av kryptering

Kommissionen menade att det var av största vikt att företag och privatpersoner får använda den senaste krypteringstekniken för att skydda de elektroniska signaturerna och det medförde att restriktionerna drogs in efter det att utvecklingen i USA tagit fart.

IT-K Dnr 99/73 Remissvar Ds 1999:73 Elektroniska signaturer

Redan i remisskedet var IT-kommissionen kritisk till att lagen öppnade för certifikatutfärdaren att välja om han ville kalla sina certifikat kvalificerade och därmed omfattas av lagen, eller att undgå skadeståndsansvaret genom en annan benämning på certifikaten. IT-K var kritiska till antalet missuppfattningar i texten och att det uppenbarligen inte har framgått vad det var för skillnader mellan signaturer, privata nycklar och certifikat.[104]

5.6 Remissorgan

GEA, gemenskapen för elektroniska affärer, lämnade ett remissyttrande över lagförslaget angående elektroniska signaturer och de framhöll i sitt yttrande att utnyttjandet av elektroniska affärer är beroende av att det går att identifiera och knyta en transaktion till en motpart vid elektronisk kommunikation. Vidare påtalades det att direktivet och lagförslaget var starkt knutna till vissa tekniska förutsättningar. Med hänsyn till den snabba tekniska utvecklingen fanns det därför en risk att många aktörer kommer att välja andra lösningar och därmed stå utanför tillämpningsområdet. Sådana bestämmelser borde enligt GEA regleras genom en förordning i stället för genom lag.[105]

---

[104] IT-K Dnr 99/73 Remissvar Ds 1999:73 Elektroniska signaturer, s 3

[105] Remissyttrande Digitala Signaturer GEA… Computer Sweden nyhetsbrev www.gea.nu ..dec 00-02-14

5.7 Olika ståndpunkter i doktrinen

Det har utan tvekan funnits en hel del skiljaktiga åsikter om vad olika begrepp och definitioner bör stå för och hur lagtexten skulle utformas. En väsentlig skillnad har gjorts mellan utformningen av lagtext enligt promemorian Ds 1999:73 och propositionen. I propositionen fastställs det att 16§ skall innehålla en regel som anger de kvalificerade elektroniska signaturernas särställning genom att de anses uppfylla krav i lag eller annan författning på egenhändig underskrift. I Ds 1999:73 fanns det istället en lagregel om rättsverkan av elektroniska signaturer. Denna förändring från Departementsskrivelsen till den fastställda och gällande i proposition och lagtext kom nog till på grund av den kritik som kom ifrån remissorganen som påpekar att artikel 5 i direktivet är mer långtgående därför att den bör läsas i sitt sammanhang med artikel 1 som reglerar direktivets tillämpningsområde. Innebörden är viktig och blir den att medlemsstaterna inte alltid behöver godta kvalificerade elektroniska signaturer i alla de fall där det finns ett krav på underskrift i nationell rätt, men om det i lagstiftning och föreskrifter är tillåtet att använda elektroniska signaturer för att uppfylla samma formkrav som med en traditionell namnteckning måste de kvalificerade elektroniska signaturerna alltid godtas enligt artikel 5.1.a. Det får till följd att om det inte finns något uttryckligt hinder mot att ge rättsverkan åt kvalificerade elektroniska signaturer så skall de godtas.
Vad gäller icke-kvalificerade signaturer så skall de enligt direktivets artikel 5.2 inte förvägras rättslig verkan eller giltighet som bevis. I förarbetena framhålls det att artikel 5.2 inte föranleder någon lagstiftningsåtgärd därför att det lika lite som i artikel 5.1 föranleder att medlemsstaterna måste godta en elektronisk signatur i de lagrum där det finns formkrav. Noterbart är att dessa bestämmelser har införts genom 17§ i lagen om kvalificerade elektroniska signaturer.[106]
Skillnaderna mellan den svenska lagen och den text som kom till uttryck i direktivet kan förklaras av hur olika remissorgan har påverkat utformningen av den slutliga lagtexten genom sina remisskommentarer. Genomgående är de flesta remissorganen positiva till lagens utformning även om det finns små stycken av dissidens. I propositionen har lagstiftarna tagit hänsyn till de kommentarer som redovisades i de remissomgångar som genomfördes med de statliga promemoriorna 1998:14 och 1999:73. Detta förfarande bidrog till att lagens namn ändrades från "lag om elektroniska signaturer" till "lag om kvalificerade elektroniska signaturer" men trots ändringen undgick den inte kritik genom att lagens namn är missvisande då den mer handlar om certifikat än om elektroniska signaturer. Till stöd för lagstiftarens val kan dock framhållas att det vid en sådan ny företeelse som elektroniska signaturer blir ofrånkomligt att delar av direktivet mer eller mindre ordagrant tas med in i den svenska lagen.[107]

[106] Proposition 1999/2000:117 Lag om kvalificerade elektroniska signaturer, m.m. s 55-57
[107] Proposition 1999/2000:117 Lag om kvalificerade elektroniska signaturer, m.m. s 33-34

6 Den elektroniska signaturens funktioner och rättsverkan

6.1 Introduktion

Det komparativa arbetet bygger på att jämföra den elektroniska signaturen med den traditionella namnteckningen. Jag har hittat en källa som går in på att det finns fem områden av stort intresse för att bedöma om en elektronisk signatur uppfyller en traditionell namnt ecknings fem grundläggande funktioner[108]

- Identifiering av dokumentets källa, Vem?
  - Signatärens identitet skall framgå av signaturen
- Äkthetsfunktionen
  - Signaturen skall ge ett dokument äkthet
- Bevisfunktionen
  - Ett dokument med signatur kan åberopas som bevis
- Avslutsfunktionen/viljefunktionen
  - Genom en underskrift så har undertecknaren gett uttryck för sin vilja att avtalet har fått sitt slutgiltiga innehåll
- Varningsfunktionen
  - Signatären skall vara medveten om att den handling, som signeringen utgör är en juridisk handling

I detta kapitel kommer jag att diskutera hur det kan skilja sig mellan att använda en elektronisk signatur och en traditionell namnteckning för ovannämnda avtalsrättsliga funktionsområden. Jag kommer även att analysera om det sker några rättsliga förändringar för olika avtalsformer. Uppfyller den elektroniska signaturen de fem funktionerna och vad gäller om det är real, konsensual eller formalavtal? Kapitlet inleds med en definitionsgenomgång där även frågor om signaturens bevisvärde, formkrav och hur avtalsrättsliga problem som motivvillfarelse och förklaringsmisstag skall lösas i en elektronisk avtalsmiljö, behandlas.
Signaturens betydelse kan sammantaget beskrivas som att identifiera den som har undertecknat och att garantera äktheten, dvs att texten oförändrad hänför sig till utställaren. Vidare fyller underskriften en bevisfunktion genom att den ger uttryck för en vilja att binda innehavaren vid den undertecknade texten. Det tillkommer en avslutsfunktion genom att texten ger uttryck för att dokumentet fått sin slutgiltiga utformning, samt en varningsfunktion genom att undertecknaren blir medveten om att handlingen kan få rättsliga konsekvenser.[109]

[108] Teletrustrapport 4/1991“ Informationssäkerhet och digital signering” s 28
[109] I princip har de flesta doktrinförfattare accepterat denna uppdelning i signaturens fem olika funktioner; Lindberg - Elektroniska orginaldokument och elektronisk signatur s 30 f,

6.2 Avtalslagen

Avtalslagen behandlar avtals ingående. När lagen skrevs 1915 hade inte författarna några elektroniska avtal att ta hänsyn till. Avtalslagen gjordes till en allmänt hållen lag, begränsad till allmänna principer, där avtalsparter har fritt svängrum vid ingående av avtal. Avtalslagens regler om avtalsslutande är dispositiva vilket innebär att lagen gäller "så vitt ej annat följer av anbudet eller svaret eller av handelsbruk eller annan sedvänja" (1§ 2 st). Lagen skall alltså gälla i de fall då parterna inte avtalat om vad som skall gälla i ett elektroniskt avtal. Lagens skapare var framsynta och gjorde en teknikneutral lag begränsad till allmänna principer som kan tillämpas på överenskommelser av skiftande slag. Det finns även en omfattande praxis som har utvecklat lagen och frågor som uppkommer i samband med elektroniska avtal är av mer detaljerad karaktär och har inte bedömts skapa något behov av särreglering. Det står parterna fritt att välja form för hur ett avtal skall ingås. Avtal som är muntliga eller slutna på elektroniskt vis är i princip lika giltiga som ett skriftligt avtal.[110]
Ett anbud och en accept är bindande för den som avgivit det. Det finns inga formkrav för anbud och accept utan de kan bytas på vilka sätt som helst; skriftligen, muntligen, per fax, eller elektroniskt. Elektroniska avtal kan ingås på flera sätt t.ex. genom att köpare och säljare kommunicerar externt. Enligt IT-utredningen uppstår det utan tvekan ett bindande avtal när parternas datasystem kommunicerar direkt med varandra.[111]
En del bestämmelser i avtalslagen kräver att det finns ett subjektivt moment i form av en mänsklig vilja för att en regel skall bli tillämpbar. Kan en dator använda sig av en elektronisk signatur utan att en individ utför den signerande funktionen? Det är viktigt att parterna reglerar detta och vilka befogenheter de får ge åt sina datorer så att det inte uppstår någon oklarhet om skyldigheter när deras respektive datorsystem har utfört orimliga eller felaktiga order eller bekräftelser. Det innebär att ett anbud skall kunna dras tillbaka även i ett datasystem innan det accepteras och det viktiga blir att utforma de tekniska lösningarna så att systemen kan fungera enligt de krav som den dispositiva avtalslagen ställer. Alternativet finns ju givetvis att parterna kan reglera detta i ett EDI-avtal.[112]

Hiselius - Elektroniska Avtalsslut med signatur s 64 f, SOU 1996:40 s 232. Dessa källor utgör dock sekundär källa för mig då primärkällan är: Aversten Daniel, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s 15

[110] Adlercreutz Axel, Avtalsrätt 1 9:e upplagan, 1989, Juristförlaget , Lund, s 48
[111] Lindberg, Dykert, Elektroniska affärer - Juridik och revision, 1996, s 38-39
[112] Lindberg Dykert, Aa, s 41-42

6.3 Definitioner

Det är av betydelse för den elektroniska signaturen att definiera begreppen: dokument, handling och urkund. Begreppet dokument definieras som en beteckning för handelstermer och används i lag och andra juridiska texter. Synonymt används ibland begreppet handling oftast i betydelsen pappersdokument. Urkund är det snävare av begreppen och används främst inom straffrätten. Sammantaget för dessa tre ovanstående begrepp är att det inte finns någon klar definition.[113]
Andra begrepp som används i lagtext och andra sammanhang är namnteckning, underskrift och signatur och de har en enhetlig betydelse i form av att det skall finnas en egenhändig underskrift och signatur på ett avtal/dokument. Av detta följer att signaturens främsta egenskap är att den utgör en individuell länk mellan person och underskrift och kan binda personen till ett avtals verkningar. Jag väljer att använda begreppet signatur.[114]

6.3.1 Urkund[115]

Det går inte att tekniskt skydda en elektronisk signatur från en kopia, den elektroniska signaturen förekommer således endast som original, när erforderligt skydd getts för dess äkthet genom tekniska krypteringsrutiner. För att få en uppfattning om elektroniska signaturer att det viktigt att förstå rättsfrågorna kring en urkund och ett elektroniskt dokument. Definitionen av urkund finns i 14 kap 1§ brottsbalken och utgörs av en exemplifierande uppräkning såsom; kontrakt, skuldebrev, intyg och annan handling, som upprättas till bevis eller eljest är av betydelse såsom bevis. En urkund definieras som en upptagning vars innehåll och utställare kan verifieras genom en underskrift.

Pappersurkunden kan sägas bestå av tre begrepp:

- Bäraren (pappersarket)
- Texten
- Underskriften

Dessa krav måste föreligga för att det skall vara fråga om en skriftlig urkund. Det måste finnas en underskrift som utgör ett äkthetstecken för att övertyga läsaren om att innehållet i handlingen inte härrör från någon annan och tilliten till uppgifternas ursprung bidrar till förtroendet för skriftliga dokument.

---

[113] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, IRI-Rapport, s 5-6
[114] Lindberg, Aa s 29-30.
[115] Elektronisk dokumenthantering - En rättslig problemorientering, Riksarkivet/ Lagerlöf & Leman, s 9-14

6.3.2 Elektroniskt dokument[116]

Det elektroniska dokumentet måste uppfylla samma funktioner som det pappersbaserade dokumentet för att duga som bevis.

- Dokumentet skall ha en individualiserande funktion, det vill säga en koppling till en individ genom underskrift.
- Dokumentet skall ha en låsande funktion, det vill säga en omöjlighet att ändra i innehållet.
- Dokumentet skall ha en synlig funktion, det skall gå att betraktas av parterna.

Det pappersbaserade originaldokumentet anses ha ett högre bevisvärde än en kopia och ett problem framkommer när man skall definiera hur ett elektroniskt originaldokument ser ut. Det egentliga originalet finns i datorns primärminne under wordarbetet. Så fort strömmen slås av töms minnet och sparas på hårddisken och utgör en kopia av det som fanns i primärminnet. Det krävs sålunda att avtalet måste sparas på hårddisken eller diskett. Det blir alltså omöjligt att skilja mellan ett elektronisk originaldokument och en kopia. Det handlar om att domstolen måste övertygas om att det elektroniska dokumentet uppfyller kriterierna för att kunna beaktas vid en bevisprövning. Eftersom praxis saknas om det elektroniska dokumentets bevisvärde så är det svårt att veta vilket värde ett elektroniskt dokument skulle ha vid en rättegång. I 38 kap 1§ rättegångsbalken finns det principer för bevisvärdet för skriftliga urkunder, men lagrummet innehåller inget om elektroniska bevismedel och det är svårt att bedöma hur långt man kan sträcka sig i en analog tolkning.

6.4 Komparativ jämförelse med namnteckning[117]

Syftet med detta avsnitt är att undersöka varför det i vissa fall ställs krav, antingen i lag eller avtal, på egenhändig namnteckning för att genomföra avtalsrättsliga handlingar. Det syfte som en namnteckning anses fylla i dessa fall skall utredas. Avsikten med detta är att utreda om inte den elektroniska signaturen minst lika bra kan uppfylla namnteckningens funktioner, ja till och med bättre i vissa fall.

[116] Hiselius, Elektroniska avtalsslut med signatur IRI-rapport 1989:2, s 30
[117] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, IRI-Rapport , s 30-41

Om man undersöker syftet med de bestämmelser som ställer krav på egenhändig namnteckning finner man enligt doktrinen fem funktioner.[118]

- identifierar
- säkerställer det undertecknades äkthet
- har bevisverkan
- fylla en viljefunktion
- ha en varningsfunktion

I det följande skall betydelsen av ovanstående fem funktioner förklaras lite närmare.

6.4.1 Identifikation

Namnteckningen identifierar den som undertecknat ett dokument. Det går också att uttrycka det så att namnteckningen visar vem som är utställare av ett visst dokument. Genom att kontrollera namnteckningen kan man dessutom verifiera att det är rätt person man har att göra med. Denna funktion kan en namnteckning fylla beroende på att den är personlig. I princip har varje människa en unik namnteckning och därför kan denna användas för att identifiera en person. Detta förutsätter dock att man sedan tidigare vet hur en viss persons namnteckning ser ut, eller att någon är närvarande när personen ifråga skriver sin namnteckning.[119]

6.4.2 Äkthet[120]

Äkthetsfunktionen är en av de viktigaste funktionerna hos en namnteckning. Att en handling är äkta är av allra största vikt för dess betydelse och nytta för mottagaren. Att en handling är äkta innebär först och främst att dess innehåll kommer ifrån den som är utställare, dvs från den som undertecknat. En namnteckning på ett dokument anses garantera att uppgifterna i detta kan hänföras till undertecknaren. Man kan också säga att innehållet i ett dokument genom namnteckningen på ett visst sätt knyts till den som undertecknat.
Äkthetsfunktionen är möjlig på grund av att namnteckningen är personlig och därmed kan användas för ett identifiera en person. För att kunna fastställa en viss namnteckningsanknytning till en viss person krävs dock normalt sett, att det finns en annan namnteckning som man kan jämföra med, om man med säkerhet vet att den härrör från personen ifråga. Möjligheten att på så sätt avslöja t.ex. förfalskningar varierar. Normalt kontrolleras inte namnteckningen så särskilt noga i de flesta vardagliga avtal. Det är oftast först när det händer något som en namnteckning undersöks.

---

[118] Aversten, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s 15
[119] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, IRI-Rapport , s 30-41
[120] Aa s 30-41

6.4.3 Bevisverkan

En namnteckning får en viktig bevisfunktion. Genom att signaturen binder papperet vid innehållet skall signaturen utgöra den sista markeringen för att ett avtal är fullbordat och att det inte får tillkomma fler avtalsvillkor. Namnteckningens bevisverkan följer av att man genom ett undertecknande förutsätts acceptera att ta på sig ett ansvar för ett dokuments äkthet, korrekthet och fullständighet och genom namnteckningen förväntas man erkänna sig bunden till dokumentets innehåll.[121]

6.4.4 Viljefunktion

En namnteckning kan sägas ha en viljefunktion på så sätt att den anses ge uttryck för undertecknarens vilja att bekräfta och binda sig till innehållet i den undertecknade dokumentet.[122]

6.4.5 Varningsfunktionen

Namnteckningen fyller även en varningsfunktion. Genom att underteckna en handling skall man bli medveten om att man genom denna åtgärd kan bli rättsligt förpliktigad på ett eller annat sätt. Denna funktion ligger ganska nära viljefunktionen på så sätt att också denna funktion bygger på att man aktivt skall göra något, i detta fall undertecknas en handling med namnteckningen. Det har blivit så vanligt förekommande att man måste skriva under med sin namnteckning i nästan alla typer av transaktioner idag, att det i de allra flesta fall sker nästan med mer eller mindre rutin. Tanken bakom vissa av de krav på egenhändig namnteckning som finns i lag är dock att det skall tjäna som en slags varningssignal t.ex. vid köp av fast egendom.[123]

6.5 Hur den elektroniska signaturen kan fylla den traditionella signaturens funktioner[124]

Genom att studera hur den elektroniska signaturen uppfyller namnteckningens grundläggande funktioner går det att få en motsvarande bild av hur pass väl lämpad en elektronisk signatur är för att användas i svensk avtalsrätt. Det finns i svensk rätt inga krav på hur en namnteckning skall se ut eller hur den skall utföras. Det finns alltså inga hinder mot att istället för namnteckning använda sig av en elektronisk signatur.

---

[121] Hultmark, Elektronisk avtalsrätt, 1998, s 86-87
[122] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, IRI-Rapport , s 30-41
[123] Aa s 30-41
[124] Ds 1998:14, s 134-137

6.5.1 Identifikation

Även den elektroniska signaturen kan användas för att identifiera en person. Detta är möjligt om den elektroniska signaturen kan verifieras på något sätt, t.ex. genom något tekniskt förfarande. Exempelvis kan en elektronisk signatur verifieras med hjälp av den öppna nyckeln. Det faktum att den elektroniska signaturen kan verifieras är dock inte tillräckligt för att identifieringsfunktionen skall uppfyllas. Detta beror på att den elektroniska signaturen inte är personlig på samma sätt som en namnteckning. Det finns inget naturligt eller nödvändigt samband mellan en person och de elektroniska signaturerna, som är fallet med en namnteckning. Det enda som binder användaren till exempelvis en elektronisk signatur är tillgången till en privat nyckel, och därför kan en sådan signatur i sig endast sägas bekräfta att det är innehavaren av den privata nyckeln som har signerat ett meddelande. För att dessutom kunna verifiera vem denna person är, dvs identifiera avsändaren, förutsätter systemet med elektronisk signaturer att kopplingen mellan en elektronisk signatur och en bestämd person fastställs.[125] Detta kan skötas av parterna själva, genom att avsändaren på något sätt för mottagaren tillfredsställande sätt, bevisar sin identitet. Detta kan dock inte alltid ske, på grund av praktiska eller andra skäl. Ett alternativ som nämnts är att låta en betrodd tredje part, en s.k. CA fastställa och intyga sambandet mellan en signatur och en person. En CA skall ge ut certifikat som beskriver vem som är innehavare av en viss elektronisk signatur, dvs binder samman en person med dennes elektroniska signatur och därmed också den privata nyckeln. Certifikatet garanterar identiteten hos innehavaren av en elektronisk signatur.[126]
Att sambandet mellan en elektronisk signatur och en bestämd person kan fastställas är dock i sig inte tillräckligt för att fylla identifieringsfunktionen. På detta sätt garanteras ju ej att det verkligen är rätt person som skapat den elektroniska signaturen. Exempelvis kan vem som helst, som har tillgång till den privata nyckeln till en elektronisk signatur, och som vet hur denna nyckel fungerar, skapa en identisk elektronisk signatur. Tanken är dock att även den elektroniska signaturen skall göras personlig på så sätt att endast en person skall kunna skapa den. Detta kan man åstadkomma på flera sätt genom att använda sig av smarta kort som endast kan öppnas med en PIN-kod, biometriska metoder eller liknande tekniska metoder.[127] Med dessa metoder kan den elektroniska signaturen göras ännu säkrare än idag, och framför allt så skulle den bli personlig på så sätt att endast en person skulle kunna skapa en viss elektronisk signatur.

[125] Aversten, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s 23
[126] Användning av ID-kort EID, SEIS-rapport, 1998, s 13-14
[127] Smarta kort - den smartaste lösningen?, Höynä Ulla-Karin, Teldok info nr 17, utgiven i maj 1997 av Teldok

6.5.2 Äkthet

Äkthet är en nästan lika viktig funktion hos den elektroniska signaturen som identifieringsfunktionen. Det måste gå att med rimlig säkerhet bevisa att ett dokument är äkta, det vill säga att innehållet inte är manipulerat och att det verkligen härrör från den angivna utställaren. En aspekt av äkthetsfunktionen är att det skall framgå att ett dokument verkligen härrör från den som framstår som utställare, en annan att man skall kunna säkerställa att dokumentet ej har förvanskats sedan avsändandet.[128]
Med hjälp av kryptering kan man garantera bada aspekterna av äkthetsfunktionen vid elektronisk signering, att det går att säkerställa att dokumentet inte har förändrats och att det härrör från den som framstår som utställare. Detta möjliggörs genom att det vid dekrypteringen av det krypterade meddelandet direkt framgår om meddelandet förvanskats på vägen och om det då är en annan utställare. Med en elektronisk signering tillsammans med kryptering kan man alltså uppfylla äkthetsfunktionen.[129]

6.5.3 Bevisverkan

Frågan om bevisverkan kan uppdelas i två huvudfrågor. Den första gäller krav på bevisning, den andra den materiella frågan. De formella rekvisiten regleras i ett lands processrättsliga regler och avser frågan vilka bevismedel som accepteras enligt RB. De materiella rekvisiten rör trovärdigheten, dvs det så kallade bevisvärdet, av viss bevisning.[130]
När det gäller den första frågan, om formella krav på bevisning, har vi i svensk rätt något som kallas fri bevisprövning. Det innebär att vi inte har några regler om vad som utgör bra eller rätt bevisning, utan princip kan vad som helst accepteras som bevisning i en rättegång. Det finns alltså i svensk rätt inga formella processrättsliga hinder för att åberopa en elektronisk signatur som bevisning. När det gäller den andra frågan så har vi även fri bevisvärdering i Sverige. Principen om fri bevisvärdering innebär att domstolarna fritt kan pröva den framlagda bevisningens värde.[131]
Om man vill åberopa en elektronisk signatur som bevisning angående något faktum, hur skall man då visa att den elektroniska signatur som användes i det aktuella fallet var säker nog för att kunna tjäna som fullgod bevisning? Med teknikens hjälp kan man göra den elektroniska signaturen så säker att den får ett minst lika högt bevisvärde som en namnteckning.

[128] Ds 1998:14, s 134-137
[129] Statskontoret skrift 1999:17, Strukturer för hantering av certifikat och krytonycklar i Sverige, bilaga 1, s 3-4
[130] Lindberg, Dykert, Elektroniska affärer - Juridik och revision, 1996, s 23
[131] Hultmark, Elektronisk avtalsrätt, 1998, s 86-87

6.5.4 Viljefunktionen

När det gäller den elektroniska signaturen så utformas rutinerna så att användaren måste ange en särskild PIN-kod för att utföra själva signeringen. På detta sätt förutsätter signeringen ett visst mått av aktivt och medvetet handlande från användarens sida. Det får till följd att den elektroniska signaturen anses vara ett uttryck för användarens vilja att bekräfta och bli bunden av det meddelande som signeras med den privata nyckeln, och därmed kan viljefunktionen uppfyllas också med den elektroniska signaturen.[132]

6.5.5 Varningsfunktionen

Varningsfunktionen kan tillgodoses vid användande av elektronisk signatur. Genom att använda den elektroniska signaturen så utformas nämligen själva proceduren vid skapandet av en elektronisk signatur så att användaren klart och tydligt blir varse när han verkligen signerar något och inte bara t.ex. loggar in på någon webbsida. Användaren uppmärksammas på det faktum att en signatur håller på att skapas. Håller man bara den elektroniska signaturens olika funktioner klart åtskilda på detta sätt, och låter användaren dubbelbekräfta en gång innan signering, så uppfylls varningsfunktionen med ett undertecknande. Nya tekniska lösningar som en elektronisk signatur har medfört ökade möjligheter att rikta särskild uppmärksamhet mot eller varna för vissa avtalsvillkor och det kan vid tvister göras en skälighetsbedömning där man tar hänsyn till i vilken utsträckning villkor har framhållits på ett sätt att motparten har kunnat överväga och bedöma konsekvenserna av avtalsvillkor eller annat kontraktsinnehåll.[133]

6.6 Avtalsformer

Det finns tre betydande avtalsformer: konsensual, formal och realavtalet. Konsensualavtalet kännetecknas av att ett bindande avtal kommer till stånd genom ett utbyte av samstämmiga viljeförklaringar utan krav på särskild form. Formalavtalet kräver särskild form för att vara bindande medan realavtalet blir bindande genom tradition.[134] I sammanhang med avtalsformer finns det fog för att resonera kring vilken teoretisk avtalsmodell som kan utgöra grunden för avtalsformernas tillämpning.
Enligt Jansson finns det två olika grundläggande modeller för avtals ingående med en specifik användning av elektroniska signaturer. Den första traditionella metoden med anbud och accept är uppbyggd på löftes och viljeprincipen. Den andra modellen för att ingå avtal är genom realhandlande och skiljer sig från grundmodellen med anbud och accept

[132] Smarta kort - den smartaste lösningen?, Höynä Ulla-Karin, Teldok info nr 17, utgiven i maj 1997 av Teldok
[133] Hultmark, Elektronisk handel och Avtalsrätt, 1998, Stockholm s 74
[134] Adlercreutz, Avtalsrätt 1, 1991, s 47

genom att det inte sker något utbyte av viljeförklaringar. Istället sluts avtalen genom att en person handlar på ett visst sätt. Det krävs att den ena parten skapar en miljö i vilken realavtal kan komma till stånd om motparten agerar på att avsett sätt. Accepterande av avtal genom realhandlande bör ske med beaktande av argumentet att det är fråga om massavtal som har upprättats av säljaren i syfte att underlätta handel med ett stort antal köpare eller avtalskontrahenter och att det är svårt att påverka avtalsvillkoren för en individuell nivå. Det finns i princip inget hinder emot att realavtal med elektroniska signaturer inte skall vara lika giltiga som vilket annat avtal som helst.[135]

Grönfors har utvecklat dessa avtalsmodeller och talar om en tredje modell för avtals ingående genom att utgå från direkta avtalsgrundande rättsfakta som innebär en friare syn på vad det är som skall ligga till grund för att ett avtal skall anses ingånget. Detta bör göras för att anpassa avtalsmodellerna till den föränderliga handeln och bidra till att realavtal kan accepteras fullt ut. Till grund för sina idéer har han förklaringsteorin som bygger på att accept och anbud skall ses som iakttagelse och ju tydligare dessa framstår för en objektiv betraktare skall ett avtal anses ingånget. Detta synsätt har inte blivit helt okritiserat, men det finns en viktig poäng i det faktum att bedömningsgrunderna har blivit bredare och omfattar mer fakta vilket indirekt skulle kunna omfatta en elektronisk signatur. Detta innebar att det är troligt att ett avtal slutet med en elektronisk signatur skulle anses som fullbordat.[136]

Jansson gör den bedömningen att avtal som sluts mellan människor med hjälp av det elektroniska mediet som t.ex. elektroniska signaturer kan regleras av avtalslagens modell för avtals ingående men att det uppstår problem med avtalsslut som åstadkommits utan mänsklig inblandning. Modellen med avtal genom realhandlande kan appliceras på automatiska elektroniska signaturer, men är ännu inte accepterat. Visserligen finns det en lag som likställer kvalificerade elektroniska signaturer med en traditionell namnteckning men ännu har det inte gått så långt att juridiskt tunga akademiska avtalsmodeller skulle omfatta nya former för avtals ingående. Förespråkarna för Grönfors modell med avtalsingående uppbyggd på direkt avtalsgrundande rättsfakta har fått stöd av utredarna i SOU 1996:40 om Elektronisk dokumenthantering som anser att Grönfors modell är den lämpligaste modellen för att tolka automatiskt skapade elektroniska avtal med ett eventuellt användande av elektroniska signaturer. Enligt utredaren finns det situationer där det är fråga om att ett praktiskt behov som har skapat avtalsverkningar, trots att det inte i formell mening föreligger någon viljeförklaring. Automatiska processer är inte alltid kompatibla med lagens krav på subjektivitet och det i sig talar för att det skulle behövas en ny modell som är fri från subjektivitet, men med klart avgränsande urskiljbara utväxlingar av viljeförklaringar.[137]

---

[135] Jansson, Den elektroniska marknadsplatsen Avtals, köp och bevisrättsliga möjligheter, IRI-Rapport 1997:1, Stockholms Universitet, s 41

[136] Jansson, Aa, s 42

[137] Jansson, Aa, s 43-46

En ny avtalsmodell skulle lättare kunna omfatta både tekniska och juridiska fakta för att anse att ett avtal skulle vara fullbordat med en elektronisk signatur.

6.6.1 Realavtal

För realavtal är det utmärkande att prestation, vanligen tradition av föremålet för avtalet, krävs för att den rättshandlande skall vara bunden. Ett exempel på den här avtalsformen är gåva. I princip är den elektroniska signaturen tillämplig även på ett gåvoavtal men det krävs tradition för gåvans fullbordande.[138] Men i övrigt nämns knappt realavtalsformen i avtalslagen eller i dess förarbeten.[139]

6.6.2 Formalavtal

Enligt huvudregeln finns det inga formkrav för anbud och accept utan dessa kan utväxlas på vilket sätt som helst; skriftligen, muntligen, per telefax eller elektroniskt. Ett muntligt avtal är lika bindande som ett skriftligt men det är lättare att bevisa innehållet i ett skriftligt än i ett muntligt avtal. De formkrav som finns består ofta i att en handling skall ha en viss form, t.ex. skriftligen eller att det krävs en egenhändig namnteckning. Avtalslagen 1§ 3 st anger att lag med formkrav står över avtalslagen, t.ex. köp och försäljning av fast egendom[140] kräver skriftlig form och i princip innebär det ett krav på ett traditionellt pappersdokument.[141]
Bestämmelsen i 17§ lag om kvalificerade elektroniska signaturer (se bilaga A) föreskriver att "om det av lag eller annan författning följer vissa formkrav för att en rättshandling skall anses giltlig eller en förpliktelse fullgjord och om dessa krav kan uppfyllas genom elektronisk kommunikation med användning av någon form av elektronisk signatur, skall en kvalificerad signatur godtas" Detta ter sig oklart i förhållande till motiveringen i Ds 1999:73[142] som anger att bestämmelsen inte påverkar krav i lag eller annan författning som utesluter användning av elektroniska rutiner oavsett hur detta kommit till uttryck.[143]
Jag tycker inte att det på något sätt klargör problematiken hur lagen bör tolkas utan det verkar som en motsatstolkning. Huvudfrågan är om en kvalificerad elektronisk signatur kan godtas i de fall då det i lag uppställts formkrav? Det går givetvis att utsträcka frågan till att bedöma om även formkravet kan uppfyllas med en icke kvalificerad elektronisk signatur.

---

[138] Adlercreutz, Avtalsrätt 1, 1991, s 233
[139] Adlercreutz, Avtalsrätt 1, 1991, s 47
[140] Vad gäller jordabalkens krav på skriftlighet så är det viktigt att äganderättsövergångar blir helt klarlagda. Formkravet kan vara ett uttryck för att överlåtelsen sker först efter ett moget övervägande och att det i sig bidrar till en precisering av avtalsinnehållet och fungerar som ett bevismedel för avtalets tillkomst och innehåll. Lindberg s 9
[141] Avtalsrätt 1, Adlercreutz Axel, 1991, s 122
[142] Ds 1999:73 s 116
[143] Elektronisk dokumenthantering - En rättslig problemorientering, Riksarkivet/ Lagerlöf & Leman, s 29

Svaret på dessa frågor borde definitivt ha klargjorts av lagstiftaren som i samband med införandet av lagen skulle ha sett till att fastslå tillämpligheten av lagen i alla formkravsfall och om nödvändigt ha ändrat lagstiftningen för att den även skulle omfatta alla former av elektroniska signaturer.
Ett sätt att kringgå detta svåra resonemang finns enligt Hultmark i sättet att bedöma det bakomliggande syftet med formkravet och därefter bedöma om det tillgodoses med hjälp av den elektroniska lösningen. Det handlar om att inte fokusera på innebörden i ordets snäva betydelse utan att med en ändåmålsenlighet se om en elektronisk lösning kan bidra till att formkravet kan uppfyllas utan att det sker på ett traditionellt skriftligt sätt.[144]

6.6.3 Konsensualavtal

En avtalsform som bygger på en viljeförklaring och som visar att den förklaring som ges syftar till att åstadkomma vissa rättsverkningar är konsensualavtalet. Avtalslagens kap 1 är anpassat för den typ av avtalsform som kallas konsensualavtal, vilket innebär att det inte behöver finnas något krav på avtalsform för avtalets ingående som formalavtal eller på att prestation skall ske som i ett realavtal. Det kännetecknande för ett konsensualavtal är det ingås genom ett ömsesidigt utbyte av viljeförklaringar med sammanställande innehåll.[145] Det möter inga hinder att använda sig av en elektronisk signatur i ett konsensualavtal därför att de tekniska rutinerna kan framställa och säkra parternas viljeförklaringar.

6.7 Avtalsproblem i en elektronisk miljö

Detta avsnitt innehåller en upprakning av problemområden i en elektronisk miljö där man avser att använda sig av en elektronisk signatur för att signera avtal, skicka anbud eller accept men där det förekommer att tekniska problem kan bidra till en avtalsrättslig oklarhet genom att meddelanden kan försvinna, förvanskas eller missförstås.

6.7.1 Avsändande av meddelande

Inom avtalsrätten inträder i vissa fall rättsverkningar redan genom att ett meddelande avsänts. Enligt huvudregeln i avtalslagen 40§ så är det avsändaren som får stå för risken för att ett meddelande inte kommer fram. Men enligt undantag i 40§ går vissa meddelanden på mottagarens risk. Det gäller meddelanden som är i mottagarens intresse.[146] En reklamation måste skickas till en anbudsgivare eller anbudsmottagare när denne befinner sig i villfarelse om ett avtal är ingånget eller inte. Om en anbudsgivare mottager en oren accept, det vill säga ändringar i anbudet från anbudstagaren, så

[144] Hultmark, Elektronisk handel och Avtalsrätt, 1998, s 65
[145] Lindberg, Elektroniska orginaldokument och elektronisk signatur s 49-50
[146] Lindberg, Dykert, Elektroniska affärer - Juridik och revision, 1996, s 69

måste anbudsgivaren reklamera för att inte bli bunden av avtalet. Ett sådant meddelande skall skickas med post eller telegraf eller eljest på ändamålsenligt sätt (40§ 1 st). Vad som är ändamålsenligt sätt kan skilja sig från fall till fall. Har parterna tidigare kommunicerat på ett visst sätt skall reklamationen göras på samma sätt.[147] I SOU 1996:40 föreslås ett tillägg till 40§ att mottagaren även skall stå för risken av förvanskningar av ett meddelande i mottagarens intresse enligt 32§ 1st. Men denna lösning skulle innebära en lagtekniskt svår lösning genom att man via ett e contrarioslut i 40§ om att 32§ 1 st endast skulle vara tillämplig på andra typer av avtal än dem som omfattas av huvudregeln om att meddelanden som sänds i motpartens intresse skall gå på dennes risk, så skall det även göras ett ytterligare e contrarioslut i 32§ 1 st.[148]

6.7.2 Mottagande av meddelande

Rättsverkningar av att ett meddelande kommer någon tillhanda är att mottagaren måste kunna ta del av meddelandets innehåll. Enligt IT-utredningen bör ett elektroniskt meddelande anses ha kommit mottagaren tillhanda när meddelandet har förts över till den funktion i mottagarens datasystem där meddelanden skall tas emot, som en e-postlåda. Det viktiga är just möjligheten att kunna ta del av det och inte när det sker. Dock kan det uppstå problem på vägen. [149] En viktig faktor för att avgöra om ett avtal med en elektronisk signatur har kommit mottagaren tillhanda är vilken adress parten anger mot omvärlden. Ett problem som har uppstått i samband med denna fråga är e-postadresser där det har visat sig att många har flera e-postadresser men att endast en av dem avläses ofta medan andra avläses mer sällan. Därför är det angeläget att meddelanden sänds till adresser som mottagaren angivit.[150]

6.7.3 Förvanskning

När ett meddelande skickas elektroniskt kan det uppkomma en förvanskning. Det innebär att hela eller delar kan bli oläsliga för mottagaren och att missförstånd kan uppstå. När ett meddelande förvanskas uppkommer frågan vem av parterna som bör bära risken för förvanskningen. Inom avtalsrätten talar man om viljeprincipen och tillitsprincipen. Enligt viljeprincipen är det vad viljeförklararens avgivare avsett som bestämmer rättshandlingens innehåll och rättsverkningar. Enligt tillitsprincipen tar man istället hänsyn till mottagaren av meddelandet och det avgörande är därför mottagarens förväntan och tillit.[151] Avtalslagen bygger på en kombination av dessa principer. Huvudregeln inom avtalsrätten är att avsändaren står för risken att hans meddelande inte kommer fram på rätt sätt eller i rätt tid.

[147] SOU 1996:40, S124
[148] Hultmark, Elektronisk handel och Avtalsrätt, 1998, s 56-57
[149] SOU 1996:40, s126
[150] Hultmark, Elektronisk handel och avtalsrätt, 1998, s 50
[151] Adlercreutz, Aa, 1991, s 32

Undantagen är meddelanden där skyldigheten att skicka meddelandet finns i mottagarens intresse.[152] Dessa principer bör även kunna tillampas i de fall då en elektronisk signatur används.

6.7.4 Förklaringsmisstag och befordringsfel[153]

Anbud och accept är enligt grundläggande regler i avtalslagen bindande för den som avgivit anbudet eller accepten, men vad händer om något blir fel i anbudet eller accepten på grund av ett skrivfel? Detta har lösts i två regler om s.k. förklaringsmisstag och befordringsfel.[154]
Den rättsliga betydelsen av en villfarelse som påverkar en rättshandling förekommer i två former.

1. Förklaringsmisstag
2. Motivvillfarelse- där avtalet fått avsett innehåll, men har påverkats av felaktiga omständigheter.

Förklaringsmisstag, kännetecknas av att ett misstag föreligger genom felaktig inmatning av data eller användandet av en elektronisk signatur. Misstaget skall ha utförts av den rättshandlande själv och att motparten skall vara i ond tro angående förklaringsmisstaget vilket innebär att mottagaren insåg det faktiska felet.[155]
Befordringsfel i Avtl 32§ 2st framkommer om en viljeförklaring som sänds via telegram förvanskas på grund av fel vid telegraferingen vilket medför att avsändaren inte är bunden av viljeförklaringen. Det har ingen betydelse att mottagaren är i god tro. Kravet är att avsändaren meddelar mottagaren detta så fort felet upptäcks för att inte bli bunden av någon passivitet.[156]
I en elektronisk miljö är det oklart hur de här reglerna skall tillämpas. IT-utredningen gör bedömningen att regeln om förklaringsmisstag inte kan tillämpas när ett elektroniskt meddelande förvanskats under överföringen till mottagaren. Inte heller reglerna om befordringsfel bedöms kunna tillämpas på fel som uppstår när meddelanden överförs elektroniskt.[157]
Lindberg gör bedömningen att själva grunden för tillämpningen av 32§ 2 st saknas därför att det inte finns någon mellanhand som förvanskar ett meddelande. Enligt honom saknas möjlighet att göra ett analogislut i relation till telegrafifallet och bedömningen bör göras utifrån 32§ 1 st att det blir avsändaren som får stå för risken. Även Grönfors kommer fram till slutsatsen att en avsändare av ett elektroniskt meddelande med elektronisk signatur blir bunden av det innehåll som förklaringen har när det kommer fram.[158]
Även Hultmark bedömer att det saknas anledning att analogisera från 32§ 2 st och att det är huvudregeln som gäller att användaren och avsändaren av ett

[152] Hultmark, Elektronisk handel och avtalsrätt, 1998, s 54
[153] EDI-AVTAL Handledning till EDI avtal 96, Toppledarforum, 1997, s 10
[154] EDI-AVTAL Handledning till EDI avtal 96, Toppledarforum, 1997, s 10
[155] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, s 66-68
[156] EDI-AVTAL Handledning till EDI avtal 96, Toppledarforum, 1997, s 10
[157] EDI-AVTAL Handledning till EDI avtal 96, Toppledarforum, 1997, s 10
[158] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, s 69

elektroniskt meddelande med en elektronisk signatur skall stå för risken för ett meddelande förvanskats.[159]

6.7.5 Återkallelse

Huvudregeln i Avtl7§ anger att ett anbud eller en accept kan återkallas även om det har kommit mottagaren tillhanda men att mottagaren inte har hunnit ta del av det. Vid elektronisk kommunikation är risken för att meddelanden oavsiktligen sänds iväg ganska stor, att möjligheten måste finnas för att en användare av en elektronisk signatur skall kunna återkalla sitt anbud eller sin accept.[160]

6.7.6 Acceptfrist

Huvudreglerna i avtalslagen är att ett anbud är ensidigt förpliktande för anbudsgivaren under acceptfristen. Den legala acceptfristen bygger på att anbudsgivaren ger anbudsmottagaren en betänketid. Anbudsgivaren ger alltså ett underförstått och indirekt löfte om att han förklarar sig ensidigt bunden under acceptfristen. Den kommunikationsteknik som anbudsgivaren använder anger inte definitivt hur lång acceptfrist som han medger anbudsmottagaren men det ger en indikation. I verkligheten minskas betänketiden när kommunikationen sker elektroniskt och vid användandet av elektroniska signaturer bör man vara medveten om acceptfristen[161]
Fristen får i regel beräknas enligt avtalslagens riktlinjer för den s.k. legala acceptfristen i 3§ då det sällan finns någon acceptfrist uttryckt. Genom loggning kan den exakta tidpunkten för ett avsändande fastställas och bidra till att kunna bedöma acceptfristens tre olika moment;[162]

1. Tiden för anbudets befordran
2. Skälig betänketid
3. Tiden för svarets befordran

Tiden för anbudets och svarets befordran är vid elektronisk kommunikation obetydlig och bedömningen av hur lång den legala acceptfristen skall vara bedöms utifrån avtalets beskaffenhet och parterna. Sammanfattningsvis så ändrar inte det elektroniska avtalet signerat med en elektronisk signatur principerna för fastställande av när avtalet anses ha ingåtts. Problemet är snarare svårigheten i att säkra bevis om när svaret har kommit mottagaren tillhanda.[163]

[159] Hultmark, Elektronisk handel och avtalsrätt, 1998, s 56
[160] Hultmark, Elektronisk handel och avtalsrätt, 1998, 60-63
[161] Hultmark, Elektronisk handel och avtalsrätt, 1998, s 47
[162] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, s 59-61
[163] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, s 59-61

6.7.7 Brotten

I princip är det en samling av ett antal brottsliga handlingar som har skapat ett behov av att skydda sig mot missbruk av elektroniska signaturer och signerade elektroniska handlingar. Denna sammanställning nedan visar på behovet av att skydda sig mot olika former av manipulationer.

- Att någon har utnyttjat någon annans namn
- Att någon har framställt ett oäkta dokument
- Att någon har använt sig av ett oäkta dokument (att med andra ord använt sig av ett manipulerat certifikat)
- Att någon har förstört ett äkta dokument (undertryckande av urkund)
- Att någon har gett ett äkta dokument ett osant innehåll
- Att någon har missbrukat ett äkta och korrekt dokument för att verifiera något som dokumentet inte skall visa, t.ex. att någon har begagnat sig av någon annans ID-kort och utgivit sig för att vara denne
- Att någon utan att göra något materiellt med handlingen har hindrat ett äkta och sant dokument från att fylla sin funktion

Denna sammanställning ovan visar de handlingar av någon som för egen vinning försöker att manipulera någons elektroniska dokument och elektroniska signaturer. Frågan är om de traditionella brottstyperna har stöd i lag för att även omfatta elektroniska företeelser och om det skall krävas lagstiftningsförändringar för att det även skall omfattas. I utredningarna om elektroniska signaturer fanns ingen annan kommentar annat än att skyddet mot brottsliga handlingar bör även gälla i IT-miljön. Det är utan tvekan så att användandet av tekniken kan lösa teknikens egna problem. Tekniken sätter alltså inget hinder utan det gäller att utnyttja den på bästa sätt för att skapa säkra och tillförlitliga signaturer och hindra manipulationer och missbruk i den mån det går.[164]

6.8 Bevis

Elektronisk bevisning kommer att bedömas efter hur tillförlitlig den är i det specifika fallet. Det medför att den tekniska säkerheten i ett system för elektronisk handel har stor betydelse för frågan om juridisk acceptans. Om avsända meddelanden kan ändras i efterhand, om en avsändare kan manipulera med avsändningsloggen eller ha tillgång till koder eller krypteringsnycklar så minskar det eller nollställer bevisvärdet av den elektroniska handlingen.[165]
Pappersdokument kan skyddas på olika sätt genom att de deponeras på ett visst ställe eller bevittnades så att man säkerställer att inte innehållet har förvanskats på något sätt. De elektroniska handlingarna kan också skyddas. Det elektroniska bevismedlets särart gör att bevisbördan bör placeras på den

[164] Lindberg, Dykert, Elektroniska affärer - Juridik och revision, 1996, s 23
[165] Lindberg, Dykert, Elektroniska affärer - Juridik och revision, 1996, s 23

part som typiskt sett har bäst möjligheter att säkra bevis och fastställa den elektroniska signaturen. Bedömningen av hur starkt bevisvärde som man skall tillmäta ett elektroniskt meddelande bör sedan göras utifrån risken för manipulation.[166]
En viktig del av skyddet är kryptering med nycklar. För närvarande anses det att 128-bitars nycklar är tillräckligt för att förhindra att krypteringen avslöjas och att någon kan förvanska handlingen och förstöra bevisvärdet. Tekniken med elektronisk signatur skyddad med kryptering möjliggör en mycket stark bevisning genom att det kan säkerställas vem som avsänt ett meddelande, om meddelande är förvanskat och tidpunkten för meddelandets avsändande.[167]

6.9 Olika ståndpunkter i doktrinen

Legala aspekter som bör tillgodoses vid elektroniska affärer kan vara av ett flertal slag där de avtalsrättsliga frågorna dominerar. En översyn kan bidra till juridisk kunskap om lagar och regler så att juridiska restriktioner inte uppstår och skapar juridiska hinder i en elektronisk miljö. En lösning som finns är att skapa s.k. standardavtal som EDI-avtal 96 för att uppnå ett allmänt juridiskt accepterande av avtal i alla former av avtalssituationer i elektronisk miljö.[168]
I elektronisk handel förekommer det inte bara elektroniska signatur utan det övergripande ramverket för signaturen är oftast sk EDI-avtal. I princip blir flera typer av avtal aktuella. Avtalsprocessen består i regel av ett ramavtal som innehåller de kommersiella villkoren för att kunna göra avrop. Till detta kommer det s.k. EDI-avtalet som reglerar formen för utväxlande av meddelande mellan parterna och vilken rättslig betydelse sådana meddelande skall ha i den inbördes avtalsrelation. EDI-avtalet innebär att parterna accepterar att de blir bundna av elektroniska viljeförklaringar, även om de är automatiska och bygger på elektroniska signaturer.[169]
Detta ger en förståelse i att de olika avtalen skiljer sig och reglerar olika frågor men att de ändå skall ses i ett sammanhang. Den elektroniska signaturens varde vid t.ex. ett avrop kan fastställas på förhand i ett ramavtal.[170] Om parterna har reglerat det som utgörs av en legal acceptans av de olika inbördes avropen så är stora problem lösta. Detta kan ske genom s.k. överföringsavtal som skall se till att överföringen sker på ett säkert sätt med logg och mottagningskvittenser.[171]
Rent tekniskt och språkligt finns det inget hinder emot att en icke-kvalificerad elektronisk signatur skulle få samma rättsverkan som en traditionell namnteckning. För att den icke-kvalificerade elektroniska signaturen skall vara juridiskt acceptabel krävs det att funktionerna hos den

[166] Hultmark, Elektronisk handel och avtalsrätt, 1998, s 86-87
[167] Hultmark, Elektronisk handel och avtalsrätt, 1998, s 96-99
[168] EDI-AVTAL Handledning till EDI avtal 96, Toppledarforum, 1997, s 8
[169] EDI-AVTAL Handledning till EDI avtal 96, Toppledarforum, 1997, s 13-15
[170] Elektronisk handel för kommuner, landsting och stat, Handbok 2, 1996, s 46-50
[171] Fredholm, Elektronisk handel: Status och trender, 1998, s 35

traditionella signaturen hålls intakta. Det finns två vägar att uppnå detta och genom den tekniska angreppsvinkeln så anpassar man tekniken till gällande rättsregler och allmänna rättsprinciper. Alternativt om det finns en lagtext som hindrar detta så får den istället den juridiska angreppsvinkeln användas, vilket får till följd att juridiken anpassas till tekniken. Huvudsaken enligt Lindberg är att pappersdokumentets fem funktioner kan hållas intakta vid användandet av den elektroniska motsvarigheten, men detta kan inte ske i dagsläget utan vissa ändringar.[172] Ett sätt att hitta lösningar till förändringarna är genom analogitolkningar av praxis.

Det finns exempel i praxis där domstolen använt sig av metoden att undersöka syftet bakom en rättsregel. Ett fall, NJA 1981 s 595, rör det krav som förr fanns i RB om att ett överklagande skall vara egenhändigt undertecknat. I detta rättsfall hade en besvärsinlaga (dvs överklagande) undertecknats med "Prisoner 1006", istället för med dömdes rätta namn. Enligt RB 52 kap 3§ 3 st, som var dess då gällande lydelse, fanns det ett krav på att överklagan skulle undertecknas av den klagande eller dennes ombud. HD godtog undertecknandet med motivering att om inte namnet användes skulle identifieringen försvåras men att "om det av andra omständigheter framgår vem som undertecknat inlagan, får kravet på egenhändigt undertecknande anses uppfyllt".[173] Detta rättsfall visade att ett krav på undertecknande inte nödvändigtvis behöver innebära ett ovillkorligt krav på att man måste underteckna med sitt rätta namn. Kanske skulle det även kunna tolkas så att det inte heller nödvändigtvis måste röra sig om ett undertecknande med namn över huvud taget, utan att det viktigaste är att det framgår från vem en handling härrör ifrån. I så fall skulle man även kunna godkänna en icke kvalificerad elektronisk signatur.

Vad beträffar modeller för avtals ingående torde avtalslagens modeller vara tillämpliga. Frågan kvarstår dock om de automatiskt behandlade viljeförklaringarna med elektroniska signaturer kan inrymmas i någon av de fristående modellerna för avtals ingående eller om en helt ny modell måste utvecklas. I vart fall bör en elektronisk signatur kunna användas i avtalsformerna: real, formal eller konsensualavtal. T.ex. Hultmark menar att elektroniska miljöer inte på något sätt så pass speciella att de kräver särskilda teoretiska förklaringsmodeller eller speciella lösningar utan att " särskilda problemställningar som elektronisk handel ger upphov till är i hög grad möjliga att hantera inom ramen för redan existerande avtalsrättsliga regler och principer."[174]

Sammanfattningsvis kan man vid en jämförelse mellan den traditionella namnteckningen och den elektroniska signaturen finna att det framgår att den elektroniska signaturen likväl , och i vissa fall till och med bättre, kan fylla de funktioner som en egenhändig namnteckning normalt fyller. Med nyttjande av krypteringsteknik kan den elektroniska signaturen garantera äktheten av ett elektroniskt dokument, dvs säkerställa att dokumentet inte har förvanskats sedan avsändandet och identifiera en persons signatur. Det

[172] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, s 19-21
[173] Lindberg, Elektroniska orginaldokument och elektronisk signatur, 1987:7, s 29
[174] Hultmark, Elektronisk handel och avtalsrätt, 1998, s 101

finns inte heller några processuella hinder att i svensk rätt åberopa elektronisk signering som bevis i en rättegång. De tekniska rutinerna bör också kunna utformas så att också vilje och varningsfunktionerna uppfylls på ett godtagbart sätt även vid elektronisk signering. Vid en samlad bedömning kan alltså den elektroniska signaturen mer än väl fylla de funktioner som motsvarande hos namnteckningen.

7 Analys

Med den nya lagen om kvalificerade elektroniska signaturer försöker lagstiftaren skapa ett regelverk för användandet och kontrollen av elektroniska signaturer. Lagar brukar komma i ett senare skede, men i detta fall vill marknaden att lagstiftningen ska föregå utvecklingen och få igång användningen. Om det i framtiden blir tillåtet att exempelvis deklarera elektroniskt med elektroniska signaturer så ska den kvalificerade signaturen accepteras. Men ännu råder stor osäkerhet om hur detta kommer att fungera i verkligheten.
Men Per Furberg, jurist på Lagerlöf & Leman Advokatbyrå, menar att det ändå finns en framkomlig väg. Han betonar att regleringen borde komma i efterhand. Vidare pekade han på att det är av yttersta vikt att tekniker och jurister kan samarbeta i detta arbete. En annan mycket viktig fråga att ta ställning till är vilka som ska få leverera certifikat, dvs bli de betrodda tredje parterna, och utgöra grundbulten i hela systemet med säker PKI användning.
I Ds 1998:14 varnades det redan för den här utvecklingen med att fastställa skadeståndsansvaret för CA genom att bestämma vem det är som ger ut kvalificerade certifikat. Det kan leda till att endast ett mindre antal företag och organisationer skulle vilja åta sig rollen att agera CA i system där kraven kommer att vara ytterst höga på tillit.[175] Helt klart har kravet på CAn blivit för omfattande. Bolagen är rädda för att tvingas betala ut betungande skadestånd därför att lagen ålägger dem ett strikt ansvar och detta i sig hindrar utvecklingen. Ingen vill ha en CA roll. Kan det bli så att det åläggs staten att i slutändan sköta det som marknaden så hett begärde att få ta hand om?

7.1 Vilka krav kommer att ställas på den tekniska lösningen?

Utvecklingen med elektroniska signaturer har under våren tagit fart genom att Posten kommer att gå ut med försäljning av elektroniska ID-kort till allmänheten innehållande signatur samt att storföretagen har börjat att utrusta sina anställda med elektroniska signaturer på smarta kort. Det pågår även utveckling av att kunna få med elektroniska signaturer på telefonkorten. Det som hindrar den explosiva utvecklingen är att signaturen enligt direktivet måste vara kvalificerad. Det innebär att den privata nyckeln måste skyddas på ett visst sätt samt att certifikaten inte får lagras i en oskyddad miljö. Det innebär att det inte får vara några mjuka certifikat som lagras i minnet på en dator eller ett telefonkort.[176]

[175] Ds 1998:14, s 181
[176] NY TEKNIK 2001:5,Alpman Marie, Digitala signaturer på väg, s 16-17

Problem uppstår i den elektroniska världen därför att det inte går att göra en meningsfull skillnad mellan original och kopia. Hur bedöms en signering som har skett direkt i internminnet och sedan har blivit översänd utan att meddelandet dessförinnan har sparats i något sekundärminne? Frågan har sin utgångspunkt i en beteckning att meddelandet har en kvasimateriell karaktär där det är oklart hur man rättsligt skall hantera något som nästan inte finns. Lösningen finns genom att det med en elektronisk signatur och kryptering går att se till att elektroniska dokument blir giltigt signerade och att innehållet blir låst så att det inte kan förändras eller förvanskas på något sätt.[177] Tekniska bolag som sysslar med dessa frågor har kommit fram till att mjukvarubaserade certifikat och signaturer inte kan åtnjuta rättsligt skydd som urkunder, men att om signaturen tillsammans med certifikatet sparas på ett s.k. smart kort så kan ett dokument utgöra en urkund.[178] Ett bolag som verkligen tar problemet med kvalificerade och säkra signaturer på allvar är Addtrust från Malmö som hyr ut teknik och tjänster till certifikatsutgivare. De har sett till att skydda sina certifikat genom att ställa in sina datorer och servrar i de bankvalv i det f.d. Riksbankspalatset där de har sin verksamhet.[179]

En uppfattning är att juridiken inte hinner med teknikutvecklingen och det förs fram förslag ifrån IT-utredningen (SOU 1996:40) som framhåller att det inte får bli någon teknikspecifik eller teknikberoende lagstiftning. Målet är att lagstiftningen skall ha en funktionell utgångspunkt och bedöma lagen utifrån de krav som juridiken ställer på tekniken. Fördelen med denna form är att tekniken kan förändras på ett funktionellt plan men att vissa frågor behöver lösas av praxis. Ett alternativ till angreppsvinkeln med funktionellt synsätt är detaljreglering. I USA tillämpar delstaterna detaljregleringar då de använder sig av lagstiftning som reglerar elektroniska signaturer ner till algoritmnivå. Det innebär att lagarna blir mycket förutsebara och tekniska men det kan också innebära ett hinder för teknikutveckling att lagens teknikavsnitt hela tiden måste utvecklas när marknaden vill utnyttja sig av det nyaste tekniska lösningarna.[180] Tyvärr saknas det praxis. Bristen på praxis kan i mångt och mycket förklaras med att även om det uppstår tvister löses de direkt mellan parterna genom skiljedomsförfarande. Det innebär att rättstvisterna inte blir offentliga och att det viktiga bedömningsunderlaget saknas för att med hjälp av praxis kunna skapa och utveckla befintlig lagstiftning.[181]

[177] Cardholm Lucas, Prevas Informationsskrift, Att ge elektroniska dokument rättslig status, s5
[178] Cardholm, Prevas Informationsskrift, Att ge elektroniska dokument rättslig status, s7-8
[179] Sydsvenskan 2000-04-05, Sundberg Ulf, Malmöföretag säkrar näthandeln, s A 23
[180] Lindberg, Dykert, Elektroniska affärer - Juridik och revision, 1996, s 106
[181] Fredholm, Elektroniska affärer, 1995, s173

7.2 Vad har en elektronisk signatur för bevisvärde?

Genom att använda standarder för överföring av meddelanden så uppfyller kvittenser och loggar olika viktiga funktioner som förändringsskydd, icke-förnekbarhet av sändning, icke-förnekbarhet av mottagning och äkthetsbevis att avsändaren är den han utger sig för att vara. Loggning innebär att logga händelser som tid, avsändare och mottagare för att ge stöd för att en accept verkligen är gjord.[182] En utväxlingslogg har fått en så stor betydelse för bevisvärdet och bedömningen för anbud och acceptfrågan att det har tagits med som en del i EDI-avtalet 96 och utväxlingsloggens data gäller om inte motparten kan motbevisa detta.[183] Ett tekniskt alternativ till att bevisa vid vilken tidpunkt som ett avtal ingicks är att med hjälp av tidstämpling kunna fastställa tidpunkten för signering av en handling. En betrodd tredje part kan genom att tidstämpla dokumentet och tillhandahålla avsändande- och mottagandebevis se till att avtalet får en högre bevisverkan och indirekt visa för avtalsparterna vid vilken tidpunkt avtalet slöts.[184] Utan tvekan är det så att tekniken kan bidra till att en elektronisk signatur kan få ett högre bevisvärde.

7.3 Uppfyller den elektroniska signaturen den traditionella namnteckningens funktioner?

Med den elektroniska signaturen i en struktur med CA, PKI, kryptering och certifikat uppfylls äkthetsfunktionen av den elektroniska signaturen och identifieringsfunktionen av det elektroniska certifikatet. Avslutsfunktionen är inte lika tydlig i detta sammanhang, då det sällan rör sig om några förhandlingar när avtalen sluts. Bevisfunktionen kan upprätthållas genom kryptering och det blir sedan en fråga om bevisvärdering. Varningsfunktionen, slutligen, kan inte uppfyllas endast med hjälp av den elektroniska signaturen. Visserligen måste användaren oftast skriva in ett lösenord, men för att denne skall bli medveten om konsekvenserna av sitt handlande brukar ytterligare varningsfunktioner användas vid beställning, köp och betalning över nätet. Varningstexter finns i den elektroniska miljön, som läsaren ofta måste intyga att han läst genom en knapptryckning och kan troligtvis uppfylla varningsfunktionen bättre och mer detaljerat för olika avtalsvillkor än motsvarande i den traditionella miljön. I övrigt kan sägas att den traditionella namnteckningens funktioner inte alltid utnyttjas i det traditionella systemet. Hur ofta kontrolleras i verkligheten underskriften på baksidan av kontokortet med det som skrivs på köpnotan? I de elektroniska systemen, däremot, kontrolleras de elektroniska signaturerna och certifikaten automatiskt och sekundsnabbt, och kan därför sägas förbättra funktionerna,

[182] Fredholm, Elektroniska affärer, 1995, s165-166
[183] EDI-AVTAL Handledning till EDI avtal 96, Toppledarforum, 1997, s 20, 29
[184] Aversten, Digitala signaturer och ansvarsproblem, IRI-rapport 1998:2, s 24

och därmed tilliten till de elektroniska signaturerna. Helt klart uppfylls den traditionella namnteckningens grundläggande funktioner genom att använda den elektroniska signaturen.

7.4 Vad har de kvalificerade elektroniska signaturerna för rättsverkan?

Uppsatsens analyserande del visar att en elektronisk signatur uppfyller samma funktioner som namnteckningen genom att den identifierar utställaren av ett dokument, garanterat dokumentets äkthet, har bevisverkan, fyller en viljefunktion och skapar en varningsfunktion. Både tekniskt och juridiskt kan en elektronisk signatur anses likvärdig med den handskrivna namnteckningen. Kravet är enligt lagen att det måste vara fråga om en kvalificerad elektronisk signatur för att den skall ha samma rättsverkan som en traditionell namnteckning.

7.5 Vad har de icke-kvalificerade elektroniska signaturer för rättsverkan?

De kvalificerade elektroniska signaturerna kommer att ha ett på förhand bestämt erkännande som funktionellt likvärdiga med en handskriven namnteckning, men det har funnits en utbredd missuppfattning om att icke kvalificerade elektroniska signaturer inte skulle omfattas av gällande rättsregler och att lagen om kvalificerade elektroniska signaturer skulle utgöra ett absolut hinder mot en rationell användning av den icke kvalificerade elektroniska signaturen. I själva verket är det möjligt att använda den icke-kvalificerade elektroniska signaturen utan några hinder. Skillnaden är att rättsverkan måste fastställas i efterhand vid någon form av rättslig prövning. Det blir helt enkelt praxis, och parternas avtalsfrihet som får råda om huruvida en icke-kvalificerad elektronisk signatur kommer att ha någon rättsverkan.

7.6 Hur ser framtiden ut?

Det finns kritiska röster till lagens införande i Sverige. IT-kommissionen menar att lagen skapar mer problem än den löser. Problemet är att ingen vill stå som utfärdare av de nödvändiga certifikaten, som gör det möjligt för två parter att kunna lita på varandra, samt att det finns så otroligt många system för elektroniska signaturer på marknaden som inte kan kommunicera fullt ut. EU-kommissionens och den svenska regeringens avsikt var att inte ta ställning till någon teknik utan överlåta åt den europeiska marknaden att själva ta fram tekniska lösningar som blir standarder. Per Furberg hos Lagerlöf & Leman håller med om den här kritiken och menar att lagen kommer att få svårt att få något större genomslag, annat än som betydande

symbolvärde, därför att det kommer att avskräcka utfärdarna från att ta fram kvalificerade certifikat på grund av det betungade skadeståndsansvaret. Dock finns det enligt honom en stor betydelse i att elektroniska signaturer skall komma att bli allmänt bekanta och accepterade och "att lagen kan komma att få stor praktisk betydelse för utvecklingen av tjänster på området, genom att signaler ges från högsta ort om att sådana kryptografiska rutiner och tjänster behövs och stöds av rättsordningen".[185] Ett bra exempel på detta är att PRV har börjat att använda icke-kvalificerade elektroniska signaturer i sin interna verksamhet.[186]

Bland framtidsforskarna finns det en tes om att det kommer att uppstå spontana regelverk, som inte kräver mer än nödvändigt, där tekniken kommer att återge makten till individen och att ansvaret kommer att ligga på oss själva. Tekniken ses alltså inte som ett hinder mot vår integritet utan som ett sätt för att hjälpa till att skydda den och skapa möjligheter att sluta avtal med elektroniska signaturer om det än må vara kvalificerade eller icke-kvalificerade.[187] Idealet vore en lagstiftning som har karaktären av ramlagstiftning och att den inte på så sätt binder tillämpningen till en viss teknik. Det tas på så sätt hänsyn till utvecklingen av ny teknik, samtidigt som den dock anger spelreglerna för användningen utan att bli för teknikberoende.

Vid en samlad bedömning är det är viktigt att undersöka var och varför de juridiska problemen uppstår och hur man närmare kan lösa dessa problem och att man inte okritiskt accepterar befintlig teknik, utan att även juridiken måste få ställa krav på tekniken så att den blir acceptabel ur juridisk synvinkel.

Genom att inleda arbetet med de juridiska frågorna blir det en förenkling att analysera vilka funktioner som finns hos den teknik som man vill ersätta, för att sedan undersöka om den nya tekniken, med en elektronisk signatur, kan fylla samma juridiska funktioner på ett bättre sätt och även i övrigt är minst lika tillfredsställande som den traditionella metoden i form av en namnteckning. Nu har alltså lagstiftaren gett marknaden och användarna ett verktyg och det är nu en tidsfråga innan det går att fastställa genomslaget för den elektroniska signaturen.

[185] Frukostmöte den 23/2 2001 hos www.zedir.se med tema elektroniska signaturer
[186] Möte med Eva Lindell-Frantz den 21/9 2001
[187] Lundblad , Teknotopier - den nya tekniken och rättens framtid, 2001, Timbro, Stockholm sida 1

8 Litteraturförteckning

Litteratur

Adlercreutz Axel, Avtalsrätt 1 9:e upplagan, 1989, Juristförlaget , Lund

Aversten Daniel, Digitala signaturer och ansvarsproblem - Framförallt nyckelinnehavarens och CAs ansvar mot förlitande part, Institutet för rättsinformatik, 1998:2, Jure AB, Stockholm

Benno Joachim, Elektronisk handel - rättsliga aspekter, 1997, Transaktionens anonymisering och dess påverkan på rättsliga problemställningar Årsbok Institutet för Rättsinformatik, Stockholm

Bogdan Mickael, Komparativ Rättskunskap, 1993, Norstedts Juridik, Falköping

Fredholm Peter, Elektronisk handel: Status och Trender, 1998:21, Telematikrapport 2001 utgiven av Teldok 1998

Fredholm Peter, Elektroniska affärer - att införa och använda EDI, 1995, EDI-Föreningen, Stockholm

Halvarsson Andreas Morin Tommy, Elektroniska signaturer - E-Affärer utan elände med identifiering, signering och kryptering, 2000, Studentlitteratur, Lund

Hiselius Patrick, Elektroniska avtalsslut med signatur (EDI och smartkort), IRI-Rapport 1989:2 , Stockholms Universitet

Hultmark Christina, Elektronisk handel och Avtalsrätt, 1998, Norstedts Juridik, Stockholm

Hultmark Christina, Digitala signaturer - Internationella utvecklingstendenser, 1998, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik s 163-69, 1998, Jure AB, Stockholm

Höynä Ulla-Karin, Smarta kort - den smartaste lösningen?, Teldok info nr 17, utgiven i maj 1997 av Teldok

Jansson Ingemar, Den elektroniska marknadsplatsen Avtals, köp och bevisrättsliga möjligheter, IRI-Rapport 1997:1, Stockholms Universitet

Jensen Ulf, Rylander Staffan, Att skriva juridik, 1995, Iustus Förlag, Uppsala

Kelleher Denis, Murray Karen, IT Law in the European Union, 1999, Sweet&Maxwell, London

Lindberg Agne, Elektroniska orginaldokument och elektronisk signatur, 1987:7, IRI-Rapport, Stockholms Universitet

Lindberg Agne, Dykert Lars, Elektroniska affärer, Juridik och revision, 1996, EDI-Föreningen, Stockholm

Lundblad Nicklas, Teknotopier - den nya tekniken och rättens framtid, 2001, Timbro, Stockholm

Made Erik, Examensuppsats Juridiska fakulteten vid Lunds Universitet, Ansvarsfrågor mellan certifikatutfärdare och mottagare vid elektroniska signaturer, s1, vt 2000

Nordisk Årsbok i Rättsinformatik, Elektronisk handel - rättsliga aspekter, 1997, Norstedts Juridik, Stockholm

Nordisk Årsbok i Rättsinformatik, IT-rätten i 1900-talets sista skälvande år, 1998, Jure AB, Stockholm

Plöen Patrick, The concept of “Urkund” and information technology, Essays on Legal Information Management, Institutet för rättsinformatik, rapport 1996:2, Stockholm

Precise Biometrics Årsrapport 2000

Riksarkivet/Lagerlöf & Leman, Elektronisk dokumenthantering - en rättslig Problemorientering, Rapport 2000:1, Riksarkivet, Stockholm

Salomonowitz Sascha, Essays on Legal Information Management, IRI-rapport 1996:2, Stockholm

SEIS-rapport, Säkrad elektronisk information i samhället, Användning av Elektroniska ID-kort EID, 1998, Stockholm

Stora Svenska Ordboken, 1998, Norstedts förlag, Stockholm

Strömholm Stig, Rätt, Rättskällor och Rättstillämpning, femte upplagan 1996, Norstedts Juridik, Stockholm

Teletrust, Informationssäkerhet och digital signering, Nr 4/1991

Trendrapport Elektronisk handel; lagstiftning och regelverk, En globalstudie, Sveriges tekniska attachéer, Lundblad Niklas, 1999

Wahlgren Peter, Om framtida rättsproblem, 1998, s 9-21, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik, 1998, Jure AB, Stockholm

Westman Daniel, Informationsteknikens påverkan på den rättsliga regleringen, 1998, s71-84, IT-rätten i 1900-talets sista skälvande år, Nordisk Årsbok i Rättsinformatik, 1998, Jure AB, Stockholm

Winberg Gustav, Elektroniska betalningssystem på Internet, IRI-Rapport 1997:3, Stockholms Universitet

Offentligt tryck

Regeringens Proposition 1999/2000: 117 Lag om kvalificerade elektroniska signaturer, m.m.

Ds 1999:73 Elektroniska signaturer

Ds 1998:14 Digitala signaturer - en teknisk och juridiskt översikt

SOU 1996:40 Elektronisk dokumenthantering

SOU 1992:110 Information och den nya Informationsteknologin

IT-Kommissionen

Organisation för hantering av certifikat och nycklar, 1999:10

Vikten av användning av kryptering, 1999:14

IT-K Dnr 99/73 Remissvar Ds 1999:73 Elektroniska signaturer

Statskontoretes IT-publikationer

99:17 Strukturer för hantering av certifikat och kryptonycklar i Sverige - Förslag till vidare arbete.

1999:30 Säkerhet med elektronisk identifiering, Statskontorets skrift

Elektronisk handel för kommuner, landsting och stat. Anskaffning och installation; Handbok 2 Statskontorets Toppledarforum, 1996 ,Solna

EDI-avtal 96 - Projektet Elektronisk handel, Statskontorets Toppledarforum, 1997.

Rikspolisstyrelsen, red Ankarberg, Rapport angående elektronisk identifiering med elektroniskt identitetskort, 2000, Riksdagens förvaltningskontor.

EU

Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer 1999/93/EG

Kommissionen har sammanställt ett flertal dokument; http://www.ispo.cec.be/eif/policy/policy.html#directive
Gemenskapens förberedande rättsakter; Dokument 599PC0195

Lagstiftning

Lag (2000:832) om kvalificerade elektroniska signaturer
Lag (1992:1119) om teknisk kontroll
Lag(1977:981) om konsumentkredit
Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område

Artiklar

Aftonbladets IT-bilaga nr 10 28/5 2001, s 15

Ny Teknik 2001:5,Alpman Marie, Digitala signaturer på väg, s 17

Svenska Dagbladet, Digital kråka lyfter e-handeln, Precht Elisabeth, Svenska Dagbladets näringslivsdel, s 15,16/5 2000

Svensk Jurist Tidning, 3 2001, årgång 86, Josefsson Carl, Lagstiftning eller självreglering?, s 206-218

Sydsvenskan 21/ 2000 C2 Delen

Sydsvenskan 2000-04-05, Sundberg Ulf, Malmöföretag säkrar näthandeln, s A 23

Möten

Frukostmöte den 23/2 2001 hos www.zedir.se med tema elektroniska signaturer

Seminarium hos Svenska föreningen för adbj……. www.adbj.se den 1999-10-26, Elektroniska signaturer - en svensk standard? Stockholm

Personligt möte med Lars Sundström, Nexus AB, under våren 2000

Internetkällor

Cardholm Lucas, Prevas Informationsskrift, Att ge elektroniska dokument rättslig status, www.prevas.se, 2000-11-22

Computer Sweden nyhetsbrev 2000-02-21, Ricknäs Mickael, Succé för elektroniska id-kort i Finland

Computer Sweden nyhetsbrev, Åsblom Joel, E-signaturer snart i var mans hand, 2000-09-15

Computer Sweden nyhetsbrev**,** Remissyttrande Digitala Signaturer GEA… www.gea.nu ..dec 00-02-14

Computer Sweden nyhetsbrev 2000-12-04, Hultkvist Jesper, 25000 Teliaanställda får digitala signaturer.

Computer Sweden nyhetsbrev 2000-10-16, Sviden Henrik, FN harmoniserar lagar om digitala signaturer

Computer Sweden nyhetsbrev 1999-12-05, Lotsson Anders, EU och USA lagstiftar om e-signaturer.

Dataföreningen i Sverige www.kompetens.dfs.se/000321b/default.htm 00-03-20

E-sign Act raises the speed limit on the information highway, Cummings Matthew, www.findlaw.com, 2001-03-22

Nyhetsbrev GEA www.gea.nu/newsletter.htm 00-03-20

Nytt standardiseringsområde, Elektroniska signaturer, www.sis.se 2000-10-31

9 Rättsfallsförteckning

NJA 1976	s 667
NJA 1981	s 595
NJA 1992	s 263

Bilaga A

Lag (2000:832) om kvalificerade elektroniska signaturer

SFS-nummer:	2000:832
Ansvarig myndighet:	Näringsdepartementet
Ikraft:	2001-01-01 överg.best.
Förarbeten:	Prop. 1999/2000:117, bet. 2000/01:TU3, rskr. 2000/01:13, EGTL13/2000 s12
CELEX-nr:	31999L0093

Allmän bestämmelse

1 § Syftet med denna lag är att underlätta användningen av elektroniska signaturer, genom bestämmelser om säkra anordningar för signaturframställning, om kvalificerade certifikat för elektroniska signaturer och om utfärdande av sådana certifikat. Lagen gäller sådana certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat till allmänheten.

Definitioner

2 § I lagen avses med elektronisk signatur: data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används för att kontrollera att innehållet härrör från den som framstår som utställare och att det inte har förvanskats, avancerad elektronisk signatur: elektronisk signatur som a) är knuten uteslutande till en undertecknare, b) gör det möjligt att identifiera undertecknaren, c) är skapad med hjälpmedel som endast undertecknaren kontrollerar, och d) är knuten till andra elektroniska data på ett sådant sätt att förvanskningar av dessa data kan upptäckas, kvalificerad elektronisk signatur: avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning, undertecknare: fysisk person som behörigen innehar en anordning för signaturframställning, signaturframställningsdata: unika data, såsom koder eller hemliga krypteringsnycklar, som används för att skapa en elektronisk signatur, anordning för signaturframställning: maskin- eller programvara för användning av signaturframställningsdata, säker anordning för signaturframställning: anordning för signaturframställning som uppfyller kraven i 3 §, signaturverifieringsdata: data, såsom koder eller öppna krypteringsnycklar, som används för att verifiera en elektronisk signatur, certifikat: intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar dennes identitet, kvalificerat certifikat: certifikat som uppfyller kraven i 6 eller 7 §, certifikatutfärdare: den som

utfärdar certifikat eller som garanterar att någon annans certifikat uppfyller vissa krav.

Säkra anordningar för signaturframställning

3 § En anordning för signaturframställning som anges vara säker skall säkerställa att signaturen är tillfredsställande skyddad mot förfalskning. Anordningen skall även säkerställa att signaturframställningsdata 1. i praktiken kan förekomma endast en gång, 2. med rimlig säkerhet inte kan härledas, och 3. på ett tillfredsställande sätt kan skyddas av den behörige undertecknaren, så att andra inte kan komma åt eller använda dem. Anordningen får inte förändra de uppgifter som skall signeras elektroniskt eller hindra att de presenteras för undertecknaren före den elektroniska signeringen.

4 § Kraven i 3 § på en säker anordning för signaturframställning skall anses uppfyllda för sådan maskin- eller programvara som överensstämmer med sådana standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

5 § En anordning som anges vara en säker anordning för signaturframställning får släppas ut på marknaden eller användas för att skapa en kvalificerad elektronisk signatur endast om den uppfyller kraven i 3 §. En prövning av om kraven är uppfyllda skall göras av ett organ som anmälts för detta ändamål enligt lagen (1992:1119) om teknisk kontroll. Med en prövning enligt första stycket likställs en prövning av ett organ som anmälts för samma ändamål av en annan stat inom Europeiska ekonomiska samarbetsområdet.

Kvalificerade certifikat

6 § För att ett certifikat skall få kallas kvalificerat skall det vara utfärdat för viss tid av en certifikatutfärdare, som uppfyller kraven i 9-12 §§ och föreskrifter meddelade med stöd av 13 §, samt innehålla 1. uppgift om att det utfärdats som ett kvalificerat certifikat, 2. certifikatutfärdarens namn och adress samt uppgift om etableringsland, 3. undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym, 4. särskilda uppgifter om undertecknaren, om de är relevanta för ändamålet med certifikatet, 5. signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren vid tidpunkten för utfärdandet har kontroll över, 6. uppgift om certifikatets giltighetstid, 7. certifikatets identifieringskod, 8. certifikatutfärdarens avancerade elektroniska signatur eller en elektronisk signatur med motsvarande säkerhetsnivå, och 9. uppgift om eventuella begränsningar av certifikatets användningsområde eller av värdet på de transaktioner för vilka certifikatet kan användas (transaktionsbelopp). Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela närmare föreskrifter om krav enligt första stycket.

7 § Om ett certifikat som uppfyller kraven i 6 § första stycket 1-9 utfärdats av en certifikatutfärdare som inte är etablerad i Sverige skall certifikatet anses kvalificerat om 1. certifikatutfärdaren är etablerad i en annan stat inom Europeiska ekonomiska samarbetsområdet och där får utfärda kvalificerade certifikat, 2. certifikatutfärdaren uppfyller krav som motsvarar dem som anges i 9-12 §§ och föreskrifter meddelade med stöd av 13 § och är ackrediterad i en annan stat inom Europeiska ekonomiska samarbetsområdet, eller 3. certifikatet garanteras vara kvalificerat av en certifikatutfärdare som avses i 1 eller i 6 § första stycket.

Utfärdande av kvalificerade certifikat

8 § En certifikatutfärdare som avser att utfärda kvalificerade certifikat till allmänheten är skyldig att anmäla detta hos den myndighet som regeringen bestämmer (tillsynsmyndigheten) innan verksamheten påbörjas.

9 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall bedriva verksamheten tillförlitligt och 1. ha personal med tillräcklig kompetens och erfarenhet för verksamheten, särskilt vad avser ledning, teknik och säkerhetsrutiner, 2. använda sådana rutiner för administration och ledning som uppfyller erkända standarder, 3. använda pålitliga system och produkter som är skyddade mot ändringar och se till att teknisk och kryptografisk säkerhet upprätthålls, 4. förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten enligt denna lag och bära risken för skadeståndsskyldighet, 5. ha säkra rutiner för identitetskontroll av de undertecknare som kvalificerade certifikat utfärdas till, 6. förfoga över ett snabbt och säkert system för registrering och omedelbar återkallelse av kvalificerade certifikat, och 7. vidta åtgärder mot förfalskning av kvalificerade certifikat och i förekommande fall se till att framställandet av signaturframställningsdata sker konfidentiellt. Kraven i första stycket 3 skall anses uppfyllda för sådan maskin- eller programvara som överensstämmer med sådana standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

10 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall 1. omedelbart återkalla ett certifikat när undertecknaren begär det eller när det annars finns anledning till det, 2. säkerställa att exakt tidpunkt kan anges för utfärdande och återkallelse av certifikat, och 3. säkerställa att av utfärdaren framställda signaturframställningsdata och signaturverifieringsdata kan användas som komplement till varandra.

11 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall bevara all relevant information om certifikaten under den tid som är motiverad med hänsyn till typen av certifikat och övriga omständigheter. Certifikatutfärdaren skall även använda tillförlitliga system

för lagring av kvalificerade certifikat i verifierbar form, så att 1. endast behöriga personer kan göra tillägg och ändringar, 2. uppgifternas äkthet kan kontrolleras, 3. certifikaten är offentligt tillgängliga endast när innehavarna av certifikaten har lämnat sitt samtycke, och 4. tekniska förändringar som äventyrar säkerhetskraven framgår för den som handhar systemet. Certifikatutfärdaren får inte lagra eller kopiera signaturframställningsdata.

12 § Innan en certifikatutfärdare ingår avtal om att utfärda ett kvalificerat certifikat skall certifikatutfärdaren skriftligen och på ett lättbegripligt språk informera motparten om 1. begränsningar och andra villkor för användning av certifikatet, 2. frivillig ackreditering eller certifiering som avses i lagen (1992:1119) om teknisk kontroll, och 3. förfaranden för klagomål och avgörande av tvister. Informationen enligt första stycket får överföras elektroniskt. Informationen skall göras tillgänglig också för annan som är beroende av certifikatet och som begär att få den.

13 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får utfärda närmare bestämmelser om krav enligt 9-12 §§.

Skadestånd

14 § En certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade skall ersätta den skada som åsamkats den som förlitat sig på certifikatet, om skadan uppkommit genom att 1. certifikatutfärdaren inte har uppfyllt kraven i 10 §, 2. certifikatet inte uppfyller kraven i 6 § första stycket, eller 3. certifikatet vid utfärdandet innehöll felaktiga uppgifter. Certifikatutfärdaren är dock inte skyldig att betala ersättning om utfärdaren kan visa att skadan inte har orsakats av vårdslöshet hos utfärdaren själv. Certifikatutfärdaren är inte heller ersättningsskyldig för en skada som härrör från att ett kvalificerat certifikat använts i strid med begränsningar som gäller användningsområde eller transaktionsbelopp och som tydligt angivits i certifikatet. Vad som sägs i första stycket 2 och 3 samt i andra stycket gäller även en certifikatutfärdare som garanterar att en annan certifikatutfärdares certifikat är kvalificerade.

15 § Avtalsvillkor som i jämförelse med 14 § är till nackdel för den som förlitar sig på certifikatet är utan verkan mot denne.

Behandling av personuppgifter

16 § En certifikatutfärdare som utfärdar certifikat till allmänheten får inhämta personuppgifter endast direkt från den som uppgifterna avser eller med dennes uttryckliga samtycke och endast i den utsträckning som är nödvändig för att utfärda eller upprätthålla ett certifikat. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från den som uppgifterna avser.

Kvalificerade elektroniska signaturer

17 § Om det i lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande och om det är tillåtet att uppfylla kravet med elektroniska medel, skall en kvalificerad elektronisk signatur anses uppfylla kravet. Vid kommunikation med eller mellan myndigheter kan dock användningen av elektroniska signaturer vara förenad med ytterligare krav.

Tillsyn

18 § Tillsynsmyndigheten skall ha tillsyn över efterlevnaden av denna lag och föreskrifter som har utfärdats med stöd av lagen. Tillsynsmyndigheten skall föra och ge offentlighet åt en förteckning över certifikatutfärdare som anmält sig enligt 8 § och som enligt denna lag får utfärda kvalificerade certifikat.

19 § Tillsynsmyndigheten har rätt att på begäran få de upplysningar och ta del av de handlingar som behövs för tillsynen. Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som står under tillsyn bedrivs. Tillsynsmyndigheten har rätt att få biträde av kronofogdemyndigheten för tillsyn enligt första och andra styckena.

20 § Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av denna lag eller av föreskrifter som meddelats med stöd av lagen. Tillsynsmyndigheten får förelägga en certifikatutfärdare, som till allmänheten utfärdar certifikat som anges vara kvalificerade, att helt eller delvis upphöra med denna verksamhet, endast om mindre ingripande åtgärder visat sig vara verkningslösa. Myndigheten får besluta hur verksamheten skall avvecklas.

21 § Förelägganden och förbud enligt denna lag får förenas med vite.

Avgifter

22 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Överklagande

23 § Tillsynsmyndighetens beslut enligt denna lag eller enligt föreskrifter som meddelats med stöd av lagen får överklagas hos allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten. Tillsynsmyndigheten får bestämma att beslut enligt denna lag skall gälla omedelbart.

Övergångsbestämmelser 2000:832 1. Denna lag träder i kraft den 1 januari 2001. 2. Certifikatutfärdare som redan före ikraftträdandet utfärdar sådana certifikat som medför anmälningsplikt enligt 8 § behöver inte göra anmälan före den 1 februari 2001. 3. 15 § tillämpas inte i fråga om avtal som träffats före ikraftträdandet.

Bilaga B

399L0093
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
Official Journal L 013, 19/01/2000 p. 0012 - 0020

Text:
DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 13 December 1999
on a Community framework for electronic signatures

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,
Having regard to the proposal from the Commission (1),
Having regard to the opinion of the Economic and Social Committee (2),
Having regard to the opinion of the Committee of the Regions(3),
Acting in accordance with the procedure laid down in Article 251 of the Treaty(4),
Whereas:
(1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;
(2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communication - towards a European framework for digital signatures and encryption;
(3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;
(4) Electronic communication and commerce necessitate " electronic signatures" and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and

services in the internal market;
(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods(5) and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods(6);
(6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;
(7) The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;
(8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;
(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;
(10) The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;
(11) Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;

(12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;
(13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;
(14) It is important to strike a balance between consumer and business needs;
(15) Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;
(16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;
(17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;
(18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;
(19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;
(20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a

person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-written signatures are fulfilled;
(21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;
(22) Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;
(23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;
(24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;
(25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;
(26) The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission(7);
(27) Two years after its implementation the Commission will carry out a review of this Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;
(28) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective,
HAVE ADOPTED THIS DIRECTIVE:

Article 1
Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.
It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2
Definitions
For the purpose of this Directive:
1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. "advanced electronic signature" means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
3. "signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
4. "signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
5. "signature-creation device" means configured software or hardware used to implement the signature-creation data;
6. "secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III;
7. "signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
8. "signature-verification device" means configured software or hardware used to implement the signature-verification-data;
9. "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
10. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;
11. "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;
12. "electronic-signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-

service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;
13. "voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3
Market access
1. Member States shall not make the provision of certification services subject to prior authorisation.
2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons, which fall within the scope of this Directive.
3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.
4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated.
A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.
5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.
6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.
7. Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

Article 4
Internal market principles
1. Each Member State shall apply the national provisions, which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services, which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.
2. Member States shall ensure that electronic-signature products, which comply with this Directive, are permitted to circulate freely in the internal market.

Article 5
Legal effects of electronic signatures
1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
(b) are admissible as evidence in legal proceedings.
2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.

Article 6
Liability
1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;
unless the certification-service-provider proves that he has not acted

negligently.
2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.
3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.
4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.
The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.
5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts(8).

Article 7
International aspects
1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:
(a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
(b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or
(c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.
2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.
3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it

may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.
Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8
Data protection
1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and on the free movement of such data(9).
2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.
3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

Article 9
Committee
1. The Commission shall be assisted by an "Electronic-Signature Committee", hereinafter referred to as "the committee".
2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.
The period laid down in Article 4(3) of Decision 1999/468/EC shall be set at three months.
3. The Committee shall adopt its own rules of procedure.

Article 10
Tasks of the committee
The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

Article 11
Notification
1. Member States shall notify to the Commission and the other Member

States the following:
(a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);
(b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);
(c) the names and addresses of all accredited national certification service providers.
2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12
Review
1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.
2. The review shall inter alia assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

Article 13
Implementation
1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof.
When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.
2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Article 14
Entry into force
This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities

Article 15
Addressees
This Directive is addressed to the Member States.

Done at Brussels, 13 December 1999.

For the European Parliament
The President

N. FONTAINE

For the Council
The President
S. HASSI

ANNEX I

Requirements for qualified certificates
Qualified certificates must contain:
(a) an indication that the certificate is issued as a qualified certificate;
(b) the identification of the certification-service-provider and the State in which it is established;
(c) the name of the signatory or a pseudonym, which shall be identified as such;
(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
(e) signature-verification data which correspond to signature-creation data under the control of the signatory;
(f) an indication of the beginning and end of the period of validity of the certificate;
(g) the identity code of the certificate;
(h) the advanced electronic signature of the certification-service-provider issuing it;
(i) limitations on the scope of use of the certificate, if applicable; and
(j) limits on the value of transactions for which the certificate can be used, if applicable.

ANNEX II

Requirements for certification-service-providers issuing qualified certificates
Certification-service-providers must:
(a) demonstrate the reliability necessary for providing certification services;
(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and

correspond to recognised standards;
(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;
(l) use trustworthy systems to store certificates in a verifiable form so that:
- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

ANNEX III

Requirements for secure signature-creation devices
1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
(a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the

signature process.

ANNEX IV

Recommendations for secure signature verification
During the signature-verification process it should be ensured with reasonable certainty that:
(a) the data used for verifying the signature correspond to the data displayed to the verifier;
(b) the signature is reliably verified and the result of that verification is correctly displayed;
(c) the verifier can, as necessary, reliably establish the contents of the signed data;
(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
(e) the result of verification and the signatory's identity are correctly displayed;
(f) the use of a pseudonym is clearly indicated; and
(g) any security-relevant changes can be detected.

Bilaga C

SFS nr: 2000:833 Departement/ myndighet: Näringsdepartementet Rubrik: Förordning (2000:833) om kvalificerade elektroniska signaturer Utfärdad: 2000-11-02 - /Träder i kraft I:2001-01-01/ Tillämpningsområde 1 § Denna förordning gäller sådana kvalificerade certifikat och utfärdare av dessa som omfattas av lagen (2000:832) om kvalificerade elektroniska signaturer. Tillsyn 2 § Post- och telestyrelsen är tillsynsmyndighet enligt lagen (2000:832) om kvalificerade elektroniska signaturer. Bemyndiganden 3 § Post- och telestyrelsen får meddela närmare bestämmelser om krav på vad ett kvalificerat certifikat skall innehålla enligt 6 § lagen (2000:832) om kvalificerade elektroniska signaturer samt om sådana krav på en certifikatutfärdare som avses i 9-12 §§ samma lag. Post- och telestyrelsen får meddela de verkställighetsföreskrifter som behövs för frågor om anmälningsplikt och tillsyn enligt lagen om kvalificerade elektroniska signaturer.

Bilaga D

Ordlista[188]

Autenticering: En funktion som verifierar identitet.

CA: Certification Authority. Det organ som i ett system för asymmetrisk kryptering kan bekräfta vilken identitet som döljer sig bakom en viss nyckel och kan återkalla dessa nycklar.

Certifikat: Ett certifikat som används för att koppla ihop den privata nyckeln med den publika och kan intyga att nyckelinnehavarens identitet och att meddelandets innehåll är korrekt och oförändrat.

Data: Representation av fakta eller instruktioner i en form lämplig för överföring eller bearbetning.

Digital: Ett exakt värde som kan representeras med ett tal.

Digitalt dokument: En elektronisk handling med digital signatur.

Digital signatur: En teknisk metod för att kontrollera om en handlings innehåll kommer ifrån den fysiska person som framstår som utställare.

Elektroniskt dokument: En upptagning vars innehåll och utställare kan bekräftas genom ett tekniskt förfarande.

Handling: Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas.

Konfidentialitet: En egenskap hos data som inte är tillgänglig eller läsbar för obehöriga.

Kryptering: En teknisk process för att skydda data från insyn.

PIN: Personal Identification Number.

PKI: Public Key Infrastructure.

Standard: En allmänt antagen teknisk beskrivning som är utformat i samarbete mellan berörda parter.

Urkund: Protokoll, kontrakt eller annan handling.

[188] SOU 199:14, s 243-255