



JURIDISKA FAKULTETEN  
vid Lunds universitet

Caroline Brauner

# Elektroniska underskrifter i en digital agenda

LAGM01 Examensarbete

Examensarbete på juristprogrammet  
30 högskolepoäng

Handledare: Eva Lindell-Frantz

Termin för examen: Period 1 VT2015

# Innehåll

<b>SUMMARY</b>	<b>1</b>
<b>SAMMANFATTNING</b>	<b>2</b>
<b>FÖRORD</b>	<b>3</b>
<b>FÖRKORTNINGAR</b>	<b>4</b>
<b>1 INLEDNING</b>	<b>5</b>
1.1 Bakgrund	5
1.2 Syfte och frågeställningar	6
1.3 Avgränsningar	6
1.4 Metod och material	7
1.5 Disposition	9
1.6 Forskningsläge	10
1.7 Definitioner	10
<b>2 TEKNIKEN BAKOM ELEKTRONISKA UNDERSKRIFTER</b>	<b>15</b>
2.1 Inledning	15
2.2 Signeringens tillvägagångssätt	15
2.3 Kryptering	16
2.3.1 Syfte och funktion	16
2.3.2 Symmetrisk kryptering	17
2.3.3 Asymmetrisk kryptering	17
2.3.4 PKI	18
2.4 Certifikat	18
2.4.1 Certifikat – funktion och syfte	18
2.4.2 Certifikatutfärdare, CA	19
<b>3 REGLERING AV ELEKTRONISKA UNDERSKRIFTER</b>	<b>20</b>
3.1 Inledning	20
3.2 Nuvarande reglering	20
3.2.1 Signatordirektivet	20
3.2.1.1 Syfte och tillämpningsområde	20
3.2.1.2 Rättsverkan	20
3.2.1.3 Kvalificerade certifikat	21

3.2.1.4	Skadestånd	21
3.2.1.5	Krav på säkra anordningar för skapande av signaturer	22
3.2.1.6	Rekommendationer för säker signaturverifiering	22
3.2.2	Signaturlagen	23
3.2.2.1	Syfte och tillämpningsområde	23
3.2.2.2	Rättsverkan	24
3.2.2.3	Avancerade elektroniska signaturer	24
3.2.2.4	Kvalificerade elektroniska signaturer	24
3.2.2.5	Skadestånd	25
3.2.2.6	Säker anordning för signaturframställning	25
3.2.2.7	Kvalificerade certifikat	25
<b>3.3</b>	<b>EIDAS-förordningen</b>	<b>26</b>
3.3.1	Bakgrund	26
3.3.2	Syfte och tillämpningsområde	27
3.3.3	Allmänt om regleringen	28
3.3.4	Elektroniska underskrifter	29
3.3.4.1	Inledning	29
3.3.4.2	Rättsverkan	29
3.3.4.3	Skadestånd	30
3.3.4.4	Avancerad elektronisk underskrift	30
3.3.4.5	Kvalificerade certifikat	30
3.3.4.6	Anordningar för skapande av kvalificerade elektroniska underskrifter	31
3.3.4.7	Validering och bevarande av kvalificerade elektroniska underskrifter	32
3.3.5	Åsikter om eIDAS-förordningen	33
<b>3.4</b>	<b>Sammanfattande slutsatser</b>	<b>33</b>
<b>4</b>	<b>ELEKTRONISKA AVTALSSLUT</b>	<b>36</b>
4.1	Inledning	36
4.2	Avtalsformer	36
4.2.1	Konsensualavtal	36
4.2.2	Formalavtal	39
4.2.3	Realavtal	42
4.3	Elektroniska underskrifters relation till avtalsformerna	42
4.4	Sammanfattande slutsatser	45
<b>5</b>	<b>ELEKTRONISKA UNDERSKRIFTERS FUNKTION</b>	<b>47</b>
5.1	Inledning	47
5.2	Vilje- och varningsfunktion	47
5.3	Identifieringsfunktion	48
5.4	Äkthetsfunktion	48
5.5	Bevisfunktion	49
5.6	Sammanfattande slutsatser	51
<b>6</b>	<b>AVTALSRÄTTSLIGA PROBLEM I EN ELEKTRONISK</b>	

<b>KONTEXT</b>	<b>53</b>
6.1 Inledning	53
6.2 Elektronisk viljeförklaring	54
6.3 Acceptfrist	55
6.4 Förklaringsmisstag	57
6.5 Förvanskning	58
6.6 Återkallelse	59
6.7 Sammanfattande slutsatser	59
<b>7 RÄTTSEKONOMISKT PERSPEKTIV</b>	<b>62</b>
7.1 Inledning	62
7.2 Mikroekonomins idealmodell	62
7.2.1 Inledning	62
7.2.2 Individens och företags rationella val	62
7.2.3 Perfekt konkurrens	64
7.3 Hinder för idealmodellen	64
7.3.1 Transaktionskostnader	64
7.3.2 Monopol och bristfällig information	65
7.4 Sammanfattande slutsatser	66
<b>8 ANALYS</b>	<b>68</b>
8.1 Teknisk bakgrund till elektroniska underskrifter	68
8.2 Innebörden av EIDAS-förordningen för svensk rätt	68
8.3 Innebörden av elektroniska underskrifter för avtalsrätten	70
8.4 Elektroniska underskrifters funktioner jämfört med traditionella underskrifter	75
8.5 Rättsekonomiska effekter	77
8.6 Avslutande ord	78
<b>KÄLL- OCH LITTERATURFÖRTECKNING</b>	<b>79</b>
<b>RÄTTSFALLSFÖRTECKNING</b>	<b>84</b>

# Summary

The digital development in society and the new eIDAS regulation which is replacing the current eSignature directive and the Swedish law on electronic signatures through which the directive is implemented, raises the interest for electronic signatures and the possibilities these provide. In this context this essay aims to analyse the functions of electronic signatures and which impact the new regulation will have on the Swedish legal system.

Furthermore, the legal effect of electronic signatures will be examined and to which extent an electronic signature can fulfill the typical functions of physical signatures. Electronic communication and the possibility of concluding contracts electronically are essential conditions for electronic signatures. Therefore these matters and some related contractual problems will be touched upon. Finally, I will discuss effects of electronic signatures from the perspective of law and economics. The conclusions are the following: Electronic signatures are based on asymmetric encryption in the Public Key Infrastructure system (PKI). As regards legal effect, the eIDAS regulation mainly prescribes mutual recognition of qualified electronic signatures under certain provisions, and, further, that a qualified electronic signature may not be denied admissibility as evidence in legal proceedings under certain circumstances. It is also stipulated that national law may not impose higher requirements on electronic signatures than that they should be qualified. As is the case with the current legislation and EU directive, the regulation does not affect national or union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form. Since Swedish law does not contain formal requirements regarding conclusion of contract to any larger extent, and due to the Swedish principle of free sifting of evidence, the impact of the regulation from a Swedish perspective will be insignificant in this respect. However, the regulation also introduces new rules on mutual recognition of electronic identification and, in addition to electronic signatures, also other trusted services. Further, the legal position has been strengthened due to the direct effect of the regulation, but has also been clarified compared to the eSignature directive, increasing the legal certainty. Within contract law, electronic signatures may be applied provided that no formal requirement, such as a requirement of hand-written signature, exist. In such case, the general position is that the legislation in question must explicitly allow the use of electronic signatures in order for such to be valid as signatures. Electronic signatures can fulfill the typical functions of the traditional signatures, such as the function of showing will, a warning function, identification function, authenticity function and function as evidence. The use of electronic communication may sometimes give rise to contract law related problems which can be solved through different approaches which is essential since it is important not to slow down the digital development of society. From a law and economics point of view, the effects of electronic signatures are mainly reduced transaction costs and increased information.

# Sammanfattning

I takt med den digitala utvecklingen i samhället samt den nya eIDAS-förordningen som ersätter det tidigare signatordirektivet och signaturlagen genom vilket direktivet implementerades, väcks intresset för elektroniska underskrifter och de möjligheter dessa erbjuder. Mot en sådan bakgrund syftar denna uppsats till att utreda hur elektroniska underskrifter fungerar och vad den nya förordningen innebär för svensk rätt. Vidare utreds hur långt en elektronisk underskrifts rättsverkan sträcker sig och hur en elektronisk underskrift kan fylla den traditionella fysiska underskriftens typiska funktioner. Möjligheten att sluta avtal på elektronisk väg och elektronisk kommunikation utgör viktiga förutsättningar för elektroniska underskrifter som till viss del behandlas och viss avtalsrättslig problematik som kan uppstå i sammanhanget. Avslutningsvis redogörs för rättsekonomiska effekter som elektroniska underskrifter kan innebära. Slutsatserna är följande: Signeringen bygger på asymmetrisk kryptering i infrastrukturen för det öppna nyckelsystemet, PKI. EIDAS-förordningens reglering av elektroniska underskrifters rättsverkan och bevisverkan innebär i huvudsak krav på ömsesidigt erkännande av kvalificerade elektroniska underskrifter, att det i nationell rätt inte får ställas högre krav på elektroniska underskrifter än att de ska vara kvalificerade och att de under vissa förutsättningar inte får förvägras bevisverkan. Liksom tidigare regleras inte elektroniska underskrifters rättsverkan när det i nationell rätt föreligger formkrav. Då den svenska rättsordningen har få formkrav och tillämpar fri bevisvärderings- och bevisprövningsprinciper förblir effekten mindre avgörande i detta hänseende. Dock innebär förordningen andra nyheter i form av bestämmelser om ömsesidigt erkännande av e-legitimationer under vissa förutsättningar och utöver elektroniska underskrifter även andra s.k. betrodda tjänster. I övrigt har regleringen förstärkts genom förordningens direkta effekt samt förtydligats jämfört med signatordirektivet och därmed ökat rättssäkerheten. Inom avtalsrätten kan elektroniska underskrifter användas förutsatt att inget formkrav såsom på egenhändig underskrift föreligger då den allmänna uppfattningen är att det då uttryckligen måste tillåtas att elektroniska underskrifter kan uppfylla kravet. Elektroniska underskrifter kan vidare fylla den traditionella underskriftens typiska viljefunktion, varningsfunktion, identifieringsfunktion, äkthetsfunktion och bevisfunktion. Elektronisk kommunikation kan ibland ge upphov till avtalsrättslig problematik som kan lösas på olika sätt vilket är viktigt för att inte bromsa den digitala utvecklingen i samhället. De rättsekonomiska effekterna av elektroniska underskrifter är framförallt sänkta transaktionskostnader och motverkande av bristande information bland konsumenterna och näringsidkarna.

# Förord

Innan jag lämnar mina studieår bakom mig vill jag rikta ett stort tack till min handledare, Eva Lindell-Frantz, för all hjälp under arbetets gång. Stort tack även till Nils Fjelkegård på E-legitimationsnämnden för att han varit mig behjälplig med information om elektroniska underskrifter.

Jag vill också passa på att tacka min sambo, Mikael Gustafsson, för att han tagit sig tid till korrekturläsning och för att han varit mitt bollplank. Avslutningsvis vill jag även tacka min mamma för allt stöd hon gett mig genom åren.

Malmö, maj 2015

*Caroline Brauner*

# Förkortningar

AD	Arbetsdomstolen
AvtL	Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område
CA	Certificate Authority
CEN	European Committee for Standardization
Ds	Departementsserie
EDI	Electronic Data Interchange
EIDAS	Electronic identification and trusted services
EU	Europeiska unionen
FEUF	Fördraget om EU:s funktionssätt
HFL	Hyresförhandlingslagen (1978:304)
JB	Jordabalken (1970:994)
MBL	Lag (1976:580) om medbestämmande i arbetslivet
NJA	Nytt juridiskt arkiv
PKI	Public key infrastructure
PTS	Post- och Telestyrelsen
SKL	Statens kriminaltekniska laboratorium



# 1 Inledning

## 1.1 Bakgrund

I dagens IT-samhälle där tekniken ständigt utvecklas uppkommer ibland frågor kring juridikens förmåga till samspel med denna nya miljö. I en alltmer globaliserad värld sluts dagligen avtal på såväl nationell som internationell nivå. Med anledning härav väcks frågan huruvida bruket av den svenska avtalslagen från 1915 fungerar idag samt hur väl lagen är anpassad till det moderna samhället? AvtL uppställer inget krav på underskrift för att avtalet ska bli giltigt och även muntliga avtal får rättsverkan. En namnunderskrift kan dock få betydelse i bevishänseende och tydliggör parternas önskan om att ingå en bindande förpliktelse. Frågan om elektroniska underskrifters möjlighet att ge sådan rättsverkan aktualiseras t.ex. då ett företag slutit ett avtal med företag beläget på annan ort eller i ett annat land och avtalet ska signeras. Det är knappast effektivt eller ekonomiskt att t.ex. skicka avtalet fram och tillbaka per post för underskrift eller skicka dit anställda för att skriva under. Ett bättre alternativ i detta hänseende utgör då elektroniska underskrifter. Sådana underskrifter kan få betydelse även i flertalet andra avtalsrättsliga sammanhang inbegripet utöver företag även för privatpersoner och myndigheter. Samtidigt är det viktigt att säkerställa att elektroniska underskrifter är lika säkra som vanliga namnunderskrifter och bruket av elektroniska underskrifter väcker även andra frågor som t.ex. när vanlig underskrift krävs för bundenhet. Fler intressanta frågor är vilka former av avtal som kan träffas genom elektroniska underskrifter, hur elektroniska underskrifter förhåller sig till avtalslagen och hur elektroniska underskrifter kan fylla en vanlig namnunderskrifts funktioner.

År 1999 tillkom det s.k. signaturdirektivet<sup>1</sup> bl.a. för att främja bruket av elektroniska underskrifter på den inre marknaden genom en tydlig och enhetlig reglering inom EU. Direktivet syftade även till att bidra till ett rättsligt erkännande av sådana signaturer.<sup>2</sup> Signaturdirektivet implementerades i svensk rätt genom den s.k. signaturlagen<sup>3</sup>. År 2014 antogs eIDAS-förordningen<sup>4</sup> som ska ersätta signaturdirektivet i syfte att bl.a. åstadkomma en mer enhetlig reglering. Förordningen föreskriver en utökad reglering av elektroniska underskrifter och tillsyn.<sup>5</sup> Mot denna bakgrund är det av intresse att närmare undersöka den elektroniska underskriftens funktion och verkan i förhållande till svensk avtalsrätt och

---

<sup>1</sup> Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer, (nedan signaturdirektivet).

<sup>2</sup> Se t.ex. skälen till signaturdirektivet p. 4 samt art. 1 signaturdirektivet.

<sup>3</sup> Lagen (2000:832) om kvalificerade signaturer, (nedan signaturlagen).

<sup>4</sup> Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (nedan eIDAS-förordningen).

<sup>5</sup> Jfr regeringskansliets faktagromemoria 2011/12:FPM162, kap. 1.3 2 st.

vad den nya förordningen skulle innebära för svensk rätt om den blir antagen.

## 1.2 Syfte och frågeställningar

Syftet med uppsatsen är mot ovanstående bakgrund att redogöra för den nya förordningen beträffande elektroniska underskrifter i förhållande till svensk avtalsrätt genom följande frågeställning:

1. Hur fungerar en elektronisk underskrift rent tekniskt?
2. Vad innebär eIDAS-förordningen för svensk rätt, främst med avseende på elektroniska underskrifter och deras rättsverkan, kvalificerade certifikat, anordningar för skapande av elektroniska underskrifter samt validering och bevarande av elektroniska underskrifter?
3. Vad innebär en elektronisk underskrift avtalsrättsligt?
4. I vilka juridiska avseenden skiljer sig en elektronisk underskrift från en vanlig namnunderskrift? Frågan innebär en genomgång av hur den elektroniska underskriften kan uppfylla namnunderskriftens typiska funktioner. Även riskerna med elektroniska underskrifter behandlas i sammanhanget.
5. Vilka rättsekonomiska effekter innebär bruket av elektroniska underskrifter istället för vanlig namnunderskrift?

## 1.3 Avgränsningar

För att uppnå djup i uppsatsen kring mina frågeställningar blir vissa avgränsningar nödvändiga. Jag har som ovan nämnts valt att behandla eIDAS-förordningens innebörd för elektroniska underskrifter i svensk rätt, samt elektroniska underskrifters funktion i förhållande till svensk avtalsrätt inom ramen för denna uppsats. EIDAS-förordningen innebär bl.a. nyheter genom att den omfattar bestämmelser om identifiering och autentisering vilket jag av utrymmesskäl inte kommer att behandla närmare då fokus ligger primärt på elektroniska underskrifter. Likväl kommer dessa tekniska instrument att beröras i den mån det är relevant för mina frågeställningar och jag har även valt att ta med begreppen i definitionsdelen i kap 1.6 samt kap. 2 för att tydliggöra den tekniska bakgrunden till elektroniska underskrifter. Viss avtalsrättslig avgränsning har gjorts genom att jag beskriver teorier och primära avtalsrättsliga aspekter i förhållande till elektroniska underskrifter inom ramen för mina frågeställningar.

Ämnesvalet innebär att en bakgrundsbeskrivning avseende de tekniska förutsättningarna för en elektronisk signatur kan anses motiverad för att

bättre förstå elektroniska underskrifters funktion och verkan i olika avseenden. Den tekniska genomgången kommer dock att hållas på en grundläggande nivå eftersom mitt fokus ligger på de juridiska aspekterna.

Andra avgränsningar har gjorts beträffande arbetsrättsliga frågor, ansvarsfrågor, straffrättsliga frågor och processuella frågor som inte behandlas närmare även om dessa till viss del berörs inom ramen för mina frågeställningar. Ämnesvalet skulle kunna aktualisera flertalet andra rättsliga aspekter såsom associationsrättsliga, IP-rättsliga, immaterialrättsliga eller offentligrättsliga. Sådana aspekter kan tyvärr inte beröras av utrymmesskäl.

Vidare redogör jag endast för elektroniska underskrifter ur svenskt perspektiv då det saknas utrymme för ett komparativt inslag.

## 1.4 Metod och material

Den inledande delen av uppsatsen är deskriptiv och syftar till att redogöra för gällande rätt ur ett de lege lata-perspektiv. Metoden som används är klassisk rättsdogmatisk utifrån rättskällevärdet vilket innebär att jag använder mig främst av lag, förarbeten, praxis och doktrin. Då det inte finns någon omfattande praxis beträffande elektroniska underskrifter är jag i huvudsak hänvisad till övriga rättskällor. Jag har valt att dra en försiktig parallell till två rättsfall inom förvaltningsrätten i diskussionen om formkrav på egenhändig underskrift. Det är viktigt att notera att förmögenhetsrätten och förvaltningsrätten är två skilda rättsområden med bl.a. olika syften men de är likväl enligt min mening aktuella i diskussionen. Beträffande förarbeten använder jag mig främst av motiven till signaturlagen genom vilken signaturdirektivet implementerades. Således används dessa till att tolka bakomliggande syften med signaturlagen.

Eftersom jag behandlar unionsrätt i form av signaturdirektivet och eIDAS-förordningen måste även unionsrätten behandlas. EU:s omfattande regelverk delas huvudsakligen in i primärrätt och sekundärrätt. Primärrätten utgörs framförallt av de grundläggande fördragen som är unionsfördraget, funktionsfördraget och rättighetsstadgan. Sekundärrätten består av lagstiftning och den övriga rättsbildning som härleds ur den kompetens som EU-fördragen gett till institutioner såsom rådet och Europaparlamentet. Huvudtyperna inom lagstiftningen är förordningar, direktiv, och beslut. Förordningar är särskilt betydelsefulla då de är bindande och direkt gällande i alla medlemsländer inklusive Sverige enligt art. 288.2 FEUF. Således ska domstolar och myndigheter tillämpa förordningar som direkt gällande rätt och ska inte inkorporera eller transformera bestämmelserna i nationell rätt om inget annat gäller enligt förordningen. Även enskilda kan åberopa förordningar. Direktiv karaktäriseras bl.a. av att de riktar sig till medlemsstater och inte enskilda. Vidare föreskriver direktiv ett resultat som medlemsstater ska förverkliga inom ramen för nationell rättsordning. Direktiv implementeras eller införlivas i nationell rätt och medlemsstaterna får välja form eller tillvägagångssätt enligt art 288.3 FEUF. Unionsrätten

skiljer sig från den svenska rättsordningen bl.a. genom beaktandet av allmänna rättsprinciper i högre grad. Vissa av dessa är idag kodifierade och andra framgår av EU-domstolens praxis. Principerna intar en hög position och kan närmast räknas till primärrätten. En annan viktig skillnad är att unionsrätten saknar förarbeten och den viktigaste källan för tolkning av lagstiftning inom EU är istället den preambel/ingress som inleder förordningen eller direktivet där syftet anges (skälen). Vid tolkning av eIDAS-förordningen görs därför detta med hjälp av dess preambel.<sup>6</sup> Jag nämner utöver signaturdirektivet även det s.k. E-handelsdirektivet<sup>7</sup> i diskussionen om elektronisk handel då det är relevant för min frågeställning om möjligheten att sluta avtal på elektronisk väg, men direktivet behandlas i övrigt inte närmare.

Viss oklarhet råder i nuläget då signaturlagen kommer att upphävas och ny lagstiftning behövs i den mån förordningen lämnar utrymme åt nationell reglering. En utredning pågår för närvarande inom Näringsdepartementet vilket kommer att resultera i en departementspromemoria som sedan är tänkt att remissbehandlas och ligga till grund för ny lagstiftning.<sup>8</sup> Det kan konstateras att det ännu saknas visst material i detta hänseende. Åsikter om förordningen finns i viss utsträckning men inte på detaljnivå. Utöver detta använder jag mig av den doktrin som finns tillgänglig om elektroniska underskrifter.

Beträffande avtalsrätten finns det betydligt mer doktrin att tillgå där jag använder mig av välkända författare såsom Axel Adlercreutz, Kurt Grönfors, Bert Lehrberg, Christina<sup>9</sup> och Jan Ramberg.

Det kan också tilläggas att jag i viss utsträckning behandlar olika former av elektronisk kommunikation, elektroniska avtalsslut och elektroniska dokument. Skälet är att jag anser det vara av vikt att utreda även möjligheten att använda sådana tekniska hjälpmedel inom avtalsrätten då dessa utgör viktiga förutsättningar för elektroniska underskrifter.

I en senare del har jag anlagt ett kritiskt rättsekonomiskt perspektiv där jag jämför vilka effekter i detta avseende en elektronisk underskrift har jämfört med en vanlig namnteckning i samhället. Inom rättsekonomin betraktas juridiken från ett nationalekonomiskt perspektiv där alla handlingar i samhället tolkas i ekonomiska termer. Utgångspunkten är att alla handlingar utförs i syfte att hushålla med tillgångar på ett effektivt sätt. Rättens roll i samhällsekonomin är av särskilt intresse samt att utreda hur välbefinnande skapas och hur samhällets resurser bäst används för att bli så effektivt som möjligt.

---

<sup>6</sup> Bernitz, Ulf, Kjellgren, Anders, Europarättens grunder, fjärde upplagan, 27 ff., 38 ff. och 105 ff.

<sup>7</sup> Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (nedan e-handelsdirektivet)

<sup>8</sup> Kontakt med Post- och Telestyrelsen (nedan PTS). Post- och telestyrelsen är den myndighet som bevakar områdena elektronisk kommunikation och post i Sverige.

<sup>9</sup> Tidigare Hultmark.

Välstånd<sup>10</sup> anses uppkomma genom produktion av varor och tjänster samt frivilliga förändringar av äganderätten till dessa. T.ex. genom frivilligt köp av en vara ökar välståndet då tillfredställelsen hos parterna ökar. Eftersom det rör sig om ett frivilligt köp borde köparen vara mer tillfredsställd över att äga varan än de pengar som vederbörande ägde innan köpet medan säljaren är mer tillfredsställd av att äga pengarna än varan. Tillfredställelsen mäts inom ekonomisk teori i pengar varför båda parterna kan anses vara rikare efter den frivilliga transaktionen vilket medför att även samhällets välstånd ökat. Rättsregler om exempelvis rätt för säljaren till betalning och köparens rätt till hävning av köpet minskar osäkerheten i avtalslut med främlingar där det inte alltid finns ett intresse av att upprätthålla en god relation.<sup>11</sup>

I den avslutande delen används ett analytiskt synsätt där jag besvarar min frågeställning ur ett de lege ferenda-perspektiv i syfte att beskriva hur gällande rätt borde se ut utifrån effektivitet, rättssäkerhet m.m.

## 1.5 Disposition

I kapitel 1.7 har jag valt att inleda med en översiktlig redogörelse för olika tekniska och juridiska definitioner som, enligt min mening, är nödvändig inför den fortsatta framställningen och som med fördel kan användas som ordlista vid behov.

Kapitel 2 är främst teknisk där jag på en grundläggande nivå redogör för hur en elektronisk underskrift går till och för relevant teknisk information. Jag beskriver närmare flertalet av begreppen i kapitel 1.7 och vilken koppling de har till elektroniska underskrifter.

I kapitel 3 redogörs för signatordirektivet och signaturlagen samt den nya eIDAS-förordningen som ersätter föregående reglering. Syftet är att jämföra skillnaderna mellan dessa bestämmelser och vad eIDAS-förordningen innebär för svensk rätt inom ramen för mina frågeställningar. Vidare redogör jag för relevanta EU-rättsliga aspekter i sammanhanget och avslutar med sammanfattande slutsatser.

I kapitel 4 beskrivs elektroniska underskrifters förhållande till svensk avtalsrätt. Här tar jag upp de olika svenska avtalsformer som finns och hur elektroniska underskrifter förhåller sig till dessa och avslutningsvis redogör jag för mina sammanfattande slutsatser.

I kapitel 5 görs en genomgång av den traditionella namnunderskriftens typiska funktioner och hur en elektronisk underskrift kan uppfylla dessa följt av sammanfattande slutsatser.

---

<sup>10</sup> Inom rättsekonomi görs en åtskillnad mellan välstånd och välfärd. Välfärd mäter människans tillfredställelse i nyttoenheter istället för pengar. Se Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 78 ff.

<sup>11</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 9 ff.

I kapitel 6 redogörs för andra avtalsrättsliga aspekter i relation till elektronisk kommunikation såsom elektroniska underskrifter där vissa problem kan uppstå, t.ex. ifråga om avtalsmodellen anbud/accept, och relevanta avtalsrättsliga fel och ogiltighetsgrunder som exempelvis förklaringsmisstag, förvanskning m.m. Kapitlet avslutas med sammanfattande slutsatser.

I kapitel 7 behandlas elektroniska underskrifter ur ett rättsekonomiskt perspektiv utifrån grundläggande rättsekonomiska principer följt av elektronisk kommunikation med en eventuell elektronisk underskrifts effekter för samhället i sammanhanget och sist kommer sammanfattande slutsatser.

I kapitel 8 avslutar jag med en analys av rättsläget där jag besvarar min frågeställning och diskuterar hur rättsläget borde se ut.

## 1.6 Forskningsläge

Elektroniska underskrifter har till viss del behandlats i doktrin, framförallt av Christina Ramberg men på senare tid även av Jon Kihlman och medförfattarna till antologin om elektronisk signering. I sistnämnda verk behandlas dessa underskrifter inom flertalet rättsområden såsom arbetsrätt, straffrätt, associationsrätt, förvaltningsrätt m.m. I övrigt behandlas elektroniska underskrifter till viss del av Axel Adlercreutz och Kurt Grönfors.

## 1.7 Definitioner

För att bättre förstå kommande kapitel kan det vara fördelaktigt att få en översikt avseende tekniska och juridiska begrepp som används i uppsatsen. Flera av begreppen beskrivs även närmare i kapitel 3.

### **Elektronisk identifiering och autentisering**

Elektronisk identifiering innebär att bevisa sin identitet på elektronisk väg istället för att fysiskt identifiera sig genom legitimation eller annan ID-handling. Autentiseringen innebär en kontroll av den uppgivna identiteten exempelvis vid inloggning vid kommunikation mellan två system alternativt vid utväxling av meddelande mellan användare.<sup>12</sup>

Ett praktiskt exempel på elektronisk identifiering och autentisering är en rapport<sup>13</sup> av Post- och Telestyrelsen avseende en Internetbank innebär att användaren loggar in genom att uppges sin identitet då vederbörande skriver

---

<sup>12</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, 18 f.

<sup>13</sup> Hanno Lindbom, Kristina m.fl. rapport från Post- och Telestyrelsen från den 30 januari 2004, rapportnummer PTS:ER, s. 11 f.

in sitt användarnamn. Därefter autentiseras/verifieras identiteten genom exempelvis ett lösenord eller med nycklar kopplade till ett elektroniskt certifikat. Därefter är användaren inloggad och kan bruka bankens tjänster såsom att kontrollera konton eller föra över pengar.

ITS<sup>14</sup> har vid definitionen av identifieringsbegreppet påpekat att verifiering ibland inkluderas i begreppet och ibland inte.<sup>15</sup> Det kan därmed konstateras att begreppet identifiering och autentisering är snarlika och används på lite olika sätt. I denna uppsats används begreppet elektronisk identifiering som beteckning för att uppge sin identitet elektroniskt och autentisering innebär den process vari en verifiering av identiteten sker.

Då autentiseringen är något som kan vara unikt för olika individer måste även de data eller fakta som identifieringen grundas på vara unika.<sup>16</sup>

Metoden för autentiseringen bygger huvudsakligen på tre olika komponenter:

något användaren *har* såsom en säkerhetsdosa för bankaffärer på internet, något användaren *vet* såsom en PIN-kod tillhörande säkerhetsdosan och något användaren *är* vilket t.ex. kan utgöras av fingeravtryck.<sup>17</sup>

Ett något mer komplicerat exempel på något användaren *vet* kan vara lösenord som i sin tur kan vara statiska eller dynamiska<sup>18</sup>, något användaren *har* kan utgöras av ett smart kort<sup>19</sup> med privat nyckel och ett elektroniskt certifikat.<sup>20</sup> Sådant som användaren *är* innebär att den mänskliga kroppens unika egenskaper används för identifiering, exempelvis handens form, rösten, ögats iris, ansiktet och DNA analyseras i ett mikrochip vid fastställandet av identiteten.<sup>21</sup>

## Signering

---

<sup>14</sup> Informationstekniska standardiseringen är ett organ som utsetts av regeringen att ansvara för telekommunikationsområdet tillsammans med SEK svensk Elstandard (SEK) och Swedish Standards Institute (SIS).

<sup>15</sup> Se Post-och telestyrelsens delrapport: Användningen av elektronisk identifiering – Hur ser marknaden ut och vilka hinder är hindren mot en ökad användning, rapportnummer PTS-ER-2003:35, från den 19 september 2003, s. 7.

<sup>16</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, 18 f.

<sup>17</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, 18 f.

<sup>18</sup> Statika lösenord innebär kortfattat samma lösenord som används under längre tid och innebär svagare skydd än det dynamiska lösenordet som används under kortare perioder (oftast bara en gång) och utgörs t.ex. av dosor. Se vidare Hanno Lindbom, Kristina m.fl. rapport från Post- och Telestyrelsen från den 30 januari 2004, rapportnummer PTS:ER, s. 11 ff.

<sup>19</sup> Hanno Lindbom, Kristina m.fl. rapport från Post- och Telestyrelsen från den 30 januari 2004, rapportnummer PTS:ER, s. 11 f.

<sup>20</sup> Hanno Lindbom, Kristina m.fl. rapport från Post- och Telestyrelsen från den 30 januari 2004, rapportnummer PTS:ER, s. 11 f.

<sup>21</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 80 f.

En underskrift innebär att egenhändigt skriva under med sin namnteckning t.ex. för att intyga tillförlitlighet eller äkthet av ett dokument.<sup>22</sup>

### **Kryptering**

Begreppet kryptering innebär att överföra information till hemlig kod och bygger på en matematisk algoritm genom vilken en läsbar datamängd kan omvandlas till att bli oläsbar, s.k. kryptotext. Denna kryptotext kan sedan lagras eller översändas utan att obehöriga kan tillgodogöra sig innehållet. En behörig avsändare eller mottagare kan sedan omvandla kryptotexten förutsatt att denne har rätt nyckel. Grundläggande för alla krypteringsmetoder är att de bygger på en eller flera hemligheter och det är mycket viktigt att nyckeln förblir hemlig genom att inte hamna i fel händer eller på ett enkelt sätt kan räknas ut.<sup>23</sup>

### **Öppna system och PKI**

Öppna system är operativsystem eller program som kännetecknas bl.a. av att de bygger på allmänt kända/öppna standarder och därför förväntas fungera ihop – vara interoperabla.<sup>24</sup> PKI, Public Key infrastructure, utgör kortfattat infrastrukturen för öppna system där de mest centrala funktionerna är certifiering - skapande av certifikat, verifiering – kontroll av certifikat samt revokering – återtagande av certifikat. Viktigast är regelverket kring verksamheten i olika organisationer som utför funktioner i enlighet med PKI:s regelverk.<sup>25</sup> Se närmare om PKI och öppna system i kap. 2.3.4 och 3.2.2.

### **Digital signatur**

Digitala signaturer är användbara inom flertalet områden inkluderat t.ex. elektroniska underskrifter och metoder för nätverkssäkerhet. Även tekniken med två sammanhörande nycklar som används till identifikation, kryptering och signering inkluderas i begreppet digital signatur.<sup>26</sup>

### **Elektronisk signatur/underskrift**

Elektroniska signaturer/underskrifter skiljer sig från de digitala genom att mer fokusera på att ge en digital eller icke-manuell signatur samma värde som en vanlig namnunderskrift i bläck, m.a.o. en digital ersättning för juridiskt bindande namnteckning på kontrakt eller annan avtalshandling.<sup>27</sup>

I art. 3.10 eIDAS-förordningen definieras begreppet elektronisk underskrift:

---

<sup>22</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, 19.

<sup>23</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, 20.

<sup>24</sup> Computer Sweden, ordlista under öppna system.

<sup>25</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 34 f.

<sup>26</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 19.

<sup>27</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, 19.



*”uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.”*

Då EU har förordat begreppet ”elektroniska signaturer” för att särskilja detta juridiska begrepp från det tekniska begreppet ”digital signatur” som beskriver en teknik kan elektroniska signaturer/underskrifter sägas ha ett mer vidsträckt fokus. I eIDAS-förordningen kallas elektroniska signaturer istället ”elektronisk underskrift” och är det begrepp som används i denna uppsats med undantag för hänvisningar till begrepp såsom ”avancerad elektronisk signatur” eller ”kvalificerad elektronisk signatur” i signatordirektivet och signaturlagen.

### **Avancerade och kvalificerade elektroniska underskrifter**

Elektroniska underskrifter ska uppfylla vissa krav vilka huvudsakligen syftar till att säkerställa att identifiera avsändaren av den elektroniskt överförda informationen och att informationen inte förändrats.<sup>28</sup> Kriterierna för avancerade elektroniska underskrifter och kvalificerade elektroniska underskrifter behandlas närmare i kap. 3.

### **Elektronisk stämpel**

En elektronisk stämpel definieras i art. 3 eIDAS-förordningen som:

*”uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form för att säkerställa den senares ursprung och integritet”.*

Elektroniska stämplat används av juridiska personer och regleras på samma sätt som elektroniska underskrifter i avsnitt 5 art. 35-40 och kraven på kvalificerade certifikat för elektroniska stämplat regleras i bilaga III.

### **Certifikat och CA**

Som anges i art. 3.14 eIDAS-förordningen är certifikat:

*”ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk underskrift till en fysisk person och bekräftar åtminstone namn eller pseudonym på den personen”.*

Certifikat utfärdas av en CA, Certificate Authority, och utgör ett bevis på en koppling mellan ett nyckelpar och en person, ett företag eller datorsystem. Då certifikat alltid är tidsbegränsade och därmed upphör att gälla efter viss tid bör användaren därefter byta ut nycklarna och certifiera ett nytt nyckelpar.<sup>29</sup> Man skiljer på hårda certifikat där den privata nyckeln lagras permanent i ett smartkort<sup>30</sup> och mjuka certifikat där nyckeln förvaras i datorminne på hårddisk.<sup>31</sup> En CA är en tredje part som ansvarar för

---

<sup>28</sup> Sjöberg Magnusson, Cecilia, ”Lag om kvalificerade elektroniska signaturer – Ny lag men fortsatt behov av åtgärder”, s. 866. I: *Juridisk Tidskrift* Nr. 4 2000/01 s. 864 ff.

<sup>29</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 34.

<sup>30</sup> Plastkort i kontokortsformat med inbyggd processor och minne som kan användas t.ex. som ID-handling eller kontokort. Kan utföra funktioner som kryptering. Definition hämtad från Computer Sweden, ordlista under smartkort.

<sup>31</sup> Computer Sweden, ordlista under mjukt certifikat.

certifikatet och bl.a. säkrar identiteten hos nyckelinnehavaren. Se vidare kap. 2.

### **Kvalificerat certifikat**

I regleringen<sup>32</sup> av elektroniska underskrifter görs skillnad på enkla elektroniska underskrifter, avancerade elektroniska underskrifter som uppfyller vissa krav och kvalificerade elektroniska underskrifter som bl.a. är baserade på kvalificerade certifikat. För kvalificerat certifikat uppställs flertalet krav på såväl utfärdare som certifikat. Fördelen med ett kvalificerat certifikat är bl.a. att det bygger på ett avancerat och tryggt system vilket för ett företag kan ha ett kommersiellt värde.<sup>33</sup> PTS utövar tillsyn över certifikatutfärdare som framställer kvalificerade certifikat åt allmänheten enligt 8 § signaturlagen.

### **E-legitimation**

En E-legitimation är en elektronisk identitetshandling i form av en programvara som innehåller en privat och en publik krypteringsnyckel och ett elektroniskt certifikat som identifierar innehavaren. PKI-systemet medför att fler än två parter kan använda tekniken. I Sverige är leverantörerna Handelsbanken, Swedbank, Nordea samt Telia Sonera Sverige AB vilka är avtalsparter i det ramavtal som staten slutit för att få tillgång till e-legitimation åt medborgarna. Ingen myndighet utövar tillsyn över e-legitimationer som är avancerade underskrifter. PTS har endast tillsynsansvar över kvalificerade underskrifter som är något mer komplicerade och säkra tekniska lösningar. Utöver detta har nio banker ett samarbete genom erbjudandet av en gemensam teknisk lösning kallad BankID vilket ägs och utvecklas av det bankägda bolaget Finansiell ID-Teknik AB.<sup>34</sup>

---

<sup>32</sup> Regleringen av elektroniska underskrifter behandlas i kap. 3.

<sup>33</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 78.

<sup>34</sup> Se vidare E-legitimation – en underutnyttjad resurs, RiR 2009:19, s. 19 ff. samt kap. 2.

# 2 Tekniken bakom elektroniska underskrifter

## 2.1 Inledning

I denna del görs en teknisk genomgång för att ge en översiktlig bild av hur en elektronisk underskrift fungerar. Syftet med en elektronisk underskrift är bl.a. att möjliggöra för en avsändare av information att signera så att en läsare kan se varifrån dokumentet härstammar. Avsändaren kan vara en dator, programvara eller en juridisk alternativt fysisk person. Grundstenarna i signeringen utgörs av identifiering, signering och kryptering och plattformen för tekniken bakom signaturen är PKI – Public Key Infrastructure.<sup>35</sup> Nedan utvecklas dessa begrepp mer utförligt.

## 2.2 Signeringens tillvägagångssätt

Signeringen sker av en datamängd som kan bestå i text, ljud bild eller information i annan form. Processen inleds med att datamängden förbehandlas med ett s.k. hashvärde vilket liknar ett slags fingeravtryck av datamängden. Hashvärdet är inte omvändbart vilket innebär att datamängden inte kan beräknas utifrån hashvärdet. Nu kan informationen eventuellt krypteras<sup>36</sup>, vilket dock inte är nödvändigt varför det är viktigt att särskilja begreppet ”signering” från ”kryptering”.<sup>37</sup> Nedan beskrivs hur en elektronisk signering med kryptering går till:<sup>38</sup>

1. Avsändaren beräknar en kontrollsumma. Detta sker genom en programvara som med en känd formel räknar fram kontrollsumman. Metoden kan liknas vid den som används vid beräkningen av sista siffran i ett personnummer som framräknats av de nio första.
2. Avsändaren krypterar kontrollsumman med en privat nyckel. Krypteringen görs av avsändarens privata och hemliga nyckel genom att kontrollsumman och krypterad information bifogas originalinformationen som inte krypterats. Bilagan utgör den digitala signaturen.
3. Information om signaturen publiceras innebärande att informationen och signaturen distribueras, exempelvis genom e-post eller på en blankett.

---

<sup>35</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 52.

<sup>36</sup> Se mer om kryptering i kap. 1.7 samt nedan.

<sup>37</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 44 f.

<sup>38</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 45.

4. Mottagaren dekrypterar bilagan med kontrollsumman genom att använda avsändarens publika nyckel. Då informationen dekrypteras av mottagaren får denne fram en ny kontrollsumma.
5. Mottagaren beräknar en ny kontrollsumma. Beräkningen sker på samma sätt som i punkt 1, d.v.s. genom den formel som avsändaren använde för att mottagaren ska kunna beräkna en ny kontrollsumma.
6. Kontrollsummorna jämförs. I detta skede jämförs den nya kontrollsumman med den kontrollsumma som mottagaren fick fram genom dekryptering av bilagan som mottogs jämte informationen. Stämmer dessa två värden överens kan mottagaren vara säker på att det är rätt avsändare (givet att man kan lita på den använda nyckeln och vet vem utfärdaren av nyckeln är) och att informationen inte ändrats.

Verifiering av underskriften är viktig och sker genom att mottagaren separerar meddelandet från underskriften. För att bearbeta meddelandet använder mottagaren samma hashfunktion som avsändaren använde för underskriften.<sup>39</sup>

## 2.3 Kryptering

### 2.3.1 Syfte och funktion

Problematiken kring hemlighållandet av viss information är knappast något nytt fenomen även om metoderna för hemlighållandet förändrats över tiden. Under 1900-talet då två världskrig, det ”kalla kriget” samt ett växande industrispionage härjade drevs utvecklingen av kryptografi framåt i ett rasande tempo. När informationen inom IT-området bröts ned till digitala signaler blev krypteringstekniken ett naturligt sätt att skydda den elektroniska informationen. Idag används tekniken främst till två saker, *konfidentialitet* genom att skydda viss information såsom ett dokument från insyn samt *dataintegritet* innebärande säkerställandet att innehållet i en datamängd inte rubbats eller förändrats. Syftet med krypteringen är m.a.o. att under bestämda och kontrollerade former manipulera information för att ingen obehörig ska kunna ta del av informationen när den sänds eller lagras.<sup>40</sup>

Kryptotekniken baseras på att ett meddelandes innehåll omvandlas genom en på förhand bestämd metod, en algoritm. Metoderna kan variera. Vid kommunikation mellan två parter måste båda känna till algoritmen och varianten. Varianten måste hemlighållas till skillnad från algoritmen. Det finns två slags krypteringsalgoritmer: symmetriska och assymetriska.<sup>41</sup>

---

<sup>39</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 46.

<sup>40</sup> Halvarsson och Morin, Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering, s. 46 f.

<sup>41</sup> Ds 1998:14 s. 18.

## 2.3.2 Symmetrisk kryptering

Symmetrisk kryptering är den äldsta och mest beprövade krypteringstekniken och bygger på att avsändaren och mottagaren vid kryptering eller dekryptering använder samma gemensamma nyckel. Eftersom samma nyckel används är det nödvändigt att denna hemlighålls för utomstående för att ingen obehörig ska kunna kryptera eller dekryptera den aktuella datamängden i ett meddelande. Av denna anledning kallas systemet ibland även en-nyckelsystem eller hemlig-nyckelsystem. En fördel med symmetrisk kryptering är att den är beprövad samt att krypteringsalgoritmerna kan göras mindre komplexa vilket även innebär att denna krypteringsteknik är snabbare. Samtidigt utgör nyckelhanteringen en stor nackdel då mottagaren ska få vetskap om den hemliga nyckeln utan att även en obehörig får det.<sup>42</sup>

## 2.3.3 Asymmetrisk kryptering

Den asymmetriska krypteringsmetoden används i öppna system såsom på Internet och bl.a. för elektroniska underskrifter.<sup>43</sup> Vid denna relativt nya krypteringsteknik används två olika nycklar för kryptering och dekryptering. Nyckelparet består av en privat och hemlig nyckel samt en publik och öppen nyckel. Assymetrisk kryptering präglas av två viktiga omständigheter: a) ett krypterat meddelande kan inte dekrypteras med samma nyckel i nyckelparet och b) trots kunskap om den ena nyckeln är det omöjligt att räkna ut den andra nyckeln i nyckelparet. Nycklarna är beroende av varandra och bildar ett unikt par. En fördel med krypteringstekniken är att den avsevärt förenklar nyckeladministrationen samt gör den säkrare. Medan den privata nyckeln hålls hemlig för andra än ägaren görs den öppna nyckeln tillgänglig för omvärlden. På så vis blir metoden säkrare och nyckeldistributionen snabbare. Vid krypteringen kan avsändaren använda den privata eller öppna nyckeln. För att meddelandeöverföringen ska bli konfidentiell ska användaren vid kryptering använda mottagarens lättillgängliga öppna nyckel och den som har tillgång till mottagarens privata nyckel är den enda som kan dekryptera meddelandet.

Används istället en privat nyckel för kryptering av avsändaren kan omvärlden dekryptera meddelandet med avsändarens öppna nyckel. Framstår meddelandet som riktigt efter dekrypteringen utgör det bevis för att meddelandet verkligen har krypterats med avsändarens privata nyckel. Funktionen är densamma vid bruket av digitala signaturer där avsändaren använder sin privata nyckel och mottagaren verifierar med motsvarande publik nyckel. En nackdel med asymmetrisk kryptering är att algoritmerna är mycket komplexa och kräver mycket processorkraft vid beräkningen vilket medför att det tar relativt lång tid vid krypteringen. I praktiken används därför ofta en kombination där den symmetriska nyckeln krypteras

---

<sup>42</sup> Ds 1998:14 s. 18 f.

<sup>43</sup> Computer Sweden, ordlista under asymmetrisk kryptering.

med en asymmetrisk algoritm. Därefter kan nyckeln som på ett säkert sätt överförs användas till att dekryptera aktuell datamängd som ska utbytas.<sup>44</sup>

## 2.3.4 PKI

PKI, även kallat ”det öppna nyckelsystemet”, utgör infrastrukturen för öppna nycklar. Systemet anses möjliggöra ett säkert och ekonomiskt rimligt sätt att använda tjänster som utnyttjar öppna nycklar såsom elektroniska underskrifter mellan större grupper, enskilda, företag och myndigheter. Det finns ingen klar definition av begreppet PKI men kännetecknande för funktionen är framför allt utfärdande av certifikat. Vidare ska innehavaren av certifikatet kunna begära hos utfärdaren att certifikatet ska spärras vilket exempelvis kan bero på att den privata nyckeln kommit bort av olika skäl, t.ex. kan det vara fråga om ett stulet elektroniskt id-kort. En annan funktion är tillhandahållande av statusinformation för certifikat genom spärrlistor eller statuskontroll on-line som är avgörande för en elektronisk underskrifts tilltro. En definition av ett certifikatformat behövs för att de samverkande parterna ska kunna kommunicera och t.ex. verifiera elektroniska underskrifter.<sup>45</sup>

## 2.4 Certifikat

### 2.4.1 Certifikat – funktion och syfte

Certifikatet utgör ett intyg av att en viss person verkligen är ägaren till ett aktuellt nyckelpar. Genom att sammanbinda den personliga identiteten med den öppna nyckeln och den tillhörande privata nyckeln styrker certifikatet att en elektronisk identitetshandling eller e-legitimation är korrekt och giltig.<sup>46</sup> Certifikatet kan innehålla olika datamängder och se ut på olika sätt. Minimikravet är dock att det ska framgå: a) vem innehavaren av certifikatet är, b) innehavarens öppna nyckel, c) vem som utgivit certifikatet, samt d) giltighetstiden för certifikatet. Det bör även finnas uppgift om vilken policy<sup>47</sup> för utgivning som följts i certifikatet.<sup>48</sup>

Användare av elektroniska underskrifter i ett öppet nyckelsystem, såsom på Internet, känner ofta inte sin motpart. Certifikatet innebär en möjlighet för parterna att från en betrodd part inhämta information om varandras signaturverifieringsdata (öppna nyckel).<sup>49</sup>

En åtskillnad görs mellan hårda och mjuka certifikat beroende på den fysiska bäraren av den privata nyckeln. Gemensamt för båda

---

<sup>44</sup> Ds 1998:14 s. 19 f.

<sup>45</sup> Prop. 1999/2000:117 s. 22.

<sup>46</sup> Ds 1998:14 s. 25, jfr Computer Sweden, ordlista under certifikat.

<sup>47</sup> I regelverket för certifikatutgivning, Certification Practise Statement – CPS, framgår reglering på detaljnivå rörande framställande, utgivning och spärrning av certifikat.

<sup>48</sup> Ds 1998:14 s. 25.

<sup>49</sup> Prop. 1999/2000:117 s. 1 och 21.

certifikattyperna är bruket av en PIN-kod eller lösenord för åtkomst till nyckeln. Hårda certifikat innebär att den privata nyckeln lagras på ett smart kort genom vilket processen med autentisering och signering sker. Då exponeringen av nyckeln minskar, och därmed även risken för att förlora nyckeln anses denna metod säkrare än mjuka certifikat. Samtidigt medför hårda certifikat högre kostnader i form av kortläsare och programvara samt underhåll av denna.<sup>50</sup>

Vid bruk av mjuka certifikat används istället hårddisk vilket förutsätter att programvara, nycklar och certifikat installeras på datorn. Ofta är det dock tillräckligt med webbläsare eller e-postklient som har inbyggt stöd för signering, autentisering och kryptering. Fördelen med mjuka certifikat är att de är billigare än hårda certifikat. Nackdelen är att säkerheten anses mindre med mjuka certifikat då nyckeln lagras på datorn vilket ökar risken för att obehöriga genom dataintrång får tag på nyckeln. Mjuka certifikat minskar vidare flexibiliteten genom behovet av att installera certifikatet och nyckeln i datorn vilket minskar möjligheten till bruk av certifikatet från olika platser.<sup>51</sup>

## 2.4.2 Certifikatutfärdare, CA

En CA utfärdar elektroniska certifikat som utgör signerad information angående någons identitet, roll eller annat förhållande. Under certifikatens giltighetstid är det CA:n som ansvarar för certifikatens status genom att bl.a. publicera spärinformation för indraget certifikat. En CA är garant för certifikaten under den policy dessa utfärdats och fungerar som en operatör med ansvar för kontinuerlig drift av nödvändiga system för det dagliga bruket. Ansvaret innebär att användare vid behov ska kunna verifiera identiteter, underskrifter och hämta krypteringsnycklar. Verksamheten för en CA kan se ut på olika sätt och kan förekomma inom ett företag eller organisation alternativt hålla sina tjänster allmänt tillgängliga.<sup>52</sup>

Utfärdare av kvalificerade certifikat<sup>53</sup> ska enligt 8 § signaturlagen anmäla detta till tillsynsmyndigheten, PTS.<sup>54</sup> Efterfrågan på sådana certifikat har inte varit särskilt stor i Sverige, istället används främst e-legitimationer<sup>55</sup> som ansetts tillräckligt säkra. Kommersiella villkor, säkerhetskrav och andra krav avseende E-legitimationer regleras civilrättsligt genom ramavtal och Kammarkollegiet är ramavtalsansvariga. CA för e-legitimationer är banker och Telia.<sup>56</sup>

---

<sup>50</sup> Hanno, Kristina m.fl. rapport från PTS från den 30 januari 2004, rapportnummer PTS:ER, s. 16, jfr Ds 1998:14 s. 25 f.

<sup>51</sup> Hanno, Kristina m.fl. rapport från PTS från den 30 januari 2004, rapportnummer PTS:ER, s. 16.

<sup>52</sup> Ds 1998:14 s. 39.

<sup>53</sup> För definition av begreppet kvalificerat certifikat se kap. 1.7 definitioner och kap. 3.

<sup>54</sup> Dessa är idag SignGuard Europe AB, Försäkringskassan samt Comfact AB. Se Post- och Telestyrelsens hemsida.

<sup>55</sup> För definition av begreppet e-legitimation se kapitel 1.7 definitioner samt kapitel 2.

<sup>56</sup> Kontakt med PTS och E-legitimationsnämnden.

# 3 Reglering av elektroniska underskrifter

## 3.1 Inledning

I detta kapitel redogörs kortfattat för den nuvarande regleringen beträffande elektroniska underskrifter. Denna reglering utgörs för tillfället av signatordirektivet samt signaturlagen. Eftersom signatordirektivet, som upphör att gälla fr.o.m. 16 juli 2016<sup>57</sup>, och signaturlagen, som kommer att upphävas, ersätts av eIDAS-förordningen har förordningen störst utrymme. En genomgång av nuvarande reglering är dock nödvändig för att kunna jämföra denna reglering med den nya.

## 3.2 Nuvarande reglering

### 3.2.1 Signatordirektivet

#### 3.2.1.1 Syfte och tillämpningsområde

Signatordirektivet, som antogs 30 november 1999, syftade enligt art. 1 till att underlätta bruket av elektroniska underskrifter samt att bidra till det rättsliga erkännandet av dessa. Detta skulle uppnås genom fastställandet av ett rättsligt ramverk för elektroniska underskrifter och aktuella certifikattjänster för säkerställandet av en väl fungerande inre marknad. Det anges vidare att från signatordirektivets tillämpningsområde är undantaget frågor om ingående eller giltighet av avtal eller andra rättsliga förpliktelser när den nationella lagstiftningen eller gemenskapslagstiftningen föreskriver vissa formkrav. Likaså undantas bestämmelser och begränsningar i nationell lagstiftning eller gemenskapslagstiftning som reglerar användningen av dokument. Signatordirektivet omfattar endast öppna system.<sup>58</sup>

#### 3.2.1.2 Rättsverkan

En central bestämmelse i signatordirektivet är art. 5 som reglerar elektroniska underskrifters rättsverkan och bevisverkan. Bestämmelsen innebär en skyldighet för medlemsstaterna att säkerställa att vissa elektroniska underskrifter uppfyller de rättsliga kraven på en underskrift i förhållande till uppgifter i elektronisk form som en handskreven underskrift har i förhållande till uppgifter på papper och dessutom godtas som bevis i rättsliga förfaranden. Sådana elektroniska underskrifter utgörs av avancerade elektroniska signaturer, som baserats på kvalificerade certifikat

---

<sup>57</sup> Vissa artiklar börjar dock gälla vid andra tidpunkter, se art. 52 eIDAS-förordningen.

<sup>58</sup> Se preambel 10 samt art. 2.7 signatordirektivet. Se definition av öppna system i kap. 1.7 samt kap. 3.2.2.1.



och har skapats av en säker anordning för skapande av signaturer,<sup>59</sup> Beträffande övriga elektroniska underskrifter anges vidare att dessa enligt art. 5 inte får förvägras rätts- eller bevisverkan vid rättsliga förfaranden enbart pga. att de är i elektronisk form. Inte heller får sådan verkan nekas dessa underskrifter bara för att de inte är baserade på ett kvalificerat certifikat alternativt inte baserat på kvalificerat certifikat utfärdat av en ackrediterad tillhandahållare av certifikattjänster. Skälet får vidare inte för sådan förvägran enbart vara för att de inte är skapade av en säker anordning för signaturer.

### 3.2.1.3 Kvalificerade certifikat

Av definitionen av kvalificerade certifikat i art. 2 signaturdirektivet framgår att för att ett certifikat ska anses vara kvalificerat måste för det första certifikatet uppfylla de i bilaga I till signaturdirektivet angivna kraven på kvalificerade certifikats innehåll. Kraven innebär att det av innehållet i kvalificerade certifikat ska framgå att certifikatet utfärdats som kvalificerat certifikat, vem som tillhandahåller certifikattjänsten samt i vilken stat denne är etablerad, certifikatets giltighetstid, eventuella begränsningar i certifikatets användningsområde eller transaktionsvärde m.m.<sup>60</sup>

För det andra krävs även att tillhandahållaren av certifikatet uppfyller kraven i bilaga II till direktivet. Dessa krav innebär bl.a. att tillhandahållaren ska visa att denne är tillräckligt pålitlig för tillhandahållandet av certifikattjänsten, använda säkra och pålitliga system och produkter som är skyddade mot ändringar m.m.<sup>61</sup>

### 3.2.1.4 Skadestånd

En annan central bestämmelse är art. 6 signaturdirektivet som reglerar en undre gräns för skadeståndsansvar. Denna regel omfattar dels, tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat, dels sådana som garanterar att andras certifikat är kvalificerade. Medlemsstaterna är skyldiga att säkerställa att sådana tillhandahållare ansvarar för skador som drabbar ett organ, fysisk person eller juridisk person som haft rimlig anledning att förlita sig på certifikatet. Ansvaret omfattar skador till följd av fel eller brister i informationen som certifikatet innehåller. Vidare omfattas också skador till följd av att den i certifikatet angivna undertecknaren vid tidpunkten för utfärdandet inte var i besittning av de uppgifter för skapandet av en underskrift som påstås. Slutligen omfattas detta ansvar även av skador uppkomna genom att uppgifter för signaturskapande respektive signaturverifiering inte överensstämmer och att ett återkallande av ett certifikat inte registrerats. Presumtionen kan brytas av tillhandahållaren ifall denne kan visa att denne inte handlat försumligt innebärande att tillhandahållaren undgår skadeståndsansvar. Ifall certifikatet

---

<sup>59</sup> För definition av begreppen avancerade elektroniska signaturer, kvalificerade certifikat enligt eIDAS-förordningen se kap. 1.7 definitioner, jfr art. 2 signaturdirektivet.

<sup>60</sup> Se vidare bilaga I till signaturdirektivet.

<sup>61</sup> Se vidare bilaga II signaturdirektivet.

använts i strid mot i certifikatet angivna begränsningar av certifikatets tillämpningsområde eller tillåtna transaktionsvärde ansvarar inte heller tillhandahållaren förutsatt att begränsningarna varit identifierbara för tredje man.

### **3.2.1.5 Krav på säkra anordningar för skapande av signaturer**

I bilaga III anges minimikrav på säkra anordningar för skapande av signaturer. Där framgår bl.a. att anordningarna genom lämpliga tekniker och förfaranden ska säkerställa att uppgifterna för skapandet av underskriften i praktiken<sup>62</sup> endast kan förekomma en gång<sup>63</sup> och att sekretessen för dessa uppgifter är säkerställd inom rimliga gränser. Vidare anges att uppgifterna inte med rimlig garanti ska kunna härledas<sup>64</sup> och att underskriften ska vara skyddad genom för närvarande tillgängliga teknik. Uppgifterna ska vidare kunna skyddas på ett tillförlitligt sätt så att inte obehöriga kan komma åt dem. Till sist anges att anordningarna inte får förändra uppgifterna som ska signeras eller hindra att dessa uppgifter presenteras för undertecknaren före undertecknandet.<sup>65</sup>

### **3.2.1.6 Rekommendationer för säker signaturverifiering**

I bilaga IV till signaturdirektivet anges rekommendationer för säker signaturverifiering<sup>66</sup> innebärande att signaturverifieringsprocessen med rimlig säkerhet garanterar att de uppgifter som används för signaturverifieringen visas korrekt för den som utför verifieringen, att kontroll av underskriften sker på tillförlitligt sätt och att resultatet av verifieringen anges korrekt. Vidare anges att den som utför verifieringen på tillförlitligt sätt ska kunna fastställa innehållet i signerade uppgifter när behov föreligger, att en kontroll av det begärda certifikatets autenticitet och giltighet då signaturverifiering utförs ska ske på tillfredställande sätt samt att resultatet av kontrollen och undertecknarens identitet anges korrekt. Slutligen anges att eventuellt bruk av pseudonym anges på tydligt sätt samt att samtliga förändringar som är av betydelse för säkerheten är möjliga att upptäcka.<sup>67</sup>

---

<sup>62</sup> Uttrycket ”i praktiken” tolkas i svensk rätt som att risken att signaturframställningsdata förekommer mer än en gång ska vara ”försvinnande liten”. Se prop. 1999/2000:117 s. 47 och 70 f.

<sup>63</sup> Uttrycket ”förekomma endast en gång” tolkas i svensk rätt som att två personer inte får tilldelas samma hemliga nyckel i ett PKI-system. Se Furberg, Per, lagkommentaren till 3 § signaturlagen, hämtad från Karnov den 25 maj 2015.

<sup>64</sup> Att signaturframställningsdata ”inte kan härledas” tolkas i svensk rätt något förenklat som att det inte ska gå att lista ut vilken hemlig nyckel en person har genom att ”knäcka” skyddet. Se Furberg, Per, lagkommentaren till 3 § signaturlagen. Hämtad från Karnov den 25 maj 2015.

<sup>65</sup> Se bilaga III signaturdirektivet.

<sup>66</sup> För definition av begreppet verifiering se kap. 1.7 definitioner och kap. 2.

<sup>67</sup> Se bilaga IV signaturdirektivet.

## 3.2.2 Signaturlagen

### 3.2.2.1 Syfte och tillämpningsområde

Signaturlagen bygger på signaturdirektivet och syftar enligt lagens 1 § till att underlätta bruket av elektroniska underskrifter genom bestämmelser om säkra anordningar för signaturframställning, om kvalificerade certifikat för elektroniska underskrifter och om utfärdande av sådana certifikat. Vidare framgår att lagen enbart omfattar certifikatutfärdare som är etablerade inom Sverige och som utfärdar kvalificerade certifikat till allmänheten.<sup>68</sup> Detta innebär att endast certifikatutfärdare som tillhandahåller certifikat i öppna nyckelsystem (PKI) omfattas av lagen. Viss osäkerhet har rått kring när ett system anses vara öppet respektive slutet. Av förarbetena framgår dock att en rimlig huvudregel borde vara att certifikatet ska anses vara utfärdat åt allmänheten då kommunikation med andra än utfärdaren föreligger, d.v.s. med en tredje part med vilken det inte finns avtalsförhållande gentemot certifikatutfärdaren. Ett tydligt exempel på ett slutet system är bankernas Internettjänster där det på förhand finns ett civilrättsligt avtal mellan banken och kunden och det endast är banken som ska förlita sig på certifikatet. Ett annat exempel är certifikat som utfärdats för att enbart användas inom ett visst företag eller organisation.<sup>69</sup> I situationer där mottagaren måste förlita sig på en underskrift eller ett certifikat utanför ett civilrättsligt avtalsförhållande är det istället fråga om öppna system. Dessa system tillåter i princip att alla kan bli certifikatutfärdare, undertecknare eller mottagare utan att på förhand ingå avtal med en annan part inom systemet.<sup>70</sup> Ett exempel på ett öppet system är elektroniska ID-kort.<sup>71</sup>

Lagen omfattar inte heller frågor kring ingående eller giltighet av avtal.

En särställning ges åt elektroniska underskrifter med viss säkerhetsnivå, s.k. kvalificerade elektroniska signaturer vilka definieras i 2 § signaturlagen (Se nedan). Dock har det påpekats att lagen kommit att handla mer om kvalificerade certifikat för elektroniska underskrifter och krav på de som utfärdar dessa än elektroniska underskrifter i sig.<sup>72</sup> Förarbetena till signaturlagen fokuserar, till skillnad från signaturdirektivet, mindre på elektroniska underskrifters bevisverkan eftersom vi i Sverige har fri bevisprövning och bevisvärdering.<sup>73</sup>

---

<sup>68</sup> Jfr dock 16 § signaturlagen om inhämtning av personuppgifter som även omfattar andra certifikatutfärdare. Jfr Prop. 1999/2000:117 s. 54 och 77.

<sup>69</sup> Prop. 1999/2000:117 s. 35 f.

<sup>70</sup> Benjamin, Yousefi, Framställning och bevarande av elektroniska signaturer, Riksarkivets rapport, s. 63.

<sup>71</sup> Prop. 1999/2000:117 s. 36.

<sup>72</sup> Prop. 1999/2000:117 s. 33 f, jfr Furberg, Per, lagkommentaren till 1 § signaturlagen.

Hämtad från Karnov den 25 maj 2015.

<sup>73</sup> Jfr prop. 1999/2000:117 s. 17 ff.

### 3.2.2.2 Rättsverkan

Art. 5.1.a signaturdirektivet som handlar om krav på elektroniska underskrifters rättsverkan, har av utredarna till signaturlagen inte tolkats som ett krav på att elektroniska underskrifter *alltid* måste accepteras när det i nationell rätt eller gemenskapsrätt uppställs krav på en underskrift. Däremot anses bestämmelsen innebära att när det i nationell rätt föreligger ett sådant krav genom lag eller annan författning alternativt genom tolkning av formkravsregler, och lagen eller författningen ifråga tillåter elektroniska rutiner att uppfylla ett sådant krav *överhuvudtaget*, måste även kvalificerade signaturer godtas. På så vis bedöms den inre marknaden gynnas genom att en standard för elektroniska underskrifter skapas. Därför infördes 17 § signaturlagen.<sup>74</sup>

I 17 § signaturlagen anges att om det i lag eller annan författning ställs krav på egenhändig underteckning eller motsvarande<sup>75</sup> och om det är tillåtet att uppfylla kravet med elektroniska medel ska kvalificerade elektroniska underskrifter anses uppfylla kravet. Detta innebär att i de fall där en lag föreskriver krav på underskrift, och elektroniska medel uttryckligen eller genom tolkning tillåts att uppfylla kravet, ska en kvalificerad elektronisk underskrift godtas. Elektroniska underskrifter med lägre säkerhet, såsom t.ex. avancerade elektroniska underskrifter, kan utan hinder av denna bestämmelse godtas. Dock får högre krav än de som ställs på kvalificerade elektroniska signaturer inte ställas.<sup>76</sup>

### 3.2.2.3 Avancerade elektroniska signaturer

Enligt 2 § signaturlagen är en elektronisk signatur avancerad ifall följande rekvisit är uppfyllda: a) den är knuten uteslutande till en undertecknare, b) gör det möjligt att identifiera undertecknaren, c) är skapad med medel som endast undertecknaren kontrollerar samt d) är knuten till andra elektroniska data på ett sådant sätt att förvanskningar av dessa data kan upptäckas.

Begreppet elektronisk signatur skiljer sig i 2 § signaturlagen från definitionen i art. 2.1 signaturdirektivet genom att begreppet ”data” används istället för ”uppgifter”. Motiveringen är att det rör sig mer om konstellationer av ett och nollor än uppgifter kopplade till information som ska förstås av så många som möjligt.<sup>77</sup>

### 3.2.2.4 Kvalificerade elektroniska signaturer

En kvalificerad signatur utgörs enligt 2 § signaturlagen av en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och skapad av en säker anordning för signaturframställning.

<sup>74</sup> Prop. 1999/2000:117 s. 57 f.

<sup>75</sup> Uttrycket ”krav på egenhändig underskrift eller motsvarande” anses innefatta även elektroniska underskrifter. Se prop. 1999/2000 s. 78.

<sup>76</sup> Prop. 1999/2000:117 s. 58 f. och 77 f., se även Furberg, Per, lagkommentaren till 17 § signaturlagen. Hämtad från Karnov den 25 maj 2015.

<sup>77</sup> Prop. 1999/2000:117 s. 38 f.

### 3.2.2.5 Skadestånd

Art. 6 signatordirektivet implementerades genom 14 § signaturlagen som i huvudsak innebär ett skadeståndsrättsligt ansvar för den som utfärdar kvalificerade certifikat till allmänheten gentemot den som förlitar sig på certifikatet. För att omfattas av regeln måste alltså bl.a. utfärdaren ange certifikatet som kvalificerat eller garantera att annans certifikat är kvalificerat. 15 § signaturlagen anger att regeln är tvingande till förmån för den som förlitar sig på certifikatet. För de fall som inte omfattas av specialregeln gäller allmänna skadeståndsrättsliga regler.<sup>78</sup>

### 3.2.2.6 Säker anordning för signaturframställning

I 3-5 §§ signaturlagen regleras säkra anordningar för signaturframställning som enligt lagens 3 § ska säkerställa att en elektronisk underskrift är skyddad mot förfalskning på ett tillfredställande sätt där kraven på anordningarna anges vilka bygger på signatordirektivets bilaga III.<sup>79</sup> 4 § anger de standarder som ska gälla och det är Europeiska organisationen för standardisering, CEN<sup>80</sup>, som utarbetar dessa standarder.<sup>81</sup> Obligatorisk kontroll av anordningar som angivits vara säkra (certifiering) regleras i 5 §. Sedan en lagändring som trädde i kraft 1 augusti 2011 är det Styrelsen för ackreditering och teknisk kontroll (Swedac) som utser organ som ska anmälas till EU för sådana uppgifter.<sup>82</sup>

### 3.2.2.7 Kvalificerade certifikat

Kvalificerade certifikat, som anses ha en högre säkerhetsnivå än andra certifikat, regleras i 6-7 §§ signaturlagen. Kraven som anges i bestämmelserna för sådana certifikat grundar sig på signatordirektivets i bilaga I uppställda krav. För att ett certifikat ska anses vara kvalificerat ska det enligt lagens 6 § vara utfärdat för viss tid vilket har sin grund i att tekniken på området utvecklas kontinuerligt. Certifikatet ska vidare vara utfärdat av en certifikatutfärdare som uppfyller de i 9-12 §§ signaturlagen uppställda kraven och föreskrifter som meddelats i enlighet med 13 § signaturlagen. Vidare anges krav på certifikatets innehåll som bygger på de ovannämnda kraven i bilaga I signatordirektivet.<sup>83</sup>

---

<sup>78</sup> Prop. 1999/2000:117 s. 51 ff. och 75 ff.

<sup>79</sup> Prop. 1999/2000:117 s. 47.

<sup>80</sup> European Committee for Standardization.

<sup>81</sup> Se Furberg, Per, lagkommentaren till 4 § signaturlagen. Hämtad från Karnov den 25 maj 2015.

<sup>82</sup> Prop. 2010/11:80 s. 98. I 5 § signaturlagen görs numera en hänvisning till Lagen (2011:791) om ackreditering och teknisk kontroll.

<sup>83</sup> Prop. 1999/2000:117, s. 41 f.

## 3.3 EIDAS-förordningen

### 3.3.1 Bakgrund

Mot bakgrund av den finansiella krisen presenterades strategin *Europa 2020*<sup>84</sup> av kommissionen i mars år 2010 i syfte att ta Europa ur krisen och förbereda EU:s ekonomi för nästa årtionde. I kommissionens meddelande *En digital agenda för Europa*<sup>85</sup>, som utgör ett av sju huvudinitiativ inom Europa 2020-strategin, identifieras befintliga hinder mot den digitala utvecklingen för Europa. Ett förslag i meddelandet är en lagstiftning om elektroniska underskrifter (nyckelåtgärd 3) och om ömsesidigt erkännande av elektronisk identifiering samt elektronisk autentisering (nyckelåtgärd 16) som fastställer ett tydligt regelverk för att undanröja fragmentering och brist på interoperabilitet<sup>86</sup>, främja det digitala medborgarskapet och förebygga IT-brottslighet. I *Inre marknadsakten*<sup>87</sup> utgör också lagstiftning om säkerställandet av ömsesidigt erkännande av elektronisk identifiering och elektronisk autentisering inom hela EU samt en översyn av signaturdirektivet en nyckelåtgärd för förverkligandet av den digitala inre marknaden. Även i *En färdplan för stabilitet och tillväxt*<sup>88</sup> framhålls vikten av en framtida gemensam rättslig ram för gränsöverskridande ömsesidigt erkännande och godtagande av elektronisk identifiering och elektronisk autentisering för utvecklingen av den digitala ekonomin.

Kommissionen bedrev bl.a. ett omfattande samråd med flertalet parter beträffande översyn av nuvarande elektroniska underskrifter och undersökningar avseende elektronisk identifiering, elektronisk autentisering, elektroniska underskrifter och närliggande betrodda tjänster. Av resultatet framkom en efterfrågan på ett förbättrat regelverk för att kunna bemöta de utmaningar som den nya teknikens snabba utveckling och den ökande globaliseringen innebär utan att regelverkets tekniska neutralitet frångås. En sådan lagstiftning bedömdes av kommissionen bidra till rättssäkerhet, säkerhet samt ett ökat förtroende för gränsöverskridande transaktioner och i förlängningen en minskning i marknadens fragmentering. En förordning, som enligt art. 288 FEUF är direkt tillämplig, ansågs vara det bästa instrumentet för att minska denna fragmentering och för att skapa förutsättningar för en ökad rättssäkerhet. Vidare bedömde kommissionen mot ovanstående bakgrund att förslaget är förenligt med subsidiaritets- och proportionalitetsprincipen. Resultatet blev eIDAS-förordningen som

---

<sup>84</sup> Europa 2020 - en strategi för smart och hållbar tillväxt för alla, KOM (2010) 2020.

<sup>85</sup> KOM (2010) 245.

<sup>86</sup> Interoperabilitet innebär två eller flera systems förmåga att utbyta information eller använda utbytt information, t.ex. är Macintosh och PC interoperabla i vissa avseenden. Definitionen hämtad från Computer Swedens ordlista, under interoperabilitet.

<sup>87</sup> KOM (2011) 206 slutlig.

<sup>88</sup> KOM (2011) 669 slutlig.

grundar sig på art. 114 FEUF som gäller antagandet av bestämmelser som avser att undanröja hinder för den inre marknadens funktion.<sup>89</sup>

### 3.3.2 Syfte och tillämpningsområde

I art. 1 eIDAS-förordningen anges att syftet med förordningen är att säkerställa en väl fungerande inre marknad och att uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster<sup>90</sup>.

Även i preambeln till eIDAS-förordningen framgår skäl för eIDAS-förordningen.<sup>91</sup> Ett uppbyggande av förtroendet för nätmiljön utpekas som en avgörande faktor för den ekonomiska och sociala utvecklingen mot bakgrund av brist på förtroende, särskilt p.g.a. upplevd bristande rättssäkerhet bland konsumenter, företag och offentliga myndigheter innebärande en tveksamhet hos dessa att utföra elektroniska transaktioner och att använda nya tjänster. Vidare anges att eIDAS-förordningen syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom tillhandahållandet av en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter. På så vis önskas en ökning i effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel inom EU.

Ett annat syfte med eIDAS-förordningen som framgår av preambeln<sup>92</sup> till eIDAS-förordningen är bl.a. att förstärka regelverket i signaturdirektivet. Direktivet, som enbart gäller elektroniska underskrifter och exempelvis inte andra betrodda tjänster och inte heller bestämmelser om eID-system, saknar enligt preambeln till förordningen ett heltäckande gräns- och sektorsöverskridande regelverk för säkra, pålitliga och lättanvända elektroniska transaktioner. I preambel 7 eIDAS-förordningen görs en hänvisning till Europaparlamentets resolution av den 21 september 2010 om fullbordandet av den inre marknaden för e-handel<sup>93</sup> där vikten av elektroniska säkerhetstjänster, särskilt elektroniska underskrifter, betonas. Flertalet bestämmelser genomförs genom genomförandebestämmelser av kommissionen angående bl.a. standarder där tas hänsyn till sådana standarder och tekniska specifikationer som redan utarbetats av framförallt standardiseringsorganen CEN, Etsi, ISO och ITU.<sup>94</sup> Vidare uttrycks ett behov av att skapa en infrastruktur för kryptering med öppen nyckel (PKI) och en uppmaning till kommissionen att inrätta en europeisk nätverksport för valideringsmyndigheter i syfte att garantera gränsöverskridande

---

<sup>89</sup> Förslag till Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, KOM (2012) 238 slutlig (nedan KOM 2012 238 slutlig).

<sup>90</sup> I art. 3.16 eIDAS-förordningen definieras betrodda tjänster som en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och består bl.a. av skapande, kontroll, validering och bevarande av elektroniska underskrifter, jfr art. 3.16 eIDAS-förordningen.

<sup>91</sup> eIDAS-förordningen preambel 1-3.

<sup>92</sup> eIDAS-förordningen preambel 3.

<sup>93</sup> Europaparlamentets resolution av den 21 september 2010 om fullbordandet av den inre marknaden för e-handel, EUT C 50 E, 21.2.2012. s. 1.

<sup>94</sup> Se bl.a. art. 29-34 samt preambel 72 eIDAS-förordningen.

interoperabilitet för elektroniska underskrifter och öka säkerheten i samband med transaktioner som görs via Internet.

I art. 2 eIDAS-förordningen anges tillämpningsområdet för förordningen som omfattar system för elektronisk identifiering som en medlemsstat har anmält samt tillhandahållare av betrodda tjänster etablerade inom EU. En avgränsning har gjorts gentemot tillhandahållare av betrodda tjänster inom enbart slutna system. Liksom signaturdirektivet, påverkar inte heller förordningen nationell eller unionsrätt avseende ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter beträffande formkrav.

### 3.3.3 Allmänt om regleringen

Den första delen av förordningen behandlar elektronisk identifiering och bygger på ömsesidigt erkännande av nationella elektroniska eID-system som notifierats till kommissionen. En bestämmelse av central betydelse här är art. 6 som i korthet innebär en skyldighet för medlemsstater att erkänna andra medlemsstaters eID-system (dvs. e-legitimationer) under vissa förutsättningar. Detta kan komma att innebära att e-legitimationer måste erkännas i gränsöverskridande sammanhang, ifall dessa bedöms uppfylla de i förordningen uppställda kraven på bl.a. att autentisering av e-legitimationen är gratis för en förlitande part i annat medlemsland, att medlemsstaten tar på sig skadeståndsansvaret för att e-legitimationen utfärdats till rätt person och krav på incidentrapportering.<sup>95</sup>

Den andra delen behandlar betrodda tjänster och innefattar utöver elektroniska underskrifter och stämplor bl.a. tidsstämplingstjänster som regleras i art. 41-42. Art. 41 och innebär bl.a. att dessas rättsverkan regleras på samma sätt som elektroniska underskrifter och en presumtion om att kvalificerade elektroniska tidsstämplor är korrekta. Kraven på kvalificerade tidsstämplor anges i art. 42. En annan betrodd tjänst är autentisering av webbplatser för vilka kvalificerade certifikat regleras i art. 45 och kraven på kvalificerade certifikat för sådan autentisering som genomförs genom genomförandeakter uppställs i bilaga IV och elektroniska dokument som regleras i art. 46 där det anges att dessa inte får förvägras rättsverkan eller bevisverkan enbart pga. av dess elektroniska form.

För att bl.a. öka förtroendet bland konsumenter och små eller medelstora företag gentemot den inre marknaden samt öka användandet av betrodda tjänster har begrepp som t.ex. kvalificerade underskrifter och kvalificerad tillhandahållare av elektroniska underskrifter införts i förordningen som ska ha en högre säkerhetsnivå genom tydliga föreskrifter.<sup>96</sup> De tämligen omfattande kraven på kvalificerade tillhandahållare av betrodda tjänster

---

<sup>95</sup> Se t.ex. art 7, art. 10 och art 11 eIDAS-förordningen.

<sup>96</sup> Se eIDAS-förordningen preambel 28.



regleras i art. 24 och säkerhetskrav på både kvalificerade och icke-kvalificerade tillhandahållare anges i art. 19.

Medlemsstaterna ska enligt art. 17 utse tillsynsorgan som ska följa flertalet krav om tillsyn, vilket bl.a. är krav på tillsyn över kvalificerade tillhandahållare av betrodda tjänster enligt art. 20 och att de som avser att starta tillhandahållande av betrodda tjänster ska anmäla detta till tillsynsmyndigheten enligt art. 21. Medlemsstaterna ska vidare upprätta och offentliggöra en förteckning över betrodda kvalificerade tjänsteleverantörer enligt art. 22 och ett särskilt EU-förtroendemärke ska enligt art. 23 inrättas som dessa betrodda tjänsteleverantörer kan använda sig av för att på ett tydligt och igenkännligt sätt visa de tjänster som erbjuds.

Mot bakgrund av frågeställningarna i denna uppsats behandlas nedan mer ingående de mest relevanta bestämmelserna kring elektroniska underskrifter som behandlas i eIDAS-förordningens andra del.

### **3.3.4 Elektroniska underskrifter**

#### **3.3.4.1 Inledning**

I avsnitt 4 art. 25-34 eIDAS-förordningen regleras elektroniska underskrifter. Nedan redogörs för centrala bestämmelser inom ramen för den här uppsatsen. Beträffande elektroniska stämplat<sup>97</sup> regleras dessa i avsnitt 5 art. 35-40 genom bestämmelser som huvudsakligen är likalydande som de för elektroniska underskrifter. Detsamma gäller för uppställda krav på kvalificerat certifikat för elektroniska stämplat i bilaga III jämfört med de för elektroniska underskrifter i bilaga I eIDAS-förordningen.<sup>98</sup>

#### **3.3.4.2 Rättsverkan**

Underskrifternas rättsverkan regleras i art. 25 eIDAS-förordningen där det stadgas att elektroniska underskrifter inte får förvägras rättslig verkan eller giltighet som bevis i rättsliga förfaranden enbart p.g.a. dess elektroniska form eller för att de inte uppfyller kraven för kvalificerade elektroniska underskrifter. För att förtydliga och utvidga art. 5 signaturdirektivets bestämmelse om elektroniska underskrifters rättsverkan anges vidare uttryckligen att kvalificerade elektroniska underskrifter ska ha motsvarande rättsverkan som handskrivna underskrifter.<sup>99</sup> Kvalificerade underskrifter, d.v.s. avancerade underskrifter som är baserade på kvalificerat certifikat och skapade av en kvalificerad anordning för underskriftframställning, som utfärdats i en medlemsstat ska dessutom godkännas som kvalificerade underskrifter i alla andra medlemsstater. Den närmare regleringen kring elektroniska underskrifters rättsverkan får definieras enligt nationell rätt

---

<sup>97</sup> För definition av elektroniska stämplat se kap. 1.7 definitioner.

<sup>98</sup> Läs vidare avsnitt 5 art. 35-40, avsnitt 4 art. 29-31 samt bilaga III eIDAS-förordningen.

<sup>99</sup> KOM (2012) 238 slutlig.

med undantag för nyssnämnda reglering kring kvalificerade elektroniska underskrifter.<sup>100</sup>

### **3.3.4.3 Skadestånd**

I art. 13 eIDAS-förordningen regleras ett skadeståndsansvar för tillhandahållare av betrodda tjänster som avsiktligt eller genom oaktsamhet underlåtit att uppfylla kraven i förordningen. Bevisbördan för avsikt eller oaktsamhet hos icke-kvalificerade tillhandahållare av betrodda tjänster åligger den fysiska eller juridiska person som påstår att sådan skada föreligger. Rör det sig istället om en kvalificerad tillhandahållare av tjänsterna är det istället denne som har att visa att sådan skada inte uppkommit avsiktligt eller genom dennes oaktsamhet. Har skadan uppkommit genom att tjänsten använts i strid med begränsningar som tillhandahållaren vederbörligen i förväg informerat sina kunder om undgår tillhandahållare av betrodda tjänster skadeståndsansvar förutsatt att tredje man haft möjlighet att ta del av begränsningarna. Vidare anges att bestämmelsen ska tillämpas i enlighet med nationell rätt.

### **3.3.4.4 Avancerad elektronisk underskrift**

I art. 26 eIDAS-förordningen anges förutsättningarna för att en elektronisk underskrift ska anses vara avancerad. Kraven innebär att a) underskriften ska vara unikt knuten till en undertecknare, b) undertecknaren ska kunna identifieras genom den, c) underskriften ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll samt att d) den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifter kan upptäckas.

### **3.3.4.5 Kvalificerade certifikat**

För att certifikat ska anses vara kvalificerade ska enligt art. 28 eIDAS-förordningen kraven i bilaga I eIDAS-förordningen på kvalificerade certifikat för elektroniska underskrifter vara uppfyllda. Även här är tanken att förtydliga kraven i jämförelse med den tidigare regleringen samt upphäva sådana bestämmelser som inte fungerade i praktiken såsom begränsningar av transaktionsvärden.<sup>101</sup>

Minimikraven i bilaga I inriktar sig på certifikatens innehåll och innebär att certifikatet ska innehålla uppgift, i en form lämplig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska underskrifter, uppgifter som tydligt anger den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, vilken medlemsstat tillhandahållaren är etablerad i samt namn

---

<sup>100</sup> Se preambel 49 eIDAS-förordningen.

<sup>101</sup> KOM (2012) 238 slutlig, jfr bilaga I signaturdirektivet.

och för juridiska personer, om tillämpligt, även registreringsnummer enligt officiella handlingar, detaljerade uppgifter om certifikatets giltighetstid m.m.<sup>102</sup>

Vidare anges i art. 28 eIDAS-förordningen att inga andra obligatoriska krav som går utöver dessa får ställas på kvalificerade certifikat. En bakomliggande tanke har här varit att främja gränsöverskridande erkännande av elektroniska underskrifter. Samtidigt anges att extra icke-obligatoriska attribut som inte påverkar de kvalificerade elektroniska underskrifternas kompatibilitet eller erkännande får omfatta de kvalificerade certifikaten. Härigenom tillåts medlemsstater att på nationell nivå inkludera vissa särskilda egenskaper i certifikaten, såsom unika identifierare.<sup>103</sup>

För det fall ett kvalificerat certifikat återkallats efter dess ursprungliga aktivering ska certifikatet anses ogiltigt från tidpunkten för återkallandet och dess giltighetsstatus ska inte under några omständigheter återgå. Dock får medlemsstaterna under vissa i artikeln angivna villkor fastställa nationella bestämmelser kring tillfälligt upphävande av kvalificerade certifikat. Villkoren innebär i huvudsak att certifikatet ska vara ogiltigt under tiden för det tillfälliga upphävandet samt att detta blir synligt på olika sätt.<sup>104</sup>

Beträffande standarder för kvalificerade certifikat anges att kommissionen får fastställa referensnummer genom genomförandeakter för vilka kraven i bilaga I ska uppfyllas och genomförandeakterna antas genom granskningsförfarandet i art. 48.2.

### **3.3.4.6 Anordningar för skapande av kvalificerade elektroniska underskrifter**

I art. 29 eIDAS-förordningen regleras anordningar för skapande av kvalificerade elektroniska underskrifter. Dessa anordningar, som tidigare kallats säkra anordningar för signaturframställning, ska nu betraktas som kvalificerade anordningar för skapande av elektroniska underskrifter.<sup>105</sup>

Tanken bakom artikeln, förutom att tydliggöra kraven på anordningarna som tidigare reglerats i art. 3.5 signaturdirektivet, är att tydliggöra att en sådan anordning har ett vidare tillämpningsområde än att bara innehålla uppgifter för skapande av elektroniska underskrifter.<sup>106</sup>

I art. 29 stadgas vidare att kvalificerade anordningar för skapande av elektroniska underskrifter ska uppfylla kraven i bilaga II till eIDAS-förordningen. Dessa minimikrav innebär att kvalificerade anordningar för skapande av elektroniska underskrifter genom lämpliga tekniker och förfaranden ska säkerställa åtminstone att konfidentialiteten avseende de

---

<sup>102</sup> Jfr bilaga I eIDAS-förordningen.

<sup>103</sup> Preamble 54, eIDAS-förordningen.

<sup>104</sup> Se vidare art. 28 eIDAS-förordningen.

<sup>105</sup> För definition av begreppet anordningar för skapande av kvalificerade elektroniska underskrifter se art. 2 eIDAS-förordningen.

<sup>106</sup> KOM (2012) 238 slutlig.

uppgifter som används vid skapandet av elektroniska underskrifter säkerställs på ett rimligt sätt, uppgifterna ska vidare i praktiken inte förekomma mer än en gång, uppgifterna ska vidare med rimlig säkerhet inte kunna härledas och den elektroniska underskriften ska på tillförlitligt sätt vara skyddad mot förfalskning med den teknik som för närvarande finns tillgänglig m.m.<sup>107</sup>

Genom art. 30 eIDAS-förordningen, som bygger på art. 3.4 signaturdirektivet, införs begreppet certifiering av kvalificerade anordningar.<sup>108</sup> I art. 30.1 eIDAS-förordningen stadgas att medlemsstaterna själva får utse lämpliga offentliga eller privata organ som certifierar att sådana anordningar överensstämmer med kraven i bilaga II till eIDAS-förordningen. Vidare anges i art. 30.3 eIDAS-förordningen vilka förfaranden som certifieringen ska bygga på.<sup>109</sup>

### **3.3.4.7 Validering och bevarande av kvalificerade elektroniska underskrifter**

I art. 32 eIDAS-förordningen har valideringskrav för kvalificerade elektroniska underskrifter införts som bekräftar sådana underskrifters giltighet under i artikeln vissa angivna förutsättningar. Valideringskraven har sin grund i de rekommendationer som anges i bilaga IV signaturdirektivet och utgör nu bindande krav i syfte att öka rättssäkerheten.<sup>110</sup> Kraven innebär bl.a. att det certifikat som stöder underskriften vid tidpunkten för undertecknandet utgör ett kvalificerat certifikat som utfärdats av en kvalificerad tillhandahållare av betrodda tjänster och som var giltigt vid tidpunkten för undertecknandet. Valideringsuppgifterna ska dessutom överensstämma med de uppgifter som lämnats till den förlitande parten.<sup>111</sup>

Beträffande kvalificerade valideringstjänster och bevarande av kvalificerade elektroniska underskrifter får dessa endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som uppfyller vissa krav enligt art. 33-34 eIDAS-förordningen.<sup>112</sup> Art. 34 syftar till att genom långsiktigt bevarande av uppgifter säkerställa elektroniska underskrifters rättsliga giltighet över längre tidsperioder och garantera att dessa kan valideras oberoende av tekniska förändringar.<sup>113</sup>

---

<sup>107</sup> Se vidare bilaga II eIDAS-förordningen.

<sup>108</sup> KOM (2012) 238 slutlig.

<sup>109</sup> Se vidare art. 30 eIDAS-förordningen.

<sup>110</sup> KOM (2012) 238 slutlig.

<sup>111</sup> Se vidare art. 32 eIDAS-förordningen.

<sup>112</sup> Se vidare art. 33-34 eIDAS-förordningen.

<sup>113</sup> Preambel 61 eIDAS-förordningen.

### 3.3.5 Åsikter om eIDAS-förordningen

Ekonomiska och sociala kommittén<sup>114</sup> har ställt sig mycket positiv till den nya förordningen och anser att denna kommer att stärka effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel inom EU vilket anses utgöra en förmån för EU-medborgare som arbetar eller studerar i annat medlemsland, samt för stora och små företag som utvecklar sin gränsöverskridande verksamhet. Även förordningens teknikneutrala strategi välkomnas av kommittén. Samtidigt framförs en åsikt att det bör finnas rådgivande informationsprogram som omfattar hela EU för att skapa högre säkerhet och integritet på Internet beträffande elektronisk identifiering, elektroniska underskrifter och närliggande betrodda tjänster.<sup>115</sup>

Även den svenska regeringen har uttryckt sig i positiva ordalag om den nya regleringen<sup>116</sup> och anser att åtgärderna är nödvändiga för utvecklingen av den digitala inre marknaden samt en ökad tillväxt till nytta för allmänheten, företagen och offentlig förvaltning. Vidare påpekas att ett ökat bruk av elektroniska tjänster innebär kostnadsbesparingar för såväl offentliga som privata aktörer. Samtidigt framhölls att en avvägning mellan säkerhet och kostnader behövs. Detta gäller även för betrodda tjänster då kostnaderna inte får bli för höga då nya aktörer kan få försämrat tillträde till marknaden eller att nya tjänster hindras. Teknikneutraliteten ställer sig regeringen positiv till.<sup>117</sup>

## 3.4 Sammanfattande slutsatser

Den nya förordningen bygger på ett omfattande utredningsarbete i syfte att undanröja den tidigare bristen på gränsöverskridande interoperabilitet av medlemsstaters elektroniska identifiering och betrodda tjänster såsom elektroniska underskrifter på den inre marknaden. Bestämmelserna och bilagorna i eIDAS-förordningen har utvecklats för att närmare precisera bl.a. kraven på elektroniska underskrifter och rättsverkan av dessa, kvalificerade certifikat och anordningar för skapande av elektroniska underskrifter. Dessutom blir dessa bestämmelser nu direkt gällande i alla medlemsstater genom förordningen vilket motverkar skillnader i implementering av direktiv i olika medlemsstater och därmed främjar det gränsöverskridande bruket av bl.a. elektroniska underskrifter på den inre marknaden. Jag instämmer med den allmänt rådande uppfattningen att det är en positiv utveckling med denna digitala agenda. Samhället utvecklas i en snabb takt och det är viktigt att få bukt med digitala hinder såsom den tidigare avsaknaden av erkännanden och interoperabiliteten mellan olika länders eID-system och betrodda tjänster. Det är dock avgörande att detta

---

<sup>114</sup> Rådgivande EU-organ som inrättades 1957.

<sup>115</sup> Se yttrande från europeiska ekonomiska och sociala kommittén, EUT C 351/73, 15.11.2012.

<sup>116</sup> Kommentarererna avser förslaget på ny förordning, KOM (2012) 238 slutlig.

<sup>117</sup> Se Regeringskansliets rådspromemoria 2012-12-05.

sker på ett sätt som innebär en hög nivå av säkerhet, särskilt för utfärdaren, undertecknaren och den förlitande parten. Det är också något som har tagits hänsyn till vid utarbetande av förordningen, t.ex. genom förtydligande reglering samt att de tidigare valideringsrekommendationerna för säker signaturverifiering har blivit krav för att öka rättssäkerheten. Det är enligt min mening positivt då regleringen blir mer enhetlig och tydlig. Samtidigt framgår inte ännu alla delar i säkerhetsnivån liksom de krav som kommer att ställas på de kvalificerade anordningarna, elektroniska underskrifter som ovan redogjorts för. Detta beror som ovan framkommit på att EU-kommissionen genom flertalet genomförande akter i nuläget arbetar fram standarder beträffande bl.a. kvalificerade certifikat och valideringskrav på kvalificerade elektroniska underskrifter. Samtidigt har det angivits att hänsyn tas till ovannämnda standardiseringsorgans utarbetade standarder och tekniska specifikationer. I nuläget är det dock något oklart exakt hur dessa krav och säkerhetsnivåer kommer att se ut.

Som inledningsvis nämndes eftersträvas tydligare bestämmelser om exempelvis elektroniska underskrifters rättsverkan genom att uttryckligen ange att kvalificerade elektroniska underskrifter ska ha samma rättsverkan som handskrivna underskrifter och att sådana ska erkännas av alla andra medlemsstater. Förtydligandet innebär troligen ingen större skillnad mot den tidigare bestämmelsen även om den ökar rättssäkerheten då risken för missförstånd eller felaktig tillämpning minskar. Detsamma kan sägas om övriga behandlade bestämmelser, det handlar om små skillnader i utformning men med större effekt då det nu regleras i en förordning. Tillämpningsområdet är också i huvudsak oförändrat och innebär enligt art. 2 eIDAS-förordningen att endast öppna system omfattas. Liksom tidigare omfattar eIDAS-förordningen inte nationell rätt eller unionsrätt angående frågor om ingående av avtal och giltigheten av dessa eller andra rättsliga eller förfarandemässiga skyldigheter i relation till formkrav. Numera omfattas även länders eID-system under vissa förutsättningar. Det anges bl.a. att tillämpningsområdet endast omfattar sådana eID-system som medlemsstater anmält och tillhandahållare av betrodda tjänster såsom elektroniska underskrifter som är etablerade inom unionen. Beträffande just utrymmet åt nationell lagstiftning är det för närvarande något oklart hur elektroniska underskrifter ska kunna användas i och med att signaturlagen försvinner innebärande bl.a. att begreppet avancerad elektronisk signatur försvinner. Dessutom hänvisar flertalet lagar såsom konsumentkreditlagen, lag om ekonomiska föreningar, bostadsrättslagen till signaturlagen vilket måste ändras. Genom förordning eller lag måste även fastställas tillsynsmyndighet. Utredningsarbete pågår för närvarande inom Näringsdepartementet och behandlar troligen sådana frågor vilket ska resultera i en departementspromemoria som troligen kommer att ligga till grund för en proposition efter remissbehandling till hösten.

En större nyhet är införandet av vissa andra bestämmelser t.ex. om långsiktigt bevarande av kvalificerade elektroniska underskrifter. Denna nyhet möjliggörs genom att utöka tillförlitligheten för valideringsuppgifter för underskrifterna bortom tidpunkten för deras tekniska giltighet för att

motverka it-brottslighet genom förfalskning. Bestämmelser om krav på kvalificerade valideringstjänster och kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter har införts som framförallt innebär att endast kvalificerade tillhandahållare av betrodda tjänster får erbjuda sådana tjänster. Fler nya bestämmelser som införts genom eIDAS-förordningen är bl.a. elektroniska stämplat som reglerats likadant som elektroniska underskrifter, elektroniska tidsstämplingar och elektroniska dokument vilka inte heller får förvägras rättsverkan enbart på grund av sin elektroniska form, krav på kvalificerade certifikat för autentisering av webbplatser, införandet av förteckningar av kvalificerade betrodda tjänsteleverantörer och ett förtroendemärke för kvalificerade betrodda tjänster. Bestämmelser om högre ställda krav på tillhandahållare av betrodda tjänster har införts och även utökade tillsynskrav på tillsynsmyndigheten.

# 4 Elektroniska avtalsslut

## 4.1 Inledning

När den svenska AvtL tillkom år 1915 förelåg inte möjligheten att ingå avtal på elektronisk väg och följaktligen inte heller något behov av att anpassa lagen efter sådana avtal. Likväl anses lagens regler avseende avtalsslut kunna tillämpas även i förhållande till elektroniska avtal. AvtL bygger på allmänna principer, reglerna är allmänt hållna utan krav på form vilket motiverar bruket av den teknikneutrala lagen även i förhållande till elektroniska avtal.<sup>118</sup>

Avtal delas traditionellt in i konsensualavtal, formalavtal och realavtal.<sup>119</sup> Nedan görs en genomgång av dessa avtalsformer och deras relation till avtalslagen följt av en redogörelse för hur elektroniska underskrifter förhåller sig till dem.

## 4.2 Avtalsformer

### 4.2.1 Konsensualavtal

Konsensualavtalet är en avtalsform som grundas på fullbordande genom åtminstone två viljeförklaringar, anbud och accept, med huvudsakligen samstämigt innehåll vilka binder parterna var för sig. Denna avtalsform omfattas av AvtL:s första kapitel.<sup>120</sup>

Ett för AvtL grundläggande begrepp är ”rättshandling”. Begreppet definieras i motiven som viljeförklaringar med syfte att ”grundlägga, förändra eller upphäva ett rättsförhållande”. Det är syftet och inte uppnåendet av detta som är det viktiga. Även ogiltiga rättshandlingar betraktas som rättshandlingar.<sup>121</sup> Vissa förutsättningar krävs likväl för att en rättshandling ska föreligga, såsom att parten har rättshandlingsförmåga.<sup>122</sup> Begreppet ”viljeförklaring” är inte helt entydigt men kan sägas innebära en avsikt från avgivaren att framkalla viss rättsverkan, t.ex. att binda sig. Därutöver ska avsikten på något sätt ha kommit till uttryck för motparten. En förutsättning för att handlingen ska få rättsverkan är enligt Adlercreutz

---

<sup>118</sup> Adlercreutz, Axel, Gorton, Lars (nedan Adlercreutz/Gorton), Avtalsrätt I (13 upplagan), s. 54, samt SOU 1996:40 s. 122.

<sup>119</sup> Adlercreutz/Gorton, Avtalsrätt I (13 upplagan) s. 56.

<sup>120</sup> Grönfors, Kurt, Dotevall, Rolf (nedan Grönfors/Dotevall), Avtalslagen – En kommentar (4:e upplagan), s. 56 f, Adlercreutz/Gorton, Avtalsrätt I (13 upplagan), s. 56 f.

<sup>121</sup> Se Obligationsrättskommitténs Förslag till lag om avtal och andra rättshandlingar på förmögenhetsrättens område, s. 116, jfr Adlercreutz/Gorton, Avtalslagen I (13upplagan), s. 24.

<sup>122</sup> Adlercreutz/Gorton, Avtalslagen I (13 upplagan), s. 129.



att viljeförklaringens uttryck, som också kallas avtalsfakta, erkänns av rättsordningen.<sup>123</sup>

Reglerna i 1 kap. AvtL<sup>124</sup> kring avtalsslut baserar sig på den s.k. löftesprincipen eller löfsteorin som uttrycks särskilt i 1 § 1 st. AvtL om avgivande av anbud samt i 7 § AvtL om den begränsade återkallelsemöjligheten av anbudet. Principen innebär i huvudsak att ett anbud som kommit till adressatens kännedom är oåterkalleligt.<sup>125</sup>

Undantaget, den s.k. re integra-regeln, i 39 § AvtL anger att återkallelse kan ske senare innan svaret hunnit inverka bestämmande på anbudsgivarens handlingssätt. Syftet bakom löftesprincipen som modell för 1 kap. AvtL var att mottagaren skulle kunna känna tillit till att ett anbud inte skulle kunna återkallas innan mottagaren haft viss tidsfrist att överväga om denne ville acceptera anbudet.<sup>126</sup>

Naturligtvis sluts inte alla avtal i överensstämmelse med anbud-accept-modellen och det har i doktrin påpekats att verkligheten inte stämmer överens med AvtL i detta avseende. 1 kap. AvtL inriktar sig på avtalsslut mellan parter på olika orter genom utväxling av brev och telegram och är särskilt lämpad för köp av bulkvaror. I modern tid har tekniken förnyats vilket medfört att brev och telegram ersatts av bl.a. elektroniskt överförda meddelanden.<sup>127</sup>

Det är inte ovanligt att avtal sluts på muntlig väg vilka också är giltiga, förutsatt att det inte i lag ställs krav på viss form, även om de kan medföra bevisproblem.<sup>128</sup> Muntliga anbud måste dock enligt 3 § 2 st. AvtL antas direkt. I 1 § 2 st. AvtL anges att 2-9 §§ AvtL är dispositiva och endast gäller såvitt inte ”*annat följer av anbudet eller svaret eller av handelsbruk eller annan sedvänja.*” Luckor i AvtL fylls ut av allmänna principer.<sup>129</sup>

Även om enighet råder i doktrin kring det faktum att AvtL inte omfattar alla slags avtal finns det olika uppfattningar i frågan om omfattningens räckvidd och hur långt anbud-acceptmodellen kan sträcka sig. Avtalsslut som särskilt varit föremål för debatt är gemensamma avtalsslut där ingen part kan sägas vara anbudsgivare, avtal som uppstått genom konkludent realhandlande där bundenheten uppstått genom en persons uppträdande samt avtalsbundenhet genom passivitet. Exempel på realhandlande är då någon stoppar in pengar i en automat och tar ut varan från maskinen.<sup>130</sup> Framförallt finns två synsätt i sammanhanget som redogörs för nedan.

---

<sup>123</sup> Adlercreutz/Gorton, Avtalslagen I (13 upplagan) s. 24.

<sup>124</sup> I övrigt regleras i lagen fullmakter 2 kap. AvtL, ogiltighet 3 kap. AvtL samt vissa allmänna bestämmelser 4 kap. AvtL.

<sup>125</sup> Adlercreutz/Gorton, s. 57 f, jfr Grönfors/Dotevall: Avtalslagen – En kommentar s. 48 f.

<sup>126</sup> Se Obligationsrättskommitténs Förslag till lag om avtal och andra rättshandlingar på förmögenhetsrättens område s. 38.

<sup>127</sup> Adlercreutz/Gorton, Avtalslagen I, 13 upplagan s. 53 ff., jfr Grönfors/Dotevall, Avtalslagen – En kommentar s. 56 ff.

<sup>128</sup> Adlercreutz/Gorton, Avtalslagen I, 13 upplagan, s. 53 ff.

<sup>129</sup> Ramberg, Jan och Christina, Allmän avtalsrätt, nionde upplagan, s. 22 f.

<sup>130</sup> Adlercreutz/Gorton, Avtalslagen I, 13 upplagan, s. 77.

Bert Lehrberg representerar synen att viljeförklaringsbegreppet är tämligen vidsträckt. Inom denna teori betraktas mer osäkra typer av beteende såsom exempelvis konkludent handlande och passivitet som en annan form av viljeförklaring, s.k. hypotetiska eller konstruerade viljeförklaringar. Enligt ett sådant synsätt uttrycks en vilja genom sådant handlande vilket därmed tolkas som en viljeförklaring som kan ge upphov till avtalsbundenhet.<sup>131</sup> Lehrbergs modell har ansetts vara tämligen väl underbyggd men har samtidigt kritiserats för att till viss del vara verklighetsfrånvärd och något otymplig.<sup>132</sup>

En motstående uppfattning har presenterats av Kurt Grönfors som i sin analys baserar sig på s.k. direkta avtalsgrundande rättsfakta. Hans modell ger uttryck för ett mer objektivet synsätt på avtalens uppkomst och avtalsbundenhet som en sanktion som grundar sig i yttre omständigheter som i förening ger upphov till bundenhet.<sup>133</sup> Tolkningen av avtalsslut grundar Grönfors på förklarings teorin som till skillnad från tillitsteorin tar sikte på yttre iakttagbara förklaringen såsom den framstår för en objektiv betraktare.<sup>134</sup> Kritik har riktats mot Grönfors synsätt som inte har ansetts passa som matris för hela avtalsrätten.<sup>135</sup> Även om det anses positivt att framhäva att avtal kan uppkomma på fler sätt än genom anbud-acceptmodellen har Grönfors modell inte ansetts vara tillräckligt väl underbyggd.<sup>136</sup>

Avtalsingåendet kan också ske genom standardavtal vilka karaktäriseras av att villkoren inte varit föremål för närmare förhandling parterna emellan.<sup>137</sup> De standardiserade villkoren kan se ut på lite olika sätt och är ofta utformade för att möta vissa branscher och relationer t.ex. för entreprenadavtal, försäkringsavtal, transportavtal m.m. Standardiserade villkor måste framgå för motpartens kännedom innan avtalsslutet på så vis att denne haft möjlighet att ta del av dessa utan att personen ifråga faktiskt gjort det. En central regel för standardavtal är vidare att oväntade villkor som t.ex. finns undan gömda eller på annat vis framstår som överraskande, eller särskilt betungande villkor såsom långtgående friskrivningsklausuler, måste framhållas särskilt för att kunna ingå i avtalet.<sup>138</sup> I en sådan bedömning tas hänsyn till partsställningen. En näringsidkare har större krav

---

<sup>131</sup> Lehrberg, Bert, *Avtalsrättens grundelement*, 2 upplagan, s. 102 ff.

<sup>132</sup> Heidbrink, Jakob, "Avtals uppkomst – dags att se bortom avtalslagen", s. 693. I: *Svensk Juristtidning*, 2007 s. 673 ff., (nedan Heidbrink, SvJT 2007).

<sup>133</sup> Grönfors, Kurt, *Avtalsgrundande rättsfakta*, andra upplagan, s. 96 f., jfr SOU 1996:40, 121 f.

<sup>134</sup> Grönfors, Kurt, *Avtalsgrundande rättsfakta*, andra upplagan, s. 31.

<sup>135</sup> Lehrberg, Bert, Anmälan av Kurt Grönfors, *Avtalsgrundande rättsfakta*. I: *Svensk Juristtidning*, 1996, s. 461-482 samt Olsson, Märten, "Ny förklaringsmodell för elektroniskt genererade avtal?", s. 1294. I: *Juridisk Tidskrift*, Nr. 4 1997/98, s. 1292-1297 (nedan Olsson, JT 4:97/98).

<sup>136</sup> Heidbrink, SvJT 2007 s. 682 f.

<sup>137</sup> Ramberg, Jan och Christina, *Allmän avtalsrätt*, nionde upplagan, s. 137 ff, Adlercreutz/Gorton, *Avtalsrätt I*, 13 upplagan, s. 21 ff.

<sup>138</sup> Ramberg, Jan och Christina *Allmän avtalsrätt*, nionde upplagan, s. 137 ff, samt Adlercreutz/Gorton, *Avtalsrätt I*, 13 upplagan, s. 21 ff.

på att ta reda på ett standardavtals innehåll. Viktigt att notera är att de standardiserade villkoren kan bli föremål för jämkning eller ogiltighetsförklaring enligt 36 § AvtL som kan aktualiseras trots att införlivandet av villkoren i sig är giltig.<sup>139</sup>

## 4.2.2 Formalavtal

Formalavtal karaktäriseras av att de utöver ovannämnda viljeförklaringar uppställer ytterligare krav för att rättshandlingar ska innebära att ett bindande avtal ska anses ha uppkommit, nämligen krav som föreskriver viss form. Ett sådant formkrav kan utgöras av skriftlighetskrav såsom vid exempelvis fastighetsköp enligt 4 kap. 1 § JB, vid kollektivavtal enligt 23 § MBL eller förhandlingsordning och förhandlingsöverenskommelse enligt 6 och 19 §§ HFL. Kravet kan innebära att avtalet ska vara skriftligt och/eller att avtalet egenhändigt undertecknats av parterna.<sup>140</sup>

Inom förvaltningsrätten finns flertalet formkrav om ansökan till myndigheter som ska undertecknas av t.ex. den ansökande m.m. Annorlunda är det inom affärlivet vid avtal om köp av varor och tjänster, samt om hyra m.m. där det finns det relativt få regler som uppställer krav på skriftligt avtal med traditionell underskrift där det istället kan sägas ha utvecklats genom vardaglig praxis där underskriften har större betydelse som kontroll och bevisning.<sup>141</sup>

Skälen för kraven på skriftlighet kan variera men ett centralt exempel på krav om en egenhändig underskrift är att formkravet utgör en varningsfunktion för att uppmana till eftertanke innan viktiga rättshandlingar företas.<sup>142</sup> En sådan tanke ligger t.ex. bakom formkravet i 4 kap. 1 § JB pga. avtalets stora ekonomiska vikt. Andra skäl för skriftlighetskrav är främjandet av tydlighet om att ett avtal föreligger och dettas innehåll samt bättre bevisning. Kravet på egenhändig namnteckning kan vidare ses som en garanti för att en part medverkat till handlingen.<sup>143</sup>

En annan omständighet som i doktrin har framhållits är skillnaden mellan överlåtelse och upplåtelse. Avtal om överlåtelse av fastighet, tomträtt eller bostadsrätt genom köp, byte eller gåva som innebär att äganderätten går över till en annan person kan anses vara särskilt skyddsvärda och kräver eftertanke. Beträffande upplåtelse genom hyra eller lån av bostadsrätt eller fastighet där äganderätten inte ändras utan endast innebär en nyttjanderätt till egendomen ifråga sänks graden av behov till eftertanke något, se nedan. I t.ex. 4 kap. 1 § JB utgörs skriftlighetskravet av att avtalet är skriftligt och

---

<sup>139</sup> Roos, Fredrik, Standardavtal i elektronisk miljö, s. 51. I: Elektronisk signering – En antologi.

<sup>140</sup> Adlercreutz/Gorton, Avtalslagen I, 13 upplagan, s. 145 f.

<sup>141</sup> Prop. 1999/2000:117 s. 15 ff.

<sup>142</sup> Prop. 1999/2000:117 s. 16.

<sup>143</sup> Bengtsson, Henrik, Bevisbönda och beviskrav vid invändning om underskriftförfalskning, s. 36. I: Elektronisk signering – En antologi.

att båda parterna undertecknat samt att avtalet anger pris, vilken fastighet som avses och en överlåtelseförklaring från säljaren. Samma krav gäller vid överlåtelse av en tomträtt. I huvudsak gäller även detsamma för överlåtelser av bostadsrätter, inget krav på överlåtelseförklaring uppställs i lag men i praktiken krävs en sådan för att kunna skriva ett överlåtelseavtal. Bestämmelser om upplåtelse av fastighet och bostadsrätt är formkraven enligt 4 kap. 5 § bostadsrättslagen att upplåtelsen är skriftlig, parternas namn, lägenheten m.m., samt enligt 13 kap. 3 § JB att avtalet ska upprättas skriftligt samt ange att det rör upplåtelse för tomträtt. Vid avtal om upplåtelse ställs det dock inte krav på egenhändig underteckning av parterna.<sup>144</sup> Av praxis och motiv framgår vidare att det inte heller krävs vid upplåtelse av bostadsrätter för giltighet även om det kan få betydelse för bevisnings- och tolkningsfrågor.<sup>145</sup>

Regler om parts rätt att kräva skriftlig form aktualiseras främst efter avtalsslutet där en vägran att dokumentera avtalet i skriftlig form kan ses som avtalsbrott och leda till hävning enligt t.ex. 26 § 1 p. lagen om handelsagentur och skadestånd enligt 34 § lagen om handelsagentur eller möjlighet att med exekutiv myndighets hjälp tvinga fram ett skriftligt avtal.<sup>146</sup>

Ett annat exempel på formkrav inom förmögenhetsrätten är 9 § konsumentkreditlagen som innebär att avtal om kredit till konsument ska vara skriftligt och undertecknas av konsumenten. I avsaknad av underskrift kan avtalet likväl bli giltigt bortsett från villkor som är till konsumentens nackdel. Är det däremot fråga om fastighetsköp enligt 4 kap. 1 § JB blir avtalet ogiltigt ifall underskrift saknas. Detsamma gäller för att t.ex. ett testamente eller äktenskapsförord ska bli giltigt.<sup>147</sup>

Inom arbetsrätten är de två viktigaste avtalen kollektivavtalet och anställningsavtalet. Den ovannämnda bestämmelsen om ingående av kollektivavtal i 23 § MBL innehåller ett skriftlighetskrav, inte på egenhändig underskrift utan skriftlig form för att avtalet ska vara giltigt. Det formella skriftlighetskravet motiveras av att sådana avtals tillämpningsområde och rättsverkningar omfattar fler personer än de som deltagit vid avtalsförhandlingarna på arbetstagsidan såväl som arbetsgiversidan.<sup>148</sup> Om inte skriftlighetskravet är uppfyllt får avtalet enligt allmänna avtalsrättsliga principer bindande rättsverkningar för parterna i en annan form av avtal än kollektivavtal. Detta innebär att andra effekter som kollektivavtal normalt medför såsom fredsplikt uteblir då parterna inte är

---

<sup>144</sup> Kihlman, Jon, Formfrihet, formkrav och kvalificerade elektroniska signaturer s. 16 ff. I: Elektronisk signering – En antologi.

<sup>145</sup> RH 2005:11 (I och II), prop. 2007/08:45 s. 60 se även Kihlman, Jon, Formfrihet, formkrav och kvalificerade elektroniska signaturer s. 18. I: Elektronisk signering – En antologi.

<sup>146</sup> Se Cederstierna, Nils, lagkommentaren till 12 kap. 2 § 1 st. JB. Hämtad från Karnov den 25 maj 2015.

<sup>147</sup> Prop. 1999/2000:117 s. 15.

<sup>148</sup> Westregård, Annamaria, Elektronisk avtalssignering och elektroniska handlingar inom arbetsrätten, s.86 ff. och 93. I: Elektronisk signering – En antologi.

bundna av ett kollektivavtal.<sup>149</sup> Samma strikta krav uppställs i 30 § MBL om uppsägning av kollektivavtal. Ingående av anställningsavtal kan ske formlost, men ett skriftlighetskrav som implementerar Upplysningsdirektivet<sup>150</sup> föreligger på att arbetsgivaren skriftligen ska informera arbetstagaren om samtliga villkor av väsentlig betydelse i anställningsavtalet enligt 6 § c-e LAS. Uppfylls inte kravet blir arbetsgivaren skadeståndsskyldig även om avtalet i sig förblir giltigt. Enligt 8 § LAS ska en uppsägning från arbetsgivaren vara skriftlig. Uppfylls inte kravet blir denne skadeståndsskyldig enligt 38 § LAS men uppsägningen förblir giltig. Likadana bestämmelser gäller beträffande avsked enligt 19 § LAS. Ett annat exempel på skriftlighetskrav inom arbetsrätten är reglerna i 10 respektive 20 §§ LAS som innebär att uppsägnings- eller avskedshandlingar ska överlämnas på särskilt sätt. Uppsägningen ska enligt 10 § LAS överlämnas personligen och endast undantagsmässigt genom rekommenderat brev.<sup>151</sup>

En annan typ av formkrav utgör kravet på bevittning vilket numera är ovanligt.<sup>152</sup> Behovet av bevittning av en egenhändig namnteckning motiveras bl.a. av att stärka underskriftens äkthet och bevisverkan exempelvis för att den inte kan förnekas av den undertecknande parten i efterhand.<sup>153</sup> Exempel på i lag uppställda vittneskrav är det strikta kravet på två samtidigt närvarande vittnen vid upprättande av testamente enligt 10 kap. 1 § ÄB. Ett mindre strikt krav på bevittning är 20 kap. 7 § p. 1 JB som rör bevittning av överlåtarens underskrift. Vanligen är bevittning det normala vid fastighetsköp. Likväl utgör numera vittneskravet i 20 kap. 7 § 1 p. JB endast förutsättning för omedelbar lagfart (jfr 4 kap.1 § JB) och kan enligt 20 kap. 8 § JB ersättas med ett särskilt delgivningsförfarande. Vem som får vara vittne när bevittning krävs enligt lag regleras i lag 1946 med särskilda bestämmelser angående vittne vid vissa rättshandlingar som diskvalificerar motparten, personer under 15 år och personer med allvarlig psykisk störning som vittne. Formkrav kan som i ovannämnda exempel uppställas i lag, men kan även tillkomma avtalsvägen.<sup>154</sup> Vittneskravet kan betraktas som en garanti för att en part medverkat till handlingen.<sup>155</sup>

I 1 § 3 st. AvtL undantas uttryckligen formalavtal från lagens tillämpningsområde.

---

<sup>149</sup> AD 1978 nr 124. Se även Annamaria Westregård elektronisk avtalssignering och elektroniska handlingar inom arbetsrätten, s.86 samt Dalekant, Per och Weihe, Anders, lagkommentaren till 23 § MBL hämtad från Karnov den 25 maj 2015.

<sup>150</sup> Rådets direktiv 91/533/EEG av den 14 oktober 1991 om arbetsgivares skyldighet att upplysa arbetstagarna om de regler som är tillämpliga på anställningsavtalet eller anställningsförhållandet.

<sup>151</sup> Se vidare AnnaMaria Westregård, elektronisk avtalssignering och elektroniska handlingar inom arbetsrätten, s.85 ff. I: Elektronisk signering – En antologi.

<sup>152</sup> Adlercreutz/Gorton, Avtalslagen I,13 upplagan, s. 146 f.

<sup>153</sup> Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 42 f.

<sup>154</sup> Adlercreutz/Gorton, Avtalslagen I,13 upplagan, s. 56 f. samt 142 ff.

<sup>155</sup> Bengtsson, Bertil, Elektronisk signering – En antologi, s. 36.

### 4.2.3 Realavtal

Kännetecknande för realavtal är att de utöver krav på viljeförklaring förutsätter prestation för att avtalet ska bli bindande. I allmänhet har prestationskravet utgjorts av tradition av det aktuella föremålet och är vanligast förekommande vid benefika rättshandlingar. Sådana ensidiga utfästelser har inte ansetts vara tillräckligt skyddsvärda för att bli bindande innan tradition har skett. Exempel på realavtal är saklån och räntefri försträckning såsom handlån. I 1 kap. 1 § gåvolagen krävs antingen tradition eller överlämnande av en urkund om gåvan alternativt offentliggörande av utfästelsen för att bundenhet ska uppstå.<sup>156</sup> Traditionsprincipen har varit föremål för kritik då den ansetts vara otidsenlig<sup>157</sup> och beträffande handel och pantsättning av lösöre kan Sverige vara på väg att övergå till avtalsprincipen.<sup>158</sup>

Realavtalen nämns varken i AvtL eller motiven men har likväl ansetts falla utanför lagens tillämpningsområde.<sup>159</sup>

## 4.3 Elektroniska underskrifters relation till avtalsformerna

Som framkommit ovan finns det inga särskilda formföreskrifter som gäller för konsensualavtal, vilket också innefattar standardavtal, vilka skulle hindra bruket av elektroniska underskrifter. Vad gäller användandet av elektroniska underskrifter i realavtal finns det inte heller något uttryckligt hinder för dessa men prestation krävs likväl för rättsverkan och det blir troligen knappast aktuellt med en elektronisk underskrift i sammanhanget då prestationen är det centrala.<sup>160</sup>

Däremot blir det något mer komplicerat beträffande formalavtal och bruket av elektroniska underskrifter. Som framgick i förra kapitlet innebär 17 § signaturlagen att när lagstiftare uppställer formkrav i lag och tillåter dessa att uppfyllas av elektroniska rutiner får det i allmänhet inte ställas högre krav på elektroniska underskrifter än att dessa ska vara kvalificerade. Bestämmelsen reglerar däremot inte civilrättsliga frågor om avtals giltighet.<sup>161</sup>

I en utredning har ordet ”skriftlig” i relation till förfaranderegler tolkats som att det avser att utesluta muntliga rutiner och inte elektroniska. Samtidigt har

---

<sup>156</sup> Adlercreutz/Gorton, Avtalslagen I, 13 upplagan, s. 56 f. samt 142 f.

<sup>157</sup> Se t.ex. Karlgren, Hjalmar, Avtalsrättsliga spörsmål, andra upplagan, s. 70 f., Håstad, Torgny, tillägg till NJA 2008 s. 684.

<sup>158</sup> Se Lösörekoepkommitténs betänkande SOU 2015:18.

<sup>159</sup> Se Björling, ”För vilka avtal är anbudet bindande enligt avtalslagens första kapitel?”. I: *Svensk Juristtidning*, 1916 s. 353 ff.

<sup>160</sup> Se dock diskussionen om vissa avtalsrättsliga problem i en elektronisk kontext i kap. 6.

<sup>161</sup> Prop. 1999/2000:117 s. 77 f.

utredarna gett uttryck för åsikten att när det i lag uppställs krav på att en handling ska vara ”undertecknad” är det troligen inte möjligt att uppfylla kravet elektroniskt. Ståndpunkten motiveras bl.a. av att telefaxmeddelanden i praxis inte ansetts uppfylla rättegångsbalkens krav på egenhändigt undertecknande eftersom det är just det egenhändigt undertecknade exemplaret som ska ges in till domstolen.<sup>162</sup>

I doktrin har en annan uppfattning framförts som grundar sig på principen om funktionell ekvivalens,<sup>163</sup> dvs. att inte diskriminera elektroniska medier genom att inte ge dem samma rättsverkan som pappersmedier enbart pga. dess elektroniska form.<sup>164</sup> Genom att analysera syftena bakom olika regler som innehåller formkrav behöver enligt detta synsätt ett krav på egenhändig underskrift inte i allmänhet innebära att dessa inte kan uppfyllas elektroniskt. Till stöd för åsikten har också påpekats att lagtolkning inom svensk rättsordning huvudsakligen bedrivs genom att se till ändamålet bakom en bestämmelse på t.ex. avtalsrättens område istället för att tillämpa en strikt bokstavstolkning.<sup>165</sup> I motiven till signaturlagen anfördes att det, ett sådant betraktelsesätt till trots, vore orealistiskt att tro att svenska domstolar och myndigheter vid tolkning av formkravsregler alltid skulle bedöma att dessa kan uppfyllas på elektronisk väg. Samtidigt framhölls att skriftliga formkrav på vissa områden tillåtits genom elektroniska rutiner, t.ex. genom telefax. Utredarna framhöll att det rör sig om en komplicerad fråga och att det är viktigt att notera att elektroniska underskrifter utförs på ett annat sätt än traditionella underskrifter, bl.a. genom att en elektronisk underskrift är kopplad till en viss text på ett annat sätt än traditionella underskrifter och att tekniken avseende elektroniska underskrifter präglas av en hög grad av säkerhet. Därmed anses elektroniska underskrifter med tillräckligt hög kvalitet kunna utgöra ett minst lika gott skydd mot förfalskning som traditionella underskrifter.<sup>166</sup>

Åsikten om att det inte alltid är möjligt att uppfylla skriftlighetskrav genom elektroniska underskrifter har också fått stöd i doktrin.<sup>167</sup> Det har bl.a. uttalats att när skriftlighetskrav som föreskriver krav på egenhändigt undertecknande förekommer i en författning, kan en utgångspunkt vara att kravet inte kan uppfyllas genom elektronisk underskrift om inte detta framgår av bestämmelsen i det enskilda fallet. Exempel på bestämmelser där sådan möjlighet uttrycks är 1 kap. 7 § lagen om ekonomiska föreningar. Enligt bestämmelsen tillåts avancerade elektroniska underskrifter enligt

---

<sup>162</sup> SOU 1996:40 s. 95.

<sup>163</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 65 ff.

<sup>164</sup> Modellagen UNCITRAL bygger på denna princip. Se särskilt art. 5 UNCITRAL som fastslår huvudregeln att information inte får förnekas rättsverknningar, giltighet eller möjlighet för verkställighet enbart pga. elektronisk form. Se Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 21.

<sup>165</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 65 ff.

<sup>166</sup> Prop. 1999/2000:117 s. 17.

<sup>167</sup> Kihlman, Jon, Formfrihet, formkrav och kvalificerade elektroniska signaturer, I: Elektronisk signering – En antologi Elektronisk signering – En antologi, s. 19 f. Se även Sjöberg Magnusson, Cecilia, ”Lag om kvalificerade elektroniska signaturer – Ny lag men fortsatt behov av åtgärder”, s. 871 f. I: *Juridisk Tidskrift* Nr. 4 2000/01 s. 864 ff.

signaturlagen förutsatt att inget annat anges innebärande att huvudregeln i lagen är att elektroniska underskrifter får användas. 1 kap. 9 § bostadsrättslagen hänvisar till bestämmelsen i 1 kap 7 § lagen om ekonomiska föreningar vilket innebär att huvudregeln i bägge lagarna är att vid krav på egenhändigt undertecknande kan avancerad elektronisk underskrift användas. Ett exempel på undantag är 6 kap. 4 § bostadsrättslagen om avtal om överlåtelse av bostadsrätt där det anges att lagens huvudregel inte ska tillämpas.<sup>168</sup>

På förvaltningsrättens område finns det två exempel på rättsfall som också talar för motsvarande inställning. Även om inte alltför stora paralleller bör dras till dessa, bl.a. pga. att förvaltningsrätten inte präglas av samma syften som förmögenhetsrätten, kan det vara intressant att nämna dessa i sammanhanget. I det ena rättsfallet<sup>169</sup> rörde det sig om ett avvisningsbeslut av ett överklagande till kammarrätten. Avvisningsbeslutet överklagades till HFD som dock avvisade överklagandet till HFD eftersom detta endast undertecknats med en kvalificerad elektronisk underskrift vilket inte bedömdes uppfylla det uttryckliga kravet på egenhändig underskrift i 3 § förvaltningsprocesslagen.<sup>170</sup> I ett annat mål<sup>171</sup> om laglighetsprövning enligt KL från Kammarrätten i Göteborg godkändes däremot en avancerad elektronisk underskrift genom e-legitimation som politiker använt sig av vid justering av protokoll. Kammarrätten delade förvaltningsrättens bedömning om att justeringen syftar till att bestyrka riktigheten av protokollets innehåll och att det inte uttryckligen framgår något krav i KL att detta bestyrkande måste ske genom undertecknande med penna och avslog överklagandet.

Skriftlighetskravet i 23 § MBL innebär att formen för översändande av handlingarna kan vara elektronisk, t.ex. genom e-post. Då inget krav på egenhändig underskrift föreligger kan handlingarna signeras elektroniskt.<sup>172</sup> Formkravet i 30 § MBL är absolut och regeln tvingande, men handlingarna anses likväl kunna sändas på elektronisk väg då det tidigare varit tillåtet att så skedde genom telegram och telefax.<sup>173</sup> Detta sker dock genom ett undantag om att avsändandet sker på avsändarens risk innebärande att om uppsägningen skickats till mottagarens senast kända adress inom en tid som borde medföra att den borde komma fram inom tidsfristen anses uppsägningen vara giltig även om den kommit fram utom denna tidsfrist.<sup>174</sup>

Anställningsavtalet, med eventuellt införda villkor enligt 6 § c-e LAS, kan också uppfyllas elektroniskt genom att dokumentet kan vara elektroniskt

---

<sup>168</sup> Kihlman, Jon, Formfrihet, formkrav och kvalificerade elektroniska signaturer. I: Elektronisk signering – En antologi, s. 20 f.

<sup>169</sup> RÅ 2002 not 206.

<sup>170</sup> Observera att kravet på egenhändig underskrift genom lagändring inte längre föreligger i 3 § förvaltningsprocesslagen. Se SFS 2013:86.

<sup>171</sup> Se Kammarrätten i Göteborg, mål nr 3459-14.

<sup>172</sup> Annamaria Westregård, elektronisk avtalssignering och elektroniska handlingar inom arbetsrätten, s.87 f. I: Elektronisk signering – En antologi.

<sup>173</sup> Prop. 1975/76:105 s. 491 och 533.

<sup>174</sup> AD 1998 nr 96. Se även Annamaria Westregård elektronisk avtalssignering och elektroniska handlingar inom arbetsrätten, s.87 f. I: Elektronisk signering – En antologi.



och även signeras elektroniskt. Elektroniska handlingar kan vidare skickas via e-post utan hinder av skriftlighetskraven i LAS. En viktig skillnad här är hur arbetstagaren kvitterar eller signerar handlingar som arbetsgivaren sänder elektroniskt. Skickas ett e-postmeddelande med mottagningsbevis blir det en kvittering på att arbetstagaren mottagit handlingen. Om däremot arbetstagaren signerar handlingen eller avtalet elektroniskt kan detta betraktas som ett ömsesidigt avtalsinnehåll vilket får arbetsrättsliga konsekvenser ifall arbetsgivaren senare vill ändra på arbetsuppgifterna. Uppsägning eller avsked bör dock inte ske genom elektronisk kommunikation då arbetsgivaren riskerar att bli skadeståndsskyldig enligt 38 § LAS. En i doktrin framförd åsikt är att bestämmelser med krav på personligt överlämnande eller rekommenderat brev onekligen är föråldrade i ett digitalt samhälle.<sup>175</sup>

Angående frågan om bestämmelser med formkrav ska tillåta en elektronisk underskrift eller inte har det i signaturlagens förarbeten påpekats att det troligen inte är lagstiftning som utgör det mest centrala hindret. Det viktiga är att arbeta fram säkra tekniska lösningar som är lätta att använda vilket ökar kunskapen och tilliten till elektroniska underskrifter i samhället.<sup>176</sup>

Beträffande uppställda lagkrav på bevitning har det i doktrin diskuterats sådana möjligheter även för elektroniska underskrifter. Elektroniska underskrifter i öppna nyckel-system erbjuder, liksom traditionella underskrifter, äkthet genom att varje token<sup>177</sup> har en unik nyckel vilken dessutom kan kontrolleras genom certifikat. Dock bygger detta på att ingen obehörig får tillgång till token-innehavarens hemliga PIN varför även bevitning kan användas vid sådana underskrifter. Antingen kan den elektroniska underskriften bevitnas genom att ytterligare en token-innehavare får elektroniskt underteckna aktuellt dokument samtidigt som upphovsmannen av dokumentet, eller så kan ett vittne elektroniskt underteckna ett redan krypterat dokument innebärande att bevitningen kan ske i efterhand.<sup>178</sup>

## 4.4 Sammanfattande slutsatser

Det kan konstateras att utvecklingen av IT inneburit en genomgripande förändring av dagens sätt att sluta avtal. Samtidigt har den teknikneutrala AvtL visat sig vara flexibel och det finns inget som hindrar en tillämpning av AvtL även i förhållande till elektroniska underskrifter, eftersom AvtL inte uppställer krav på egenhändig underskrift. I avsaknad av uppställda formkrav på avtalsingående i denna lag är det en naturlig slutsats att elektroniska underskrifter kan användas för att ingå bindande avtal.

---

<sup>175</sup> Se vidare Annamaria Westregård elektronisk avtalssigenering och elektroniska handlingar inom arbetsrätten, s.89 ff.

<sup>176</sup> Prop. 1999/2000:117 s. 16.

<sup>177</sup> Token innebär i korthet en informationsbärare som används för identifiering t.ex. i form av dosa, fil eller kort. Computer Sweden, ordlista under token.

<sup>178</sup> Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 42 ff.

Konsensualavtal innehåller alltså inga särskilda krav på avtalsingående eller giltighet som skulle utgöra hinder för elektroniska underskrifters rättsverkan. Beträffande realavtal som innehåller krav på prestation, vanligen tradition, finns inga hinder för elektroniska underskrifter men prestation krävs likväl. Den typen av avtal är inte typiskt sett skriftlig varför frågan om en elektronisk underskrift bör tillåtas inte aktualiseras på samma sätt.

Däremot kan hinder uppstå vid formalavtal som t.ex. ställer upp skriftlighetskrav på egenhändig namnteckning. En allmänt delad syn är att utgångspunkten vid ett sådant skriftlighetskrav är att det då bör framgå i lagbestämmelsen ifråga att elektroniska underskrifter får användas för att dessa ska få rättsverkan. Exempel på sådana möjligheter finns i 1 kap. 7 § lag om ekonomiska föreningar och bostadsrättslagen där avancerade elektroniska underskrifter enligt får användas som huvudregel. Ett undantag är överlåtelse av bostadsrätter enligt 6 kap. 4 § bostadsrättslagen där traditionell underskrift krävs för rättsverkan. Det finns i övrigt få formalavtal i svensk rättsordning på förmögenhetsrättens område. Regler med formkrav kan motiveras av hänsyn till att man vill varna en part som är på väg att ingå en bindande förpliktelse som kräver viss eftertanke. Ett exempel är 4 kap. 1 § JB där det rör sig om stora ekonomiska värden samt en överlåtelse av äganderätten till en fastighet. Viss åtskillnad kan göras mellan just överlåtelse och upplåtelse av t.ex. en fastighet där överlåtelsen kan anses påkalla något mer eftertanke vilket motiverar ett skriftlighetskrav som ännu inte anses kunna uppfyllas av en elektronisk underskrift såsom är fallet i t.ex. 4 kap. 1 § JB och 6 kap. 4 § bostadsrättslagen. Det kan dock återigen poängteras att viss rättslig oklarhet i nuläget råder då signaturlagen är på väg att upphävas och ny nationell reglering på området ännu inte presenterats. Ett annat exempel på formkrav är vittneskravet i t.ex. 10 kap. 1 § ÄB. Krav på bevittning motiveras av bl.a. av att traditionella underskrifter ibland anses ha ett lägre bevisvärde och undertecknande parten kan förneka att det verkligen är denne som skrivit under en handling. Bevittning kan då stärka bevisningen genom garanti för underskriftens äkthet. Elektroniska underskrifter i öppna nyckelsystem kan också fylla en sådan funktion. Dock gäller det att inte en obehörig får tag i den hemliga nyckeln varför det kan anses vara en bättre lösning att införa bevittning på elektronisk väg. En sådan lösning kan utgöras antingen av att låta ytterligare en tokeninnehavare underteckna ifrågavarande dokument samtidigt som upphovsmannen eller att ett vittne får underteckna ett redan krypterat dokument så att bevittningen kan ske i efterhand.

# 5 Elektroniska underskrifters funktion

## 5.1 Inledning

Som framgick av förra kapitlet finns det i affärlivet vid avtal om köp av varor och tjänster, samt om hyra m.m. få regler som uppställer krav på skriftligt avtal med traditionell underskrift. Dock kan underskriften få stor betydelse ur bevishänseende. En befogad fråga beträffande elektroniska underskrifters rättsliga funktion är hur väl de kan ersätta en vanlig namnunderskrift. Det finns ingen reglering kring hur en underskrift ska ske och den kan bestå av undertecknarens fulla namn, initialer, sigill m.m. Ramberg har påpekat att det inte är symbolen för identifiering utan avsikten bakom bruket av symbolen som är det väsentliga.<sup>179</sup> I förarbetena till signaturlagen diskuterades namnunderskriftens rättsliga funktion och elektroniska underskrifters förhållning till dessa. Underskriftens främsta funktioner ansågs här vara viljefunktion, varningsfunktion, identifieringsfunktion, äkthetsfunktion samt bevisfunktion.<sup>180</sup> Nedan behandlas dessa funktioner samt i vilken utsträckning elektroniska underskrifter kan fylla dessa funktioner.

## 5.2 Vilje- och varningsfunktion

Viljefunktionen sammanhänger med undertecknandet som anses ge uttryck för en vilja att handla på ett visst sätt. Undertecknaren visar att denne accepterar aktuellt textinnehåll i anslutning till underskriften. Viljefunktionen är även kopplad till en tillitsida innebärande att personen kan utgå ifrån att denne kan handla på visst sätt. Varningsfunktionen anses också vara förbunden med underskriften då det tydligt framgår att det härigenom kan uppstå en bindande förpliktelse. Som framgick i föregående kapitel kan varningsfunktionen bli särskilt viktig t.ex. vid avtal som av olika skäl kräver viss extra eftertanke. Ett sådant exempel utgörs av 4 kap. 1 § JB där det rör sig om en äganderättsövergång och normalt av ett större ekonomiskt värde.

Bruket av en privat nyckel, som vid t.ex. en elektronisk underskrift, anses också kunna ge uttryck för en vilja. Den närmare frågan om hur långtgående elektroniska underskrifters förmåga att uppfylla varningsfunktionen är, anser utredarna i departementspromemorian vara beroende av den allmänna uppfattningen om huruvida en bindande förpliktelse därigenom anses uppkommen.<sup>181</sup> Som framgår av diskussionen i kap. 6.2 (se nedan) om

---

<sup>179</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 30.

<sup>180</sup> Ds 1998:14 s. 134 ff., se även Prop. 1999/2000:117 s. 14 ff.

<sup>181</sup> Ds 1998:14 s. 134 f.

standardavtal finns det många sätt att framhålla särskilda avtalsvillkor elektroniskt vilket borde innebära att även elektroniska underskrifter kan ha en sådan varningsfunktion.

## 5.3 Identifieringsfunktion

Underskriften har vidare en identifieringsfunktion. Exempelvis kan en kontroll av undertecknande parten ske genom att en kontrollant närvarar vid signeringen samt jämföra underskriften med en annan underskrift från undertecknaren i fråga. Beträffande elektroniska underskrifter anser utredarna att identifiering kan ske vid verifiering genom den öppna nyckeln men påpekar att anknytningen mellan nyckelparet och personen ifråga måste fastställas, något som kan utföras av en CA.<sup>182</sup> Värt att poängtera är också att det troligen är sällsynt förekommande att en särskilt utbildad handläggare alltid kontrollerar en persons identitet vid traditionella fysiska underskrifter i motsats till elektronisk identifiering som alltid kontrolleras mot den avancerade eller kvalificerade elektroniska underskriften som utfärdats på ett sådant sätt att man med mycket hög säkerhet kan binda den fysiska personen som den avser.<sup>183</sup>

## 5.4 Äkthetsfunktion

Äkthetsfunktionen är sammanbunden med identifiering av undertecknaren och utgör ett skydd mot manipulation av texten eller underskriften. Genom att underskriften dels kopplar visst innehåll med namnteckningen, dels kopplar innehållet till den av namnteckningen utpekade personen anses den person som ska bindas till innehållet kunna identifieras. Visst skydd mot manipulation ges genom att text och underskrift fästs på samma papper och att namnteckningen är personlig. Samtidigt finns risken att namnteckningen förfalskas och personers underskrifter kan vara närapå identiska. Möjligheten att upptäcka förfalskningar vid kontroll av underskrift som med säkerhet rör från personen ifråga varierar. Dock påpekar utredarna att närmare analyser i efterhand oftast ger goda resultat. Här skiljer sig namnteckningen från sigillet som saknar denna möjlighet. Beträffande elektroniska underskrifter saknar även de den personlighet som en vanlig namnunderskrift har men eftersom dessa är knutna till det signerade meddelandet på visst sätt kan likväl manipulationer upptäckas i efterhand. För att undvika manipulering och för att kunna identifiera sig måste dock innehavaren av den privata nyckeln hemlighålla denna nyckel.<sup>184</sup>

Vid en kontroll av en traditionell underskrifts äkthet hos SKL kan penntryck, skriftflöde och bokstavsdetaljer granskas. För att kunna värdera en underskrift eller ett dokument på ett tillförlitligt sätt krävs kvalitets- och

---

<sup>182</sup> Ds 1998:14 s. 135.

<sup>183</sup> Kontakt med e-legitimationsnämnden.

<sup>184</sup> Ds 1998:14 s. 135 f.

kompetenssäkring av metod och personal genom utbildning, erfarenhet och vetenskaplig metodik. Ju högre kvalitet en handling med en eventuell underskrift har desto säkrare kan ett utlåtande bli. Ett sätt att öka kvaliteten är s.k. dokumentssäkringar. För fysiska dokument kan detta utgöras av vattenmärke, olika holografiska bilder och säkerhetsstråd. Exempel på handlingar som innehåller många säkringar av det slaget är ID-handlingar och sedlar vilka därmed blir svårare att förfalska. En annan intressant företeelse är biometriska dokumentssäkringar genom fingeravtryck, ansiktsbild och iris vilka kan säkerställa en persons identitet och kan utgöra ett alternativ till bevitning av en underskrift i t.ex. affärsavtal. Även för elektroniska dokument behövs en dokumentssäkring i någon form för att ingå avtal eller styrka någons identitet. PKI-systemet utgör ett tekniskt hjälpmedel som kan säkerställa att viss information fortfarande överensstämmer med originaldokumentet, att informationen under transporten är krypterad och därmed skyddas från obehörig åtkomst och att en autentisering står som garant att rätt parter skickat respektive mottagit dokumentet. För att kontrollera ett mottaget dokument eller fil överensstämmelse med originalet används hashsummeringen, dvs. den digitala signaturen. Det är komplicerat att säkerställa och styrka att ett elektroniskt dokument skapats och godkänts av ifrågavarande avtalsparter. Idag finns möjligheten att ha ett dokument på databärare såsom smartphones eller datorn vilket inte nödvändigtvis innebär att identiteten styrks hos avtalsparterna. Därför är det viktigt med kvalitetssäkringar. Liksom kvaliteten och säkerheten på jämförelsematerial m.m. för fysiska dokument eller underskrifter finns det i PKI-systemen olika nivåer av säkerhet. Den idag säkraste metoden för elektroniska dokument med eventuella elektroniska underskrifter är att kombinera PKI-systemet med biometriska egenskaper.<sup>185</sup>

Som framkom i kap. 3 syftar regleringen i eIDAS-förordningen bl.a. till att säkerställa att uppgifterna i en avancerad elektronisk underskrift inte på något sätt förändrats och att undertecknaren kan identifieras genom underskriften. Sammanfattningsvis kan alltså både identifierings- och äkthetsfunktioner finnas även hos en elektronisk underskrift.

## 5.5 Bevisfunktion

Namnunderskrifter kan få betydelse när behov av bevisning föreligger, t.ex. för att i efterhand styrka rättshandlingar. Grunden för detta är den äkthetsfunktion och identifieringsfunktion som namnteckningen erbjuder. Även elektroniska underskrifter kan som ovan angivits ha sådana funktioner innebärande att även dessa kan ha en bevisfunktion.<sup>186</sup> Det finns till följd av principen om fri bevisprövning som gäller i svensk rättsordning inga formella processrättsliga hinder för att åberopa exempelvis en elektronisk

---

<sup>185</sup> Andersson, Helene m.fl., Hur analyserar man äktheten av ett dokument?, s. 79 ff. I: Elektronisk signering – En antologi

<sup>186</sup> Ds 1998:14 s. 136.

underskrift som bevisning. Domstolarna får vidare fritt värdera denna form av bevisning grundat på vår fria bevisvärderingsprincip och beträffande bevisbördeplacering vid namnunderskriftsförfalskning har lagutredarna inte funnit skäl att tillämpa andra bevisregler för elektroniska underskrifter än vad som gäller för vanliga underskrifter.<sup>187</sup> Bevisbörderegler finns både i lag och i praxis. Beträffande underskrifter är det mest aktuellt att diskutera bevisbördan för när en person förnekar en namnunderskrift och påstår att den är förfalskad. Sådan bevisbörda har inte reglerats i lag men ett centralt rättsfall är NJA 1976 s. 667 där en person nekade till att det verkligen var han som undertecknat en skuldförbindelse. Högsta domstolen uttalade i målet att om någon gör gällande att namnunderskriften är äkta är det den påstådde fordringsägaren som ska visa att handlingen är äkta. Är det däremot ett påstående om att namnunderskriften är äkta men att innehållet på något sätt ändrats, s.k. innehållsförfalskning, är det istället gäldenären som ska bevisa detta. Ett annat mål av intresse är NJA 1992 s. 263 där Högsta domstolen uttalade sig i samband med påstådda förfalskningar av inköpsnotor vid användande av kontokort. Här ansågs bevisbördan åvila kontohavaren som åtminstone skulle göra det antagligt att en förfalskning förelåg. Skulle detta uppfyllas är det istället kontokortsföretaget som ska visa att notan är äkta.

Det har i doktrin påpekats att praxis på senare tid varit något oenhetlig genom att bevisvärdering och beviskraven tillämpats på olika sätt.<sup>188</sup> Som nämndes ovan ansågs inte bevisbörderegler behöva ändras enbart för att det rör sig elektroniska underskrifter. I motiven till signaturlagen påtalades också att det vore en farlig väg att gå. Vid en bedömning av placering av bevisbördan ska istället beaktas omständigheter såsom vad det är för slags uppgifter som bekräftats med den elektroniska underskriften, vad det är för typ av rättshandling och vad det är för förhållande som ska bevisas. Även parternas inbördes förhållande kan ha betydelse.<sup>189</sup> Det kan också tilläggas att UNCITRAL:s modellag för elektronisk handel flera gånger återopats av Högsta domstolen som rättskälla. Därför är det antagligt att svenska domstolar kan beakta UNCITRAL:s parametrar för bevisvärdering av elektroniska underskrifter.<sup>190</sup> Det krav som eIDAS-förordningen, och signaturdirektivet, uppställer avseende bevisverkan av elektroniska underskrifter är därmed mindre effektfulla i svensk rätt till följd av den fria bevisprövningen och bevisvärderingen.

---

<sup>187</sup> Se Ds 1998:14 s. 185 och Ds 1999:73 s. 23. Jfr även SOU 2010:54 s. 123 ff.

<sup>188</sup> Se t.ex. Svea hovrätts dom 2011-11-16, mål nr T6836-10 och 2012-01-02, mål nr T 6564-11 där ett lågt beviskrav riktades mot gäldenären som gjorde gällande att en underskriftsförfalskning förelåg av en namnteckning i en borgensförbindelse. I Hovrätten för västra Sveriges dom 2012-10-10, mål nr T 2990-12 bedömdes det istället att borgenären skulle göra det övervägande sannolikt att gäldenären undertecknat en handling. Se vidare Bengtsson, Henrik, Bevisbörda och beviskrav vid invändning om underskriftsförfalskning, i Elektronisk signering – En antologi, s. 68 ff.

<sup>189</sup> Prop. 1999/2000:117 s. 17 f.

<sup>190</sup> Se t.ex. NJA 2008 s. 733 och NJA 2010 s. 219. Se vidare även Bengtsson, Henrik, Bevisbörda och beviskrav vid invändning om underskriftsförfalskning, I: Elektronisk signering – En antologi, s. 74 f.

Grundat på elektroniska underskrifters särart innebärande bl.a. en större möjlighet till förfalskning än vanliga pappersdokument bör viss försiktighet iakttas innan elektroniska underskrifter tillmäts avgörande betydelse som bevismedel.<sup>191</sup> Samtidigt kan det anmärkas att det finns krypteringsmetoder som är mycket svåra att dechiffrera. Anförtros dessutom den privata nyckelhanteringen åt en trovärdig tredje part såsom banker eller statliga myndigheter kan elektroniska underskrifter vara säkrare än vanliga namnunderskrifter. Detta innebär också att innehavaren av en sådan nyckel inte kan förneka att denne undertecknat visst textinnehåll, s.k. oavvislighet.<sup>192</sup> En annan fördel med elektroniska underskrifter är att de vanligen kan spåras genom möjligheten till kontroll av tidpunkten för den elektroniska underskriften av ett dokument och att se ifall denna använts vid andra tidpunkter. En förutsättning för sådana möjligheter är dock att det går att rekonstruera signeringssystemet samt att det går att föra bevisning om hur detta system fungerade när dokumentet undertecknades.<sup>193</sup>

## 5.6 Sammanfattande slutsatser

Den traditionella underskriften typiska funktioner anses bl.a. utgöras av en viljefunktion som uttrycks genom undertecknandet och ger en indikation om tillit. Elektroniska underskrifter anses också fylla denna funktion där den privata nyckeln har ansetts ge uttryck för en sådan vilja.

Den traditionella underskriften anses vidare ha en varningsfunktion innebärande en uppmaning till eftertanke för en part som är på väg att ingå en rättshandling med vissa konsekvenser och underskriften varnar för att en bindande förpliktelse kan uppstå genom denna. Särskilt viktig blir denna vid t.ex. överlåtelse av fastighet enligt 4 kap. 1 § JB där det rör sig om en överlåtelse av äganderätten till en fastighet med större ekonomiskt värde. Beträffande elektroniska underskrifters förmåga att uppfylla denna funktion har det inte getts något tydligt svar men som framkom i diskussionen av standardavtal på Internet finns det goda förutsättningar till en varningsfunktion även för elektroniska underskrifter.

Traditionella underskrifter anses vidare ha en identifieringsfunktion som säkerställer från vem underskriften härrör vilket elektroniska underskrifter minst lika bra kan göra, särskilt där nyckelhanteringen sköts av en betrodd tredje part, CA. Dock krävs att ingen obehörig får tag på den hemliga nyckeln. Vidare bedöms elektroniska underskrifter ha den äkthetsfunktion som traditionella underskrifter erbjuder genom att även dessa, dock under vissa förutsättningar, kan kontrolleras i efterhand. Säkerheten i PKI-systemet är viktig för sådan analys och biometriska metoder av olika slag förstärker trovärdigheten ytterligare.

---

<sup>191</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt s. 85 ff.

<sup>192</sup> Lindberg, Agne, Elektroniska originaldokument, s. 40 f., Prop. 1999/2000:117, s. 14 f.

<sup>193</sup> Bengtsson, Henrik, Bevisbörda och beviskrav vid invändning om underskriftförfalskning, i Elektronisk signering – En antologi.

Till följd av den svenska rättsordningens principer om fri bevisvärdering och bevisprövning kan elektroniska underskrifter också användas som bevisning. Elektroniska underskrifter anses vidare kunna uppfylla en sådan bevisfunktion även om viss försiktighet kan vara påkallad. Viktigast vid denna bedömning är hur hög säkerheten är i signeringssystemet. Innebörden av bevisfunktionen hos en underskrift kopplar också till s.k. oavvislighet, d.v.s. att den undertecknande parten inte kan neka till underskriften ifråga. Detta innebär att för det fall en elektronisk underskrift med tillräckligt hög kvalitet, som t.ex. en avancerad eller kvalificerad elektronisk underskrift, är oavvislig.



# 6 Avtalsrättsliga problem i en elektronisk kontext

## 6.1 Inledning

Elektroniska underskrifter har en nära koppling till elektroniska dokument, elektronisk kommunikation och elektroniska avtal genom att de på olika sätt skapar viktiga förutsättningar för elektroniska underskrifter. Som tidigare framgått ser dagens avtalsslut till följd av förändrad teknik och handelsbruk annorlunda ut än i början av 1900-talet och erbjuder mer varierande möjligheter jämfört med AvtL:s tämligen enkla anbud-acceptmodell. Samtidigt har regler om avtalsslut varit flexibla något som bl.a. framgår av 40 § vari stadgas att kommunikation vid avtalsslut kan ske genom post och telegraf men även på annat ”ändamålsenligt sätt”.<sup>194</sup> Idag brukas betydligt oftare e-post som kommunikationsmedel och frågan är hur detta elektroniska kommunikationsmedel kan ge upphov till bindande avtal. Det som skiljer sådan post från traditionella avtal är endast den elektroniska kommunikationen.<sup>195</sup>

Elektroniska avtalsslut ska enligt art. 9 E-handelsdirektivet vara tillåtna i samtliga medlemsländers rättssystem. Implementeringen av direktivet gav inte upphov till några större förändringar i AvtL<sup>196</sup> vilket borde innebära att det redan fanns utrymme att ingå elektroniska avtal i enlighet med AvtL. Dock går åsikterna isär beträffande vilka typer av elektroniska avtal som omfattas av AvtL:s anbud-accept modell. Att elektroniska medel kan ge upphov till avtalsbundenhet är inte det problematiska, det är istället viljeförklaringen som i vissa fall kan ifrågasättas i samband med automatiska processer.<sup>197</sup> Nedan redogörs för elektroniska viljeförklaringar och synen på dessas förenlighet med AvtL. Därefter följer en beskrivning av vissa avtalsrättsliga fel och ogiltighetsgrunder enligt AvtL som medför tillämpningsproblem som är säregna för elektroniska avtalsslut. Genomgången berör inte alla former av ogiltighetsgrunder men rent allmänt kan avtalsrättsliga ogiltighetsgrunder delas in i tre kategorier: a) sådana som hänför sig till brister i avtalsrekvisit, såsom bristande rättshandlingsförmåga eller behörighet, b) sådana som hänför sig till omständigheterna kring avtalets tillkomst, exempelvis svek eller tvång samt c) sådana som hänför sig till avtalets innehåll som betraktas som otillåtet. Att innehållet betraktas som otillåtet beror antingen på att det strider mot god sed, såsom avtal om att begå brott, alternativt att det strider mot lag.<sup>198</sup>

---

<sup>194</sup> Grönfors/Dotevall, Avtalslagen – En kommentar, s. 53.

<sup>195</sup> Janson, Ingemar, Den elektroniska marknadsplatsen – Avtals-, köp- och bevisrättsliga aspekter, s. 43.

<sup>196</sup> Jfr prop. 2001/02:150, s. 78 f., där diskussion kring behov av förändring av svensk lagstiftning med anledning av direktivet förs.

<sup>197</sup> Jfr Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 23.

<sup>198</sup> Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 68.

## 6.2 Elektronisk viljeförklaring

I SOU 1996:40 har Grönfors i kap. 4.2.1 presenterade modell framhållits som lämplig utgångspunkt i hanteringen av automatiskt genererade elektroniska avtal. Ett sådant synsätt skulle innebära att man kan undvika många förhastade lagändringar. Den bakomliggande tanken har här varit att det rör situationer där praktiska behov framtvingar avtalsverkningar, trots avsaknaden av en viljeförklaring i traditionell subjektiv mening.<sup>199</sup>

I doktrin har en diskussion förts kring huruvida elektroniska avtalsslut kan tolkas enligt AvtL:s modell, eller om de bör betraktas som avtalsslut genom realhandlande alternativt avtalsgrundande rättsfakta. Beträffande avtal mellan människor där elektroniskt medium endast används som hjälpmedel möter det enligt Janson inga hinder att använda AvtL:s modell. Däremot ställer denne sig tveksam om detta fungerar ifråga om avtalstyper med automatiska processer som saknar mänsklig inblandning såsom exempelvis EDI-avtal<sup>200</sup> alternativt köp på Internet genom on-line-beställningar eller e-post från köparen. Janson är av den åsikten att elektronisk handel ännu inte uppnått sådan status som realhandlande i samhället där parterna fullt ut förstår konsekvenserna av handlandet alternativt där det är underförstått i syfte att underlätta handeln. Dessutom påpekar Janson att avtal genom realhandlande normalt omfattar transaktioner av lägre värden medan transaktioner inom elektronisk handel varierar betydligt mer. Därmed borde en avtalsmodell grundad på mer objektiva rekvisit såsom Grönfors modell passa bättre för dessa avtal. Dock har Grönfors kritiserade modell ännu inte vunnit tillräckligt stort stöd för att ingå i de accepterade avtalsmodellerna.<sup>201</sup>

Flera har framfört önskemål om en avtalsmodell baserad på mer objektiva rekvisit.<sup>202</sup> Det finns även olika sätt att se på den elektroniska viljeförklaringen. Enligt ett angivet synsätt finns det alltid en mänsklig inblandning vid elektroniska avtal, även bakom automatiska processer. Grunden för tankesättet är programmeringen där datorn agerar enligt människans vilja och därmed uttrycker denna indirekt. Vidare kan fenomenet även<sup>203</sup> betraktas mer kopplat till förklaringsteorin och objektiva faktorer där hela förfaringsättet syftar till att åstadkomma bindande avtal.<sup>204</sup>

Till diskussionen om automatiserade avtalsslut och avtal on-line hör standardavtal som erbjuds för en rad olika varor och tjänster på Internet,

---

<sup>199</sup> SOU 1996:40 s. 121.

<sup>200</sup> EDI-avtal är ett standardavtal som utarbetats av internationella organ och används främst inom slutna system. Se t.ex. Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 70 ff.

<sup>201</sup> Jansson, Ingemar, Den elektroniska marknadsplatsen – Avtals-, köp- och bevisrättsliga aspekter, IRI-rapport 1997:1, s. 42 ff.

<sup>202</sup> Se t.ex. SOU 1996:40 s. 121 och 129 ff., Grönfors, Kurt, Avtalsgrundande rättsfakta, andra upplagan, 27 ff., Jansson, Ingemar, Den elektroniska marknadsplatsen – Avtals-, köp- och bevisrättsliga aspekter, s. 43. Jfr Olsson, JT 4:97/98.

<sup>203</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 26.

<sup>204</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 26, jfr SOU 1996:40 s. 121 och 129 ff.

exempelvis genom s.k. point-and-click eller click-wrap-avtal.<sup>205</sup> Beträffande standardavtal i en elektronisk miljö har det framhållits att det finns bättre möjligheter att påvisa överraskande eller särskilt betungande villkor genom att styra vad som visas på motpartens skärm.<sup>206</sup> Det har dock uttalats att det inte bör ställas alltför höga krav på hur sådana villkor ska framhållas då det riskerar att metoden för avtalsslut blir alltför komplicerad och tidskrävande. Viktigt att notera är att de standardiserade villkoren kan bli föremål för jämkning eller ogiltighetsförklaring enligt 36 § AvtL som kan aktualiseras trots att införlivandet av villkoren i sig är giltig. Ett exempel på en central bestämmelse i annan lag är 3 § personuppgiftslagen som innebär ett ansvar att vid t.ex. point-and-click-förfaranden att samtycke till behandling av personuppgifter ska vara i form av en frivillig, särskild och otvetydig viljeyttring. Det är därför viktigt att uppmärksamma motparten på att godkännandet av standardvillkor inkluderar ett samtycke till personuppgiftsbehandling före avtalsslutet.<sup>207</sup> Ett problem med point-and-click-avtal som kan uppkomma i bevishänseende är att många företag ofta justerar sina standardvillkor efter hand och att företagen då har bevisbördan för dels att villkoren godkänts av motparten, dels vilken version som godkänts.<sup>208</sup>

## 6.3 Acceptfrist

Som ovan framkommit krävs att en accept av ett anbud lämnas inom acceptfristen för att avtalet ska bli ömsesidigt bindande. När en part lämnar ett anbud genom brev eller telegram och inget annat angetts blir det den legala acceptfristen i 3 § 1 st. AvtL som ligger till grund för beräkningen. Beträffande elektroniska kommunikationsmedel såsom telefax, e-post, eller EDI-instruktioner är det antagligt att samma regel är tillämplig på dessa. Liksom det finns skillnader i fördröjning vid avsändandet av ett anbud i brev jämfört med muntliga anbud finns det skillnader i elektronisk vid kommunikationsmedel. Som exempel sker anbud genom e-post med viss fördröjning till skillnad från kommunikation i realtid där parterna är direktuppkopplade med varandra såsom vid chatt där den text som skrivs visas omedelbart för motparten.<sup>209</sup> Vid sistnämnda kommunikationsform är uppfattningen att dessa måste antas direkt liksom muntliga anbud.<sup>210</sup> Acceptfristens längd utgår som ovan nämnts från att ge motparten skälig

---

<sup>205</sup> Point-and-click innebär att användaren måste godkänna leverantörens villkor genom att klicka i en ruta före avtalsslut. Click-wrap innebär att standardiserade licensvillkor presenteras efter avtalsslut när en produkt eller tjänst ska användas. T.ex. vid installation av ett datorprogram då licensvillkoren måste godkännas för att kunna använda programmet. Se vidare Roos, Fredrik, Standardavtal i elektronisk miljö, s. 48 ff. I: Elektronisk signering – En antologi.

<sup>206</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, 74., se även Roos, Fredrik, Standardavtal i elektronisk miljö, s. 51. I: Elektronisk signering – En antologi.

<sup>207</sup> Roos, Fredrik, Standardavtal i elektronisk miljö, s. 45 ff.,

<sup>208</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 75, och Roos, Fredrik, Standardavtal i elektronisk miljö, s. 52.

<sup>209</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 46.

<sup>210</sup> SOU 1996:40 s. 128.

betänketid. Detta innefattar även den tid det tar att överföra ett meddelande vilket på 1900-talet tog betydligt längre tid än idag. Tidsfristen beror därför på avtalstyp, partsställning och övriga omständigheter. Något man bör vara medveten om när det gäller elektronisk kommunikation är att betänketiden reduceras i praktiken vilket beror på överföringstiden under vilken mottagaren inte kan utnyttja den korta betänketiden. Vid t.ex. avsändandet av vanlig post kan mottagaren ta del av betänketiden hela dagen från det att brevet anlant tills svaret måste postas. Vid elektronisk kommunikation bedöms betänketiden istället isolerat från överföringstiden vilket resulterar i en kortare betänketid. För EDI-kommunikation inom slutna system kan acceptfristen beräknas enligt med hjälp av EDI-programmets processtider. Det bästa för en anbudsgivare som vill ha längre betänketid är att uttryckligen ange denna acceptfrist. Acceptfristen kan även utsträckas genom partsbruk eller handelsbruk.<sup>211</sup>

En annan fråga är om mottagaren ska kunna välja att skicka accept genom ett långsammare medium än anbudsgivarens för att på så sätt vinna mer betänketid. Rimligen borde det inte vara så pga. anbudsgivarens ensidiga bundenhet och undvikandet av haltande rättsförhållanden. Även det faktum att den legala acceptfristen grundas på endast en presumtion om att anbudsgivaren anser sig vara bunden och att det är anbudsgivaren som väljer den kommunikationsteknik som denne vill utnyttja talar för denna ståndpunkt.<sup>212</sup>

Acceptfristen regleras även i 2 § AvtL där det anges att bindande avtal uppstår redan när accepten kommit mottagaren till handa. Anbudsgivaren behöver alltså inte ta del av accepten och kan på så vis inte undkomma bundenhet genom att hävda att accepten kommit för sent.<sup>213</sup> Ett brev anses vara mottagaren till handa då det avlämnas direkt till denne eller i dennes brevlåda.<sup>214</sup> För elektronisk kommunikation såsom e-post borde därför accepten anses vara anbudsgivaren till handa då meddelandet når dennes inkorg.<sup>215</sup> Genom loggning kan man fastställa den exakta tidpunkten för avsändandet av e-postmeddelandet vilken blir avgörande för beräkningen t.ex. vid transaktioner direkt mellan parterna. Mer oklar är situationer där anbudet finns lagrat i en databas och avges på användarens begäran. Det saknas då kunskap på förhand om vilka som blir anbudstagare och när. Det anses därför lämpligare att i sådana situationer ange en sista tidpunkt då accepten ska vara anbudsgivaren tillhanda än tillämpning av 2 § AvtL som mer grundar sig på direktkontakt mellan två parter vid kommunikation.<sup>216</sup>

Elektroniska avtal kan alltså beräknas enligt samma avtalsrättsliga principer som andra avtal. Däremot kan dessa medföra problem att säkra bevisning

---

<sup>211</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 46 ff.

<sup>212</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 48.

<sup>213</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 49.

<sup>214</sup> Grönfors/Dotevall, Avtalslagen en kommentar, fjärde upplagan, s. 76.

<sup>215</sup> SOU 1996:40 s. 125 f, se även Grönfors/Dotevall, Avtalslagen en kommentar, fjärde upplagan, s. 77 och Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 59.

<sup>216</sup> Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 59.

om när accepten kommit anbudsgivaren till handa. Nya metoder för säkring av bevis kan dock brukas vid elektroniska transaktioner genom t.ex. loggning av ut- och ingående transaktioner.<sup>217</sup>

## 6.4 Förklaringsmisstag

Förklaringsmisstag regleras i 32 § 1 st. AvtL och karaktäriseras av att rättshandlingen fått annat innehåll än det åsyftade.<sup>218</sup> Ett exempel på förklaringsmisstag utgörs av att anbudsgivaren tror sig ha angivit 1 000 kr i anbudet men pga. felaktigt tangentnedslag slagit in 100 kr istället. Det är ingen ovanlighet med den typen av misstag vid elektroniska transaktioner, dels pga. att det är lätt att slå fel, dels för att det kan brista i kontrollen av det avsända meddelandet. Samtidigt finns det möjligheter till kontroll inom IT-teknik utan motsvarighet vid vanlig pappersdokumenthantering. Exempelvis kan rimlighetskontroller införas innebärande att systemet kontrollfrågar användaren vid transaktioner över visst värde.<sup>219</sup>

Skulle ett förklaringsmisstag väl uppstå undgår anbudsgivaren bundenhet<sup>220</sup> av sin viljeförklaring förutsatt att tre omständigheter föreligger. Det ska för det första faktiskt föreligga ett förklaringsmisstag genom felskrivning, felsägning eller därmed jämförligt misstag. För att avgöra detta får domstolen inledningsvis fastställa det objektiva förklaringsinnehållet genom tolkning av viljeförklaringen som den faktiskt ser ut med beaktande av ordalydelsen och övriga omständigheter. Därefter beaktas även anbudsgivarens vilja vid undersökningen huruvida viljeförklaringens objektiva innehåll avviker från denna vilja där anbudsgivaren har bevisbördan för avvikelsen.<sup>221</sup> För det andra ska misstaget ha begåtts av den rättshandlande själv och inte någon som enbart överför viljeförklaringen då det i så fall istället föreligger förvanskning.<sup>222</sup> För det tredje ska motparten vara i ond tro angående misstaget innebärande att denne ska ha insett eller bort inse misstaget utifrån objektiva omständigheter.<sup>223</sup> Anbudsgivaren har bevisbördan även för den onda tron. Den onda tron tar i sammanhanget inte sikte på vad anbudsgivaren avsett utan enbart på att denne avsett annat än denne gett uttryck för.<sup>224</sup> Det viktigaste i regeln anses vara det i

---

<sup>217</sup> Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 61.

<sup>218</sup> Adlercreutz/Gorton, Avtalsrätt I, 13 upplagan, s. 272. En till förklaringsmisstag närliggande företeelse är motivvillfarelse som kännetecknas av att rättshandlingen fått rätt innehåll med den rättshandlande har påverkats av felaktig omständigheter som legat till grund för handlingen. Se Adlercreutz/Gorton, Avtalslagen I, 13 upplagan, s. 272 f.

<sup>219</sup> Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, IRI-rapport 1987:7, s. 67 f.

<sup>220</sup> Rättsföljder kan även bli omtolkning av innehållet och skadestånd upp till det begränsade kontraktsintresset, se Grönfors/Dotevall, Avtalslagen – En kommentar, 4 upplagan, s. 218 f.

<sup>221</sup> Grönfors/Dotevall, Avtalslagen – En kommentar, 4 upplagan, s. 215 ff., jfr Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 67 f.

<sup>222</sup> Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 67.

<sup>223</sup> Grönfors/Dotevall, Avtalslagen – En kommentar, 4 upplagan, s. 218., Jfr Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 67 f.

<sup>224</sup> Adlercreutz/Gorton, Avtalsrätt I, 13 upplagan, s. 275.

bestämmelsen uttalade motsatsslutet i godtrofallen att anbudsgivaren blir bunden. Bestämmelsen ger uttryck för tillitsprincipen som står i kontrast mot viljeprincipen. Skälen för regelns utformning var att det ansågs obilligt att helt avskära möjligheten att ta hänsyn till misstag där mottagaren var i god tro, särskilt vid benefika rättshandlingar.<sup>225</sup>

## 6.5 Förvanskning

I 32 § st. 2 AvtL regleras vad som gäller vid förvanskning eller befordringsfel vilket utgörs av fel där innehållet uttrycks annorlunda än anbudsgivaren åsyftat. I detta fall är felet istället beroende av transporten från anbudsgivaren, muntligen genom bud eller genom telegram, till mottagaren oberoende av parterna. Regeln ger uttryck för viljeprincipen och ger inget omedelbart godtrosskydd för mottagaren såsom vid förklaringsmisstag. För att anbudsgivaren ska undgå bundenhet krävs dock att denne reklamerar inom skälig tid efter det att denne fick kunskap om felet.<sup>226</sup> Skillnaden vid transport på elektronisk väg är att det inte finns någon ansvarig person bakom förvanskningen. Därför anses inte analogislut med bestämmelsen tillämplig utan istället bör 32 § 1 st. AvtL tillämpas i sådana fall innebärande att anbudsgivaren blir bunden av innehållet gentemot godtroende mottagare.<sup>227</sup> Ett annat argument för en sådan lösning är att eventuella förvanskningar är mer märkbara vid elektronisk kommunikation. Ett angivet förslag är att sanktionen i form av avtalsbundenhet enligt 32 § st. 1 AvtL bör ändras till skadeståndsskyldighet då mottagaren får ersättning till den del felet faktiskt orsakat denne skada.<sup>228</sup> 40 § 1 st. AvtL som nämnts i kap. 6.1 innebär ett undantag från huvudregeln att avsändaren står risken för att rättshandlingen inte framkommit som avsett. Bestämmelsen anger istället att mottagaren står risken för reklamationer vilket grundas på att avsändandet av sådana meddelanden ligger i mottagarens intresse. I SOU 1996:40 föreslogs ett tillägg till bestämmelsen rörande förvanskningar av reklamationsmeddelanden av olika slag så att mottagaren står risken även för dessa. Det skulle då innebära ett undantag från 32 § 1 st. AvtL.<sup>229</sup> Kritik har riktats mot förslaget då det skulle innebära en onödig komplikation lagtekniskt med e contrarioslut i både 40 § och 32 § 1 st. AvtL.<sup>230</sup>

---

<sup>225</sup> Grönfors/Dotevall, Avtalslagen – En kommentar, s. 214 f., och 218. Samt Adlercreutz/Gorton, Avtalslagen I, 13 upplagan, s. 275 ff.

<sup>226</sup> Adlercreutz/Gorton, Avtalslagen I, 13 upplagan, s. 278 f.

<sup>227</sup> Grönfors/Dotevall, Avtalslagen – En kommentar, 4 upplagan, s. 221 f., samt Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, s. 68 f.

<sup>228</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 54 ff.

<sup>229</sup> SOU 1996:40 s. 133 f.

<sup>230</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 56 f.

## 6.6 Återkallelse

Enligt 7 § AvtL kan ett anbud återkallas fram till tidpunkten där mottagaren tagit del av detta. Ifall anbudet bara är mottagaren till handa är det alltså fortfarande möjligt att återkalla detta. Bestämmelsen anses även vara tillämplig på anbud i elektronisk form där det går att åtskilja tidpunkten för när meddelandet är mottagaren till handa och när mottagaren tagit del av meddelandet, t.ex. e-post. Särskilt som det finns en stor risk att meddelanden på elektronisk väg avsänds felaktigt. Vissa problem angående bevisning föreligger dock då det är svårt att visa när mottagaren faktiskt tagit del av t.ex. ett e-postmeddelande i sin inkorg. Särskilt som det kan variera hur ofta en person avläser sina meddelanden. Därför har det föreslagits att bevisbördan som normalt åligger avsändaren inte bör vara alltför tung. Det anses vidare föreligga ett behov av att ovannämnda re integra-regeln i 39 § AvtL kan tillämpas på elektroniska meddelanden ifall de inte medför ekonomisk skada för mottagaren då risken ökar att avsändandet sker genom ett oavsiktligt musklick. En möjlighet till återkallelse föreligger dock inte för meddelanden i helautomatiska system.<sup>231</sup>

## 6.7 Sammanfattande slutsatser

Hur avtal som slutits på elektronisk väg ska definieras råder det som ovan framgått delade meningar om och att besvara frågan är inte okomplicerat. När nya mönster uppkommer i samhället tillkommer även nya problem med hur dessa ska passas in i ett gammalt mönster. Oavsett om elektroniska avtalsslut ska betraktas som en form av realhandlande som kräver ny lagstiftning eller passas in enligt modellen i AvtL kan det konstateras att bindande avtal kan uppkomma på elektronisk väg. Elektroniska underskrifter kan alltså vara bindande förutsatt att det inte är fråga om särskilda formföreskrifter såsom kravet på egenhändig namnteckning i vissa fall. Ett annat problem är sådana avtal innehållandes automatiska processer som saknar mänsklig inblandning med EDI-avtal, köp genom online-beställningar på Internet eller e-post från köparen som exempel. Frågan ställs ifall en viljeförklaring i traditionell subjektiv mening kan anses föreligga då en dator knappast kan anses ha en självständig vilja. Ett tänkbart sätt att se på saken är att viss mänsklig inblandning likväl förekommer genom programmeringen som ger ett indirekt uttryck för vilja. Det har även framförts att man kan se saken från ett mer objektivt synsätt kopplat till förklarings teorin där hela förfarings sättet syftar till att ingå en bindande förpliktelse varför man beaktar mer objektiva faktorer.

En annan närliggande diskussion utgörs av standardavtal på Internet genom t.ex. point-and-click eller click-wrap-avtal där. Standardiserade avtalsvillkor ska framgå för motparten innan avtalsslutet på ett sådant sätt så att denne

---

<sup>231</sup> Hultmark, Christina, Elektronisk handel och avtalsrätt, s. 60 ff.

haft möjlighet att ta del av dessa oavsett ifall motparten faktiskt gjort det eller ej. En viktig regel om standardavtal är vidare att oväntade villkor som exempelvis finns undan gömda eller på annat vis framstår som överraskande, eller särskilt betungande villkor såsom långtgående friskrivningsklausuler, måste framhållas särskilt för att kunna ingå i avtalet. Vid bedömningen om så är fallet beaktas partsställningen där näringsidkare har större ansvar att ta reda på innehållet än en konsument. Det finns goda möjligheter att framhålla sådana villkor på Internet genom att styra vad som visas på motpartens skärm. Det har dock inte ansetts böra ställas alltför höga krav på hur villkoren ska framställas då metoden för avtalsslut i så fall blir alltför komplicerad och tidskrävande. Centralt i sammanhanget är att villkoren trots korrekt införlivande kan bli ogiltigförklarade eller jämkade enligt 36 § AvtL. Beträffande t.ex. point-and-click-avtal finns det viktiga regler i andra lagar att ta hänsyn till, t.ex. 3 § personuppgiftslagen som innebär ett ansvar att samtycke till behandling av personuppgifter ska vara i form av en frivillig, särskild och otvetydig viljeyttring. Det är därför viktigt att uppmärksamma motparten på att godkännandet av standardvillkor även inkluderar ett samtycke till personuppgiftsbehandling före avtalsslutet.

Enligt 3 § AvtL är den legala acceptfristen för anbud genom brev eller telegram beroende av överföringstid, parternas ställning, avtalstyp m.m. Regeln är också tillämplig på elektronisk kommunikation såsom e-post men man bör vara medveten om att acceptfristen bedöms isolerat från överföringstiden varför anbudstagaren får kortare betänketid och bör istället vid behov se till att anbudet innehåller en längre frist. Acceptfristen kan också påverkas av partsbruk och handelsbruk. Elektronisk kommunikation i realtid såsom chatt betraktas som muntliga anbud som därmed ska antas direkt enligt 3 § 2 st. AvtL om inget annat avtalats. Anbudsmottagaren bedöms inte kunna styra acceptfristen genom att välja ett långsammare elektroniskt medium för svar vilket motiveras av bl.a. undvikande av haltande rättsförhållanden och att det är anbudsgivaren som väljer kommunikationsmedel och blir ensidigt bunden under acceptfristen.

Acceptfristen för brev och telegram regleras även i 2 § AvtL där det anges att det är tillräckligt att accepten ha kommit mottagaren till handa inom acceptfristen oavsett om denne tagit del av accepten eller ej. I annat fall skulle anbudsgivaren alltför ensidigt kunna styra ifall accepten inkommit inom acceptfristen. Regeln är också tillämplig på elektronisk kommunikation där accepten anses vara mottagaren till handa när det befinner sig inom den s kontrollsfär. E-post anses t.ex. anses kommit mottagaren till handa när meddelandet nått dennes inkorg även om det kan vara svårt att bevisa. Dock finns det möjlighet att genom loggning av in- och utgående transaktioner föra sådan bevisning. Vid avtal där anbudet finns lagrat i en databas passar 2 § AvtL mindre bra då den baserar sig mer på direktkontakt mellan parterna.

I övrigt gäller samma avtalsrättsliga principer för elektronisk kommunikation t.ex. genom e-post som för andra avtal angående acceptfrister.



Exempel på avtalsrättsliga problem vid bruk av elektroniska underskrifter är förklaringsmisstag som regleras i 32 § 1 st. AvtL då det inte är ovanligt med skrivfel inom elektronisk kommunikation. Dock kan kontroller för högre transaktioner införas vilket kan lösa problemet. Tillämpningen av 32 § 2 st. AvtL vid förvanskning är mer oklar vid elektroniska meddelanden. Dock är det svårt att undgå upptäckt av förvanskning av elektroniska meddelanden eftersom sådana förvanskningar normalt framgår tydligt. Analogisk tillämpning av regeln anses därför onödig för elektroniska meddelanden innebärande att avsändaren enligt 32 § 1 st. AvtL står risken även för förvanskningar av elektroniska meddelanden men det har föreslagits att sanktionen kan ändras från bundenhet till skadeståndsskyldighet. Ett annat förslag innebär en ändring av 40 § AvtL så att anbudsmottagaren står risken även vid förvanskningar av meddelanden som ligger i dennes intresse vilket kritiserats då det skulle innebära en komplicerad lagteknisk lösning med e contrarioslut i både 40 § och 32 § 1 st. AvtL. Ett annat problem gäller risken att elektroniska meddelanden avsänds av misstag vilket medför att återkallelse enligt 7 § AvtL borde tillämpas även på dessa meddelanden. Enligt 7 § AvtL får återkallelse göras ifall meddelandet är mottagaren till handa och denne ännu inte tagit del av meddelandet. Problem vid elektroniska meddelanden är att det kan vara svårt att bevisa när mottagaren av t.ex. ett e-postmeddelande faktiskt tagit del av meddelandet. Det har föreslagits att den bevisbörda som åvilar avsändaren därför inte bör vara alltför tung.

# 7 Rättsekonomiskt perspektiv

## 7.1 Inledning

I denna del syftar jag till att belysa de rättsekonomiska aspekterna av elektronisk kommunikation och elektroniska underskrifter. Nedan redogörs inledningsvis för ekonomernas teori om den perfekta marknaden. Därefter beskrivs några hinder för den ideala modellen som förekommer på verklighetens marknad och hur rättsregler och elektronisk kommunikation med en eventuell elektronisk underskrift kan undanröja dessa så att samhällets resurser används på ett optimalt sätt.

## 7.2 Mikroekonomins idealmodell

### 7.2.1 Inledning

Inom mikroekonomisk teori analyseras hur ekonomiska aktörer, individ som företag, gör sina val vilka styrs av behov och begränsningar i resurser. Då resurserna är begränsade tvingas konsumenter välja vad de vill konsumera och företagen vad de vill producera och i vilken mängd. Priset för en vara eller nytthet är en avgörande faktor där prisskillnader ger olika incitament för konsumtion eller produktion. Det pris som konsumenterna är villiga att betala för en vara styrs av dennas nytta, medan företagen kräver pris efter kostnader för producerandet. Mot denna bakgrund beskriver mikroekonomin samspelet mellan företag och konsumenter och vilka konsekvenserna blir för den ekonomiska effektiviteten i samhället. En central fråga är vidare hur nyttan som marknaden ger konsumenterna och den vinst marknaden ger företagen maximeras. Man talar här om ett optimalt resursutnyttjande ur effektivitetssynpunkt där samhällets begränsade resurser utnyttjas på optimalt sätt.<sup>232</sup>

### 7.2.2 Individers och företags rationella val

Individer inom mikroekonomin betraktas som rationella nyttomaximerare som alltid väljer det alternativ som maximerar deras nytta.<sup>233</sup> Denna deskriptiva teori om individen som en "economic man" beskriver deras beteende. Teorin innebär i korthet att individer i valsituationer väljer det alternativ som bäst tillfredsställer sina egna subjektiva preferenser av varor, resurser, möjligheter etc. som varierar i styrka beroende på hur stark individens önskan är och grad av tillfredsställelse när önskan uppfylls. Nyttan bestäms av antalet tillfredsställda preferenser samt dessas styrka i en preferensordning. Inom mikroekonomin används framförallt en s.k. ordinal

---

<sup>232</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 15 f.

<sup>233</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 16 ff., se även Skogh/Lane, Äganderätten i Sverige – En lärobok i rättsekonomi, andra upplagan, s. 51.

preferensordning vilket innebär att ingen hänsyn tas till hur mycket starkare preferensen är utan endast att den är starkare än en annan.<sup>234</sup>

Konsumenternas värderingar i valsituationer är beroende av viktiga villkor som individen måste uppfylla för att anses välja rationellt, fullständighet, reflexivitet och transitivitet. Kortfattat innebär dessa villkor att individen antas kunna jämföra alla olika typer av nyttigheter, värdera varje alternativ som likvärdigt med sig själv (en individs värderingar måste vara konsekventa) och värdera nyttigheter konsekvent (en individs värderingar måste vara konsekventa även i förhållande till en tredje nyttighet). Den mikroekonomiska teorins utgångspunkt är att villkoren är uppfyllda.<sup>235</sup>

Företagens val styrs av vinstmaximering. Optimal produktionsvolym innebär att den sist producerade enhetens marginalkostnad är densamma som marginalintäkten varför företagets beslut om produktionens storlek av nyttigheter är viktigt för att göra vinst.<sup>236</sup>

Som nämnts ovan är priset styrande för efterfrågan och utbud på marknaden vilket i korthet beror på individens och företags nytto- respektive vinstmaximerande vilja. Idealtillståndet på marknaden inom ekonomi beskrivs vanligen som att marknadsvikt föreligger, d.v.s. jämviktsläge av marknadskrafterna där marginalkostnaden<sup>237</sup> för producerandet av den sista enheten varor är lika med betalningsviljan för enheten i en skärningspunkt mellan utbud- och efterfrågekurvorna. Därmed är alla potentiella handelsvinster uttömda vilket innebär en allokativ effektivitet. Vidare föreligger perfekt konkurrens, se nedan, vilken är pareto-optimal. Detta grundas på det ekonomiska effektivitetsbegreppet där en vanlig typ är pareto-kriteriet som kortfattat innebär att detta är uppfyllt ifall en förändring innebär att ingen missgynnas av denna, åtminstone att en individ får det bättre utan att den andre får det sämre.<sup>238</sup> Pareto-optimalitet föreligger förenklat när ingen individ kan få det bättre utan att en annan individ får det sämre.<sup>239</sup>

---

<sup>234</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 16 ff.

<sup>235</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 19 ff.

<sup>236</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 38 ff.

<sup>237</sup> Begreppet marginalkostnad innebär något förenklat företagets positiva förändring av de totala intäkter som en producerad och såld vara ger. Se vidare Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 39 f.

<sup>238</sup> Ett annat vanligt kriterium är Kaldor-Hicks-kriteriet vilket uppfylls när en förändring medför att en individ eller flera får det bättre än vad övriga individer får det sämre. Således innebär bägge kriterierna att individerna totalt sett gynnas av en förändring. Se vidare Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 56., se även Skogh/Lane, Äganderätten i Sverige, andra upplagan, s. 55 ff.

<sup>239</sup> Dahlman, Christian m.fl.: Rättsekonomi – En introduktion, andra upplagan, s. 45 ff., se även Skogh/Lane, Äganderätten i Sverige, andra upplagan, s. 53.

## 7.2.3 Perfekt konkurrens

För att uppnå perfekt konkurrens på marknaden krävs att alla köpare har perfekt information om alla produkter, priser, kvaliteter m.m. samt att dessa handlar rationellt utifrån sin kunskap för att maximera sin nytta under budgetramarna. Likaså krävs att alla producenter har perfekt information för att kunna utforma produktionen på optimalt vis för vinstmaximering. Ingen konsument eller producent ska kunna påverka pris eller utbud på marknaden vilket kräver flertalet oberoende köpare och säljare av helt homogena varor med relativt små transaktioner på den totala marknaden. Tillträdet till och ut ur marknaden måste dessutom vara helt fritt. I en sådan perfekt konkurrens råder optimal allokativ effektivitet och produktionseffektivitet. Produktionseffektiviteten innebär att effektivt kombinera tillgängliga produktionsresurser och tillgänglig teknologi för att undvika att företag gör förluster och tvingas lämna marknaden. När resurserna i samhället på så vis används på ett optimalt sätt råder statisk effektivitet.<sup>240</sup>

Ett annat effektivitetsperspektiv än det statiska är dynamisk effektivitet. Detta innebär förenklat ett beaktande av kontinuerlig utveckling i form av förändringar och förbättringar av produkter och produktionsprocesser medförande bättre kvalitet, minskade kostnader, bredare sortiment och ett utbud som motsvarar konstant förändrade konsumentpreferenser. Det på senare tid uppmärksamade perspektivet saknar dock tydlig marknadsmodell men har visat stor möjlighet att öka samhällets välbefinnande.<sup>241</sup>

## 7.3 Hinder för idealmodellen

### 7.3.1 Transaktionskostnader

Ett problem för den ovan presenterade idealmodellen är transaktionskostnader som normalt delas in i tre kategorier. Den första kategorin avser kostnader för kontakt som kan uppstå för parterna då de inte känner varandra på förhand och därför måste vidta åtgärder, t.ex. genom en annons av varierande storlek och pris. Den andra kategorin är kostnader för avtalslut såsom förhandling om t.ex. pris, rättigheter och skyldigheter såsom tidpunkt för leverans, vem som står risken ifall varan skadas av transporten m.m. Förhandlingar kan ta tid och medföra kostnader, exempelvis i form av parternas anlitate jurister. Den tredje kategorin avser kostnader för kontroll och innebär pengar en part lägger ned för att erhålla de rättigheter som kontraktet medför, exempelvis i form av anlitate av inkassoföretag för att förmå köparen att betala enligt kontraktet. Problemet med transaktionskostnader är för det första att de minskar antalet transaktioner till nackdel för samhällets välbefinnande. För det andra att resultatet

---

<sup>240</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 143 ff., jfr Werin, Lars, Ekonomi och rättssystem, s. 96 ff.

<sup>241</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 149 ff.

av transaktioner inte alltid blir som förväntat innebärande att en part missgynnas och en minskning av välbefindandet i samhället uppstår.<sup>242</sup>

Rättsregler sänker transaktionsreglerna där förmögenhetsrätten utgör ett centralt regelverk. Obligationsrätten som exempel kan genom tydliga regler såsom, om avtals ingående, giltighet och riskfördelning, sänka transaktionskostnaderna då parterna slipper förhandla om detta. Exempel på detta är avtalslagens regler om anbud och accept, standardavtal eller 13 § köplagen som innebär att säljaren står risken för varan fram till tidpunkten för avlämnandet. En förutsättning för att dispositiva regler ska sänka transaktionskostnader är dock att de är tydliga och fördelar rättigheter och skyldigheter såsom parterna skulle ha gjort vid en förhandling. Annars kommer parterna troligen avtala bort regeln.<sup>243</sup>

Elektronisk kommunikation kan också sänka transaktionskostnader, dels genom att en stor mängd information kan överföras till en stor krets av personer till låg kostnad, dels genom att med datorers hjälp utföra pedagogiska uppgifter, såsom att genom frågor leda konsumenter till rätt informationskälla, som tidigare krävt en stor och personlig insats. Lagstiftningen kan skydda konsumenter och påverka transaktionskostnader. Samtidigt innebär denna påverkan endast att kostnaden flyttas till näringsidkaren vilket inte medför att kostnaderna minskas och kan resultera i högre priser eller minskad service vilket i slutändan drabbar konsumenten. Konsumenter kan på Internet få vägledning efter enskilda behov till den relativt låga kostnad det innebär att få tillgång till Internet. Genom denna minskade kostnad för kommunikation innebär detta en fördel för konsumenterna.<sup>244</sup>

### 7.3.2 Monopol och bristfällig information

Den perfekta konkurrens som ovan redogjorts för där ingen ska kunna påverka pris eller utbud på marknaden och perfekt information föreligger skiljer sig från den som råder på verklighetens marknad. Faktorer som inom ekonomin betraktas som hinder för perfekt konkurrens är olika monopolsituationer såsom rena monopol som ger företag ensamrätt för tillhandahållande av viss produkt eller tjänst, eller oligopol som är vanligare idag där ett litet antal företag genom beslut och strategier kan påverka marknaden. Även olika former av monopolistisk konkurrens föreligger till följd av att produkter inte är homogena genom olika fysiska attribut eller varierande uppskattning av olika märken från konsumenter. Det förekommer även hinder i form av monopolliknande beteenden genom

---

<sup>242</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 83 ff., Se även Skogh, Göran, & Lane, Jan-Erik (nedan Skogh/Lane), Åganderätten i Sverige – En lärobok i rättsekonomi, andra upplagan, 58 ff.

<sup>243</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 83 ff., samt 90 ff.

<sup>244</sup> Hultmark, Christina, "Konsumentskydd på Internet – rättsekonomiska synpunkter", s. 80 f. I: *Juridisk Tidskrift*, Nr. 1 1998/99, s. 876 ff.

företags samverkan som exempelvis vid karteller där företagen kan påverka marknadsvillkoren så att en monopolliknande situation uppkommer. Ett annat hinder är bristfällig information. Konkurrensrätten är ett medel som främjar en fungerande konkurrens på marknaderna genom att motverka ovannämnda skadliga beteenden. Konkurrensrätten kan sägas verka dels för allokativ effektivitet och produktionseffektivitet där handel och produktion optimeras genom konkurrensutsatta marknader, dels för teknologisk utveckling eller innovationseffektivitet vilket medför en stärkt konkurrens då det blir nödvändigt att erbjuda de bästa produkterna.<sup>245</sup>

Som framkommit ovan kan elektronisk kommunikation på Internet förbättra informationsspridning till olika kretsar innebärande att konsumenter får bättre uppfattning kring tillgängliga alternativ på marknaden till lägre kostnader. Mer komplicerade produkter, såsom läkemedel, kräver mer utrymme i reklam än exempelvis blöjor. Genom mer utrymme för information på Internet och större spridning till konsumenter förbättras möjligheten för dessa att jämföra produkter och fatta riktiga beslut. Vidare ges konsumenterna ökade möjligheter att sprida information kring oseriösa näringsidkare genom Internet och därigenom nå ut till en betydligt större krets samt till en lägre kostnad.<sup>246</sup>

## 7.4 Sammanfattande slutsatser

Mot bakgrund av det ovanstående kan det konstateras att rättsregler på olika sätt kan förbättra marknaden ur ett rättsekonomiskt perspektiv, kanske framförallt genom sänkta transaktionskostnader där obligationsrätten är central och konkurrensrätten som främjar konkurrensen. Vidare finns rättsekonomiska fördelar med att utforma rättsregler som främjar elektronisk kommunikation. För det första kan konsumenter och säljare komma i kontakt på Internet vilket också sänker transaktionskostnaderna då parterna slipper vidta mer kostsamma åtgärder genom annonser, resande m.m. Detsamma gäller informationspridning på både konsument- och säljarsidan där konsumenter t.ex. kan varna för oseriösa näringsidkare samtidigt som mer information kring produkter, tjänster m.m. och villkoren för dessa tillgängliggörs på Internet. På så vis når näringsidkare ut till en större krets till en lägre kostnad vilket dessutom innebär visst skydd för konsumenten som får mer information. En annan positiv konsekvens av detta är att transaktionerna rimligen borde öka. Det blir billigare för säljaren att annonsera och nå ut till fler och köparen lockas av lägre pris på produkten. Den elektroniska underskriften som kan användas bl.a. till att betala för en vara är viktigt i sammanhanget. Att med hjälp av rättsregler som syftar till att utforma standarder för elektroniska underskrifter och nyttjandet av dessa, kunna slippa förhandla och att på Internet kunna tillgodogöra sig relevant information om produkter och tjänster är mycket positivt ur ett rättsekonomiskt perspektiv. För att kunna fullborda ett köp direkt blir den

---

<sup>245</sup> Dahlman, Christian m.fl., Rättsekonomi – En introduktion, andra upplagan, s. 143 ff.

<sup>246</sup> Hultmark, JT 1:98/99 s. 80 f., samt 86 f.

elektroniska underskriften ett avgörande tekniskt hjälpmedel som förmodligen främjar transaktioner i samhället som görs på elektronisk väg. Detta eftersom incitamentet för näringsidkare att marknadsföra sig på Internet och konsumenters vilja att använda Internet som informationskälla ökar.

Det faktum att flertalet betalar sina räkningar elektroniskt istället för att gå till banken är också ett exempel på lägre transaktionskostnader genom färre kontor, mindre personal m.m. Samtidigt innebär detta vissa svårigheter för de som inte nyttjar elektroniska tjänster, t.ex. äldre personer. Totalt borde trots detta samhällets välbefinnande öka då övervägande delen av befolkningen idag betalar sina räkningar på mobilen eller liknande elektroniskt sätt.

Således ur ett konkurrensperspektiv är den elektroniska kommunikationen positiv då fler får tillträde till marknaden genom sänkta transaktionskostnader och möjligheten att nå ut till fler. Genom att information om företags olika produkter, tjänster m.m. tillgängliggörs i större utsträckning motverkas den bristfälliga information som utgör ett hinder mot perfekt konkurrens. Naturligtvis krävs att informationen överensstämmer med verkligheten. Skulle det exempelvis röra sig om läkemedel bör detta i högre grad kontrolleras än t.ex. mindre komplicerade produkter såsom blöjor. I takt med att informationssamhället ökar ställs också fler krav på konsumenten och säljaren.

Fördelen med eIDAS-förordningen är att denna utgör en tydligare, säkrare och mer enhetlig reglering på den inre marknaden. Därigenom sänks också transaktionskostnaderna p.g.a. den interoperabilitet och ömsesidigt erkännande av betrodda tjänster som förordningen syftar till att uppnå och ett ökat bruk av bl.a. elektroniska underskrifter.

# 8 Analys

## 8.1 Teknisk bakgrund till elektroniska underskrifter

I kap. 2 diskuterades den tekniska bakgrunden till elektroniska underskrifter. Huvudsakligen innebär denna teknik att viss information såsom t.ex. text, ljud eller bild kan signeras genom att datamängden förbehandlas med ett hashvärde vilket inte är omvändbart varvid information kan krypteras. Elektroniska underskrifter bygger på den assymetriska krypteringsmetoden innebärande att ett unikt nyckelpar bestående av en privat hemlig nyckel och en publik används för kryptering och dekryptering. Krypteringen syftar främst till att säkerställa konfidentialitet för viss information och dataintegritet så att det går att säkerställa att informationen inte ändrats. PKI utgör infrastrukturen för öppna nyckelsystem inom vilket en CA utfärdar elektroniska certifikat och ansvarar för dessa under dess giltighetstid. Certifikatet utgör signerad information om någons identitet, roll eller liknande.

## 8.2 Innebörden av EIDAS-förordningen för svensk rätt

Som framgick av kap. 3 är eIDAS-förordningen resultatet av ett omfattande utredningsarbete för att motverka interoperabilitet och fragmentering på den inre marknaden mellan medlemsländernas olika eID-system och betrodda tjänster. Genom en mer tydlig och enhetlig reglering med bl.a. ömsesidigt erkännande av sådana tjänster bedöms säkerheten och förtroendet för bl.a. elektroniska underskrifter öka. EIDAS-förordningen är teknikneutral liksom den tidigare regleringen i signaturdirektivet genom vilken signaturlagen implementerades. Förhoppningen är att den nya regleringen bättre ska kunna möta den snabba tekniska utvecklingen och den ökande globaliseringen som av kommissionen bedöms stärka rättssäkerheten, säkerheten och ett ökat förtroende. För att uppnå dessa ändamål ansågs en förordning som är direkt tillämplig vara den bästa lösningen och ansågs vara förenlig med proportionalitetsprincipen och subsidiaritetsprincipen.

Detta syfte framstår för mig som ett rimligt sätt att lösa den typ av problem som förekommer på den inre marknaden, eftersom direkt effekt är ett säkrare sätt att säkerställa harmonisering än nationell lagstiftning grundad på direktiv, särskilt som det finns fler lösningar kring elektroniska underskrifter. En annan sak är hur det ska fungera i praktiken. Det framstår som att bestämmelser i eIDAS-förordningen om t.ex. ömsesidigt erkännande av sådana medlemsländers eID-system som notifierats till kommissionen i enlighet med förordningen och betrodda tjänster såsom



kvalificerade elektroniska underskrifter ställer höga krav på medlemsländerna som avser att använda sådana elektroniska kommunikationsmedel på ett gränsöverskridande sätt. Det är i nuläget oklart i flera avseenden vilka standarder och tekniska specifikationer som kommer att användas men som anges i eIDAS-förordningens preambel tas hänsyn vid kommissionens arbete genom genomförandeakter till sådana standarder och tekniska specifikationer som redan utarbetats av framförallt standardiseringsorganen CEN, Etsi, ISO och ITU.

Tillämpningsområdet för eIDAS-förordningen är enligt art. 2 sådana system som medlemsstater anmält och tillhandahållare av betrodda tjänster såsom elektroniska underskrifter som är etablerade inom EU. Liksom tidigare reglering omfattas enbart öppna system av förordningen. En annan likhet är att förordningen inte heller påverkar nationell rätt eller unionsrätt angående frågor om ingående av avtal och giltigheten av dessa eller andra rättsliga eller förfarandemässiga skyldigheter i relation till formkrav. Detta innebär, liksom tidigare, att svensk rätt inte påverkas i större utsträckning av förordningen eftersom vi har få regler om formkrav samt våra principer om fri bevisvärdering och bevisprövning. Effekten av bestämmelsen om elektroniska underskrifters rättsverkan är liksom tidigare snarare inriktad på erkännande av utländska motsvarigheter på den inre marknaden.

Beträffande ovannämnda utrymme åt nationell lagstiftning att närmare reglera elektroniska underskrifters rättsverkan råder viss rättslig oklarhet för närvarande eftersom signaturlagen kommer att upphävas vilket bl.a. innebär att begreppet avancerad elektronisk signatur försvinner. Genom förordning eller lag måste vissa åtgärder vidtas för att t.ex. peka ut tillsynsmyndighet. Vidare krävs ändringar i de lagar som hänvisar till signaturlagen såsom lag om ekonomiska föreningar, bostadsrättslagen, konsumentkreditlagen m.m. Hur dessa ändringar kommer att se ut och innebära är i nuläget oklart men utredningar pågår och en departementspromemoria om dessa frågor är på väg. Som framkommit tidigare innebär 17 § signaturlagen att när det i lag eller annan författning krävs en egenhändig namnteckning eller motsvarande och elektroniska rutiner tillåts får det inte ställas högre krav på elektroniska underskrifter än att de ska vara kvalificerade. Att vi inte får ställa högre krav följer fortfarande av förordningen men den svenska regleringen försvinner med signaturlagen.

Bestämmelserna i förordningen om elektronisk identifiering kan sägas vara mer utformade att reparera eventuella skador i efterhand genom t.ex. skyldighet till incidentrapportering och skadeståndsansvar jämfört med bestämmelserna om betrodda tjänster i förordningens andra del som utöver incidentrapportering och skadeståndsskyldighet även reglerar tillsynsansvar på ett mer förebyggande sätt.

Regleringen av betrodda tjänster i eIDAS-förordningens andra del innefattar jämfört med signaturdirektivet fler elektroniska tjänster än enbart elektroniska underskrifter. Bestämmelserna om elektroniska underskrifter och deras rättsverkan har vidare förtydligats för att skapa rättssäkerhet vilket

enligt min mening är positivt då vi minskar oförutsebar rättstillämpning och säkerheten höjs. I övrigt anser jag inte att bestämmelsen om dessa underskrifter i art. 25 eIDAS-förordningen innebär någon större skillnad mot den tidigare i art. 5 signatordirektivet. Då den svenska rättsordningen innehåller tämligen få formkrav förblir alltså effekten inte särskilt stor vad gäller elektroniska underskrifters rättsverkan. Till följd av de fria bevisvärderings- och bevisprövningsprinciperna i den svenska rättsordningen är effekten om elektroniska underskrifters bevisverkan inte heller särskilt påtaglig. Däremot blir effekten större av att elektroniska underskrifter nu regleras i en förordning vilket jag ställer mig positiv till då regleringen blir mer enhetlig. Även säkerheten höjs genom denna enhetlighet då det blir tydligare för de som tillhandahåller sådana tjänster vilka krav som ställs på dessa och de avancerade eller kvalificerade elektroniska underskrifterna, anordningarna för skapandet av kvalificerade underskrifterna, de kvalificerade certifikaten m.m. Den närmare regleringen kring bestämmelserna om kvalificerade certifikat, anordningar för skapande av kvalificerade elektroniska underskrifter och kraven på dessa och valideringen av de kvalificerade elektroniska underskrifterna har inte förändrats väsentligt. En skillnad som framkommit tidigare om validering är dock att de tidigare rekommendationerna i signatordirektivets bilaga IV för säker signaturverifiering nu har införts som bindande valideringskrav. Detta borde öka rättssäkerheten och säkerheten då det blir tydligare vad som gäller. Kraven innebär att kvalificerade elektroniska underskrifters giltighet på olika sätt bekräftas vilket stärker förtroendet för underskrifterna. Dessutom har det införts regler om långsiktigt bevarande av kvalificerade elektroniska underskrifter vilket ytterligare motverkar missbruk av underskrifterna. Bestämmelser om krav för kvalificerade valideringstjänster och kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter har även införts som bl.a. innebär att endast kvalificerade tillhandahållare av betrodda tjänster får tillhandahålla sådana tjänster.

Jag ställer mig positiv till den digitala ambition som eIDAS-förordningen resulterat i. Det är viktigt att skapa tydliga regler som utövas likadant i samtliga medlemsländer och stärker säkerheten och därmed förtroendet för elektronisk handel och elektroniska underskrifter. En osäkerhet som kvarstår är hur vi ska klara av att uppnå kraven som ställs i förordningen på så kort tid. Rättsläget är också något oklart i nuläget beträffande svenska regler som kommer att bli resultatet av den nya förordningen.

### **8.3 Innebörden av elektroniska underskrifter för avtalsrätten**

Som tidigare konstaterats innebär dagens former för avtalslut betydande skillnader från 1900-talets då AvtL skrevs. Det finns dock inget som hindrar en tillämpning av AvtL även vid elektronisk signering. Tack vare lagens teknikneutrala utformning passar reglerna i 1 kap. om avtals ingående tämligen väl även i förhållande till elektroniska underskrifter. AvtL som

avser konsensualavtal innehåller alltså inga särskilda krav på hur avtal ingås som hindrar att elektroniska underskrifter kan få bindande verkan. Med beaktande av hur dagens samhälle ser ut vore motsatsen orimlig. Tekniken uppdateras kontinuerligt och bruket av elektroniska underskrifter bör inte bromsas av lagstiftning enbart grundat på sin elektroniska form. Jag håller med Christina Ramberg om att avsikten bakom en symbol med vilken man identifierar sig är viktigare än hur den kommer till uttryck. När det kommer till realavtal finns det som jag tidigare konstaterat inte heller något som hindrar bruket av elektroniska underskrifter men någon form av prestation krävs, vanligen tradition, varför bruk av elektronisk underskrift blir mindre aktuellt.

Beträffande formalavtal är det en allmänt rådande uppfattning att vid krav på egenhändig namnunderskrift måste det som utgångspunkt uttryckligen ges möjlighet i lag för att elektroniska underskrifter ska kunna leda till ett giltigt avtal. Detta har uttryckts i såväl lagförarbeten som i doktrin. På förvaltningsrättens område har detta framkommit i rättspraxis vilket talar för samma inställning inom detta område. Som tidigare nämnts ges i lag uttryckligen möjligheter att använda avancerade eller kvalificerade elektroniska underskrifter i t.ex. lagen om ekonomiska föreningar och bostadsrättslagen där huvudregeln är att elektroniska underskrifter kan användas vid krav på egenhändig namnunderskrift. Förekomsten av sådana bestämmelser är också något som talar för den ovan angivna inställningen. Undantaget i sistnämnda lag är beträffande överlåtelse av bostadsrätter. Det finns förhållandevis få formalavtal i den svenska rättsordningen, framförallt inom förmögenhetsrätten. Avsikten bakom sådana skriftlighetskrav såsom egenhändig underskrift är framförallt att uppmärksamma parterna på att dessa är på väg att ingå ett avtal som kräver viss varning eller eftertanke, exempelvis då det rör sig om större värden så som vid fastighetsöverlåtelser enligt 4 kap. 1 § JB. Detta kan jämföras med bestämmelsen om överlåtelse av bostadsrätter som också uppställer krav på skriftlig namnunderskrift. Som tidigare diskuterats har det i doktrin uppmärksammats att det görs en åtskillnad mellan överlåtelser och upplåtelser. Avtal om överlåtelse av t.ex. genom köp, byte eller gåva där äganderätten går över till en annan person kan anses vara särskilt skyddsvärda och kräver eftertanke. Beträffande upplåtelse genom hyra eller lån av bostadsrätt eller fastighet där äganderätten inte ändras utan endast innebär en nyttjanderätt till egendomen ifråga sänks graden av behov till eftertanke något vilket jag anser är en logisk följd av att sådana avtal normalt inte innebär en lika stor affär för parterna. Det rådande rättsläget om krav på uttrycklig möjlighet att använda elektroniska underskrifter vid krav på egenhändig underskrift kan förändras genom lagändring eller praxis. Beträffande tolkning av rättsregler instämmer jag i den tidigare nämnda funktionella ekvivalensprincipen om att en underskrift inte ska diskrimineras enbart pga. sin elektroniska form. Såsom Ramberg har framhållit ser man i svensk rättsordning vid lagtolkning huvudsakligen bakom ändamålet med en bestämmelse på t.ex. avtalsrättens område istället för strikt bokstavstolkning och man kan då överväga ifall ändamålet kan uppnås även genom t.ex. en elektronisk underskrift. Det

rådande rättsläget verkar likväl som att sådan tolkning inte kan ske vid skriftlighetskrav just på egenhändig underskrift.

Det är inte omöjligt att det i framtiden även är möjligt att underteckna fler formalavtal såsom vid fastighetsöverlåtelser såsom 4 kap. 1 § JB genom en elektronisk underskrift. I frågan om en eventuell framtida lagändring eller tolkning av 4 kap. 1 § JB kanske ett liknande tankesätt kan framhållas som den nyss nämnda om funktionell ekvivalens innebärande att vi kan undersöka ifall en elektronisk underskrift kan uppfylla de ovan angivna syften som skriftlighetskravet i bestämmelsen grundas på. Vi går mot en tid där tekniken ständigt utvecklas innebärande att säkerheten ökar även om kunskapen kring hur man genom hacking kan obehörigen utnyttja annans elektroniska underskrift också gör det. Säkerhetsfrågan är viktig och det gäller att tekniken används på rätt sätt för att skydda den elektroniska underskriften så att ingen obehörig kan bruka den. Tanken bakom kvalificerade elektroniska underskrifter är just att ge dessa ett högre mått av säkerhet och kanske vi i framtiden kan använda dessa underskrifter även vid fler formalavtal såsom det i 4 kap. 1 § JB vilket skulle öka effektiviteten. Dock tror jag inte att vi är redo för ett sådant steg ännu beträffande mer strikta formkrav såsom egenhändig underskrift i t.ex. 4 kap. 1 § JB eller 10 kap. 1 § ÄB. Men arbetet kring stärkandet av medvetenheten kring och förtroendet för elektroniska underskrifter tar oss ett steg i en sådan riktning. Jag är av åsikten att avtal om köp av en fastighet kan vara den enskildes största och viktigaste avtal i livet. Det kräver sålunda viss eftertanke och att det faktiskt kan vara positivt att det tar lite tid så att vederbörande hinner med i processen att fundera över sitt val. Vi går mot en tid där alltmer kan göras på Internet och risken kan vara att den här eftertanken försvinner i viss mån om lån, lagfartsansökan och parternas underskrifter görs utan närmare personlig kontakt. Samtidigt är det viktigt att inte hindra tekniken och kanske viss avvägning måste göras. Som diskuterats i samband med varningsfunktionen vid en egenhändig underskrift finns det även en sådan för elektroniska underskrifter. Som framkom i redogörelsen för hur man beträffande standardavtal på Internet på olika sätt kan framhålla särskilda villkor blir det uppenbart att man på samma sätt kan varna en undertecknande part att tänka över sitt beslut en extra gång. Det är en avgörande faktor enligt min mening för att det ska gå att sluta den här typen av avtal genom en elektronisk underskrift. Som också diskuterats är det också avgörande att bygga upp ett förtroende bland allmänheten för elektroniska underskrifter samt att säkerheten är tillräcklig hög. Att använda avancerade eller kvalificerade elektroniska underskrifter baserade på avancerade eller t.o.m. kvalificerade certifikat är ett sätt att säkerställa detta. För att ytterligare stärka säkerheten anser jag att biometriska metoder genom fingeravtryck, ansikte m.m. bör användas vid identifieringen.

En annan intressant fråga om formkrav är huruvida vittneskrav t.ex. i 10 kap. 1 § ÄB, skulle kunna uppfyllas genom elektroniska underskrifter. Som framkommit i kap. 4 är bevittning av egenhändiga underskrifter en garanti för underskriftens äkthet då underskrifter ibland har ett svagt bevisvärde. Ifall någon förnekar att denne undertecknat ett visst dokument styrks

underskriftens bevisvärde genom existensen av vittnen som garanterar att vederbörande har undertecknat handlingen. Elektroniska underskrifter i öppna nyckel-system kan också garantera äktheten på detta sätt vilket talar för att man kanske kan använda en elektronisk underskrift i bestämmelser som innehåller vittneskrav. Mot en sådan lösning talar att en obehörig kan få tag i den hemliga nyckeln och därför är det förmodligen bättre att införa en motsvarighet till bevitning på elektronisk väg. Det är enligt min mening viktigt att även här göra en avvägning av de motstående intressen som finns i frågan om att eventuellt tillåta elektroniska underskrifter uppfylla kraven på egenhändig underskrift och bevitning beträffande testamente och äktenskapsförord. Som framkommit tidigare kan elektroniska underskrifter också ha en bevisfunktion vilket är särskilt betydelsefullt i dessa sammanhang. Genom att låta vittnena personligen närvara vid undertecknandet av ett testamente eller äktenskapsförord kan fler omständigheter påtalas i efterhand, t.ex. om det förekom tvång eller det psykiska tillståndet hos parterna. Detta saknas vid en elektronisk bevitning. Samtidigt är det helt inte säkert att vittnena talar sanning. Något som talar för bevitning genom elektroniska underskrifter är att det kan bli säkrare ur bevisningssynpunkt avseende äkthet och identifiering förutsatt att dessa är av tillräckligt hög kvalitet.

För att kunna använda sig av elektroniska underskrifter är det viktigt att vissa andra förutsättningar föreligger för t.ex. elektronisk kommunikation och möjligheten till elektroniska avtal överhuvudtaget. Som framkom i kap. 6 råder det delade meningar kring hur den elektroniska viljeförklaringen ska tolkas i förhållande till AvtL, framförallt beträffande sådana avtalstyper med automatiska processer som saknar mänsklig inblandning såsom exempelvis EDI-avtal eller köp på Internet genom on-line-beställningar eller e-post från köparen. Det som komplicerar diskussionen är frågan om en dator kan anses ha en vilja. Dock kan jag instämma med Christina Rambergs tankegång att det är tanken bakom programmeringen som indirekt ger uttryck för en vilja. Den närmare definitionen kring hur denna ska förstås och tolkas i förhållande till AvtL:s anbud-acceptmodell är komplicerad. Som jag tidigare nämnt är det svårt att passa in nya mönster i gamla. Kanske finns ett behov av att kunna tolka sådana företeelser i mer objektiva former av den traditionellt sett subjektiva viljeförklaringen.

En närliggande diskussion föreligger angående standardavtal för köp av varor och tjänster på Internet. Dock har det konstaterats att det finns flera möjligheter att uppmärksamma en part om betungande eller oskäligen villkor på Internet. Används dessutom en elektronisk underskrift vid avtalsslut blir det en ytterligare säkerhetsåtgärd och uppmaning till eftertanke.

I kap. 6 diskuterades acceptfrister i relation till elektroniska underskrifter. Det kan konstateras mot bakgrund av denna diskussion att den legala acceptfristen som regleras i 3 § AvtL för anbud avgivna genom brev eller telegram även kan tillämpas på avtal genom elektronisk kommunikation om inget annat avtalats, t.ex. e-post eller EDI. Parterna bör dock vara medvetna om att betänketiden reduceras något för anbudsmottagaren jämfört med

bruket av mer traditionella metoder såsom avsändande av vanlig post. Det har framhållits att anbud inom elektronisk kommunikation som sker i realtid, t.ex. genom chatt, anses vara detsamma som muntliga anbud som således ska antas direkt om inget annat avtalats. Det har också framkommit att det bör anses vara anbudsgivaren som väljer det kommunikationsmedel som styr acceptfristen innebärande att acceptmottagaren inte kan välja ett långsammare kommunikationsmedel för att på så sätt förlänga sin betänketid. De skäl som framförts för detta antagande såsom anbudsgivarens ensidiga bundenhet och undvikandet av haltande rättsförhållanden framstår för mig som rimliga. Det hela skulle annars framstå som tämligen oseriöst och rättsosäkert ifall anbudsmottagaren ensidigt skulle kunna påverka tidsfristen på detta sätt.

Det har också påtalats att en accept enligt 2 § AvtL anses ha kommit in i tid ifall den är anbudsgivaren till handa inom acceptfristen, det krävs alltså inte att acceptmottagaren ska ha tagit del av accepten. Detta anses för brev och telegram vara när svaret inkommit antingen direkt till anbudsgivaren eller till dennes brevlåda. Inom elektronisk kommunikation gäller samma regel där accepten anses inkommen när den inkommit inom acceptmottagarens kontrollfär, t.ex. genom att e-posten kommit in till dennes inkorg. Vissa svårigheter med bevisning kan förekomma om när accepten kommit mottagaren till handa, men som tidigare angivits kan dessa lösas genom t.ex. möjligheten till loggning av ut-och ingående transaktioner. Mer komplicerat blir det när anbudet är lagrat i en databas och mottagaren inte är känd på förhand. Troligen lämpar sig inte 2 § AvtL för sådana avtalstyper då den baserar sig mer på direktkontakt mellan parterna genom telegram eller brev.

I övrigt kan det konstateras att elektroniska avtal där den elektroniska kommunikationen sker genom exempelvis e-post kan bedömas enligt samma avtalsrättsliga principer som gäller för andra avtal beträffande acceptfrister.

Det är inte ovanligt med förklaringsmisstag inom elektronisk kommunikation och elektroniska transaktioner regleras likadant som vanliga fysiska sådana enligt 32 § AvtL. Samtidigt finns fler kontrollmöjligheter vid elektroniska transaktioner, se närmare diskussionen i 6 kap. Partiell förvanskning är däremot mindre vanlig då motparten borde se tydligare i ett elektroniskt anbud att något blivit fel. Därför har inte 32 § 2 st. AvtL ansetts behövas tillämpas på elektronisk kommunikation. Därmed står avsändaren risken för förvanskningar enligt huvudregeln i 32 § 1 st. AvtL. Christina Rambergs förslag att ändra sanktionen från avtalsbundenhet till skadeståndsskyldighet är enligt min mening en rimlig lösning eftersom möjligheten som 32 § 2 st. erbjuder försvinner. Förslaget att införa ett tillägg till 40 § AvtL så att anbudsmottagaren står risken även vid förvanskningar av meddelanden som ligger i denne intresse har kritiserats då det skulle innebära e contrarioslut i både 40 § och 32 § 1 st. AvtL vilket är en onödigt komplicerad lösning. Jag håller med om kritiken och förespråkar också en mindre krånglig och mer lättförståelig lösning. Ett annat problem som diskuterades i kap. 6 är den stora risken att elektroniska meddelanden

avsänds av misstag och att 7 § AvtL om möjligheten till återkallelse ifall mottagaren ännu inte tagit del av anbudet också borde tillämpas på sådana meddelanden, exempelvis e-post. Problemet är åtskillnaden mellan tidpunkten där meddelanden är mottagaren till handa och när mottagaren faktiskt tagit del av meddelandet ifråga. Jag håller med om åsikten att IT-system i sig inte har någon självständig vilja varför jag inte heller anser att mottagaren ska anses ha tagit del av ett elektroniskt meddelande vid tidpunkten där meddelandet har mottagits. Det är dock som tidigare påtalats svårt att bevisa vid vilken tidpunkt mottagaren tagit del av meddelandet och vissa svårigheter föreligger i praktiken såsom hur ofta en person läser sina e-postmeddelanden. Därför anser även jag att bevisbördan inte bör vara alltför tung för avsändaren för vilken denna börda åvilar.

## **8.4 Elektroniska underskrifters funktioner jämfört med traditionella underskrifter**

I kap. 5 diskuterades elektroniska underskrifters förmåga att uppfylla den traditionella underskriftens funktioner vilka typiskt sett ansetts utgöras av en viljefunktion, varningsfunktion, identifieringsfunktion, äkthetsfunktion samt en bevisfunktion.

Genom viljefunktion uttrycks en vilja exempelvis att underteckna ett dokument och ger samtidigt en indikation om tillit till att vederbörande kan skriva under. Den privata nyckeln som bl.a. används vid bruket av en elektronisk underskrift har ansetts ge uttryck för en sådan vilja.

Varningsfunktionen diskuterades även ovan i kap. 8.3 ifråga om t.ex. fastighetsöverlåtelser där den kan anses vara särskilt betydelsefull. Syftet med en sådan funktion är som framkommit att varna en part som är på väg att ingå en rättshandling med vissa konsekvenser och underskriften varnar för att en bindande förpliktelse kan uppstå genom denna. Beträffande frågan om även en varningsfunktion bör tillmätas den elektroniska underskriften anser jag att detta är fullt möjligt. Som framkommit i diskussionen om standardavtal och möjligheten att uppmärksamma motparten på betungande eller oväntade villkor finns det även flertalet möjligheter att uppmärksamma den som är på väg att skriva under på elektronisk väg att en bindande förpliktelse är på väg att uppstå. Ett exempel där en elektronisk underskrift brukas är vid betalning av räkningar i mobilen där man vid betalningen får fram en textruta från BankID med texten "Jag skriver under" varpå undertecknaren får skriva in sin PIN-kod för att genomföra transaktionen. Det är enligt min mening ett exempel på en tydlig varningsfunktion. Som framhållit tidigare kan nya tekniska lösningar innebära att man kan varna användaren genom att man måste klicka sig förbi och särskilt godkänna särskilda villkor. En sådan lösning borde även kunna fungera i exemplet med mobilen där man t.ex. kanske införa kontrollfrågor i personens bankID. Dock utförs redan en sådan kontrollfråga på bankens app.

Den identifieringsfunktion som traditionella underskrifter har syftar till ange från vem underskriften härrör. Som framkommit tidigare kan även elektroniska underskrifter fylla en sådan funktion. Vid bruket av en tredje betrodd part, CA, kan säkerheten t.o.m. sägas vara högre för att säkerställa att det är rätt person som skrivit under. Men detta bygger som sagt på att ingen obehörig fått tag i nyckeln. Samtidigt kan en CA återkalla nycklar som utsatts för sådant missbruk. För traditionella underskrifter krävs för kontroll av identifikation antingen att jämföra underskriften med tidigare underskrifter från samma person (grafologi) eller att underskriften sker med en tredje part närvarande (bevitning) som kan intyga vederbörandes identitet. Därför kan det sägas vara smidigare och effektivare med den identitetskontroll som elektroniska underskrifter erbjuder.

Nära identifieringsfunktionen ligger den äkthetsfunktion som en traditionell underskrift erbjuder vilken innebär ett skydd mot manipulation av ett textinnehåll eller en underteckning. Som tidigare påpekats sammankopplar underskriften ett visst innehåll med namnteckningen och kopplar innehållet till den person som namnteckningen pekar ut varför personen som ska bindas till detta innehåll ska kunna identifieras. Tidigare diskuterades även de risker som finns med en traditionell underskrift vilka främst är att någon förfalskar namnteckningen vilket försvåras av att personer kan ha nästintill identiska namnteckningar. Möjligheten att upptäcka sådana förfalskningar varierar men oftast kan utredningar i efterhand ge goda resultat. I detta avseende skiljer sig denna underskrift från sigillet som saknar denna möjlighet. Även elektroniska underskrifter saknar den personlighet som en traditionell underskrift erbjuder. Samtidigt är elektroniska underskrifter knutna till det signerade meddelandet på sådant vis att manipulationer kan upptäckas i efterhand även för dessa. Detta bygger emellertid på att innehavaren av den privata nyckeln hemlighåller sin nyckel.

Vidare fyller traditionella underskrifter en bevisfunktion. Som framkom av kap. 5 innebär detta att sådana underskrifter vid behov kan användas som bevismedel, exempelvis för att styrka rättshandlingar. Detta bygger på de identifierings- och äkthetsfunktioner som den traditionella underskriften erbjuder. Som tidigare konstaterats, kan även elektroniska underskrifter erbjuda en sådan bevisfunktion. Den svenska rättsordningens principer om fri bevisprövning och bevisvärdering uppställer inga formella hinder för den elektroniska underskriftens möjlighet som bevismedel. Det har inte ansetts nödvändigt att tillämpa andra bevisbörderegler för elektroniska underskrifter än vad som gäller för traditionella underskrifter. Som tidigare diskuterats kan det till följd av elektroniska underskrifters särart anses vara påkallat med viss försiktighet innan dessa underskrifter tillmäts en avgörande betydelse som bevismedel. Samtidigt kan beaktas att det finns vissa krypteringsmetoder som är mycket svåra att dechiffrera vilka höjer säkerheten hos elektroniska underskrifter betydligt. Om det dessutom rör en elektronisk underskrift vars nyckelhantering anförtratts en betrodd tredje part, CA, kan dessutom den elektroniska underskriften vara säkrare än en traditionell underskrift. Den rutinmässiga identitetskontroll som görs mot bakgrund av avancerade eller kvalificerade elektroniska underskrifter är av



mycket hög kvalitet. Lika ofta kontrolleras inte fysiska underskrifter. Är det dessutom fråga om en kvalificerad elektronisk underskrift kan det konstateras att trovärdigheten hos denna är ännu större. Innebörden av att en elektronisk underskrift fyller en sådan funktion är dessutom att den är oavvislig, dvs. innehavaren kan inte förneka att denne undertecknat ett visst textinnehåll. En annan fördel som påtalats är att det under vissa förutsättningar går att spåra elektroniska underskrifter genom kontroll av tidpunkten för när den elektroniska underskriften av ett dokument skedde och se ifall denna använts vid andra tidpunkter.

## 8.5 Rättsekonomiska effekter

I kap. 7 behandlades de rättsekonomiska effekterna av elektronisk kommunikation med en eventuell elektronisk underskrifts rättsekonomiska effekter. Slutsatser som drogs av detta är bl.a. att elektronisk kommunikation innebär fördelar för rättsekonomi genom sänkta transaktionskostnader vilket minskar hindren för den perfekta konkurrensen. Skäl för detta är att det kan bli billigare för säljare och köpare att få kontakt på Internet då parterna slipper vidta andra dyrare åtgärder såsom annons eller resande. Även den informationsspridning till lägre kostnad och till en större krets som Internet innebär är positiv för båda sidor och sänker transaktionskostnader eftersom parterna slipper vidta andra åtgärder såsom fysisk annonsering eller kringresande. Samtidigt kvarstår vissa kostnader för utrustning och tillgång till Internet. Totalt sett blir det troligen ändå lägre kostnader med elektronisk kommunikation. Konsumenter får dessutom bättre information om produkter och tjänster samtidigt som de varnas för oseriösa näringsidkare. Näringsidkarnas fördel är att de når ut till fler om sina produkter och villkor och kan ingå avtal elektroniskt, t.ex. med en elektronisk underskrift. Transaktionerna i samhället borde vidare öka genom elektronisk kommunikation då fler får kontakt, marknadsföringen blir mer effektiv och transaktionskostnaderna sjunker. Den lägre kostnaden medför en möjlighet för säljaren att annonsera mer och medför lägre priser för varor och tjänster vilket lockar konsumenterna till köp.

Elektroniska underskrifters centrala roll i sammanhanget är att utgöra ett tekniskt hjälpmedel som möjliggör att köpet kan fullbordas direkt på Internet vilket hjälper till att öka transaktioner i samhället. Det har också konstaterats att fler kan betala sina räkningar genom en elektronisk underskrift istället för att gå till det lokala bankkontoret vilket medför lägre transaktionskostnader genom färre kontor, mindre personal m.m. Detta kan utgöra problem för de som inte utnyttjar elektroniska tjänster, såsom en del äldre personer. Övervägande delen brukar dock sådana tjänster varför välbefindandet totalt sett borde öka i samhället.

Ur ett konkurrensperspektiv är elektronisk kommunikation således positiv då fler får tillträde till marknaden genom sänkta transaktionskostnader och förbättrade marknadsföringsmöjligheter. Bristfällig information vilket utgör ett hinder mot perfekt konkurrens kan som ovan nämnts motverkas genom

elektronisk kommunikation såsom Internet. Det krävs dock att informationen som sprids är korrekt men även att den uppfattas korrekt av mottagaren. Man kan skilja mellan mer avancerade produkter såsom läkemedel som troligen regleras hårdare än t.ex. blöjor. Det ökande informationssamhället ställer högre krav på både konsumenter och näringsidkare. Men totalt sett finns det mot ovanstående diskussion viktiga fördelar med elektronisk kommunikation och elektroniska underskrifter ur en rättsekonomisk synvinkel.

Som framkom i kap. 7 anser jag att eIDAS-förordningen bidrar till sänkta transaktionskostnader och därmed även till perfekt konkurrens genom en mer tydlig, enhetlig och säker reglering som syftar till att motverka digitala hinder på den inre marknaden och bl.a. öka bruket av elektroniska underskrifter.

## **8.6 Avslutande ord**

Av det som framkommit i denna uppsats kan det konstateras att den nya tekniken som är under ständig utveckling medför mycket juridiskt arbete för att elektroniska tjänster såsom elektroniska underskrifter ska kunna användas och bli juridiskt giltiga. Den nya förordningen medför som konstaterats vissa oklarheter i nuläget men ambitionen att öka förtroendet och säkerheten kring bl.a. elektroniska underskrifter är mycket positiv. Det är som tidigare framhållits viktigt att motverka digitala hinder så att inte tekniken och utvecklingen av den digitala marknaden bromsas i onödan. Mycket arbete kvarstår för att alla medlemsländer som vill kunna bruka elektroniska underskrifter över gränserna på den inre marknaden och det är ännu något oklart exakt hur det ska gå till. Det återstår helt enkelt att se hur vi kommer att leva upp till kraven i förordningen och huruvida vi kommer att få till ett interoperabelt system inom EU. Med tanke på de följder som skapas både sett till enskilda konsumenter och näringsidkare och sett med ett övergripande rättsekonomiskt perspektiv, tror jag att drivkraften finns där för att arbetet ska lyckas trots allt.

# Käll- och litteraturförteckning

## **Offentligt tryck**

### *Propositioner*

Förslag till lag om avtal och andra rättshandlingar på förmögenhetsrättens område 1914

Regeringens proposition 1975/76:105 med förslag till ny arbetsrättsreform m.m.

Prop. 1999/2000:117 Lag om kvalificerade elektroniska signaturer m.m. [Prop. 1999/2000:117]

Prop. 2001/02:150 Lag om elektronisk handel och andra informationshällets tjänster m.m.

Prop. 2007/08:45 s. 60 Elektronisk ingivning för ekonomiska föreningar och vissa andra företag, m.m.

Prop. 2010/11:80 Ny lag om ackreditering och teknisk kontroll

### *Statens offentliga utredningar*

SOU 1996:40 Elektronisk dokumenthantering [SOU 1996:40]

SOU 2010:54 Förbättrad återbetalning av studieskulder [SOU 2010:54]

SOU 2015:18 Lösöre och registerpant [SOU 2015:18]

### *Departementsserie*

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

Ds 1999:73 Elektroniska signaturer

### *Promemorior*

Regeringskansliets faktapromemoria 2011/12:FPM162

Regeringskansliets rådspromemoria 2012-12-05

## **EU-rättsligt tryck**

### *Förslag*

Förslag till Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, KOM (2012) 238. slutlig [KOM (2012) 238 slutlig]

### *Resolutioner*

Europaparlamentets resolution av den 21 september 2010 om fullbordandet av den inre marknaden för e-handel, EUT C 50 E, 21.2.2012.

### *Meddelanden*

Europa 2020 - en strategi för smart och hållbar tillväxt för alla, KOM (2010) 2020

Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och regionkommittén, En digital agenda för Europa, KOM (2010) 245

Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och regionkommittén, Inre marknadsakten, Tolv åtgärder för att stimulera tillväxten och stärka förtroendet för inre marknaden "Gemensamma insatser för att skapa ny tillväxt", KOM (2011) 206 slutlig

Meddelande från kommissionen, En färdplan för stabilitet och tillväxt, KOM (2011) 669 slutlig

#### *Yttranden*

Yttrande från Europeiska ekonomiska och sociala kommittén om "Förslag till Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden" KOM (2012) 238 slutlig, (2012/C 351/16), EUT C 351/73

#### **Litteratur**

Adlercreutz, Axel och Gorton, Lars, Avtalsrätt I, 13 upplagan, Lund: Juristförlaget i Lund, 2011

Andersson, Helene, Holmquist, Jesper, Rütten, Sabine, Hur analyserar man äktheten av ett dokument?, I: Elektronisk signering – En antologi, Stockholm: Norstedts Juridik AB, 2013

Bengtsson, Bertil, telefonavtal och elektroniska avtal med konsumenter, I: Elektronisk signering – En antologi, Stockholm: Norstedts Juridik AB, 2013

Bengtsson, Henrik, Bevisbörda och beviskrav vid invändning om underskriftförfalskning, I: Elektronisk signering – En antologi, Stockholm: Norstedts Juridik AB, 2013

Bernitz, Ulf, Kjellgren, Anders, Europarättens grunder, fjärde upplagan, Stockholm: Norstedts Juridik AB, 2010

Dahlman, Christian, Glader, Marcus, Reidhav, David, Rättsekonomi – En introduktion, andra upplagan, Lund: Studentlitteratur, 2004

Grönfors, Kurt, Dotevall, Rolf, Avtalslagen – En kommentar, 4:e upplagan, Stockholm: Norstedts Juridik AB, 2010

Grönfors, Kurt, Avtalsgrundande rättsfakta, andra upplagan, Stockholm: Santerus förlag, 2013

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

Hultmark, Christina, Elektronisk handel och avtalsrätt, Stockholm: Norstedts juridik, 1998

Janson, Ingemar, Den elektroniska marknadsplatsen – Avtals-,köp-och bevisrättsliga aspekter, IRI-rapport 1997:1, Stockholm: Stockholms universitet, 1997

Karlgren, Hjalmar: *Avtalsrättsliga spørsmål*, andra upplagan, Stockholm: P.A. Norstedt & söners förlag, 1954

Kihlman, Jon, Formfrihet, formkrav och kvalificerade elektroniska signaturer, I: Elektronisk signering – En antologi, Stockholm: Norstedts juridik AB, 2013

Lindberg, Agne, Elektroniska originaldokument och elektronisk signatur, IRI-rapport 1987:7, Stockholm: Stockholms universitet, 1987

Lehrberg, Bert, Avtalsrättens grundelement, 2 upplagan, Stockholm: I.B.A. Institutet för Bank- och Affärsjuridik AB, 2006

Ramberg, Jan och Christina, Allmän avtalsrätt, nionde upplagan, Stockholm: Norstedts Juridik AB, 2014

Roos, Fredrik, Standardavtal i elektronisk miljö, I: Elektronisk signering – En antologi, Stockholm: Norstedts juridik AB, 2013

Skogh, Göran, Lane, Erik, Äganderätten i Sverige – En lärobok i rättsekonomi, andra upplagan, Stockholm: SNS Förlag, 2000

Werin, Lars, Ekonomi och rättssystem, Lund: LiberFörlag, 1982

Westregård, Annamaria, elektronisk avtalssignering och elektroniska handlingar inom arbetsrätten, I: Elektronisk signering – En antologi, Stockholm: Norstedts juridik AB, 2013

### **Periodiskt tryck**

Björling, ”För vilka avtal är anbudet bindande enligt avtalslagens första kapitel?”. I: *Svensk Juristtidning*, 1916 s. 353-362.

Heidbrink, Jakob, ”Avtals uppkomst – dags att se bortom avtalslagen”. I: *Svensk Juristtidning*, 2007 s. 673-708 [Heidbrink, SvJT 2007]

Olsson, Mårten, ”Ny förklaringsmodell för elektroniskt genererade avtal?”. I: *Juridisk Tidskrift*, Nr. 4 1997/98, s. 1292-1297 [Olsson, JT 4:97/98]

Hultmark, Christina, ”Konsumentskydd på Internet – rättsekonomiska synpunkter”. I: *Juridisk Tidskrift*, Nr. 1 1998/99, s. 876-886. [Hultmark, JT 1:98/99]

Sjöberg Magnusson, Cecilia, ”Lag om kvalificerade elektroniska signaturer – Ny lag men fortsatt behov av åtgärder”. I: *Juridisk Tidskrift*, Nr. 4 2000/01 s. 864-882

## **Myndighetspublikationer**

E-legitimation – en underutnyttjad resurs, RiR 2009:19, Stockholm:

Riksdagstryckeriet, 2009

Benjamin, Yousefi, Framställning och bevarande av elektroniska signaturer,

Riksarkivets rapport, 2014

## **Elektroniska källor**

Hanno Lindbom, Kristina, Cristvall, Peder, Jönsson, Camilla, Olofsson,

Kenneth, Öst, Fredrik, rapport från Post- och Telestyrelsen från den 30

januari 2004, rapportnummer PTS:ER, Hämtad den 28 januari 2015 från:

[https://www.pts.se/upload/Documents/SE/Anv\\_elektronisk\\_identifiering\\_signaturer\\_PTS\\_ER\\_2004-3.pdf](https://www.pts.se/upload/Documents/SE/Anv_elektronisk_identifiering_signaturer_PTS_ER_2004-3.pdf).

Post- och telestyrelsens delrapport: Användningen av elektronisk

identifiering – Hur ser marknaden ut och vilka hinder är hindren mot en

ökad användning, rapportnummer PTS-ER-2003:35, från den 19 september

2003. Hämtad den 28 januari 2015 från:

[https://www.pts.se/upload/Documents/SE/Delrapport\\_elektronisk\\_identifiering\\_0919.pdf](https://www.pts.se/upload/Documents/SE/Delrapport_elektronisk_identifiering_0919.pdf).

Furberg, Per, lagkommentaren till 1 § signaturlagen hämtad från Karnov  
den 25 maj 2015:

[http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/530811/elem/SFS2000-0832\\_K0\\_P1?versid=146-1-2005](http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/530811/elem/SFS2000-0832_K0_P1?versid=146-1-2005).

Furberg, Per, lagkommentaren till 3 § signaturlagen, hämtad från Karnov  
den 25 maj 2015:

[http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/530811/elem/SFS2000-0832\\_K0\\_P3?versid=146-1-2005](http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/530811/elem/SFS2000-0832_K0_P3?versid=146-1-2005).

Furberg, Per, lagkommentaren till 4 § signaturlagen. Hämtad från Karnov  
den 30 april 2015.

[http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/530811/elem/SFS2000-0832\\_K0\\_P4?versid=146-1-2005](http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/530811/elem/SFS2000-0832_K0_P4?versid=146-1-2005).

Furberg, Per, lagkommentaren till 17 § signaturlagen. Hämtad från Karnov  
den 25 maj 2015.

[http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/530811/1?frt=signaturlagen&hide\\_flash=1&page=1&rank=1&versid=146-1-2005#SFS2000-0832\\_K0\\_P16-annotations](http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/530811/1?frt=signaturlagen&hide_flash=1&page=1&rank=1&versid=146-1-2005#SFS2000-0832_K0_P16-annotations).

Cederstierna, Nils, lagkommentaren till 12 kap. 2 § 1 st. JB. Hämtad från  
Karnov den 25 maj 2015.

[http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/527712/elem/SFS1970-0994\\_K12\\_P2?versid=146-1-2005](http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/527712/elem/SFS1970-0994_K12_P2?versid=146-1-2005).

Dalekant, Per och Weihe, Anders, lagkommentaren till 23 § MBL. Hämtad  
från Karnov den 25 maj 2015.

[http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/528004/elem/SFS1976-0580\\_K0\\_P23?versid=146-1-2005](http://juridik.karnovgroup.se.ludwig.lub.lu.se/document/528004/elem/SFS1976-0580_K0_P23?versid=146-1-2005).

Computer Sweden, ordlista under öppna system, hämtat den 5 maj 2015 från: <http://cstjanster.idg.se/sprakwebben/ord.asp?ord=interoperabilitet>.

Definition hämtad från Computer Sweden, ordlista under smartkort, hämtat den 19 februari från: <http://cstjanster.idg.se/sprakwebben/ord.asp?ord=smartkort>.

Computer Sweden, ordlista under mjukt certifikat, hämtat den 19 februari från: <http://cstjanster.idg.se/sprakwebben/ord.asp?ord=mjukt%20certifikat>.

Computer Sweden, ordlista under assymetrisk kryptering, hämtat den 18 februari från: <http://cstjanster.idg.se/sprakwebben/ord.asp?ord=asymmetrisk%20kryptering>.

Computer Sweden, ordlista under certifikat, hämtat den 18 februari från: <http://cstjanster.idg.se/sprakwebben/ord.asp>.

Computer Swedens ordlista, under interoperabilitet, hämtat den 17 april från: <http://cstjanster.idg.se/sprakwebben/ord.asp>.

Computer Sweden, ordlista under token, hämtat den 13 maj 2015 från: <http://cstjanster.idg.se/sprakwebben/ord.asp>.

Definition av Post- och Telestyrelsen, hämtat den 19 februari från: <https://www.pts.se/sv/Om-PTS/>.

Tillhandahållare av kvalificerade elektroniska certifikat enligt Post- och Telestyrelsens hemsida. Hämtat den 29 april 2015 från: <http://www.pts.se/sv/Bransch/Internet/Elektroniska-signaturer/>.

# Rättsfallsförteckning

## *Högsta domstolen*

NJA 2008 s. 684

NJA 2008 s. 733

NJA 2010 s. 219

## *Hovrätt*

RH 2005:11 (I och II)

Svea Hovrätt, dom 2011-11-16, mål nr T6836-10

Svea Hovrätt, dom 2012-01-02, mål nr T 6564-11

Hovrätten för västra Sverige, dom 2012-10-10, mål nr T 2990-12

## *Högsta förvaltningsdomstolen*

RÅ 2002 not 206

## *Kammarrätt*

Kammarrätten i Göteborg, dom 2014-09-24, mål nr 3459-14

## *Arbetsdomstolen*

AD 1998 nr 96