INTERNATIONELLA HANDELSHÖGSKOLAN
HÖGSKOLAN I JÖNKÖPING

Elektronisk signatur

Hur säkra är elektroniska signaturer ur avtalsrättslig synpunkt?

Filosofie magisteruppsats inom avtalsrätt

Författare: Malin Levén

Handledare: Björn Westberg

Jönköping Juni 2005

JÖNKÖPING INTERNATIONAL BUSINESS SCHOOL
Jönköping University

Electronic signature

What kind of security can an electronic signature provide for according to contract law?

Master's thesis within contract law

Author: Malin Levén

Tutor: Björn Westberg

Jönköping June 2005

Magisteruppsats inom avtalsrätt

Titel:	**Elektronisk signatur – hur säkra är elektroniska signaturer ur avtalsrättslig synpunkt?**
Författare:	**Malin Levén**
Handledare:	**Björn Westberg**
Datum:	**2005-05-23**
Ämnesord	**Elektronisk signatur, digital signatur och avtalsrätt.**

Sammanfattning

Kommunikation mellan parter är en viktig process i ett avtalsförhållande. Denna kommunikation kan exempelvis bestå av ett handskrivet avtal eller ett avtal formulerat på elektronisk väg. Avtalslagen gör ingen skillnad mellan dessa. För att underlätta ingående av och pågående avtal finns möjligheten att använda standardavtal för såväl handskrivna som elektroniska. Ett avtal kan alltså formuleras utifrån ett standardavtal eller utifrån parternas viljor.

En elektronisk signatur ska säkerställa att elektroniskt överförd information inte har ändrats och för att identifiera informationens avsändare. Genom kryptering skyddas uppgifter i ett dokument mot obehörig åtkomst. Elektroniska signaturer kommer till genom användande av krypteringsteknik som delats upp i två grupper, symmetrisk och asymmetrisk kryptering. Denna kryptering kan sedan skyddas i ett ”smart kort” vilket fungerar ungefär som ett bankkort gör. Verifiering av ett dokument är lika viktigt som att kunna kryptera det. En tredje oberoende part kan anlitas av avtalsparterna. En sådan tredje part kan vara en myndighet eller ett företag som saknar intresse i den förmedlade informationen. Vem den oberoende parten är kan sedan styrkas i ett certifikat. Detta certifikat kan även innehålla detaljer om avsändaren för att styrka att denne är rätt part.

Existerande lagstiftning finns att tillgå eftersom avtalslagen är tillämplig på elektroniska avtal. Förutom avtalslagen har det tillkommit två EG-direktiv på området. De båda direktiven tillerkänner elektroniska avtal och signaturer samma rättsliga verkan som svensk avtalsrätt tillerkänner redan existerande avtalsformer, exempelvis handskrivna eller muntliga. Direktiven tillåter inga nationella lagar som försvårar eller förbjuder elektronisk kommunikation.

Master's Thesis in contract law

Title:	**Electronic signature – what kind of security can an electronic signature provide for according to contract law?**
Author:	**Malin Levén**
Tutor:	**Björn Westberg**
Date:	**2005-05-23**
Subject terms:	**Electronic signature, digital signature and contract law.**

Abstract

Communication between parties is an important process in their relationship that can be based on a contract. This communication can for exemple be composed by a handwritten contract or an electronic contract. Contract law makes no difference between these two forms. To create more favourble requierements for commencing a contract or an ongoing contract there are possibilities to use standard agreements. Therefore a contract can be based on the will of the parties or on a standard agreement.

En electronic signature shall secure that electronic transferred information has not been altered and also to identify the sender of the information. By way of encryption information in a document is guarded from unauthorized access. Electronic signatures are produced by using encryption technology which is devided into two groups, symmetrical and asymmetrical encryption. It is possible to secure this encryption in a "smart card" which functions like a charge card. To verify a signature is just as important as using encryption to secure information. A third party can be engaged by both parties. A company or a public authority can be engaged as long as they have no interest in the intermediary information. Who this third party is can be confirmed in a certificate. This certificate can also consist of details about the sender confirming that it is the right party.

Existing legislation is available since swedish contract law is applicable on electronic contracts and signatures. Two EC-directives concerning this area are also available for the parties to apply when using electronic contracts. Both directives are acknowledging electronic contracts and signatures the same legal effect as other form of contracts, like handwritten and oral ones. Further they do not accept national laws that are making it difficult or that are forbidding the use of electronic communication.

Innehåll

Förkortningslista iii

1 Inledning 1
1.1 Bakgrund 1
1.2 Syfte 1
1.3 Metod 2
1.4 Avgränsningar 3
1.5 Terminologi 3
1.6 Disposition 4

2 Avtal 5
2.1 Kommunikation mellan parter 5
2.2 Elektronisk kommunikation 5
2.3 Electronic Data Interchange 6
2.4 Accept av ett anbud 7
2.5 Olika avtalsformer 8
2.6 Sammanfattning 9

3 Elektronisk signaturs funktion 10
3.1 Varför elektronisk signatur? 10
3.2 Elektronisk signatur medelst kryptering 11
3.2.1 Symmetrisk kryptering 11
3.2.2 Asymmetrisk kryptering 12
3.3 ”Smarta kort” 13
3.4 Tillvägagångssätt för elektronisk signering 14
3.5 Sammanfattning 14

4 Verifiering av elektronisk signatur 16
4.1 Bakgrund 16
4.2 Betrodd Tredje Part 16
4.3 Certifikat 17
4.4 Sammanfattning 18

5 Skydd med hjälp av avtal och lagstiftning 20
5.1 Ansvarsfördelning 20
5.1.1 Mellan parter 20
5.1.2 Mellan CA och nyckelinnehavaren 21
5.1.3 Tredje man 21
5.2 Rättsligt skydd 22
5.3 Reglera elektronisk signatur i lag 22
5.4 Sammanfattning 23

6 EG-rätt och svensk rätt 25
6.1 EG-rätt 25
6.1.1 Direktiv 1999/93/EG 25
6.1.2 Direktiv 2000/31/EG 26
6.2 Svensk lagstiftning 27
6.3 Sammanfattning 28

7 Slutsatser 29
Referenslista..... 32
Bilaga 1 EDI-avtal 96 34
Bilaga 2 EDIS EDI-avtal 98..... 36
Bilaga 3 EDI-avtal 2004 36

Förkortningslista

ARN	Allmänna Reklamationsnämnden
Art.	Artikel
AvtL	Avtalslagen
BTP	Betrodd Tredje Part
CA	Certification Authority
DES	Data Encryption Standard
Ds	Departementsserien
EDI	Electronic Data Interchange
EDIS	Electronic Data Interchange-föreningen i Sverige
EG	Europeiska Gemenskapen
EID	Elektroniskt ID-kort
EU	Europeiska Unionen
IDEA	International Data Encryption Algorithm
Ibid.	*Ibidem* som är den latinska termen för ”se föregående”
IRI	Institutet för rättsinformatik
IT	Informationsteknik
Kap.	Kapitel
NJA	Nytt Juridiskt Arkiv
PIN	Personal Identification Number
PKI	Public Key Infrastructure
Prop.	Proposition
RSA	Rivest, Shamir och Adelman
SOU	Statens Offentliga Utredningar
TTP	Trusted Third Party

1 Inledning

1.1 Bakgrund

Avtal torde alltid ha varit en stor del av den rättsliga processen genom tiderna och avtalet får då användas som riktlinjen i ett förhållande där missförstånd uppstått. Exempelvis i ett förhållande där parterna ej uttryckligen beskrivit ansvarsförhållandet dem emellan, gåvobrev, övertagande av ett företag eller kvitto på ett köp som gjorts i ett visst varuhus är alla avtal som kan göras gällande gentemot motpart. Att kunna göra sin rätt gällande genom ett avtal är ett sätt att stärka sin rätt.

Informationsteknik (IT) är ett koncept som på mycket kort tid har blivit något alla tar del av. Användning av datorer tillhör numera vardag och alltfler tjänster utövas via Internet. Att utföra något via Internet går väldigt fort och utveckling av tekniken likaså. Utvecklingen av Internet gör att det i allt större utsträckning går att använda det för fler tjänster, som att betala sin deklaration, betala räkningar eller köpa varor. Det finns mycket som talar till fördel för användandet av Internet men för att det ska fungera både juridiskt och praktiskt bör hänsyn tas till ett flertal faktorer.

När elektronisk kommunikationsteknik används måste säkerheten stå i centrum precis som den gör när avtal ingås på ett mer traditionellt sätt. I Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område (AvtL) bekräftas detta redan i första paragrafen som säger att avtal ska vara bindande för den som avgivit anbud eller svar. Resterande paragrafer som följer behandlar exempelvis undantag när ett avtal är bindande, tidsfrister och inskränkningar. För att våga ingå avtal bör det finns någon rättslig grund att stå på och att parter via den kan styrka sin rätt att kräva att motparten agerar i enlighet med det avtal de kommit överens om.

I vissa situationer där avtal uppstår ska det signeras på något vis. När det gäller handskrivna avtal har parter sedan länge signerat med sin personliga namnteckning. Nu när elektronisk kommunikation blir ett allt vanligare medel för att uppnå avtal parter emellan har det börjat diskuteras andra sätt att sluta avtal än med handskriven signatur. Användningen av elektroniska dokument har intensifierats och därför har även tillämpningen av elektroniska signaturer tilltagit. Därmed ställs den juridiska aspekten i fokus. Avtalslagen har tillämpats i många år och kommer att tillämpas i många fler. Den är möjlig att tillämpa på de flesta situationer som rör avtal. Dock kan det krävas någon form av tillägg till avtalslagen för att kommunikation i andra former ska kunna tillmätas samma auktoritet som den handskrivna.

1.2 Syfte

Beträffande elektronisk signatur måste var och en försäkra sig om att det är lika säkert som att signera ett avtal med en handskriven namnteckning. Tanken med uppsatsen är att undersöka om elektroniska signaturer uppfyller detta och därmed kan användas inom avtalsrättens värld i samma utsträckning som den handskrivna. Genom utredningen i uppsatsen kommer det att klarläggas att det finns fler sätt att ingå avtal på än genom det handskrivna avtalet. Denna klarläggning är viktig att poängtera eftersom det är möjligheten att ingå avtal via elektronisk väg som står i centrum för uppsatsen förutom signeringen. Det kommer även att visas hur rättsläget skulle kunna lösas när nya former av kommunikation uppstår.

Valet av uppsatsämne beror på bristen av kunskap inom området, sett utifrån min egen erfarenhet och därför har bävan för att använda denna kommunikationsform uppstått. Den-

na inställning torde infinna sig hos fler än mig själv och därför anser jag att det finns ett intresse av att klargöra vad för sorts rättslig ställning elektronisk signatur har i jämförelse med handskriven signatur. Intresset för en utredning inom detta område torde finnas bland aktörer inom näringslivet som träffar avtal men även för privata aktörer som ingår avtalsförhållanden.

1.3 Metod

I uppsatsen används den rättsdogmatiska metoden. Utredning grundar sig därmed på lagtext, förarbeten, praxis och doktrin. Hierarkin av rättskällorna är ställd i den ordning jag skrivit dem. Primär rättskälla är lagstiftning och sekundära rättskällor är förarbeten, praxis och doktrin.

Eftersom lagstiftning är den primära rättskällan läggs mest vikt vid denna. Den lagstiftning som har studerats mest ingående är avtalslagen eftersom uppsatsen tar sikte på avtal och signaturer och för en diskussion ur en avtalsrättslig synpunkt. I och med inträdet i EU måste hänsyn även tas till EG-rättslig lagstiftning.[1] Utredningen fokuserar på två direktiv som är relevanta för utredningen. Dessa två är Direktiv 1999/93/EG om ett gemenskapsverk för elektroniska signaturer[2] och Direktiv 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden[3]. Genom implementering av EG-direktiven har det tillkommit en svensk lag, Lag (2000:832) om kvalificerade elektroniska signaturer. Ytterligare svensk rätt som använts är Jordabalken (1970:994). Jordabalken är medtagen för att visa vissa undantag.

För att förstå lagstiftningens syfte undersöktes vad som sägs i förarbetena. De förarbeten som använts i utredningen är en proposition[4], ett utskottsbetänkande från departementsserien[5] och en offentlig utredning[6].

Eftersom elektronisk handel är ett relativt nytt sätt att ingå avtal på existerar därmed inte alltför mycket praxis på området ännu. Ett avgörande från Allmänna Reklamationsnämnden torde kunna anses vara relevant. Det fastställer att störningar kan förekomma när parter nyttjar Internet. Jag diskuterar ett rättsfall och anledningen till att det är medtaget i uppsatsen beror på att det till viss del går att dra paralleller mellan uppsatsen och rättsfallet.

---

[1] Artikel (art.) 234 EG, EGT 2002 C 325/33.

[2] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 1999/93/EG av den 13 december 1999 om ett gemenskapsverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12, Celex 31999L0093).

[3] 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 (”Direktiv om elektronisk handel”) (EGT L 178, 17.7.2000, s. 1, Celex 32000L0031).

[4] Proposition 1999/2000:117.

[5] Ds 2001:13 E-handelsdirektivet – genomförande av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster.

[6] SOU 1996:40 Elektronisk dokumenthantering.

Den parallell som går att skönja är ansvaret som finns mellan olika parter och vad för sorts krav det kan ställas på parterna i vissa situationer.

För att få en helhetsbild av sakläget och vad andra författare anser har doktrin undersökts. Information har också hämtats från två rapporter som kommer från Institutet för rättsinformatik som skriver speciellt om elektronisk handel. Slutligen har viss information hämtats från Internetsidor som är relevanta för uppsatsen.

1.4 Avgränsningar

Det område som uppsatsen fokuserar kring är begränsat till att gälla enbart Sverige, den utveckling som skett här och de lagregler som är berörda. Det enda område som kommer att beröras är det avtalsrättsliga med hänsyn till både handskrivna och elektroniska avtal och deras signaturer.

Jag har inskränkt uppsatsen till att enbart redovisa ett modellavtal, EDI-avtalet[7], eftersom jag har avgränsat min uppsats att enbart gälla Sverige. Jag har även begränsat mig till vilken form av teknik som säkerställer den elektroniska signeringen, det vill säga kryptering. Min uppfattning efter att ha läst doktrin är att kryptering kan anses vara en teknik som verkar säker nog att beaktas och begagnas för att säkerställa elektroniska signaturer. För att visa vad för sorts säkerhet som råder kring kryptering har jag valt att avhandla ”smarta kort” som ett exempel på hur parterna kan gå tillväga för att skydda sig. Jag diskuterar inte internationella avtal och dess förhållanden ingående utan nämner dem enbart i två kapitel.

Anledningen till att jag har gjort just nyss nämnda begränsningar beror på att elektronisk signatur är i utvecklingsstadiet och därför uppstår det många frågor kring just säkerheten av att använda denna kommunikationsform. Att behandla alla former som finns tillgängliga elektronisk signatur skulle göra min uppsats alltför omfattande. Därför har jag valt det som verkar säkert, inte alltför komplicerat att använda och som är lättillgängligt.

I uppsatsen bland bilagorna finns tre olika standardavtal presenterade vilka är anpassade till elektroniska avtal. Anledningen till att just dessa tre är med är för att exemplifiera hur avtal skulle kunna formuleras. De avtal som är medtagna är från 1996, 1998 och 2004. Avtalet från 1996 är relevant för den litteratur informationen till uppsatsen hämtats från. 1998 anpassades avtalen till att även omfatta internationella ingåenden av avtal. Avtalet från 2004 är medtaget för att visa hur standardavtalen är utformade idag. Till bilagorna hör tekniska bilagor. Dessa har inte tagits med då tanken med bilagorna är att statuera exempel på hur sådana är utformade.

1.5 Terminologi

Genom hela uppsatsen använder jag uttrycket elektronisk signatur men vill uppmärksamma att det även går att använda uttrycket digital signatur. Att jag valt uttrycket elektronisk signatur beror på att det är så det tituleras i lagtext. Aversten använder uttrycket digital signatur i sin bok[8] vilken jag refererar till vid ett flertal tillfällen.

---

[7] Se bilaga 1 EDI-avtal 96 – meddelandeutväxlingsavtal.

[8] Aversten David Digitala signaturer och ansvarsproblem (1998).

Ett genomgående tema i uppsatsen är jämförelsen mellan handskrivna och elektroniska avtal. För att poängtera att det handskrivna avtalet har begagnats under en längre tid titulerar jag det handskrivna avtalet även som det traditionella avtalet. Jag har gjort samma bedömning vad gäller signaturerna, att poängtera att handskriven signatur begagnats under en längre tid än elektronisk genom att använda uttrycket traditionell signatur.

1.6 Disposition

För att förstå hela situationen kring en signatur inleder jag andra kapitlet med att klargöra hur ett avtal kommer till stånd. Jag diskuterar viljan att ingå avtal och hur parterna kommer överens om att avtal ingåtts när det gäller handskrivna avtal. Jag redovisar sedan avtals ingående när elektroniska avtal tillämpas. Jag avslutar första kapitlet med att diskutera accept av ett anbud och olika former av avtal. Tyngdpunkten i uppsatsen har jag lagt på resterande kapitel där jag avhandlar elektronisk signatur. Jag börjar med att redogöra för vad som åstadkoms med elektroniska signaturer och sedan redovisar jag olika sätt att säkerställa dessa. Därefter avhandlar jag hur elektroniska signaturer verifieras och vilket tillvägagångssätt som beaktas för att genomföra den på bästa säkra sätt. Jag fortsätter uppsatsen med att kartlägga rättsläget kring denna form av kommunikationsteknik för att sedan i näst sista kapitlet resonera kring den lagstiftning som finns i nuläget. I sista kapitlet sammanfattar jag vad jag kommit fram till i uppsatsen. Tre bilagor har tillförts uppsatsen efter sista kapitlet. Dessa tre är inte utformade likadant och detta beror på att avtalen från 96 och 2004 inte var korrekta efter införts i uppsatsmallen som jag använt för att skriva uppsatsen. Därför har jag egenhändigt skrivit in dem och det är anledningen till att avtalet från 98 skiljer sig från de andra två.

2 Avtal

2.1 Kommunikation mellan parter

Ett avtal uppstår genom att två parter erkänner sin vilja att ingå avtal. Problem kan uppstå om det föreligger skilda åsikter om ett avtal överhuvudtaget har uppkommit eller inte. Dessa problem uppstår eftersom det finns olika sätt att kommunicera med varandra.[9]

Olika former av kommunikation kan framträda på ett flertal olika sätt. 1§ 2st AvtL behandlar handelsbruk eller annan sedvänja och menar att dessa former av kommunikation ska efterlevas. I förarbetena till avtalslagen framställs sedvänja som gängse bruk och skick.[10] Störst betydelse inom handeln har den särskilda sedvänja som benämns handelsbruk.[11] Det rör sig om handelsbruk som är så allmänt utbredda och har iakttagits så länge att de har accepterats som en normal och riktig standard. Det är något som parterna på marknaden har att rätta sig efter. I fall som dessa kan beteenden få rättslig verkan. Om part i egenskap av köpare går på auktion så betyder en höjd hand i luften att denne vill bjuda på föremålet som visas. Ett handslag eller till och med en röksignal kan fungera som en viljeförklaring eller för att acceptera ett avtal.[12] I vissa fall där parter kommit överens om att ingå avtal ett antal gånger kan partsbruk uppstå.[13] Det vill säga att parterna har visat sin vilja att komma överens på ett sätt unikt för dem, en form av sedvänja. Att använda sig av elektronisk kommunikation vid viljeförklaring ter sig inte annorlunda än vad det gör när parter exempelvis tar i hand.[14]

När parter kommunicerar via elektroniska avtal gör de precis som när avtal ingås på papper. Anbud görs känt genom ett elektroniskt meddelande och därigenom visar part sina avsikter. Svar på ett anbud sker via samma kommunikationsform.

2.2 Elektronisk kommunikation

När det gäller mer inarbetade beteenden där sedvänja accepteras som normal standard får vissa beteenden rättsverkningar.[15] Elektronisk kommunikation har ej ännu använts i den utsträckningen att vissa beteenden kan anses ge rättsverkningar.[16] Parter som ingår avtal kan ännu inte lita till sedvänja på området. Detta kan ses som negativt eftersom sedvänja är ett

---

[9] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 23.

[10] Förarbeten till 1§ 2st som visar var handelsbruk och sedvänja har sitt ursprung ur har varit svårt att hitta. I Allmens och Eklunds bok Lagen om avtal och andra rättshandlingar på förmögenhetsrättens område (1960) sägs det ingenting om sedvänja. I Grönfors bok Avtalslagen (1995) finns det inte heller någon hänvisning till förarbeten. Dock skrivs det i Juridikens källmaterial, s.155, av Eek, Grönfors med flera att det finns förarbeten till avtalslagen. Efter genomfört en grundlig undersökning där svar ej funnits lämnas detta därhän nu med slutledning att det finns sedvänja som tydligen framställs som gängse bruk och skick enligt förarbetena till avtalslagen.

[11] Eek m.fl. Juridikens källmaterial (1979) s. 155.

[12] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 23.

[13] Eek m.fl. Juridikens källmaterial (1979) s. 155

[14] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 23.

[15] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 24.

[16] Ibid. s. 24.

ytterligare sätt för parterna att kunna styrka sin rätt i ett avtal. Det inger en slags trygghet att möjliggöra sin rätt på mer fler sätt än enbart genom att åberopa avtalslagen. Om nyttjandet av elektroniska avtal ökar kommer det att kunna urskönjas en sedvänja anpassad till denna form av kommunikation.

Om parterna ingått avtal tidigare och gjort detta elektroniskt kan det mellan parterna uppstå partsbruk som parterna kan stödja sig på.[17] Parterna kan i ett avtal komma överens om att all kommunikation ska ske via elektronisk kommunikation. Att kunna ha den friheten att ingå avtal så att det passar just de parter som är involverade gör att det finns möjlighet att kunna tillgodose alla parters önskan. Avtalsrättsligt sett uppstår inga problem då 1§ 2st AvtL fastslår att paragraferna i första kapitlet i avtalslagen är dispositiva. Parters avtal kan anta andra former än den som anges i 1§ 1st AvtL. Avtal har samma status oavsett vilken annan form parterna kommer överens om. Utformandet av avtal mellan parter är individuellt och det är upp till parterna hur de vill utforma det. Parter kan ännu inte lita till sedvänja när de använder elektroniska avtal och därför borde det finnas andra möjligheter som underlättar ett ingående av avtal. Denna möjlighet infinner sig när parterna kan använda sig av färdiga standardavtal.[18] Ett sådant skulle kunna vara ett EDI-avtal.

2.3 Electronic Data Interchange

Electronic Data Interchange förkortas EDI[19]och går ut på att parter kan utväxla affärsmeddelanden på ett standardiserat sätt.[20] Partena kan kommunicera med varandra automatiskt direkt från dator till dator genom att begagna standardiserade meddelanden.[21] . Denna form av standardavtal kan användas istället för pappersdokument när de exempelvis fakturerar eller gör inköpsorders.[22] En utbredning av EDI-avtal skulle göra att förtroendet för elektroniska avtal ökar i samma takt som användningen av avtalen. Ju mer avtalen används ju fortare kan en mer utpräglad sedvänja ta form. Eftersom avtalslagens första kapitel är dispositivt är det angeläget att EDI-avtal formas och därigenom kunna anses utgöra sedvänja. En stabil rättslig grund för elektroniska avtal skapas.

En form av EDI-avtal är så kallade slutna PKI-system[23]. Avtal kan ingås mellan parter om exempelvis hur de ska gå tillväga eller hur ansvaret ska fördelas om oklarheter under avtalstiden uppstår.[24] Då skapas en intressegemenskap inom vilken parterna använder elektroniska signaturer för särskilda ändamål som kommits överens om.

---

[17] Eek m.fl. Juridikens källmaterial (1979) s. 155.

[18] Tornéus Mats EDI-avtal – ett kommersiellt kommunikationsavtal för utväxling av elektroniska affärsmeddelanden (2001) s. 10.

[19] Se bilaga 1 EDI-avtal 96 – meddelandeutväxlingsavtal.

[20] Tornéus Mats EDI-avtal – ett kommersiellt kommunikationsavtal för utväxling av elektroniska affärsmeddelanden (2001) s. 10.

[21] Seipel Peter Juridik och IT- Introduktion till rättsinformatiken (1997) s. 174.

[22] Bidgoli Hossein Electronic Commerce Principles and Practice (2002) s.158.

[23] PKI står för Public Key Infrastructure. Public Key förklaras i avsnitt 3.2.2.

[24] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 45.

EDI-föreningen i Sverige, EDIS, har arbetat fram ett nytt svenskt standardavtal för EDI-kommunikation som går under benämningen EDIS EDI-avtal 98[25] och är en vidareutveckling av EDI-avtal 96.[26] Avtalet kan tillämpas oavsett bransch och till skillnad från sin föregångare är det möjligt att tillämpa det på såväl nationella som internationella EDI-transaktioner. Elektroniska avtal gör det möjligt att ingå avtal med parter över hela världen och till följd därav tillgång till en omfattande marknad. Med tanke på hur lätt det är att ingå avtal mellan parter över gränser är det viktigt att det finns standardavtal att tillgå som tar hänsyn till både nationella och internationella avtal. Ju mer utpräglat användandet av elektroniska avtal blir ju fler avtal kan komma att ingås elektroniskt. För att inte ställas inför ytterligare problem i en utveckling som går fort är det viktigt att avtal som EDIS EDI-avtal 98 arbetas fram och att den utvecklingen går hand i hand med elektronisk handel.

2.4 Accept av ett anbud

Avtalslagen reglerar hur lång acceptfrist parterna har i olika situationer, 3§ AvtL. I situationer som dessa tillgodoser avtalslagen möjligheten att tillämpa lagen på elektroniska avtal eftersom den inte specifikt uttalar att det gäller handskrivna avtal. Därför uppstår det inte problem rättsligt sett att tillämpa avtalslagen på elektroniska avtal. Att detta är möjligt är inte förvånande av den orsaken att det inte påträffas någon större skillnad mellan handskrivna och elektroniska avtal. Elektronisk kommunikation kan i vissa fall ske med fördröjning, exempelvis elektronisk post.[27] Under sådana omständigheter existerar acceptfristen som nämns i 3§ 1st AvtL.[28] Dock kan tiden mellan att ena parten skickar ett meddelande via elektronisk post fram till att det kommer den andra parten tillhanda vara kortare än när parterna skickar anbud och accept med reguljär postservice. Detta kan uppfattas såväl positivt som negativt. På samma gång som betänketiden är kortare är också tiden till att avtal är ingånget kortare, vilket kan vara till fördel i många situationer. En sådan situation kan vara ett köp som rör valuta där dagens valuta kan vara det som gör avgör om det blir någon affär mellan parterna eller inte. I situationer som dessa är det enbart till fördel att avtalslagen gör det möjligt för parterna att faktiskt välja vilken kommunikationsform som är bäst lämpad. I situationer där det ska gå fort kan elektronisk kommunikation där parterna talar direkt med varandra via datorer vara mer lämplig än ett avtal som skickas via reguljär postservice. Däremot är det annorlunda i situationer där parter är direkt uppkopplade via datorer till varandra. Då liknar avtalet mer ett muntligt sådant och då löper ingen acceptfrist, 3§ 2st AvtL.[29]

Både anbud och accept kan återkallas trots att det kommit mottagaren tillhanda med reservation för att denne ännu inte tagit del av det, 7§ AvtL. När det gäller elektronisk kommunikation där tidpunkterna för kommit tillhanda och tagit del av inte sammanfaller torde det

---

[25] Se bilaga EDIS-EDI-avtal 98 – elektroniska meddelandeutväxling.

[26] Tornéus Mats EDI-avtal - ett kommersiellt kommunikationsavtal för utväxling av elektroniska affärsmeddelanden (2001) s. 72.

[27] Ibid. s. 72.

[28] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 46.

[29] Ibid. s. 46.

finnas utrymme för återkallelse.[30] Genom att skicka anbud och accept via elektronisk post uppstår möjligheten för parterna att återkalla ett anbud eller accept.

2.5 Olika avtalsformer

I enlighet med 1§ AvtL blir avtal bindande genom anbud och accept, dock med undantag[31] för avtal som det ställs formkrav på, 1§ 3st AvtL. Att ett avtal som finns nedskrivet alltid är säkrare än ett muntligt torde vara klart sett ur alla perspektiv. Bevismässigt sett är det absolut det mest fördelaktiga men även avtalsmässigt sett måste det ses som det mest fördelaktiga sättet att gå tillväga. Om det finns ett skriftligt avtal att tillgå är det lättare att styrka sin rätt och visa att det aktuella avtalet eller ett villkor som ena parten gör gällande verkligen existerar. Avtal där muntligt löfte ges i en situation där enbart parterna finns närvarande uppnår inte samma bevisstyrka. Detta beroende på att enbart de involverade parterna kan styrka det de själva eller den andra har sagt.

Formkrav kan verka i förebyggande syfte och även i ett avskräckande sådant.[32] Att avtala om något skriftligt gör att parter blir medvetna om konsekvenserna av sin förpliktelse. I fall där parter är medvetna om konsekvenserna av ett avtal minskar även riskerna för framtida missförstånd om vad avtalet egentligen reglerar. Upprättelse av avtal ger också parterna möjlighet att in i detalj tillgodose alla deras behov. Om avtal inte upprättas kan det i vissa fall vara omöjligt att göra dessa behov gällande gentemot den andra parten.

Det torde tala till parternas fördel att de kan komma överens i avtal hur framtida dispositioner ska göras innan ett affärsförhållande upprättas. Att inte komma överens i avtal skulle kunna leda till att det uppstår villfarelser som rör avtalets villkor. Därigenom riskerar parterna avtalet och det de vill uppnå med det. Eftersom det inte är möjligt att reglera alla situationer genom att tillämpa avtalslagen bör avtalet i sig vara så pass detaljerat som det är möjligt och på samma gång tillfredställa de krav parterna ställer på avtalet. Det bör också tas hänsyn till vad för sorts krav på flexibilitet som parterna ställer på avtalet. Om avtalet berör exempelvis en bransch som kräver att avtal kan anpassas med kortare intervaller, är det kanske inte lika intressant för parterna att ha ett avtal som är alltför detaljerat. En sådan bransch skulle kunna vara transportbranschen där situationen kan förändras under tiden varor transporteras. Om inget avtal kommer till stånd kommer tolkning av avtalet att tillämpas och därmed blir de allmänna reglerna i avtalslagen gällande.

Viss verksamhet som tillhandahåller varor och tjänster via en hemsida på Internet använder sig av elektroniska avtal, så kallade ”point-and-click-contracts”. Avtalets villkor där tillhandahållaren binder sin motpart finns tillgängliga på hemsidan och visas i samband med att en beställning görs.[33] Vanligtvis kommer part inte vidare utan att först godkänna de villkor som tillhandahållaren ställer. Att inte kunna ta sig vidare utan att först godkänna villkoren är en lämplig funktion antaget att parten läser igenom villkoren. Ansvaret att läsa villkoren åligger parten som ska anta villkoren. Om detta inte fullgörs och avtal sedan ingås, bör parten som godkände avtalet själv stå för följderna. Det finns risk för att tillhandahållaren av hemsidan tillgodoskriver sig långtgående friskrivningar genom dessa avtal. För att åstad-

[30] Adlercreutz Axel Avtalsrätt I (2002) s. 61.

[31] Se avsnitt 6.2.

[32] Se exempelvis Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 66.

[33] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 72.

komma någon form av skydd tar 33§ AvtL sikte på omständigheterna kring avtalets tillkomst och strider dessa mot tro och heder får avtalet ej göras gällande gentemot den som rättshandlingen företogs. I 36§ AvtL finns ett skyddsnät för villkor som anses oskäliga med hänsyn till avtalets innehåll. Med hjälp av paragrafen kan villkoren i avtalet antingen jämkas eller lämnas utan avseende i sin helhet. 36§ 2st AvtL erbjuder även skydd för konsument eller eljest som intar en underlägsen ställning. Att känna en så pass stark trygghet som detta innebär skulle kunna vara ett avgörande element när parter ingår avtal. Om trygghetskänslan inte infinner sig finns det risk att avtal aldrig kommer till stånd. I och med att avtalslagen inte specifikt uttalar vad för avtal det gäller, torde den även vara tillämplig på elektroniska avtal.

2.6 Sammanfattning

För att ingå avtal måste viljan mellan två parter finnas. För att informera en part om att viljan finns måste de hitta ett sätt att kommunicera på. I dagsläget torde det vara så att elektroniska avtal inte praktiseras i den utsträckningen att parter är fullständigt medvetna om hur rättsläget ser ut. Enligt avtalslagen ställs inga krav på hur avtal ska se ut förutom vissa undantag.[34] Därför är det fullt möjligt att tillämpa avtalslagen på elektroniska avtal vad gäller kommunikation mellan parter, accepterande av avtal och återkallelse av sådana.

Avtal som existerar i skriftlig form är säkrare då det oftast är klart uttryckt vilka förutsättningar som ställs för just den speciella situationen. Ju mer säkerhet parterna vill ha för att känna tillit desto mer bör de ta med i avtalet. Å andra sidan kan ett avtal där parterna garderat sig fullt ut förlora sin flexibilitet. Ett avtal som är flexibelt kan i vissa situationer vara lika viktigt som att det ska känns säkert. Flexibilitet kan vara till fördel i omgivningar där beslut måste tas snabbt och avtal måste omarbetas för att stämma överens med hur situationen ser ut dagen därpå. Det spelar dock ingen roll om avtalet gestaltas på papper eller i elektronisk form. I båda fallen inträder möjligheten att använda standardavtal om parterna anser sig behjälpliga av ett sådant.

Att komma så pass långt i utvecklingen att övervägande antalet avtal görs via elektronisk kommunikation precis så som traditionella avtal görs bör lämpligen medföra att dessa inte uppfattas som mindre säkra än det handskrivna avtalet. Om parter inte har haft möjlighet att använda några andra avtal än elektroniska skulle avtalsformen kanske aldrig ifrågasättas. Avtalsrätten skyddar elektroniska avtal i lika stort omfång som den gör för traditionella vad gäller situationer i detta kapitel. Det enda som saknas i dag då situationen inte är fullt ut som den jag nyss beskrev, är att parterna börjar använda elektroniska avtal. Det torde inte finnas någon anledning att ersätta handskrivna avtal med elektroniska. Möjligheten att nyttja fler sätt att skriva avtal ska alltid vara en självklarhet för parterna så länge utvecklingen inte bromsas på grund av existerande avtalsformer.

[34] Se avsnitt 6.2.

3 Elektronisk signaturs funktion

3.1 Varför elektronisk signatur?

Vare sig det är en handskriven signatur eller en elektronisk sådan uppfyller den en viktig del av avtalet. En signatur på ett dokument har som funktion att verifiera dokumentet på vilket det framträder. Med elektroniska signaturer avses att säkerställa att elektroniskt överförd information inte har förändrats och för att identifiera informationens avsändare.[35] Båda formerna av kommunikation vill förmedla att det är rätt innehåll och att det är rätt part som har skrivit under. Att signera ett dokument är inte ett måste utan det kan räcka med ett handslag. Avtalsrättsligt sett finns det ett flertal sätt att signera ett avtal med. Avtalet kan skrivas under med en handskriven signatur eller med en elektronisk sådan av den orsaken att 1§ AvtL inte klart uttrycker att det ska ske på ett visst sätt.

En traditionell underskrift med bläck kan i viss mån skyddas mot manipulationer. Detta uppnås genom att underskriften låses vid dokumentet och dess text, eventuellt i förening med stämplar eller andra äkthetstecken.[36] Underskriften identifierar den som har skrivit under dokumentet samtidigt som den har den äkthetsfunktionen som nyss nämndes.[37] När parterna har med ett elektroniskt dokument att göra finns inte samma möjlighet av kontrollering som vid traditionell signering. Det krävs i stället att det görs någon form av kontroll som säger att det aktuella dokumentet härrör från en viss utställare.[38] Det skulle kunna uppnås genom elektronisk signatur som kopplar samman ett ”hashvärde”[39] av data med dess utställare.[40] I och med detta ”hashvärde” som skickas när part signerar ett elektroniskt avtal kan det kontrolleras om ytterligare tecken har tillförts dokumentet efter signering. Både handskriven och elektronisk signatur uppnår viss form av säkerhet. Dock är en enstaka handskriven signatur lättare att förfalska genom att studera tidigare underskrifter än att studera ett ”hashvärde” som skiljer sig från dokument till dokument beroende på dess innehåll.

Precis som handskrivna signaturer fyller en elektronisk signatur olika funktioner. Det kan exempelvis vara att[41]:

- bekräfta att den som signerar ett dokument vill bli bunden
- bekräfta att den som signerar ett dokument är upphovsman till dokumenttexten
- bekräfta att den som signerar ett dokument ansluter sig till innehållet i de fall dokumentet härrör från någon annan samt

---

[35] Ds 2001:13 E-handelsdirektivet – genomförande av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster (2001) s. 109.

[36] SOU 1996:40 s. 232.

[37] Ibid. s. 232.

[38] Seipel Peter Juristen och datorn Introduktion till rättsinformatiken (1994) s. 190.

[39] Se avsnitt3.4. ”Hashvärde” förklaras även i Averstens bok s. 20.

[40] Seipel Peter Juristen och datorn Introduktion till rättsinformatiken (1994) s. 191.

[41] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 29.

- bekräfta att den som är part i avtalet befunnit sig på en viss plats vid ett visst tillfälle.

Om ytterligare tecken skulle tillföras ett dokument efter det signerats, bör det ses som manipulation och inte uttryck för vad den som signerade dokumentet ville.[42] Detta gäller både traditionella och elektroniska avtal. Det finns alltid risk att kommentarer eller att villkor tillförs dokumentet i efterhand och därför är datering av signaturer lika viktiga som signeringen i sig. Ett ”hashvärde” torde vara ett lämpligt sett att just kontrollera att dokumentet stämmer med det som ursprungligen skickades. Den kontrollmöjligheten tillhandahålls inte när avtal undertecknas med en fristående signatur på ett papper. Detta på grund av att den handskrivna signaturen inte är kopplad till dokumentet på samma sätt som den elektroniska signaturen är.

3.2 Elektronisk signatur genom kryptering

Kryptering fyller en funktion som skydd mot obehörig åtkomst av uppgifter men den har även en funktion som rör identifiering och elektronisk signatur.[43] Elektroniska signaturer tillskapas med användande av krypteringsteknik. Denna form av teknik förvränger datasignaler med hjälp av en hemlig nyckel.[44] När part använt sig av denna nyckel är dokumentet ej längre läsbart. Det kan därefter bli läsbart igen med hjälp av nyckeln. Skapandet av elektroniska signaturer som sker genom att kryptering tillhandahåller en tillräckligt invecklad process för att det inte ska anses lätt att förfalska sådana signaturer och därigenom ökar förtroendet för elektroniska signaturer. Möjligheten att kunna forcera en kryptering får liksom ”hashvärdet” anses mer problematiskt än att förfalska en handskriven signatur. Ett elektroniskt dokument som görs oläsligt torde inge en annan trygghetskänsla än vad en signatur på ett pappersdokument gör. Att det skulle kunna upplevas så kan bero på att ett avtal med en traditionell signatur finns tillgängligt i sitt ursprungliga skick. Ett elektroniskt dokument som krypterats måste genom en särskild process återställas i sitt ursprungliga skick för att kunna läsas av den andra parten. Det finns två olika former av kryptering, symmetrisk och asymmetrisk.

3.2.1 Symmetrisk kryptering

Denna form av teknik använder parterna när de krypterar och dekrypterar med samma nyckel.[45] Tekniken ska även skydda mot obehörig insyn. Frekvent använda symmetriska krypteringsalgoritmer[46] är DES och IDEA.[47] Det problem som verkar mest relevant är att avsändare och mottagare måste ha tillgång till samma hemliga nyckel.[48] Ett annat problem som visar att det inte är en friktionsfri funktion gäller förhållanden där avsändaren skulle

---

[42] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 29.

[43] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 16.

[44] Ibid. s. 16.

[45] Ibid. s. 16.

[46] Algoritm är en metod eller schema för lösning av matematiskt eller logiskt problem.

[47] DES betyder Data Encryption Standard och IDEA betyder International Data Encryption Algorithm.

[48] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 16.

vilja kommunicera med flera motparter än en. Då måste avsändaren ha en nyckel till varje motpart. Denna form av teknik är en aning bräcklig med tanke på att båda parter i avtalet har tillgång till samma hemliga nyckel.[49] Kunskapen om att enbart en part har tillgång till en nyckel inger trygghet. Det inger även en form av säkerhet i och med att parten själv blir ansvarig för att den skyddas på ett lämpligt sätt. I ett förhållande där två parter tillsammans har tillgång till samma nyckel finns det risk att de försöker lägga ansvaret på varandra och därigenom försvårar konstaterandet av vem som egentligen är ansvarig. Ett förhållande mellan parter kan stöta på missförstånd om det inte finns en uttalad ansvarsfördelning dem emellan.[50]

3.2.2 Asymmetrisk kryptering

När parter begagnar asymmetrisk kryptering krävs det en nyckel för kryptering och en för dekryptering.[51] Den bygger på avancerade matematiska samband där förhållandet mellan de båda nycklarna är sådan att den ena innehavaren av nyckeln inte kan räkna ut den andra innehavarens nyckel. En metod för asymmetrisk kryptering är exempelvis Diffie-Hellman.[52] Det är ett protokoll för nyckelutbyte där parter kan förhandla fram en gemensam krypteringsnyckel utan att någon obehörig som råkar ta del av förhandlingen ska förstå vad de kommer fram till. Den mest kända algoritmen är RSA[53] som bygger på att det är tämligen lätt att finna stora primtal[54] men att det är svårt att faktorisera stora tal till deras primfaktorer. Således kan ett nyckelpar konstrueras där det ej går att härleda de motstående nycklarna från varandra förutsatt att nyckellängden är skäligt lång[55]. Ena parten disponerar över den ena nyckeln, den privata nyckeln.[56] Den andra nyckeln kan göras publik utan att äventyra att den privata nyckeln blir blottad och kallas därför den publika nyckeln. Oberoende av vilken nyckel som brukas först kan den motstående nyckeln i paret dekryptera meddelandet.[57] Det är detta som ligger bakom tanken med asymmetrisk kryptering, även kallad *public key encryption*.

Asymmetrisk kryptering erbjuder ett större utrymme för förtroende då parterna själva är ansvariga för sina nycklar. Därmed delas ansvaret upp från början utöver det som parterna kommer överens om i avtalet. Denna uppdelning av nycklarna underlättar själva processen att härleda rätt ansvar till rätt part. Med det åsyftas att om det är den privata nyckeln som

---

[49] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 16.

[50] Ansvarsförhållanden och problem som kan tänkas uppstå i samband med detta utreds i avsnitt 5.1.

[51] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 17.

[52] Ibid. s. 17.

[53] RSA är döpt efter sina uppfinnare; Rivest, Shamir och Adelsman vid Massachusetts Institute of Technology. Algoritm förklarades i fotnot 46.

[54] Ett primtal är ett heltal som är större än 1 och som ej kan skrivas som en produkt av två eller flera heltal, exempelvis 3,5,7,11,13 medan 4 eller 12 inte är det (eftersom 2*2=4 och 2*2*3=12).

[55] En nyckel består av flera olika variationsmöjligheter som finns i kryptot. För närvarande anses det att 128 bits-nycklar är tillräckligt säkra för att i praktiken inte kunna knäckas. All information som behandlas av datorn kan representeras som en följd av ettor och nollor, en bitföljd. En bit är en etta eller en nolla och en bokstav, exempelvis G, består av 8 bits. Informationen har hämtats ur Franzén Torkel Java från grunden (2001) s. 16-17.

[56] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 17.

[57]Ibid. s. 17.

blivit felaktigt bevarad bör det vara nyckelinnehavaren av den som i första hand får ställas till svars. För att användandet av elektronisk signatur ska öka måste tillräcklig säkerhet erbjudas de parter som kan tänkas använda elektroniska avtal. En handskriven signering i sig själv erbjuder inte tillräcklig säkerhet men i samband med bevittning exempelvis skulle känslan av säkerhet öka. När ett meddelande krypteras ökar chanserna att ett meddelande inte kan läsas och därmed inte manipuleras. Detta erbjuder stora möjligheter vid autentisering och vid användning av elektronisk signatur.[58]

3.3 ”Smarta kort”

”Tanken är att de elektroniska ID-korten skall kunna användas av alla, mot alla, i ett öppet system för autenticering, signering, och verifiering av digitala signaturer och för dekryptering”.[59]

”Smarta kort” är plastkort som har samma format som ett bankkort och är försett med ett chip och en mikroprocessor, alltså som en liten dator.[60] ”Smarta kort” kan med hjälp av RSA nyttjas för att frambringa elektroniska ID-kort (EID). Ett sådant kort formges visuellt som ett vanligt ID-kort och i dess minne lagras innehavarens privata RSA-nyckel.[61] Krypteringsberäkning kan göras av kortets microprocessor och därmed kan nyckeln ej kompromitteras under själva krypteringen. Kortet kan även skyddas genom en fyrsiffrig PIN-kod. Att kunna skydda en hemlig nyckel i ett smart kort stärker ytterligare säkerheten kring elektronisk signatur. När nyckelinnehavaren begagnar elektroniska signaturer tillskapade med ett åtkomstskyddat ”smart kort” kan denne själv motverka förfalskning genom att vara försiktig med hur kortet och PIN-koden förvaras så att ingen obehörig kan utnyttja den, precis som med bankkort kan kortet åtkomstskyddas genom en fyrsiffrig kod.[62] Precis som för traditionella signaturer handlar det om hur parterna själva har agerat för att upprätthålla den säkerhetsnivå som krävs för att ett avtal inte ska manipuleras.

”Smarta kort” kan användas på fler sätt, exempelvis som betalningsmedel, informationsbärare eller identitetskort/tjänstekort.[63] På kortet kan även information lagras som ska meddelas motparten, exempelvis personuppgifter eller information för att kunna verifiera en elektronisk signatur.

Processen för att få fram en elektronisk signatur börjar med att en hemlig nyckel tas fram genom kryptering av dokumentet och denna nyckel kan sedan kan förvaras i ett ”smart kort”. Detta ”smarta kort” skyddas i sin tur genom en fyrsiffrig PIN-kod. Om jämförelse av denna process görs med en handskriven signatur som kan kompletteras med exempelvis stämplar för att bevisa äktheten torde valet vara enkelt. Den elektroniska signaturen består av fler säkerhetsmoment än vad en handskriven signatur gör. Därmed kan den elektroniska signaturen anses vara säker, till och med säkrare än den handskrivna signaturen. Den snabba utvecklingen gör dessutom att säkerheten ökar för varje år.

---

[58] Ibid. s. 17.

[59] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 19.

[60] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 18.

[61] Ibid. s. 18.

[62] Ibid. s. 18.

[63] Ibid. s. 18.

3.4 Tillvägagångssätt för elektronisk signering

Att signera ett avtal elektroniskt innebär att delar av ett dokument krymps ihop till en så kallad ”hashalgoritm”.[64] Det är en funktion som känner av dokumentet och krymper ihop delar av det till ett ”hashvärde” som även kallas ”kondensat”. Det fungerar som ett fingeravtryck som är unikt för just den kombinationen som har sitt ursprung i dokumentet. Denna kontrollsumma krypteras sedan med den hemliga nyckeln. Summan är unik för just den nyckeln och det dokumentet. Dokumentet skickas sedan till motparten där den krypterade kontrollsumman är medsänd. När mottagaren tar emot ett sådant meddelande verifierar han den elektroniska signaturen genom att utföra samma ”hash-operation” som utfördes vid signeringen och får därigenom fram en kontrollsumma, den andra.[65] Därefter dekrypterar mottagaren signaturen med avsändarens publika nyckel och då framträder den första kontrollsumman i ett ej krypterat format. När detta är gjort jämförs båda kontrollsummorna[66] Är dessa summor samstämmiga vet mottagaren att inga ändringar gjorts i dokumentet efter att det har signerats och att signeringen skett med avsändarens nyckel.

Tillvägagångssättet mellan handskrivna och elektroniska signaturer skiljer sig ganska markant. För part att kompromettera en elektronisk signatur krävs att denne tar sig igenom hela processen som föregås en sådan. En handskriven signatur skrivs under av parterna och bevittnas i många fall av en tredje part. Det skulle vid denna jämförelse kunna anses som att elektronisk signatur tillhandahåller parterna en säkrare process än vad som finns tillgängligt vid en traditionell sådan. Ett dokument som krymps ihop till ett ”hashvärde” som sedan genomgår samma operation som vid krympningen av dokumentet för att sedan dekrypteras utgör en process som torde räta ut några frågetecken kring säkerheten. Det borde kunna anses att det har arbetats fram ett tillvägagångssätt som skyddar en elektronisk signatur på ett tillfredsställande sett.

3.5 Sammanfattning

Tredje kapitlet tar upp utsikterna om att göra ett elektroniskt avtal säkert att förfoga över förutom den säkerheten som avtalet i sig självt erbjuder. En signatur på ett avtal indikerar att en part har godkänt det som står i det aktuella avtalet. Det första som tas upp i kapitlet är; varför elektronisk signatur? Varför inte blir den direkta motfrågan. Om utvecklingen ska fortsätta måste elektroniska avtal kunna signeras på något sätt. Ett handskrivet avtal utan underskrift är inte mycket värt i parters ögon och det lär inte elektroniska heller vara om de inte är signerade. Om det finns möjlighet att uppnå tillräcklig säkerhet, finns det heller ingen anledning att neka elektroniska signaturer den tillit som handskriven signatur besitter.

Säkerhet kan uppnås på olika sätt och ett av dem är kryptering. Ordet kryptering är den grekiska benämningen för dold eller hemlig. Det säger mycket om just elektroniska signaturer av den orsaken att de skapas med användande av just krypteringsteknik. Ett dokument som inte är läsbart är det svårt att ändra eller lägga till i. Har parterna därutöver skyddat krypteringen i ett smart kort har de därigenom skyddat avtalet genom två olika processer. Till slut är det visserligen upp till parterna hur de skyddar krypteringsnycklarna och det ”smarta kortet” för att bäst uppnå tillräcklig säkerhet. Hur parterna skyddar sina nycklar

---

[64] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 20.

[65] Ibid. s. 20.

[66] Ibid. s. 20 och 21.

och ”smarta kort” skiljer sig inte från hur parterna skyddar dokumentet där deras handskrivna signaturer framträder. Det kan ändå anses att elektroniska signaturer genom kryptering som kan skyddas i ett smart kort egentligen uppnår högre grad av säkerhet än vad handskrivna signaturer gör.

Vad som alltid kommer att påverka hur nutida och framtida parter ser på en kommunikationsform är hur många som använder det. Detsamma gäller elektroniska signaturer. Hur säkra de än må vara måste det finnas någon form av bekräftelse av att de är säkra. En sådan kan vara att tillräckligt många använder den. Vad som är tillräckligt många är relativt och kopplat till vem som använder elektroniska signaturer och vem det är som ställer frågan om hur säkert det är. Ju större gruppen användare blir desto fler lär dessa locka framtida användare att börja använda elektroniska avtal och signaturer.

4 Verifiering av elektronisk signatur

4.1 Bakgrund

Verifiering av ett dokument är en viktig del för att fullgöra ett avtal. Det är också viktigt att det genom signering är klart och att det inte föreligger något tvivel om signeringen i sig. Elektronisk signatur är en ny företeelse och därför finns det risk att tvivel uppstår kring dess säkerhet. Förtroende för en ny form av signering kan inledningsvis vara svår att uppnå. Det gäller att någon börjar använda tekniken frekvent för att fler ska följa exemplet. Om trenden håller i sig ökar förtroendet för användningen och därmed torde tvivlen försvinna med tiden.

För att elektronisk signatur ska kunna uppnå samma status som en handskriven signatur krävs det att parter känner tillit till denna form av kommunikation. Ett sätt att uppnå tillit är att kunna ha till förfogande en tredje part. En handskriven signatur kan bevittnas av tredje part och samma möjligheter borde finnas tillgängliga till elektronisk signatur. En betrodd tredje part kan bekräfta kopplingen mellan en individ och dennes nyckel.[67] Detta görs genom att tredje part ställer ett certifikat[68] till förfogande som intygar att en viss person är innehavare av en publik nyckel vilken hör ihop med en viss privat nyckel.[69] Innehavare av en privat nyckel identifierar sig för betrodd tredje part som sedan i ett certifikat bekräftar dennes identitet. Om en innehavare av en privat nyckel beställer ett elektriskt ID-kort[70] får han identifiera sig för en betrodd tredje man som därefter intygar i ett certifikat dennes identitet. Vid handskriven signering identifieras signaturen genom jämförelse av tidigare signaturer och genom att bevittning av tredje man görs. Båda formerna ger parterna anledning att lita till dem i den mån det är möjligt. Med det menas att det alltid föreligger risk för förfalskning. Vad gäller verifiering av elektronisk signatur torde denna anses säkrare.[71] Tredje part i ett avtalsförhållande måste kunna anta en oberoende ställning.[72] Trots att en tredje part som anlitas för att granska tidigare handskrivna signaturer kan anses inta en oberoende ställning i samma utsträckning som tredje part som granskar en elektronisk signatur, borde en elektronisk signatur med den process som krävs för att ta fram en sådan i gemenskap med oberoende tredje part ses som ett säkrare alternativ. En enskild handskriven signatur kan lätt bli manipulerad genom förfalskning av en annan individ medan det krävs mer kunskap för att förfalska en elektronisk signatur. Vad gäller tredje part torde det inte uppstå någon större skillnad ur säkerhetssynpunkt.

4.2 Betrodd Tredje Part

Betrodd Tredje Part (BTP), ska vara en oberoende part som inte har något intresse i den förmedlade informationen.[73] Det benämns *Trusted Third Party* på engelska.[74] Det krävs ett

---

[67] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 22.

[68] Se avsnitt 4.3.

[69] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 22.

[70] Se avsnitt 3.3.

[71] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 22.

[72] Se vidare diskussion i avsnitt 4.2.

[73] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 22.

särkskilt mått av oberoende som exempelvis myndighet eller företag såväl privat som offentligt kan erbjuda.[75] Vem tredje part ska gestalta bör därför var avhängigt av vilka som är parterna och innehållet i avtalet.

Certification Authority är en form av BTP och förkortas CA.[76] Någon svensk terminologi för ordet har ännu inte införts. Att det finns CA beror på att det inte är klart om företag och myndigheter verkligen kan förhålla sig som fristående part som saknar intresse i en pågående transaktion.[77] Det bör tas hänsyn till vilka det aktuella avtalet står mellan och vad avtalet avser. Därefter kan den BTP som anses bäst lämpad utses. Genom att tillämpa ett tillvägagångssätt som detta tillgodoses möjligheten att kunna anlita en opartisk BTP. CA kan agera i situationer där företag och myndigheter inte kan anses vara opartiska. Att parter har tillgång till en oberoende tredje part är nödvändigt för att kunna erhålla verifiering från annan än parterna själva. Risken att företag eller myndighet skulle ha ett visst intresse av avtalet eller parterna är inte omöjligt om det avtalet avser och sysselsättningen som företaget utför har alltför klar koppling dem emellan. Ett sådant exempel skulle kunna bestå av en situation där en BTP skulle kunna erhålla ekonomisk vinning om avtalet innehåller fördelaktiga villkor för endera parten. Det är dock inte ett skäl till att neka företag möjligheten att kunna agera som BTP. Det ställer istället krav på att en mångfald företag och myndigheter faktiskt har den kunskap som krävs och rätten att bistå som BTP.

Fristående BTP i Sverige anser sig exempelvis Posten vara.[78] De utvecklar system för att kunna ge ut elektroniska ID-kort och certifikat. Även banker kan fungera som BTP för sina kunder i slutna system. Nordea tillhandahåller exempelvis elektronisk legitimation på ett ”smart kort”. Den innehåller en elektronisk identifieringshandling och detta kan fås som en funktion i användarens bankkort eller som ett enskilt kort.[79] En elektronisk legitimation är en elektronisk handling vilken kan jämföras med en vanlig identifieringshandling, exempelvis körkortet. En elektronisk legitimation används av part för att legitimera sig och för att skriva under en handling elektroniskt.[80]

4.3 Certifikat

För att kunna använda och tillhandahålla elektroniska signaturer i ett öppet system, där parterna ej känner varandra, finns det behov för parterna att erhålla information om kopplingen mellan den elektroniska signaturen och en bestämd individ.[81] Det är därför det finns möjligheter att få ett elektroniskt intyg, ett certifikat, utfärdat av CA eller annan BTP. Ett sådant certifikat kan beskrivas som ett elektroniskt dokument som är elektroniskt signerat

---

[74] Det engelska uttrycket kommer inte att användas i fortsättningen utan istället kommer den svenska förkortningen att användas.

[75] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 22.

[76] Ibid. s. 22.

[77] Ibid. s. 22.

[78] Ibid. s. 22.

[79] Se http://www.nordea.se/sitemod/default/index.aspx?pid=207924. Tillgänglig 05-05-19.

[80] Se http://www.e-legitimation.se. Tillgänglig 05-05-19.

[81] Ds 2001:13 E-handelsdirektivet – genomförande av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster (2001) s. 109.

av CA.[82] Dokumentet talar om vilken CA som utfärdat det. Det namnger, identifierar eller skildrar ett kännetecken hos nyckelinnehavaren. Slutligen så innehåller certifikatet nyckelinnehavarens publika nyckel. Certifikatet kan finnas tillgängligt på ett flertal sätt, ett sådant sätt kan vara i en databas.[83] Ett annat sätt är att förmedla certifikatet till innehavaren av den privata nyckeln som sedan vidarebefordrar detta till det elektroniskt signerade dokumentet som slutligen ska verifieras av motparten. Att kunna erhålla ett certifikat förlänger säkerheten av den elektroniska signaturen då den tillkommer utöver själva signeringen. Den verifierar att det är rätt part. Denna verifiering är viktig eftersom elektronisk signering är relativt anonym.

För att känna tillit till ett certifikat måste möjligheter till manipulation elimineras i möjligaste mån. Det kan uppnås genom att CA signerar certifikatet med sin privata nyckel för att sedan verifieras av dennes publika nyckeln.[84] En sådan publik nyckel kan vara allmänt känd eller finnas tillgänglig i ett certifikat från en annan CA. För att uppnå tillit krävs även att det finns möjlighet att återkalla ett certifikat om det finns misstanke om att den privata nyckeln blivit komprometterad.[85] Det förfarandet bygger på ungefär samma tanke som när borttappade bankkort spärras. Nyckelinnehavaren tar kontakt med CA vid misstanke om kompromettering och CA i sin tur utfärdar ett så kallat revokeringscertifikat. I och med detta finns det en markering i den katalog som tillhandahåller certifikat att det aktuella certifikatet är återkallat.[86]

4.4 Sammanfattning

Efter att ha avhandlat kryptering och smarta kort som rör signaturen i sig går proceduren nu vidare till att beröra verifiering. Med det menas säkerställande av att det är rätt signering på rätt avtal. Det finns en risk att en signatur på ett avtal inte nödvändigtvis tillhör någon av de parter som är de som förklarat sig villiga att ingå avtal. Ovisshet för manipulering måste parterna alltid räkna med och skydda sig mot i bästa möjliga mån. I och med detta riskmoment är det viktigt att en process som klargör att avtal signeras på rätt sätt finns tillgängligt för parterna att tillgå när avtalsförhållande uppstår. Det skulle kunna möjliggöras genom att säkerställa att parterna kan erhålla verifikation att avtal ingås med rätt part.

Verifiering av signatur inger förtroende och tillit för både handskrivna och elektroniska avtal. En tredje part gör manipulering svårare att genomföra framgångsrikt. BTP är en lämplig jämlike till tredje man som bevittnar en traditionell signatur. Det finns inget som säger att det måste vara en individ utan det kan exempelvis även vara ett företag. Att inte anta att företag och myndigheter kan hålla sig neutrala verkar lämpligt. Det finns alltid viss risk att någon del av ett avtal är sammankopplat med den part som är i fokus att agera som BTP i ett avtal.

För att parter ska kunna vara säkra på att de ingår avtal med rätt part krävs det någon form av bekräftelse av att kopplingen mellan elektronisk signering och en bestämd part stämmer.

---

[82] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 23.

[83]Ibid. s. 23.

[84]Ibid. s. 23.

[85] Ibid. s. 23.

[86] Ibid. s. 23.

Därför finns det möjlighet att erhålla ett certifikat som bekräftar just detta. Att kunna få en sådan bekräftelse är viktigt i och med att denna form av kommunikation är anonym.

5 Skydd med hjälp av avtal och lagstiftning

5.1 Ansvarsfördelning

Fördelning av ansvar bör vara en självklarhet när parter ingår avtal. Detta torde vara ett område som det lätt kan uppstå missförstånd kring. Avtalsrättsligt sett underlättar det ett avtals ingående om parterna från början bestämmer fördelningen. Ansvarsfördelning kan göras upp mellan tre olika konstellationer av partsförhållanden. Denna fördelning kan ske mellan två parter som ingår ett avtal, mellan CA och nyckelinnehavaren och tredje konstellationen rör förhållandet till tredje man.

5.1.1 Mellan parter

Om det skulle uppstå en situation där ett elektroniskt meddelande kommer till någon form av skada och därigenom förser den mottagande parten med ett meddelande som är inkorrekt signerat, uppkommer frågan vem som är den mest skyddsvärda av parterna. Om nyckelinnehavaren har agerat vårdslöst ska den som förlitat sig på signaturen skyddas.[87] Vårdslöshet kan uppstå om nyckelinnehavaren har förvarat nyckeln på ett otillfredsställande sätt som resulterat i att den blivit använd av någon annan eller att innehavaren självmant låtit någon annan använda den.[88] Det krävs likväl att mottagaren inte varit medveten om vårdslösheten och att han vidtagit rimliga åtgärder i de fall han misstänker något liknande samt kontrollerar att nyckeln inte är återkallad.[89] Möjligheten att skydda sig mot part som beter sig på ett regelvidrigt sätt torde ha stor betydelse för om tillit ska nås för en ny form av kommunikation.

När avtal ingås via elektroniska former bör exempelvis störningar i enskilda datorsystem tas i beaktande. Allmänna Reklamationsnämnden (ARN) har fastslagit att utvecklingen inom informationsområdet inte har kommit så långt att störningar i enskilda datorsystem helt har eliminerats.[90] Sådana störningar anses alltjämt vara normala. Sådana störningar kan bland annat bestå av avbrott i förbindelsen till ett bolags datorsystem vid handel av värdepapper via Internet.[91] Om parterna bestämmer sig för att upprätta avtal via elektronisk kommunikation bör de i avtalet diskutera eventuella störningar som kan uppstå och hur ansvarsfördelningen i sådana fall ska se ut.[92] Genom att ingå avtal om ansvarsfördelning förebygger parterna framtida problem som egentligen inte har med själva innehållet i huvudavtalet att göra.

---

[87] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 36.

[88] Ibid. s. 36.

[89] Ibid. s. 36.

[90] ARN 97-4042, avgörande 1997-12-04.

[91] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 40.

[92] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 41.

5.1.2 Mellan CA och nyckelinnehavaren

En annan ansvarsfråga som kan anses relevant är vilket ansvar CA bör bära i fall där nyckelinnehavaren åsamkas skada på grund av att han inte kan nyttja sitt elektroniska ID-kort.[93] I viss utsträckning kan CA tänkas bli ansvarig för att ett elektroniskt ID-kort inte fungerar i tänkt miljö. Att nyckelinnehavaren kan nyttja sitt elektroniska ID-kort är en förutsättning för att ingå avtal med annan part. Detsamma kan sägas gälla bankkort. Det torde ej kunna anses vara en affärs problem om ett bankkort inte fungerar på grund av bankens förehavanden. I just den stunden när innehavaren av kortet står i affären får innehavaren själv lösa situationen på bästa sätt. Därefter bör kortinnehavaren kunna göra banken ansvarig för den skada innehavaren lidit. En liknande ansvarsfördelning torde kunna göras mellan CA och nyckelinnehavaren.

Mellan CA och nyckelinnehavaren föreligger ett avtalsförhållande och därmed kan respektive parts ansvar regleras i avtal dem emellan. Reglering av ansvar är till fördel för båda. Dock bör CA:s möjligheter till långtgående friskrivningar tas i beaktande.[94] Är det ett förhållande där det står mellan näringsidkare och konsument kan det finnas anledning att bedöma friskrivningarna som oskäliga och därmed jämkas, 36§ AvtL. Skulle ett sådant problem eller ytterligare andra problem uppstå är det som sagt enklare att lösa problemen med hjälp av ett avtal som säger hur ansvarsfördelning ska fördelas. Om inte måste huvudavtalet i sig tolkas och då riskerar parterna att det kan påverka antingen avtalet eller dem själva negativt. Vad gäller CA idag regleras inte denna form av BTP i lag vilket skulle kunna bero på att elektronisk handel och därmed elektroniska avtal fortfarande är relativt nytt på marknaden. Därför är ansvarsfördelningen en del av avtalsprocessen som måste tas i beaktande.

5.1.3 Tredje man

Omständigheter som berör tredje man i förhållande till CA och nyckelinnehavare bör också uppmärksammas. Tredje man har egentligen ingen part i avtalsförhållandet mellan CA och nyckelinnehavaren utan skulle kunna ses som en part vid sidan av ett förhållande mellan två parter. I vissa fall skulle det kunna vara möjligt och även till fördel om förhållandet mellan CA och tredje parten kunde ses som kvasi-kontraktuellt.[95] Det finns ett rättsfall som det går att dra vissa paralleller till.[96] Fallet berör ett felaktigt fastighetsvärderingsintyg som upprättades enligt ett avtal mellan fastighetsvärderaren och fastighetsägaren som senare presenterades för banken. Banken kunde rikta anspråk direkt mot fastighetsvärderaren av den orsaken att han vetat om att intyget skulle användas för att erhålla kredit hos banken. Detta trots att det dem emellan inte existerade något avtal och trots att fastighetsvärderaren inte åsamkat banken den rena förmögenhetsskadan. Till skillnad från rättsfallet där det var klart vad intyget skulle användas till, är att när parter använder elektronisk signatur kan CA vanligtvis inte överblicka vad för transaktioner som den elektroniska signaturen ska användas till.[97] Det torde därför inte vara troligt att den förlitande parten i dessa situationer kan rikta anspråk mot CA med stöd om kvasi-kontraktuellt ansvar. Enda möjligheten skulle vara att

---

[93] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 41.

[94] Ibid. s. 41.

[95] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s.38.

[96] NJA 1987 s 692.

[97] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 38.

det framgår vad för sorts transaktioner som ska genomföras.[98] Då skulle det kunna anses att CA var medveten om transaktionerna och därmed kunna anses inneha kvasi-kontraktuellt ansvar. Om tredje part är medveten om att det avtal han signerar ska användas på ett regelvidrigt sett bör det åligga honom någon form av ansvar.

5.2 Rättsligt skydd

För att elektronisk signatur ska vara säker måste den vara skyddad från obehörig åtkomst och användning.[99] Att kunna uppnå avtal som parterna kan lita till att vara fullständigt säkra emot den ena partens potentiella regelvidriga beteende är inte möjligt vare sig för handskrivna eller elektroniska avtal och inte heller för dess signaturer. Parter måste likväl kunna ställa högsta möjliga säkerhet för dem själva för att vilja ingå avtal med annan part. Det kan uppnås om parterna använder sig av tillräckligt långa nycklar[100] och att nycklarna skyddas fysiskt i ett smart kort[101]. I och med smarta kort, verifiering av elektronisk signatur och certifikatet som verifierar nyckelinnehavaren uppnås samma föreställning av säkerhet som handskriven signatur gör. Därmed kan det tyckas som att det inte skiljer för mycket mellan den traditionella och den elektroniska signaturen. Det krävs dock att parterna är medvetna om den allmänna utvecklingen som pågår och förnyar sina nycklar regelbundet. Med det menas att ”tillräckligt långa nycklar” är ett relativt uttryck som är beroende av hur långt utvecklingen har kommit. Det krävs att parterna är uppmärksamma på vad som anses vara ”tillräckligt långa nycklar” för att de ska kunna anses som säkra.

5.3 Reglera elektronisk signatur i lag

Att reglera förhållanden i lag torde inge tillit i första hand. Elektroniska avtal och signaturer skulle framstå som en tilltalande form att kommunicera via i och med att parterna därigenom kan stödja avtal och sina rättigheter i lag. När det gäller elektronisk signatur handlar det om en kommunikationsform som även tillhandahåller ett väldigt snabbt sätt att göra affärer på. En sådan form av kommunikation som erbjuder en snabb process för att åstadkomma avtal torde anses vara gynnsamt. Därför kan det kännas angeläget att uppnå tillit som sträcker sig så långt att parter är villiga att gagna denna form av kommunikation. Avtalsrättsligt sett tillgodoses väldigt många aspekter i avtalslagen. Utvecklingen är i ständig rörelse och att ha lagstiftning som är så pass anpassningsbar är enbart till fördel. Vissa delar som tillhör elektroniska avtal och signaturer skulle möjligtvis regleras och verka som komplettering till avtalslagen. Ett sådant område är det CA tillhör. Att reglera CA skulle göra att alltfler parter känner sig säkra och torde därmed använda sig av elektroniska avtal och signaturer och det skulle i sin tur troligtvis även leda till att fler CA bildas. Ju fler CA som existerar ju mer kan de specialisera sig och därmed rikta in sig på vissa specifika avtal och parter. Det skulle också ge mer uttryckliga spelregler och skulle därför stimulera olika CA, stora allmänna och små specialiserade.[102] Dock bör det tas i beaktande att det kan uppstå problem för internationell handel om varje land har specifika lagregler som enbart kan tilläm-

---

[98] Ibid. s. 38.

[99] Aversten David Digitala signaturer och ansvarsproblem (1998) s. 31.

[100] Se avsnitt 3.2.2.

[101] Se avsnitt 3.3.

[102] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 43.

pas på inhemska parter i det landet.[103] Det måste tas i beaktande att det finns avtalsförhållanden där antingen CA eller någon av parterna hör hemma i ett annat land. Eftersom jag enbart diskuterar hur det förhåller sig i Sverige går jag inte in på den problematiken här.

Det som skulle kunna uppnås med lagreglering är tillit och detta uppnås genom[104],

- att reglera CA:s verksamhet och därigenom ställa krav på teknisk kompetens, interna säkerhetsrutiner, och så vidare,
- att reglera när ett meddelande ska anses ha sitt ursprung från innehavaren av den privata nyckeln och
- att reglera CA:s ansvar i relation till parter som förlitar sig på CA:s uppgifter.

5.4 Sammanfattning

Förvissningen om att inte råka ut för vårdslöst handlande är av stor vikt och troligtvis en faktor som avgör om parter är villiga att använda en viss form av kommunikation. Fördelning av ansvaret tillhör en del av en process för att motverka missförstånd och problem. Så länge det föreligger ett avtalsförhållande mellan två parter bör avtal upprättas för att motverka framtida problem. Om avtal inte upprättas som rör ansvarsfördelning blir det huvudavtalet som tolkas vilket kan för parterna leda till, visserligen positiva resultat, men likväl till negativa sådana. Vad som är positiva och negativa resultat torde bero på den situation som är för handen och vilken part som får rätt. Genom att inte komma överens i avtal om ansvarsfördelning riskerar parterna att stjälpa huvudavtalet. Huvudavtalet som är den egentliga anledningen till att parterna involverats och därmed bör detta skyddas i bästa möjliga mån.

Hur långt ett ansvar för tredje man bör sträcka sig är svårt att säga. Det torde bero på situationen det berör. Om ansvar inte skulle föreligga överhuvudtaget finns det risk att oskyldiga parter utsätts för bland annat vårdslöst beteende. En sådan situation kan anses helt omotiverad eftersom det ej korrekta avtalet då redan uppmärksammats av tredje part. Att erkänna att det uppstått ett kvasi-kontraktuellt ansvar skulle göra att avtal känns säkrare att ingå eftersom det finns möjlighet för parter som exempelvis CA, de parter som ingår huvudavtalet och tredje man att ta del av ansvarsfördelningen. Visserligen skulle det kunna det kunna få verkan som avskräckande men det torde egentligen inte ses som något negativt. Bestämd ansvarfördelning skulle kunna verka i avskräckande syfte i och med att det klart visar vem som är ansvarig i vilken situation. Det är dock mer troligt att ansvarsfördelningen utmynnar i att de som väl ingår avtal är seriösa parter och vet vad för sorts ansvar som åligger dem.

Avtalslagens utformning gör att den är tillämplig på väldigt många förhållanden vilket måste ses som en fördel. En sådan lagstiftning torde ha möjlighet att kvarhålla sin slagkraftighet trots framtida utveckling. Dock kan det finnas anledning i vissa fall att komplettera redan existerande lagstiftning. CA innehar en viktig roll då den består av att verifiera elektroniska signaturer. Om användningen av elektroniska avtal och signaturer ökar kan trycket öka på att reglera CA i lag då CA intar en viktig roll i ett avtalsförhållande. Att kunna verifiera en

---

[103] Detta problem diskuteras i viss mån av Ramberg i hennes bok Elektronisk handel och avtalsrätt (1998) s. 43 och 57.

[104] Hultmark Christina Elektronisk handel och avtalsrätt (1998) s. 35.

elektronisk signatur är en viktig del av avtalsprocessen och därmed torde det kunna anses väsentligt att klargöra förhållandena kring CA. Reglering av CA i lag skulle kunna vara ett lämpligt sätt att uppmuntra parter att nyttja elektroniska avtal i samma utsträckning som handskrivna. Möjligheten att kunna styrka sin rätt i lag skulle vara ett positivt resultat av en lagreglering. En sådan reglering i lag skulle inte påverka annan än nuvarande och framtida CA:s. Det innebär att lagreglering av CA inte hindrar annan kommunikation att slå igenom på marknaden eftersom regleringen enbart berör CA. CA förfogar över ett stort ansvar och därför bör just den delen av processen kring elektroniska avtal regleras. CA bekräftar både en elektronisk signatur och att det är rätt part som signerat. Dessa två moment är av stor vikt när parter ingår avtal och bör behandlas därefter.

6 EG-rätt och svensk rätt

6.1 EG-rätt

EG-rätten är en självständig rättsordning som även ingår i varje medlemsstats rättsordning.[105] Enligt första stycket artikel (art.) 249 EG ska Europaparlamentet och Rådet gemensamt, Rådet eller Kommissionen, i enlighet med fördragets bestämmelser ”utfärda förordningar och direktiv, fatta beslut samt avge rekommendationer och yttranden”. Förordningar ska enligt art. 249 2st EG vara direkt tillämpliga i medlemsstaterna och därmed ges de giltighet framför stridande nationella regler. Ett direktiv är bindande för medlemsstaten till vilken den är riktad i vad avser det resultat som ska uppnås.[106] Det överlåts åt de nationella myndigheterna att bestämma form och tillvägagångssätt för att genomföra direktiv.[107]

6.1.1 Direktiv 1999/93/EG

Ett direktiv kan riktas till en eller till flera medlemsstater gemensamt.[108] Direktiv används för att frambringa en harmonisering eller tillnärmning av lagstiftning inom Europeiska Gemenskapen. Medlemsstaterna är skyldiga genom fördragen att se till att nationella bestämmelser står i överensstämmelse med direktivet då det ska implementeras, art.10 EG.

Direktiv 1999/93/EG[109] ska verka som ett ramverk inom gemenskapen för elektroniska signaturer. Elektronisk signatur definieras som så här i direktivet art.2 p1:

”Elektronisk signatur: uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska uppgifter och som används som en metod för autentisering”.

För att en elektronisk signatur ska få anses vara avancerad krävs det bland annat enligt direktivets art.2 p2 att den är knuten uteslutande till undertecknaren och att undertecknaren kan identifieras genom den. Det krävs även att den är skapad med medel som undertecknaren kan behålla under sin egen kontroll och att den är kopplad till de uppgifter den avser så att ändringar som skett efter påskrift kan uppdagas.

I direktivet art.5 klargörs den rättsliga verkan för elektroniska signaturer. Artikelns första punkt talar om att medlemsstaterna ska säkerställa att avancerade elektroniska signaturer som är baserade på kvalificerade certifikat[110] och som har skapats av en säker anordning för skapande av signaturer ska uppfylla vissa krav. Dessa krav ska vara samma rättsliga krav ställda på en signatur i förhållande till uppgifter i elektronisk form på samma sätt som en handskriven signatur uppfyller samma krav i förhållande till uppgifter på papper. Slutligen säger artikeln att elektroniska signaturer ska godtas som bevis vid rättsliga förfaranden.

---

[105] Allgårdh Olof och Norberg Sven EU och EG-rätten En handbok och lärobok om EU och i EG-rätt (1999) s. 120.

[106] Art. 249 3st EG-fördraget EGT 2002 C 325/33 EGT 2002 C 325/33..

[107] Ds 2001:13 E-handelsdirektivet – genomförande av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster (2001) s. 81.

[108] Allgårdh Olof och Norberg Sven EU och EG-rätten En handbok och lärobok om EU och i EG-rätt (1999) s. 229.

[109] Direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer EGT L 13, 19.1.2000, s.12.

[110] Se avsnitt 6.2.

Andra punkten i samma artikeln klargör vad som inte kvalificerar som giltiga ursäkter i fall där elektronisk signatur nekats rättslig verkan eller giltighet som bevis.

Direktivets syfte är att eliminera problemen kring själva möjligheten att använda en elektronisk signatur, att det inte ska uppstå dåliga ursäkter som förklaring till varför signaturen nekas rättslig verkan. Direktivet skyddar just den rättsliga verkan av elektronisk signatur och därmed förbättra chanserna att parter kommer ta till sig denna form av kommunikation än vad som gjorts tidigare. Ju mer lagstiftning som värnar om kommunikationsformer desto större chans att den kommer användas. Om lagstiftning finns tillgänglig för avtal oberoende av vilken form av kommunikationen som använts mellan parter, infinner sig troligtvis tillit till en sådan kommunikation. Det bör ändock påpekas att regleringen inte får överdrivas eftersom det då troligtvis skulle få negativa följder. Sådana följder kan bero av ett alltför stort regelverk kring avtals ingående. Då riskerar både intresset och användandet av den aktuella formen av kommunikation att utebli. Känslan av att en process kräver alltför mycket arbete kan resultera i att parter väljer ett annat sätt att upprätta avtal på. Direktivet tillsammans med avtalslagen skyddar avtalet och signeringen. EG-direktivet och svenska avtalsreglerna kompletterar med andra ord varandra.

6.1.2 Direktiv 2000/31/EG

Direktivet handlar om informationssamhällets tjänster och då särskilt elektronisk handel.[111] Art.1 p1 klargör att direktivet ska bidra till att den inre marknaden ska fungera väl genom säkerställande av den fria rörligheten för informationssamhällets tjänster.

I direktivets ingresspunkt 34 förtydligas det att medlemsstaterna bör upphäva eventuella formkrav som kan hämma användningen av elektroniska avtal. Art.9 p1 i direktivet redogör att Medlemsstaterna ska se till att deras rättssystem tillåter att avtal ingås på elektronisk väg. Staterna ska särkskilt se till att de rättsliga krav som är tillämpliga på avtalsprocessen varken skapar hinder för användningen av avtal på elektronisk väg eller medför att sådana avtal frånkänns rättslig verkan och giltighet på grund av att de kommit till stånd på elektronisk väg. Det finns undantag i direktivets art.9 p2 gällande avtal som rör fast egendom, vissa borgensavtal, familjerättsliga avtal och avtal som enligt lag kräver att domstolar, myndigheter eller yrken som inkluderar myndighetsutövning involveras.

Direktivet lägger tyngden på själva avtalet och inte signeringen. Det ska inte förekomma någon skillnad vad gäller rättslig verkan mellan elektroniska avtal och handskrivna sådana. För att elektronisk signatur ska ha rättslig verkan synes det rimligt att detsamma gäller för själva avtalet Vad som sägs i direktivet tillgodoses i avtalslagen. Det tillgodoses genom att direktivet klargör att Medlemsstaterna själva ska se till att deras rättssystem tillåter att avtal ingås på elektronisk väg. Med andra ord är det möjligt enligt svensk lag att ingå avtal via elektronisk kommunikation eftersom avtalslagen inte klart uttrycker vilka former avtal måste ta. Förbehållet de undantag som både direktivet och avtalslagen tar upp.[112]

---

[111] Direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) EGT L 178, 17.7.2000, s.1.

[112] Undantagen i svensk lag, vilka är desamma som i direktivet, behandlas i avsnitt 6.2.

6.2 Svensk lagstiftning

Implementering av direktiven[113] har medfört att Lag (2000:832) om kvalificerade signaturer har kommit till. Syftet med lagen är enligt 1§ att skapa gynnsammare förutsättningar för användningen av elektroniska signaturer, genom bestämmelser om säkra anordningar för signaturframställning, om kvalificerade certifikat för elektroniska signaturer och om utfärdandet av sådana certifikat.

Som kan förstås av benämningen av lag (2000:832) om kvalificerade elektroniska signaturer inbegrips förutom elektronisk signatur även kvalificerad elektronisk signatur. I direktiv 1999/93/EG definieras inte kvalificerad signatur. Svensk lag tar därmed den nationella lagstiftningen ett steg längre än vad den EG-rättsliga gör. 2§ 3st säger att kvalificerad signatur är en avancerad elektronisk signatur[114] som är baserad på ett kvalificerat certifikat[115] och som är skapad av en säker anordning[116] för signaturframställning.

Anledningen till att svensk lagstiftning definierar kvalificerad elektronisk signatur torde vara för att parterna ska kunna ställa höga krav på säkerheten kring elektronisk signatur. När teknik är ny finns det risk att den inte nyttjas enbart för att den inte känns säker eller i vart fall inte lika säker som den teknik parterna nyttjat hittills. Därför kan en sådan definiering som görs i lag vara viktig. Att kunna hänvisa till ett direkt lagrum kan inge förtroende för att använda en viss kommunikationsform. Denna säkerhet utmynnar i att part kan åberopa sina rättigheter inte enbart i enlighet med avtalet utan också i enlighet med lagen.

I lagen om kvalificerade elektroniska signaturer framgår det att om det i lag eller annan författning ställs krav på personlig underskrift eller motsvarande och om det är tillåtet att tillfredsställa kravet med elektroniska medel, ska en kvalificerad elektronisk signatur anses tillfredsställa kravet.[117] Parterna kan använda sig av signaturer av lägre säkerhetsnivå men det får aldrig ställas högre krav på elektronisk signatur än vad som ställs på kvalificerade elektroniska signaturer.[118] Därmed uppenbarar sig frågan om vilken av signaturerna som lämpar sig bäst. När parter använder digital signatur bör förutsättningen vara att den är både säker och lättanvänd. Det som talar för enkel elektronisk signatur är att det inte är onödigt svårt för parter att ingå avtal på elektronisk väg.[119] Det torde även vara så att enkla signaturer kan ge tillräcklig säkerhet i slutna system. Det kan gälla exempelvis sådana system som banker tillhandahåller. Det som talar för kvalificerad elektronisk signatur måste vara att det ställs större säkerhet till förfogande eftersom en sådan signatur är baserad på ett kvalificerat certifikat och skapad av en säker anordning för signaturframställning. Det finns risk för att parterna skulle kunna anse kvalificerad elektronisk signatur som ett krångligare sätt att signera avtal på. Det skulle kunna ha en negativ effekt på antalet avtal som ska ingås elektroniskt.

---

[113] Se avsnitten 6.1.1 och 6.1.2.

[114] 2§ 2st Lag (2000:832) om kvalificerade elektroniska signaturer.

[115] 2§ 10st Lag (2000:832) om kvalificerade elektroniska signaturer.

[116] 2§ 7st Lag (2000:832) om kvalificerade elektroniska signaturer.

[117] 17§ Lag (2000:832) om kvalificerade elektroniska signaturer.

[118] Prop 1999/2000:117 s. 77. Vad kvalificerad signatur är förklaras i avsnitt 6.2 stycke 2.

[119] Ds 2001:13 E-handelsdirektivet – genomförande av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster (2001) s. 111.

Det finns ingenting som säger att avtalslagen inte är tillämplig då det varken definieras i avtalslagen eller annan svensk lagtext vilken form ett avtal ska gestalta.[120] Hur ett avtal ska utformas är upp till parterna vad som stämmer bäst överens med deras krav. Det är egentligen själva förklaringarna från parterna som är det som ska ligga till grund för ett avtal.[121] Det är dessa förklaringar som ska granskas och som kan avgöra om avtal föreligger eller ej. Första kapitlet i avtalslagen visar bara en av flera möjligheter att sluta avtal. Det finns ytterst få undantag där avtal måste ingås skriftligen.[122] Avtal som måste ingås skriftligen för att anses giltigt är exempelvis köp av fast egendom, 4 kap. 1§ jordabalken. För att ansökan om lagfart inte ska förklaras vilande krävs att avtalet bevittnas, 20 kap. 7§ jordabalken.

Lag (2000:832) om kvalificerade elektroniska signaturer har kommit till av den orsaken att svensk lagstiftning måste överensstämma med direktiven på området. Lagen om kvalificerade elektroniska signaturer torde därmed precis som direktiven ses som ett komplement till avtalslagen. Denna lagstiftning säkerställer att elektronisk signatur verkligen har de förutsättningar som krävs för att uppnå samma ställning som en handskriven signatur. Att komplettera redan existerande lagstiftning på det här viset är ett enkelt sätt att anpassa äldre lagstiftning med ny tids förändringar. För att lagstiftning ska vara slagkraftig och ge verkan måste den kunna anpassas till dagens samhälle och de situationer som uppstår.

6.3 Sammanfattning

Reglering i lag är ett grundläggande tillvägagångssätt för att angripa problem som parter kan ställas inför. Lagstiftning inger trygghet och förtroende för att situationer löses på ett sätt som stämmer överens med regler som är satta för samhället. Att reglering av lagar inte enbart sker på nationell nivå utan även på europeisk nivå skapar också trygghet och förtroende. Avtalsrättsligt sett skapar dessa två organs lagregleringar inga problem i Sverige av den orsaken att dessa är så pass samstämmiga. Inga större förändringar behövdes göras inför implementeringen av direktiven eftersom avtalsrätten i Sverige redan gav elektroniska avtal rättslig verkan. Avtalslagen är formad så att alla former av avtal är möjliga att ingå. Dock har det gjorts en komplettering till avtalslagen vilket inte torde ses som en svaghet utan som en förstärkning. Förstärkningen består av att gynna användningen av elektroniska signaturer. Det skulle kunna ses som en sorts assistans för att få igång användningen på allvar, att parterna känner tillit till elektroniska signaturer. Många gånger kan det troligtvis behövas stöd av ett sådant slag och genom att komplettera lagen på det här viset gör lagstiftaren det lätt att anpassa ny lag till ursprunglig lag istället för att göra en lagändring. Det är en snabb utveckling som kräver snabba lösningar och en komplettering till redan existerande lag kvalificerar som en sådan snabb och effektiv lösning.

---

[120] Ds 2001:13 E-handelsdirektivet – genomförandet av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster (2001) s. 38.

[121] Grönfors Kurt Avtalslagen (1995) s. 52.

[122] Ds 2001:13 E-handelsdirektivet – genomförandet av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster (2001) s. 37.

7 Slutsatser

En elektronisk signatur uppstår genom att dokumentet krymps ihop till ett ”hashvärde” som sedan skyddas genom kryptering. Kryptering sker när datasignalerna förvrängs med hjälp av en hemlig nyckel. Meddelandet kan senare dekrypteras antingen med samma nyckel eller med en annan. Den nyckel som innehåller den elektroniska signeringen kan sedan skyddas i ett smart kort som i sin tur skyddas genom en fyrsiffrig PIN-kod som är personlig. För att ta ytterligare steg att göra denna form av kommunikation säker finns det olika BTP som utfärdar certifikat som verifierar att det är rätt signatur och att det är rätt part som har skickat den. Detta får anses vara en komplicerad process som finns tillgänglig att tillgå om parter vill nyttja elektroniska avtal och signaturer. I vissa fall är det fler än två parter som skriver under ett avtal, i detta fall ett handskrivet avtal. Det kan till exempel vara fler delägare involverade som signerar avtalet. Därför måste ett flertal avtal återfinnas för att sedan kunna påverka innehållet eller de namnteckningar som återfinns på dokumenten. Det torde i alla fall inte kunna anses vara lika komplicerat som att försöka kompromettera processen som följer en elektronisk signatur.

Avtalslagen spelar en stor roll vad det gäller elektroniska avtal och signaturer eftersom den ger dessa avtal samma rättsverkan som handskrivna sådana. Känslan av säkerhet ökar i takt med användningen men den stora säkerheten ligger i att kunna styrka sin rätt enligt lag. Viljan att ingå avtal torde utebli i många fall om det inte skulle finns någon laglig grund att stå på förutom avtalet i sig. Avtalet är det centrala men att lyckas få med alla detaljer som rör framtida händelser är svårt. Självfallet ska detta eftersträvas när avtal ingås mellan parter förutom att komma överens om vad som är väsentligt just när avtalet skrivs. I och med implementering av direktiven har avtalslagen kompletterats med en lag som behandlar kvalificerade elektroniska signaturer. Svensk lag tar steget längre än vad det gjorts på EG-nivå och därmed torde det anses som att lagstiftningen i Sverige har ambitionen att ge elektroniska avtal och signaturer samma förutsättningar som handskrivna avtal har säkerhetsmässigt sett. Att svensk avtalsrätt är så pass lätthanterlig och anpassningsbar och därmed kan motsvara de behov som marknaden har måste ses som positivt. Detta kommer sig av att nästan alla avtalsformer är tillämpliga enligt 1§ AvtL, med reservationer för bland annat 33 och 36§§ AvtL. 33 och 36§§ AvtL tillåter inte avtal som strider mot tro och heder eller avtal som anses oskäliga. Att formkrav skulle producera ett bättre resultat torde det inte finnas något stöd för. Det skulle enbart ha en bromseffekt när det gäller avtalsprocessen. Med tanke på hur mycket parter ska kunna lita till ett avtal måste det vara ett avtal som de känner sig bekväma med och därmed bör det vara upp till dem själva att ställa formkrav dem emellan.

Att skriva avtal på ett papper eller på ett elektroniskt dokument gör inte någon skillnad i avtalslagen. Detta beror på att avtalslagen inte klart uttrycker hur ett avtal ska formas. Utöver det finns det direktiv på området som skyddar användandet av både elektroniska avtal och signaturer. Elektroniska avtal liksom handskrivna har tillgång till modellavtal att utgå ifrån när parter ska ingå avtal. Det kan därmed konstateras att det skiljer sig inte i någon större utsträckning mellan att ingå avtal på elektronisk väg gentemot att ingå ett handskrivet avtal.

Det som gör sig påmint och som har betydelse för parterna är hur de ser på användningen av en ny form av kommunikation. Säkerheten spelar troligtvis störst roll men vem som använder den spelar en väldigt stor roll också. Om stora aktörer på marknaden som exempel-

vis Bill Gates[123] skulle ha varit en av de första att använda elektroniska avtal och signaturer skulle mindre företag följa i ett helt annat förlopp än om Gösta Svensson som tillverkar stolar i Gnesta skulle vara först. Därmed kan det förstås att mycket handlar om publicitet och hur en kommunikationsform presenteras för allmänheten. Ju fler som använder elektroniska avtal och signaturer ju fler kommer att anse det vara en säker kommunikationsform. Detta är ett återkommande tema inom många områden. Ett klädesplagg blir bara modernt om majoriteten av människor bär det och om det är rätt designer som står för det. Äta sallad till hamburgaren har inte varit ett alternativ men nu satsas det på ett sundare liv och eftersom berömdheter äter sundare så följer den stora massan trenden. Detta är exempel som uppstår i vardagen men som det ändå kan göras paralleller med till avtalsvärlden.

Nu har möjligheten att deklarera via Internet kommit. På deklarationspapperna erhåller deklaranten en kod för identifiering och en annan kod för underskrift. För att locka den stora massan har skatteverkat tillstått att de som deklarerar via Internet har möjlighet att erhålla sina pengar före midsommar. Trots detta verkar det som om många ändå deklarerar på det traditionella sättet genom att skriva under med sin namnteckning. När det handlar om pengar uppstår ofta en viss försiktighet. Denna tar sig olika utrymme beroende på vad för sorts kommunikationsform som funnits att nyttja en längre tid. Det skämtas i tid och otid om att pensionärer tar ut alla sina pengar och gömmer dem i sina madrasser. Troligtvis och förhoppningsvis göms pengarna inte i madrassen men det är inte ovanligt att pensionärer tar ut sina pengar eftersom de inte anser banken vara tillräckligt säker. En situation vilken nämndes tidigare i detta stycke och som nyligen hamnat i fokus är att deklarera via Internet. Det har inte kunnat göras tidigare och hur säkert det är att deklarera elektroniskt är inte känt och därmed torde det traditionella sättet framstå som tryggare. Vad som troligtvis också är en anledning till att deklarationen sker på traditionellt sätt i större utsträckning än vad det görs via Internet är att det anses komplicerat. Ett nytt sätt att utföra saker på uppfattas många gånger som mer problematiskt än det tillvägagångssätt som finns tillgängligt sedan tidigare. Det enda sättet att få ett tillvägagångssätt att verka lättanvänt är att börja använda det.

Kunskapen om att andra parter använder en viss form av kommunikation stärker förtroendet att använda den och därmed torde känslan av säkerhet stiga. Ett avtal kan bland annat avse ansvarsfördelning som troligtvis kan vara avgörande för att avtalsförhållandet ska fungera. Om en part inte anser att det känns säkert finns det en risk att denne nekar bruket av en sådan avtalsform eller till och med nekar avtalsförhållande om förhållandet bygger på ett elektroniskt avtal. Ytterligare tillvägagångssätt för att uppnå en känsla av säkerhet ligger hos parterna själva. Om ett avtal är säkert beror på hur parterna väljer att skydda sina nycklar precis som hur de väljer att skydda det skrivna dokumentet med signaturen på. En nyckel kan förvaras på ett smart kort med PIN-kod och om det ska anses som säkert beror mycket på hur kortet och PIN-koden förvaras. I vilka situationer som än uppstår måste parterna alltid ställa sig frågan: litar jag på den jag skriver avtalet med? Om svaret är nej bör avtal inte ingås men om så sker bör alla former av säkerhet som parten själv kan sörja för vidtas. Avtal som inte uttryckligen ger klara besked i alla situationer måste tolkas i den form det framstår i avtalet vilket kan leda till både negativa och positiva utfall. Även om parterna litar på varandra och till och med känner varandra bör alla detaljer som kan tänkas komma att hamna i fokus regleras för att undkomma avtalstolkning. Det bör dock tas hänsyn till hur pass flexibelt ett avtal bör vara för att det ska fungera. Ett avtal som är alltför detaljerat tenderar att bli opraktiskt om förhållandet mellan två parter skulle ändras antingen det rör

[123] Bill Gates grundade programvaruföretaget Microsoft 1975.

små eller stora förändringar. Hur pass flexibelt ett avtal bör vara borde beaktas utifrån vad som ska åstadkommas med det aktuella avtalet.

Den utvecklingsprocess som rör elektroniska avtal och signaturer är fortfarande i rörelse och kommer att fortsätta så. För att kunna behålla den form av säkerhetsstatus de når upp till nu måste utvecklingen fortsätta framåt. De privata och publika nycklarna, ”smarta kort”, CA och certifikaten måste hela tiden uppdateras för att kunna anses som tillräckligt säkra. Ju mer elektroniska avtal och signaturer används desto större risk för kompromettering. Allt fler parter kan komma att nyttja denna form av kommunikation och därför kommer desto fler sätt att överlista denna kommunikationsform att uppdagas. En kommunikationsform som bygger på datateknik måste ha en ständigt rörlig utveckling för att kunna överleva och fortsätta anses som säker.

Syftet med uppsatsen var att uppnå förståelse som rör säkerheten av elektroniska signaturer. Är elektroniska signaturer lika säkra som handskrivna? Ja, de är lika säkra då avtalslagen tar hänsyn till elektroniska avtal. Det synes inte heller finns någon anledning att inte erkänna elektroniska avtal samma rättsliga verkan som handskrivna. Nuvarande problem har lösts genom att implementera direktiv genom lagen om kvalificerade elektroniska signaturer som erkänner elektroniska signaturer rättslig verkan. Vad som inte gjorts hittills och som skulle kunna åtgärdas är att reglera CA i lag eftersom CA i rollen som BTP har ett viktigt uppdrag. Det torde vara viktigt att ta hänsyn till förhållanden som rör dessa.

Numera när användare av datorer ska låsa sin dator för att värja sig emot intrång kan de installera sitt tumavtryck som läses av via skärmen. Det kan ses som en sorts kod för att antingen låsa eller låsa upp datorn. Tidigare användes och görs fortfarande en personlig kod som användaren installerar för att låsa och låsa upp datorn. Det skulle kunna tänkas att det är framtidens sätt att tackla problemen med verifiering av om det är rätt part som skriver på ett avtal. Ett tumavtryck som är personligt skulle kunna, efter viss genomarbetning, ändock ses som säker, kanske till och med lika säker som traditionell eller elektronisk signatur.

Referenslista

EU:s lagstiftning

Fördraget om upprättandet av Europeiska Gemenskapen 25 mars 1957, EGT 2002 C 325/33

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 1999/93/EG av den 13 december 1999 om ett gemenskapsverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12, Celex 31999L0093)

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 (”Direktiv om elektronisk handel”) (EGT L 178, 17.7.2000, s. 1, Celex 32000L0031)

Svensk lagstiftning

Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område

Jordabalken (1970:994)

Lag (2000:832) om kvalificerade elektroniska signaturer

Propositioner

Proposition 1999/2000:117

Utskottsbetänkande

Ds 2001:13 E-handelsdirektivet – genomförande av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster

Offentliga utredningar

SOU 1996:40 Elektronisk dokumenthantering

Allmänna Reklamationsnämnden

ARN 97-4042, avgörande 1997-12-04

Rättsfall

NJA 1987 s 692

Litteratur

Adlercreutz, Axel, *Avtalsrätt I,* tolfte upplagan, Studentlitteratur, Lund 2002

Allgårdh Olof och Norberg Sven, *EU och EG-rätten En handbok och lärobok om EU och i EG-rätt,* upplaga 3:1, Norstedts Tryckeri AB, Stockholm 1999

Almen T. och Eklund R., *Lagen om avtal och andra rättshandlingar på förmögenhetsrättens område*, sjunde upplagan, Kungliga Boktryckeriet P.A. Norstedt & Söner, Stockholm 1960

Bidgoli Hossein, *Electric Commerce Principles and Practice*, A Harcourt Science Technology Company, San Diego, California 2002

Eek Hilding, Grönfors Kurt, Hellner Jan, Thornstedt Hans, Vahlén Lennart och Welamson Lars, *JURIDIKENS KÄLLMATERIAL*, nionde upplagan, Norstedts Tryckeri, Stockholm 1979

Franzén Torkel, *Java från grunden,* andra upplagan, Studentlitteratur, Lund 2001

Grönfors, Kurt, *Avtalslagen*, upplaga 3:1, Fritzes Förlag AB , Göteborg 1995

Hultmark, Christina se Ramberg, *Elektronisk handel och avtalsrätt*, Norstedts Juridik AB, Stockholm 1998

Seipel Peter, *Juristen och datorn Introduktion till rättsinformatiken*, upplaga 5:1, Kristianstads Boktryckeri AB, Kristianstad 1994

Seipel Peter, *Juridik och IT Introduktion till rättsinformatik*, upplaga 6:1, Norstedts Tryckeri AB, Stockholm 19997

Rapporter

IRI-rapport 1998:2, Aversten David, *Digitala signaturer och ansvarsproblem Framförallt nyckelinnehavarens och Certification Authority´s ansvar mot förlitande part*, Reprocentralen Stockholms universitet, Stockholm 1998

IRI-rapport 2001:1, Tornéus Mats, *EDI-avtal – ett kommersiellt kommunikationsavtal för utväxling av elektroniska affärsmeddelanden*, Nykopia Tryck AB, Stockholm 2001

Elektroniskt material

EDI-avtal 96, http://hem.passagen.se/vixen/edi/ediavtal.html. Tillgänglig 05-05-19.

EDIS EDI-avtal 98, http://www.nea.nu. Tillgänglig 05-05-20

EDI-avtal 2004, http://www.nea.nu. Tillgänglig 05-05-20

Elektronisk legitimation, http://www.e-legitimation.se. Tillgänglig 05-05-19.

Elektronisk identifiering, http://www.nordea.se/sitemod/default/index.aspx?pid=207924. Tillgänglig 05-05-19

Teldok info nr 17, Maj 1997, Smarta kort – den smarta lösningen?, ISSN 0280-9567,

http://www.teldok.org/. Tillgänglig 05-05-16

Bilaga 1 EDI-avtal 96

EDI-avtal 96

(Meddelandeutväxlingsavtal)

Allmänna villkor

1. Omfattning och syfte

1.1 Detta EDI-avtal reglerar parternas utväxling av elektroniska meddelanden och, i den mån det uttryckligen anges nedan, vilken rättslig betydelse sådana meddelanden skall ha mellan parterna.

1.2 Parterna är överens om att Köpeavtal kan ingås genom utväxling av EDI-meddelanden enligt vad som framgår av detta EDI-avtal och eventuellt ramavtal avseende ingående av Köpeavtal. Detta EDI-avtal reglerar endast form och teknik för utväxling av de EDI-meddelanden som formar ett Köpeavtal.

1.3 Part är bunden av Köpeavtal först när de EDI-meddelanden vilka enligt avtalslagen skall anses vara anbud och accept har utväxlats mellan parterna.

1.4 Den Tekniska bilagan, bilaga 1, preciserar parternas användning av EDI. Om detta EDI-avtal och den Tekniska bilagan innehåller motstridiga bestämmelser har detta EDI-avtal företräde. Den Tekniska bilagan kan komma att förändras under avtalstiden. Ändringar skall vara skriftliga och undertecknade av parterna.

2. Definitioner

I detta EDI-avtal skall följande ord och begrepp ha nedanstående betydelse:

2.1 UN/EDIFACT är FN:s regler för elektroniskt datautbyte för administration, handel och transport, i den utformning de godkänts och publicerats i United Nations Trade Data Interchange Directory (UN/TDID).

2.2 EDI är elektronisk överföring av strukturerade data efter överenskommen meddelandestandard mellan två Informationssystem.

2.3 EDI-meddelanden är en sammanhängande uppsättning med data, som strukturerats efter överenskommen meddelandestandard i ett format som kan överföras mellan och bearbetas av Informationssystem på ett automatiskt sätt.

2.4 Informationssystem är datorsystem (maskin- och programvara), kommunikationsutrustning och övrig utrustning för digital bearbetning, överföring eller lagring av information.

2.5 Mottagningsbekräftelse är ett meddelande som bekräftar att ett EDI-meddelande kommit till det mottagande Informationssystemet och i förekommande fall anger konstaterade fel enligt vad som närmare anges i den Tekniska bilagan.

2.6 Arbetsdag är dag utom lördag, söndag och officiell svensk helgdag i den mån inget annat anges i den Tekniska bilagan.

2.7 Utväxlingslogg är ett historiskt arkiv som innehåller de i den Tekniska bilagan specificerade uppgifterna om samtliga EDI-meddelanden som utväxlats mellan parterna, inkluderade kvittens- och säkerhetsmeddelanden.

2.8 ”TPP” (Third Party Provider) är en tredjeman som till part levererar nätverkstjänster, kommunikationstjänster, databastjänster eller andra tjänster i samband med utväxling av EDI-meddelande enligt detta avtal.

2.9 Köpeavtal är de avtal om bl a köp av varor och tjänster, inkluderade avrop under ett ramavtal mellan parterna, som ingås mellan parterna genom utväxling av EDI-meddelanden enligt detta EDI-avtal.

2.10 Med utväxling av EDI-meddelande avses såväl avsändande som mottagande av EDI-meddelande.

2.11 Med elektronisk adress avses den funktion hos mottagande parts Informationssystem där EDI-meddelanden tas emot eller, om TPP anlitas av mottagande part för att mottaga EDI-meddelanden, den funktion hos TPP där inkommande EDI-meddelanden mottas för parts räkning. Parts elektroniska adress specificeras närmare i den Tekniska bilagan.

3. EDI-system och övrig utrustning

3.1 Parterna skall införa EDI-system enligt detta avtal i enlighet med tidplan som framgår av Teknisk bilaga eller som överenskommes mellanparterna i ett införandeprojekt. Parterna skall genom tester kontrollera att EDI-systemet uppfyller avtalade krav. EDI-systemet skall inte driftsättas för produktion förrän parterna godkänt EDI-systemet. De närmare formerna för tester och godkännande framgår av Tekniska bilagan eller överenskommes mellan parterna under införandeprojektet. Vardera part svarar för sina egna kostnader härför i den mån inget annat anges i den Tekniska bilagan. Vardera part svara för att vid driftsättning och fortlöpande under avtalstiden genom tester och andra metoder tillförsäkra att Informationssystemet uppfyller avtalade krav.

3.2 Part äger rätt att på egen bekostnad och på eget ansvar anlita TPP för att utföra utväxling, bearbetning, lagring eller annan åtgärd avseende EDI-meddelanden.

4. Utväxling av EDI-meddelanden

4.1 Parterna är ense om att de meddelandetyper som anges i Tekniska bilagan skall utväxlas genom EDI. Om EDI-meddelande inte går att avsända genom EDI, får part avsända meddelandet enligt reservrutin om sådan finns beskriven i den Tekniska bilagan eller på sätt som motparten före avsändandet godkänt. Inte heller får andra

meddelanden än de som angivits i den Tekniska bilagan utväxlas genom EDI, såvida inte motparten före avsändandet godkänt detta.

4.2 Om inte annat anges i den Tekniska bilagan, skall samtliga EDI-meddelanden som utväxlas mellan parterna i enlighet med detta avtal följa UN/EDIFACT standarden i de versioner som anges i Tekniska bilagan. Tillämpning av nya versioner förutsätter att parterna träffar överenskommelse härom genom att ändra den Tekniska bilagan.

4.3 Part som mottar EDI-meddelande enligt detta avtal skall behandla och bearbeta EDI-meddelandet utan dröjsmål under de tider som parterna avtalat att EDI-systemet skall vara tillgängligt.

4.4 Vardera part är skyldig att informera sig om de rättsliga krav på EDI-meddelanden som gäller för honom och tillse att EDI-meddelanden utväxlas, bearbetas och lagras i enlighet med dessa krav.

5. Avsändande och mottagande av EDI-meddelande

5.1 Ett EDI-meddelande skall, om inte endera parten kan visa annat, anses avsänt av avsändande part när EDI-meddelandet loggats som avsänt enligt avsändande parts Utväxlingslogg eller – i den mån EDI-meddelande avsänds via parts TPP – enligt Utväxlingslogg som förs hos sådan TPP.

5.2 Ett EDI-meddelande är mottaget när det kommit mottagande part tillhanda enligt vad som anges i denna punkt 5.2. Ett EDI-meddelande skall anses ha kommit mottagande part tillhanda när EDI-meddelandet har kommit till mottagande parts Elektroniska adress så att det kan göras läsbart för mottagande part. om inte endera parten kan visa annat, anses EDI-meddelande ha kommit till mottagande parts Elektroniska adress om det har loggats som mottaget enligt mottagande parts Utväxlingslogg eller – i den mån EDI-meddelandet mottas av parts TPP – enligt Utväxlingslogg som förs hos sådan TPP.

5.3 Ett EDI-meddelande som kommit mottagaren tillhanda kan inte återkallas av den avsändande parten förutom i de fall som anges i 6.3.

6. Mottagningsbekräftelser

6.1 Mottagningsbekräftelser skall avsändas av part som mottager EDI-meddelande i den utsträckning och inom de tidsfrister som anges i den Tekniska bilagan. Om inget krav på Mottagningsbekräftelse anges i den Tekniska bilagan, behöver part som mottager ett EDI-meddelande inte avsända Mottagningsbekräftelse till motparten.

6.2 Mottagningsbekräftelse är endast en teknisk bekräftelse på att ett EDI-meddelande har kommit mottagande part tillhanda och Mottagningsbekräftelse har ingen annan juridisk verkan än att utgöra ett bevis för detta.

6.3 Om part avsänder EDI-meddelande (avsändande part), för vilket Mottagningsbekräftelse skall avsändas av mottagande part, och Mottagningsbekräftelse inte kommit avsändande part tillhanda inom överenskommen tidsfrist, äger avsändande

part återkalla det aktuella EDI-meddelandet varefter detta meddelande inte har någon bindande verkan. Sådan återkallelse skall avsändas utan dröjsmål efter utgången av tidsfristen för avsändande av Mottagningsbekräftelse. Om inte annat anges i den Tekniska bilagan, skall återkallelse av EDI-meddelande ske genom EDI. Om avsändande part inte återkallar EDI-meddelande utan dröjsmål efter utgången av tidsfristen för avsändande av Mottagningsbekräftelse, är EDI-meddelandet bindande för avsändande part på samma sätt som om Mottagningsbekräftelse avsänts och mottagits.

6.4 Om mottagningsbekräftelse skall avsändas, äger part som mottager EDI-meddelande inte vidta åtgärder med anledning av EDI-meddelande före avsändandet av Mottagningsbekräftelse. Parterna är dock medvetna om att bindande Köpeavtal kan kräva att mer än ett EDI-meddelande utväxlas.

7. EDI-meddelandes bindande verkan

7.1 EDI-meddelanden som avsänds i enlighet med detta EDI-avtal skall utgöra för avsändande part bindande förklaringar.

7.2 Part ansvarar för sin egen interna av behörighet för olika EDI-meddelanden. EDI-meddelanden som avsänts från part i enlighet med detta EDI-avtal skall anses vara behörigen avsänt och bindande för avsändande part såvida inte denne kan visa att EDI-meddelandet obehörigen avsänts och att motparten hade eller borde haft kännedom om detta.

8. EDI-meddelandes säkerhet

8.1 Parterna skall införa och underhålla procedur och teknik för att skydda EDI-meddelanden och Utväxlingsloggen mot obehörig tillgång, förvanskning, försening och mot förlust av information. Den närmare utformningen av datasäkerheten framgår av den Tekniska bilagan. Part skall vidare behandla EDI-meddelanden konfidentiellt enligt vad som anges i punkt 9.

8.2 Datasäkerheten innefattar, men är inte begränsat till, att EDI-meddelandes innehåll och utställare skall kunna verifieras på ett tillförlitligt sätt.

8.3 Om ett EDI-meddelande inte kan utväxlas eller om ett tekniskt fel eller förvanskning upptäcks i ett EDI-meddelande, skall motparten omedelbart meddelas. Meddelandet skall sändas på sätt som anges i den Tekniska bilagan eller, om inget anges, genom telefax. Parterna är därefter inte skyldig att motta eller sända EDI-meddelande till dess att bristen avhjälpts.

8.4 Part har rätt att, på egen bekostnad, genom oberoende revisor kontrollera att motparten uppfyller sina förpliktelser enligt denna punkt 8, kompletterad med den Tekniska bilagan. Den part som anlitar TPP skall verka för att även TPP är skyldig att tillåta kontroll enligt denna punkt. TPP omfattas dock av kontrollskyldighet först efter särskild överenskommelse.

9. Sekretess

9.1 Information som part erhåller genom Informationsutbytet enligt detta EDI-avtal, med undantag av vad som följer av 9.3, får inte utnyttjas för annat ändamål än som avsetts av parterna eller avslöjas för utomstående om inte motparten på förhand skriftligen medgivit detta. Sekretesskyldigheten gäller inte information som part kan visa var allmänt känd eller som kommit till parts kännedom från tredje man utan brott mot detta avtal.

9.2 För det fall Part anlitat TPP, skall Part tillse att TPP är bunden av sekretess enligt punkt 9.1.

9.3 För det fall information hos part är att anse som allmän handling, skall för denna part vad som sägs i lag rörande allmänna handlingars offentlighet respektive sekretess äga tillämpning före vad som anges i 9.1 och 9.2.

9.4 Om part mottager EDI-meddelande som avsänts av motpart och som uppenbart är avsett för annan, är den mottagande parten skyldig att omedelbart meddela avsändande part att radera meddelande, dock inte ur Utväxlingsloggen.

10. Lagring av Utväxlingslogg och EDI-meddelanden

10.1 Vardera parten skall föra en komplett Utväxlingslogg över de EDI-meddelanden som avsänds av part respektive kommer part tillhanda. Utformningen av Utväxlingsloggen anges i den Tekniska bilagan.

10.2 Vardera parten skall lagra och bevara Utväxlingsloggen och de EDI-meddelanden som kommit part tillhanda i enlighet med de krav som framgår av för part tillämplig lag eller, om något sådant krav ej uppställts, i minst tre år eller den tid som anges i den Tekniska bilagan. Lagring av EDI-meddelanden sker i överföringslogg. Vardera part ansvara för att parten uppfyller de lagrings- och arkiveringsregler som är tillämpliga för parten. Lagring skall ske på ett betryggande sätt och på ett sätt som förhindrar ändring, förlust och obehörig åtkomst. Lagrad information skall kunna tas fram i läsbar form när som helst under lagringstiden.

10.3 Part är skyldig att på begäran från motparten omgående till motparten tillhandahålla begärda utdrag ur sin Utväxlingslogg rörande mellan parterna EDI-meddelanden. Utdragen skall vara i läsbar form och tillhandhållas till självkostnad.

10.4 Part har rätt att, på egen bekostnad, genom oberoende revisor kontrollera att motparten och, i förekommande fall, TPP uppfyller sina förpliktelser enligt denna punkt 10, kompletterad med den Tekniska bilagan.

11. Ansvar

11.1 Parts skadeståndsansvar för egen och av part anlitad tredje mans försummelse enligt detta EDI-avtal omfattar, såvida inte uppsåt eller grov vårdslöshet föreligger, endast ersättning för direkt förlust och är per skadetillfälle begränsat till 35 gånger det vid tiden för skadans uppkomst gällande basbelopp enligt lagen (1962:381) om

allmän försäkring. Part ansvarar således inte för indirekt skada såsom utebliven vinst, förväntad besparing eller förlust av inkomst.

11.2 Om parts fullgörelse av detta avtal förhindras eller försvåras av omständighet utanför hans kontroll som han inte skäligen kunde förväntas ha räknat med vid avtalets träffande och vars följder han inte heller skäligen kunde ha undvikit eller övervunnit eller av att hand underleverantörs fullgörelse av leverans förhindras eller försvåras på grund av omständigheter som här angivits, skall detta utgöra befrielsegrund, som medför framflyttning av tidpunkten för prestation och befrielse från påföljd enligt detta EDI-avtal.

11.3 I enlighet med regleringen av EDI-avtalets omfattning, punkt 1, avser ansvarsbegränsning enligt denna punkt 11 endast parts skadeståndsansvar för försummelse enligt detta EDI-avtal. Denna ansvarsbegränsning påverkar inte den ansvarsreglering som följer av Köpeavtal.

12. Avtalstid

12.1 Detta EDI-avtal gäller tills vidare med tre (3) månaders ömsesidig uppsägningstid.

12.2 Part äger säga upp avtalet till omedelbart upphörande om motparten har gjort sig skyldig till väsentligt kontraktsbrott och motparten inte vidtager rättelse inom trettio (30) dagar från det att han fått skriftligt meddelande med begäran därom.

12.3 Part äger vidare säga upp avtalet till omedelbart upphörande om motparten försätts i konkurs eller ansökan om försättande i konkurs inges till domstol, träder i likvidation, inleder ackordförhandlingar, blir föremål för företagsrekonstruktion eller av annan anledning kan antas vara på obestånd.

12.4 Efter avtalets upphörande gäller alltjämt åtagandena rörande sekretess (9.1, 9.2), bevarande av Utväxlingsloggen och EDI-meddelanden (10.1, 10.2) och utlämnande av meddelande ur Utväxlingsloggen (10.3).

13. Ändringar och tillägg

13.1 Ändringar och tillägg till detta EDI-avtal skall, för att vara gällande, vara skriftliga och underskrivna av behöriga ställföreträdare för båda parter.

14. Överlåtelse

14.1 Ingen av parterna kan överlåta sina rättigheter eller skyldigheter enligt detta EDI-avtal till en tredje man utan den andre partens skriftliga godkännande.

15. Tillämplig lag och tvistelösning

15.1 Svensk rätt skall äga tillämpning på detta EDI-avtal.

15.2 Tvist enligt detta avtal skall avgöras av svensk allmän domstol.

15.3 I händelse av konflikt mellan val av lag och forum mellan detta EDI-avtal och Köpeavtal avseende tvist som berör båda avtalen, skall vad som anges i detta EDI-avtal äga företräde och äga tillämpning även för Köpeavtalet.

Bilaga 2 EDIS EDI-avtal 98

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 1 -

Rekommendation

för utformning av EDI-avtal

EDIS EDI-Avtal 1998

inklusive Teknisk Bilaga med malltexter och förklaringar

Utgiven av EDI-föreningen i Sverige (EDIS)

Detta EDI-Avtal fastställdes av

EDIS Styrelse 30 november 1998.

Ansvaret för Avtalets förvaltning och

vidareutveckling har därefter övertagits av

GEA, Gemenskapen är Elektroniska

Affärer.

För mer information:

gea@gea.ihb.se

http://www.gea.nu/

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 2 -

Innehåll: Sida

KAPITEL 1: INTRODUKTION

1.1 BAKGRUND 3

1.2 EDIS EDI-AVTAL 1998..... 3

1.3 ÖVRIGA DELAR AV RAPPORTEN 4

1.4 MÅLGRUPP FÖR RAPPORTEN..... 4

1.5 AVGRÄNSNINGAR..... 5

1.6 PUBLICERING..... 5

1.7 ARBETSGRUPPEN..... 5

1.8 SYNPUNKTER OCH KOMMENTARER UTANFÖR ARBETSGRUPPEN..... 6

1.9 FASTSTÄLLELSE I EDIS STYRELSE..... 6

Kapitel 2: EDIS EDI-AVTAL 1998

2.1 EDI-AVTAL 1998 -- KONTRAKTSFORMULÄR 7

2.2 EDI-AVTAL 1998 -- ALLMÄNNA BESTÄMMELSER 10

2.3 EDI-AVTAL 1998 -- TEKNISK BILAGA (MALLDOKUMENT) 16

KAPITEL 3: EXEMPEL PÅ ANDRA BILAGOR TILL ETT EDI-AVTAL (UPPGIFTER OM PARTER)23

KAPITEL 4: ILLUSTRATIONSEXEMPEL VID ANVÄNDNING AV EDIS EDI-AVTAL 1998 27

KAPITEL 5: TEKNISK BILAGA MED MALLAR, ALTERNATIV OCH FÖRKLARINGAR 36

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

Kapitel 1: Introduktion

1.1 Bakgrund

I takt med att antal EDI-tillämpningar växer, ökar behovet av att i ett avtal reglera de förutsättningar som parterna avser skall gälla. Förslag till modellavtal och standardavtal har tidigare utvecklats både internationellt och nationellt. Gemensamt för dessa är att det är de juridiska förhållandena som regleras, ofta med utgångspunkt i de affärsmässiga relationer som tillämpas inom utvecklarnas bransch eller sektor, medan däremot inget eller ringa stöd ges för utformning av de tekniska lösningarna.

EDIS styrelse tillsatte därför en Arbetsgrupp under Tekniska Rådet med uppgift att under 1998 ta fram en rekommendation för hur EDI-avtal som helhet bör utformas. Till uppdraget fogades kravet att resultatet skulle vara **generellt** tillämpbart, enkelt och lättanvänt och ge

stöd till, inte minst, små och medelstora företag i deras utveckling av EDI-relationer.

En utgångspunkt för arbetet har varit EDI-avtal 96, som i samband med projektet Elektronisk

Handel utvecklades av IT-företagen, Landstingsförbundet, Statskontoret och Svenska

Kommunförbundet. Arbetsgruppen har dock funnit skäl att modifiera förebilden, dels för att

höja dess profil som allmänna bestämmelser med generell tillämpbarhet vid EDI, dels för att

ge tydligare kopplingar till de tekniska lösningar som är vanliga på marknaden.

Resultatet av arbetet i EDIS Tekniska Råd presenteras nu i form av denna Tekniska Rapport,

EDIS Rekommendation för utformning av EDI-avtal.

1.2 EDIS EDI-Avtal 1998

En väsentlig del av EDIS Tekniska Rapport nr 6 utgörs av det som i kapitel 2 kallas för EDIS

EDI-Avtal 1998. Där beskrivs tre viktiga komponenter i ett EDI-avtal, nämligen Kontraktsformulär,

Allmänna Bestämmelser samt Teknisk Bilaga.

De tre delarna av EDIS EDI-Avtal 1998 presenteras efter något varierande princip beroende

på sin karaktär:

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 4 -

• **EDI-Avtal 1998 – Kontraktsformulär** är en mall för avtalsparternas underskrift. Det är

ett formulär för ifyllande av variabla uppgifter. Mallen kan också kompletteras med

uppgift om vilka bilagor som ingår i ett givet avtal.

• **EDI-Avtal 1998 -- Allmänna Bestämmelser** är ett fast dokument där ingen komplettering

eller strykning skall behöva ske. Dokumentet avses utgöra en obligatorisk bilaga till varje

enskilt EDI-avtal mellan två parter.

• **EDI-Avtal 1998 -- Teknisk Bilaga** innehåller 10 avsnitt där det kan finnas behov av att

specificera hur EDI-trafiken mellan två parter skall ske. För varje avsnitt finns det en

rekommendation till avtalstext, samt förslag till hur man utformar kompletterande detaljspecifikationer. EDI-Avtal 1998 – Teknisk Bilaga är sålunda en _lathund_ som beskriver de val som parterna måste göra, och som för varje val anger lämplig avtalstext. Avtalstexterna kan kopieras över till den tekniska bilaga som avses utgöra en obligatorisk bilaga till varje enskilt EDI-avtal.

Rekommendationen förutsätter att det finns ett överordnat affärsavtal som reglerar parternas affärsrelation, och att EDI-avtalet enbart behandlar användning av EDI-teknik för att utväxla informationen mellan parterna.

1.3 Övriga delar av rapporten

Utöver de obligatoriska bilagorna enligt EDIS EDI-Avtal 1998 kan det speciellt i större organisationer finnas behov av ytterligare uppgifter i ett EDI-avtal. Ett sådant exempel är förteckning av associerade parter som också omfattas av EDI-avtalet. Detta behandlas i ett separat avsnitt av rapporten, och där finns också förslag till mallar med lämpliga avtalstexter.

Andra exempel kan vara bilagor om speciell kostnadsfördelning, avsiktsförklaringar som införandeplaner eller driftsstart, eller operativ information som sändningstider, frekvens och volym. Utformning av sådana bilagor överlåts på användarna själva eller deras företrädare inom branschgrupperingarna.

I rapporten ges också ett illustrationsexempel på ett komplett avtal utformat enligt EDIS EDIAvtal 1998. Det ger en uppfattning om antalet sidor i ett verkligt EDI-avtal mellan två parter.

Det är denna informationsmängd som en enskild användare kommer i kontakt med i samband med avtalstecknande.

1.4 Målgrupp för rapporten

EDIS Teknisk Rapport nr 6 avses utgöra ett stöd till de som utformar standardiserade EDIavtal för användargrupperingar, koncerner eller i partsspecifika relationer. Målgruppen antas ha goda insikter i EDI eller tillgång till EDI-teknisk expertis.

Kontraktsformulär

Ev övriga

bilagor

Teknisk

bilaga

Allmänna

bestämmelser

EDI-avtalets struktur:

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 5 -

Genom att utgå från EDIS EDI-Avtal 1998 är det EDIS förhoppning att man skall uppnå en

enhetlig struktur för EDI-avtal, med enhetliga formuleringar av avsnitt som återkommer i alla

avtal. Formen av mall har också medvetet använts för att i EDI-Avtalets grundutförande

begränsa antalet alternativ i tekniska lösningar, så att införande av EDI i större skala

underlättas och förbilligas.

EDIS EDI-Avtal 1998 ger utrymme för att tillägg, underbilagor etc kan tillföras för att ge

kompletterande regler och bestämmelser där parterna så önskar. Exempel på avsnitt som

användargrupper behöver komplettera är beskrivning av protokoll för datakommunikation och

säkerhetslösningar. Detta kan lösas så att ansvariga för ett branschområde eller organisation

utformar ett standardavtal för sina EDI-användare baserat på EDIS EDI-Avtal 1998.

1.5 Avgränsningar

EDIS Teknisk Rapport nr 6 återspeglar dagens sätt utforma datautväxling med EDI.

Rapporten är framtagen utifrån en modell för kommunikation genom traditionell, satsvis EDI.

EDIS EDI-Avtal 1998 förutsätter ingen specifik standard för EDI-lösningen. Däremot är

många av mallarna i den Tekniska Bilagan skapade med UN/EDIFACT som grund, vilket är

en följd av att den är den vanligast använda standarden, med genomslag i många

användargrupper. I mallarnas specifikationer uttrycks även vissa preferenser för EDIFAC-Tanvändning

utifrån samlad erfarenhet.

Det är angeläget att understryka att det rekommenderade EDI-Avtalets struktur och tänkta

användning tillåter såväl andra val inom ramen för UN/EDIFACT som användning av helt

andra satsvisa syntaxer. Det har emellertid ej känts meningsfullt att arbetsgruppen specificerar

alternativen för dessa fall, utan detta överlämnas åt de som utformar standardiserade EDI-avtal.

Den Tekniska Bilagan ger således ett mer genomarbetat underlag vid användning av

UN/EDIFACT, men endast en stomme vid andra alternativ.

1.6 Publicering

Denna Tekniska Rapport, inklusive formulär och textmallar, kan hämtas från EDIS

webbplats, www.edis.se.

1.7 Arbetsgruppen

I EDIS Arbetsgrupp för EDI-Avtal med Teknisk Bilaga har följande personer ingått:

Gösta Mellquist, EDIFACT Transport, ordförande

Leif Forsman, EDIFACT Transport (till 15 augusti 1998)

Jeremy Morton, EDI Center Handel

Sten Lindgren, Svenska Odette

Sören Lennartsson, sekreterare

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

Bengt Kriström, Verkstadsindustrierna, har bidragit med juridisk expertis vid utformning av

Allmänna Bestämmelser för EDIS EDI-Avtal 1998.

1.8 Synpunkter och kommentarer utanför arbetsgruppen

Under arbetets gång har särskilda överläggningar hållits med företrädare för olika

intressenter inom EDIS, inte minst utifr ån olika juridiska och legala frågeställningar.

En arbetsutgåva distribuerades den 1 september 1998 till samtliga medlemmar i EDIS.

De många värdefulla kommentarer som därvid kommit in har bildat underlag vid

Arbetsgruppens överväganden inför sammanställningen av föreliggande utgåva av EDIS

Tekniska Rapport nr 6. Synpunkterna har inkommit från

- Bankföreningen, genom Barbro Hedström och Nicklas Skår

- Byggentreprenörerna, genom Claes Winberg

- Ann Börestam

- Peter Fredholm

- Ulf Höglind, Högskolan Örebro

- ICA, genom Bo Wieweg

- Kommunförbundet, genom Hans Ekman och Kerstin Wiss Holmdahl

- Landstinget Östergötland, genom Anders Norr

- Schenker - BTL, genom Per Stenberg

- Statskontoret, genom Christina Thorsson.

De finns publicerade som separat dokument på EDIS webb (se 1.6 ovan).

1.9 Fastställelse i EDIS styrelse

Denna rapport har antagits för publicering som EDIS Teknisk Rapport den 30 november 1998

av EDIS styrelse.

Styrelsen uttalade samtidigt att EDIS bör svara för att samla in synpunkter och erfarenheter

från användarna när avtalet kommer i bruk. Genom en sådan förvaltningsprocess kan EDIS

åtaga sig att behandla inkomna synpunkter löpande och vid behov publicera en ny version av

rapporten, detta förutsätts dock inte behöva ske tidigare än under hösten 1999. Ansvaret för

denna förvaltning avses som hittills ligga inom Tekniska Rådet.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

Kapitel 2: EDIS EDI-Avtal 1998

2.1 EDI-Avtal 1998 -- Kontraktsformulär

Detta formulär för EDI-avtal ger en fast ifyllnadsmall för identifierande uppgifter om de avtalsslutande parterna, till EDI-avtalet hörande bilagor samt tid och plats då EDI-avtalet sluts.

Mallen skall endast ändras vad gäller i ingående bilagor.

Not. Kontraktsformuläret är framtaget för användare som tecknar separat EDI-avtal. Användare som så föredrar kan i stället inordna EDI-avtalets bilagor direkt i affärsavtalet, varvid kontraktsformuläret ej blir tillämpligt.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 8 -

Avtalsblad med underskrifter

Komplett formulär visas på nästa sida. Här nedan ges kommentarer till avtalssidans olika komponenter.

Rubriken EDI-avtal

- Med begreppet EDI-avtal avses denna avtalssida samt däri angivna bilagor.

Identifikation av avtal

- Den entydiga identifikationen av avtalet utgörs av parternas namn samt datum för underskrift. EDI-avtalet kan vid behov tilldelas ett avtalsnummer för att underlätta referens.

Parter och underskrifter

- Ett EDI-avtal träffas alltid mellan två parter.
- Om avtalet skall gälla även för andra organisatoriska enheter skall dessa anges i separat partsbilaga.
- I partsbilagan kan även anges identifikationsbegrepp, lokaliseringskoder, leveransadresser mm.

Bilagor

- Innehåll och utformning av bilagorna beskrivs i separata kapitel i denna rekommendation.
- Bilagan för Allmänna Bestämmelser och Teknisk Bilaga skall alltid förekomma (se kapitel

2.2 respektive 2.3).

• Separat partsbilaga kan användas vid behov (se kapitel 3).

• Ytterligare bilagor kan föras till enligt de avtalsslutande parternas önskemål.

Underbilagor

• Till Tekniska Bilagan kan förekomma underbilagor. Dessa har samma _avtalsenliga status_ som övriga bilagor.

Ändring av EDI-avtalet

• Regler för hur EDI-avtalet eller där ingående bilagor kan ändras framgår av Allmänna Bestämmelser.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 9 -

EDI-avtal

Avtalsnummer: _____

Part 1 Part 2

Företag/myndighet Företag/myndighet

_____ _____

Postadress Postadress

_____ _____

Postnummer _____ Postnummer _____

Postort _____ Postort _____

Organisationsnummer Organisationsnummer

_____ _____

Ovan angivna parter ingår härigenom avtal om utväxlande av EDI-meddelanden.

Villkoren för denna utväxling framgår av denna sida jämte nedanstående bilagor.

Bilagor:

1. Allmänna bestämmelser (inkluderas alltid)

2. Teknisk bilaga jämte underbilagor (inkluderas alltid)

3. Uppgifter om parter (inkluderas vid behov)

4. ...

Detta avtal har upprättats i två exemplar, varav parterna har tagit var sitt.

Ort _____ Ort _____

Datum _____ Datum _____

Företag/myndighet Företag/myndighet

_____ _____

Underskrift Underskrift

_____ _____

Namnförtydligande Namnförtydligande

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 10 -

2.2 EDI-Avtal 1998 -- Allmänna Bestämmelser

Allmänna Bestämmelser avses utgöra en bilaga med fast text som skall kunna användas generellt i EDI-avtal utan ändringar. Uppgifter som kan variera i olika partsrelationer beskrivs antingen i den Tekniska Bilagan, i partsbilagan eller, om parterna har specifika behov, i egenutvecklad fristående bilaga.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 11 -

1. Omfattning och syfte

1.1 Detta EDI-avtal reglerar parternas utväxling av information i form av elektroniska meddelanden. Det kompletterar parternas affärsavtal och påverkar inte i övrigt parternas relation.

1.2 Parterna är ense om att utväxla information med EDI på det sätt som specificeras i Tekniska Bilagan. Den Tekniska Bilagan preciserar parternas användning av EDI. Om dessa Allmänna Bestämmelser och den Tekniska Bilagan innehåller motstridiga bestämmelser har dessa Allmänna Bestämmelser företräde.

2. Definitioner

Med EDI-avtalet avses i dessa bestämmelser parternas skriftliga avtal om utväxlande av EDImeddelanden

med samtliga bilagor jämte eventuella underbilagor och avtalade ändringar och

tillägg.

I EDI-avtalet skall följande ord och begrepp ha nedanstående betydelse:

2.1 EDI-meddelande är en sammanhängande uppsättning med data, som strukturerats efter

överenskommen meddelandestandard i ett format som kan överföras mellan och bearbetas av

parternas informationssystem på ett automatiskt sätt.

2.2 Med EDI avses elektronisk utväxling av EDI-meddelanden mellan två parters

informationssystem. Med utväxling av EDI-meddelande avses såväl avsändande som mottagande

av EDI-meddelande.

2.3 Med en överföring avses en enhet bestående av ett eller flera EDI-meddelanden som

utväxlas samlat vid ett och samma tillfälle mellan två parter.

2.4 Med en utväxlingsfil avses den dataenhet som utväxlas mellan två kommunikationssystem

vid ett och samma utväxlingstillfälle. En utväxlingsfil kan innehålla en eller flera

överföringar, men det finns ingen allmängiltig princip för att ge information om vilka

överföringar som ingår.

2.5 Informationssystem är datorsystem (maskin- och programvara), kommunikationsutrustning

och övrig utrustning för bearbetning och lagring av information. Med

informationssystem avses i EDI-avtalet kommunikationssystem, EDI-system och

affärssystem.

2.5.1 Med kommunikationssystem avses de delar av ett informationssystem som hanterar

extern fysisk kommunikation mellan datorer. Ett kommunikationssystem har alltid en

kommunikationsadress, som entydigt anger hur en utväxlingsfil skall komma

kommunikationssystemet tillhanda.

2.5.2 Med EDI-system avses de delar av ett informationssystem som bearbetar, lagrar,

övervakar och journalför enskilda överföringar. Ett EDI-system har alltid en

överföringsadress, som inom ramen för en parts kommunikationssystem anger hur en

överföring skall komma EDI-systemet tillhanda.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 12 -

2.5.3 Med affärssystem avses i EDI-avtalet de delar av ett informationssystem som bearbetar

ett enskilt EDI-meddelande och dess innehåll ur funktionell synpunkt. Adressen till ett

affärssystem identifieras av EDI-systemet vid dess bearbetning av den överföring som EDImeddelandet

ingår i.

2.6 Med TPP (Third Party Provider) avses en tredjeman som för parts räkning tillhandahåller

kommunikationssystem och/eller EDI-system i samband med utväxling av EDI-meddelanden

enligt EDI-avtalet. Om en part anlitar TPP skall därvid med partens kommunikations-adress

respektive överföringsadress avses motsvarande funktioner hos TPP.

2.7 Med affärsavtal avses det avtal om köp av varor och tjänster, inklusive avrop under ett

ramavtal, eller annat avtal, med avseende på vilket parterna utväxlar meddelanden enligt EDIavtalet.

2.8 En utväxlingslogg är ett tidsbegränsat arkiv som best år av en överföringslogg och en

händelselogg. De två delarna kan rent tekniskt realiseras som en logg eller två separata loggar.

2.8.1 Med överföringslogg avses en logg som omfattar sända och mottagna överföringar

inklusive däri ingående EDI-meddelanden.

2.8.2 Med händelselogg avses en logg som innehåller de i Tekniska Bilagan specificerade

uppgifterna om händelser som registrerats vid behandling av samtliga överföringar.

2.9 Mottagningsbekräftelse är ett bevis i elektronisk form, ej nödvändigtvis ett EDImeddelande,

på att en utväxlingsfil, överföring eller EDI-meddelande har kommit mottagande

part tillhanda och att denne därmed övertagit ansvaret för vidare behandling.

2.9.1 En utväxlingskvittens är ett bevis på att en utväxlingsfil har mottagits av

kommunikationssystemet och utväxlingstekniska kontroller gjorts.

2.9.2 En överföringskvittens är ett bevis på att en viss överföring har nått fram till mottagande

parts EDI-system på där angiven överföringsadress, och där har genomgått syntaxkontroller.

2.9.3 En meddelandekvittens är ett bevis på att ett visst EDI-meddelande nått fram till

mottagande parts EDI-system på där angiven överföringsadress, och där har genomgått

syntaxkontroller.

2.9.4 En affärskvittens är ett bevis på att ett visst EDI-meddelande nått fram till parts

affärssystem, och där har genomgått kontroller av datainnehåll.

2.9.5 En positiv kvittens innebär att inga formella fel har upptäckts vid kontroller som har

utförts fram till tillfället för kvittensens avsändande. Omfattningen på utförda kontroller sker

efter mottagande parts eget val.

2.9.6 En negativ kvittens innebär att formella fel har upptäckts, att vidare behandling har

avbrutits, och att ansvaret för utväxlingen åvilar part som avsänt utväxlingsfil, överföring eller

EDI-meddelande.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

3. Informationssystem för EDI-utväxling

3.1 Parterna svarar var för sig för att de har tillgång till informationssystem som möjliggör

avtalad utväxling av EDI-meddelanden. Gränssnitten för de kommunikationssystem som

parterna använder skall specificeras i Tekniska Bilagan.

Vardera parten skall vid driftsättning och fortlöpande under avtalstiden genom tester och

andra metoder tillförsäkra att Informationssystemet uppfyller kraven enligt detta avtal.

Vardera parten svarar för sina egna kostnader för EDI-utväxling, i den mån inte annat avtalas.

3.2 Part äger rätt att på egen bekostnad och på eget ansvar anlita annan för att utföra

utväxling, bearbetning, lagring eller annan åtgärd avseende EDI-meddelanden. För det fall

parterna anlitar samma TPP eller annan tredje man och fråga uppkommer om ansvar för viss

åtgärd denna vidtagit bär den part, för vars räkning åtgärden vidtagits, ansvaret gentemot den

andra parten.

3.3 Part som avser ändra delar av sitt informationssystem på sätt som kan förväntas påverka

utväxling av EDI-meddelanden, skall meddela avtalspartnern detta i så god tid att parterna

gemensamt kan genomföra erforderliga tester för att säkerställa att EDI-utväxlingen kan ske

på avtalat sätt även efter ändring av informationssystemet.

4. Utväxling av EDI-meddelanden

4.1 Om ett meddelande inte kan utväxlas genom EDI, eller om förvanskning upptäcks i ett

EDI-meddelande, skall motparten omedelbart meddelas. Part får därefter avsända

informationen enligt reservrutin som anges i Tekniska Bilagan eller enligt förfarande som i

förväg godkänts av motparten. Om parterna använder reservrutin skall de, efter att felet

avhjälpts, tillsammans bedöma behovet av tester innan utväxling genom EDI återupptas.

4.2 Part som mottar EDI-meddelande enligt EDI-avtalet skall behandla och bearbeta EDImeddelandet

utan dröjsmål under de tider som anges för EDI-systemens öppethållande i

Tekniska Bilagan.

5. Utväxlingslogg

5.1 Vardera parten skall som en del av sitt informationssystem föra en utväxlingslogg enligt

nedanstående beskrivning.

5.2 Avsikten med utväxlingsloggen är att kunna återskapa, och göra om bearbetningar av

överföringar samt ge underlag för avstämning/bevisning av EDI-meddelandens status i

respektive informationssystem.

5.3 Loggning i utväxlingslogg skall ske som en del av respektive parts EDI-system.

Utväxlingsloggen skall sparas under en tidsperiod som anges i Tekniska Bilagan.

5.4 Vid tvist eller felsituationer har part rätt att få utdrag ur andra partens utväxlingslogg

avseende den gemensamma EDI-trafiken. Utdrag skall vara i läsbar form och tillhandahållas

utan kostnad.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 14 -

6. Mottagningsbekräftelser och kvittenser

6.1 Om mottagningsbekräftelse överenskommits i den Tekniska Bilagan skall mottagande

part avsända mottagningsbekräftelse till motparten efter mottagande av utväxlingsfil,

överföring eller EDI-meddelande.

6.2 Mottagningsbekräftelser och andra kvittenser skall avsändas av part som mottager EDImeddelande

i den utsträckning och inom de tidsfrister som anges i den Tekniska Bilagan.

7. EDI-meddelandes bindande verkan

7.1 I den mån affärsavtal eller regler i lag eller annan författning kräver att meddelande

lämnas skriftligen anses detta krav uppfyllt av EDI-meddelande som utväxlas enligt EDIavtalet.

7.2 Ett EDI-meddelande skall, om inte annat visas, anses avsänt av avsändande part när den

överföring som EDI-meddelandet ingår i har loggats som avsänt enligt avsändande parts

Utväxlingslogg eller, i den mån EDI-meddelande avsänds via parts TPP, enligt

Utväxlingslogg som förs hos sådan TPP.

7.3 Ett EDI-meddelande skall, om inte annat visas, anses ha kommit mottagande part tillhanda

när den överföring som det ingår i har loggats som mottaget enligt mottagande parts

Utväxlingslogg eller, i den mån parten utnyttjar TPP, enligt Utväxlingslogg som förs hos

denne. Den av parterna som står risken för att ett EDI-meddelande förloras eller försenas står

också risken för att EDI-meddelandet förvanskas vid överföringen.

7.4 EDI-meddelande som avsänds från part i enlighet med EDI-avtalet skall anses vara

behörigen avsänt och bindande för avsändande part såvida inte denne kan visa att EDImeddelandet

obehörigen avsänts och att motparten hade eller borde haft kännedom om detta.

7.5 Om part avsänder EDI-meddelande (avsändande part), för vilket Mottagningsbekräftelse

skall avsändas av mottagande part, och Mottagningsbekräftelse inte kommit avsändande part

tillhanda inom överenskommen tidsfrist, äger avsändande part återkalla det aktuella EDI-meddelandet

varefter detta meddelande inte har någon bindande verkan. Sådan återkallelse

skall avsändas utan dröjsmål efter utgången av tidsfristen för avsändande av Mottagningsbekräftelse.

Återkallelse skall ske per telefax eller e-post, såvida det inte i Tekniska Bilagan

specificeras ett särskilt meddelande för detta.

Om avsändande part inte återkallar EDI-meddelande utan dröjsmål efter utgången av

tidsfristen för avsändande av Mottagningsbekräftelse, är EDI-meddelandet bindande för

avsändande part på samma sätt som om Mottagningsbekräftelse avsänts och mottagits.

8. EDI-meddelandens säkerhet

8.1 Parterna skall införa och underhålla procedurer och teknik för att skydda EDImeddelanden

och Utväxlingsloggen mot obehörig tillgång, förvanskning, förlust av

information och annan skada. Den närmare utformningen av datasäkerheten vad gäller

utväxling av EDI-meddelanden framgår av Tekniska Bilagan.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

- 15 -

9. Sekretess

9.1 Information som part erhåller genom informationsutbytet enligt EDI-avtalet skall hanteras

enligt de sekretessregler som framgår av affärsavtalet. För det fall Part anlitar TPP, skall Part

tillse att TPP är bunden av sådan sekretess.

9.2 För det fall information hos part är att anse som allmän handling, skall för denna part vad

som sägs i lag rörande allmänna handlingars offentlighet respektive sekretess äga tillämpning.

9.3 Om part mottager EDI-meddelande som avsänts av motpart och som uppenbart är avsett

för annan, är den mottagande parten skyldig att omedelbart meddela avsändande part och

radera meddelandet, dock inte ur Utväxlingsloggen.

10. Ansvar

10.1 Parts ansvar för egen och av part anlitad TPP eller annan tredje mans försummelse enligt

EDI-avtalet skall i första hand regleras enligt bestämmelserna i affärsavtalet.

10.2 Part har rätt att, på egen bekostnad, genom oberoende revisor kontrollera att motparten

uppfyller sina förpliktelser enligt EDI-avtalet. Den part som anlitar TPP skall tillse att även

TPP är skyldig att tillåta kontroll enligt denna punkt.

11. Avtalstid

11.1 EDI-avtalet gäller, om inte annat avtalas, tills vidare med tre (3) månaders ömsesidig

uppsägningstid.

11.2 Part äger säga upp avtalet till omedelbart upphörande om motparten har gjort sig skyldig

till väsentligt kontraktsbrott och motparten inte vidtager rättelse inom trettio (30) dagar från

det att han fått skriftligt meddelande med begäran därom.

11.3 Efter avtalets upphörande gäller alltjämt åtagandena rörande bevarande av

Utväxlingsloggen, utlämnande av meddelande ur Utväxlingsloggen samt sekretess.

12. Ändringar och tillägg

12.1 Ändringar och tillägg till dessa Allmänna Bestämmelser skall, för att vara gällande, vara

skriftliga och underskrivna av behöriga ställföreträdare för båda parter. Den Tekniska Bilagan

kan komma att förändras under avtalstiden. Ändringar skall vara skriftliga.

13. Tillämplig lag och tvistlösning

13.1 Vid tvist med anledning av EDI-avtalet skall reglerna i affärsavtalet gälla med avseende

på tillämplig lag och sättet för tvistlösning. Framgår inte annat av affärsavtalet skall tvist lösas

av svensk allmän domstol med tillämpning av svensk rätt.

EDIS Teknisk Rapport nr 6

Version 1.0 30 november 1998

Bilaga 3 EDI-avtal 2004

NEA Nätverket för Elektroniska Affärer AB EDI 2004 1 (2)

ALLMÄNNA BESTÄMMELSER FÖR EDI-AVTAL 2004

www.nea.nu e-post: kansli@nea.nu

1. Omfattning och syfte

1.1 EDI-avtalet reglerar uteslutande parternas utväxling och loggning av information i form av elektroniska meddelanden.

1.2 Parterna är ense om att utväxla information med EDI på det sätt som anges i dessa Allmänna Bestämmelser och i Tekniska Bilagan. Om dessa Allmänna Bestämmelser och Tekniska bilagan innehåller motstridiga bestämmelser har dessa Allmänna Bestämmelser företräde.

2. Definitioner

2.1 Med EDI-avtal avses parternas för ändamålet särskilt upprättande skriftliga avtal om Utväxling av EDI-meddelanden inklusive

- dessa Allmänna Bestämmelser,
- Tekniska Bilagan,
- alla övriga bilagor, samt
- avtalade ändringar och tillägg.

Om parterna inte särskilt upprättat ett skriftligt avtal om Utväxling av EDI-meddelanden men låtit dessa Allmänna Bestämmelser och Tekniska Bilagan utgöra en integrerad del av affärsavtalet, gäller istället att med EDI-avtalet avses följande delar av Affärsavtalet:

- den bilaga till Affärsavtalet som har rubriken EDI-avtal,
- dessa Allmänna Bestämmelser,
- Tekniska Bilagan,
- alla övriga bilagor, samt
- avtalade ändringar och tillägg härtill.

Med Tekniska Bilagan avses det dokument som innehåller de tekniska villkoren och specifikationerna som närmare preciserar parternas användning av EDI, med därtill i förekommande fall hörande underbilagor. I EDI-avtalet ska följande understrukna ord och uttryck anses ha den innebörd som anges nedan:

2.2 Med EDI-avtal avses en sammanhängande uppsättning av data, som strukturerats efter överenskommen meddelandestandard i ett format som kan överföras mellan och bearbetas av parternas respektive Informationssystem.

2.3 Med EDI avses automatiserad elektronisk utväxling av EDI-meddelanden mellan parternas Informationssystem.

2.4 Med utväxling av EDI-meddelande avses såväl sändande som mottagande av EDI-meddelande.

2.5 Med överföring avses en enhet bestående av ett eller flera EDI-meddelanden som utväxlas samlat vid ett och samma tillfälle mellan parternas EDI-system.

2.6 Med Utväxlingsfil avses den dataenhet som utväxlas mellan två Kommunikationssystem vid ett och samma tillfälle. En Utväxlingsfil kan innehålla en eller flera Överföringar.

2.7 Med Informationssystem avses Affärssystem, EDI-system och Kommunikationssystem. Dessa system utgörs av datorsystem (maskin- och programvara), kommunikationsutrustning och övrig utrustning/rutiner för bearbetning och lagring av information.

2.7.1 Med Affärssystem anses de delar av ett verksamhetsstödjande Informationssystem som bearbetar EDI-meddelandets innehåll ur funktionell synpunkt.

2.7.2 Med EDI-system avses de delar av ett Informationssystem som bearbetar, lagrar, övervakar och journalför varje Överföring. Ett EDI-system ska ha en Överföringsadress, som inom ramen för en parts Kommunikationssystem anger hur en Överföring ska komma EDI-systemet tillhanda.

2.7.3 Med kommunikationssystem avses de delar av ett Informationssystem som hanterar fysisk kommunikation mellan datorer. Ett Kommunikationssystem ska ha en Kommunikationsadress, som entydigt anger hur en Utväxlingsfil kommer Kommunikationssystemet tillhanda.

2.8 Med VAN-leverantör avses tredje man som tillhandahåller Kommunikationssystem och/eller EDI-system åt part i samband med Utväxling av EDI-meddelanden. Om en part anlitar VAN-leverantör ska därvid med partens kommunikationsadress respektive Överföringsadress avses motsvarande funktioner hos VAN-leverantören.

2.9 Med Affärsavtal avses det avtal om köp av varor, tjänster eller andra nyttigheter, inklusive avrop under ett ramavtal, eller annat avtal vilket parterna utväxlar meddelanden under EDI-avtalet.

2.10 Med Utväxlingslogg avses ett tidsbegränsat arkiv som består av en Överföringslogg och en Händelselogg. De två delarna får rent tekniskt realiseras som en logg eller två separata loggar.

2.10.1 Med Överföringslogg avses en logg som omfattar sända och mottagna Överföringar inklusive däri ingående EDI-meddelanden.

2.10.2 Med Händelselogg avses en logg som innehåller de i Tekniska Bilagan specificerade uppgifterna om händelser som registrerats vid behandling av samtliga Överföringar.

2.11 Med Mottagningsbekräftelse avses en kvittens i elektronisk form, ej nödvändigtvis ett EDI-meddelande, på att Utväxlingsfil, Överföring eller EDI-meddelande har kommit mottagande part tillhanda och att denne därmed övertagit ansvaret för vidare behandling. Fyra olika slag av Mottagningsbekräftelser kan förekomma, se 2.11.1-2.11.4. Vidare kan kvittenser indelas i Positiva kvittenser och Negativa kvittenser beroende på den innebörd kvittensen har, se 2.11.5-2.11.6.

2.11.1 Med Utväxlingskvittens avses en kvittens på att Utväxlingsfil har mottagits av mottagande parts Kommunikationssystem och utväxlingstekniska kontroller gjorts.

2.11.2 Med Överföringskvittens avses en kvittens på att en Överföring har nått fram till mottagande parts EDI-system på där angiven Överföringsadress, och där har genomgått partsidentifikation.

2.11.3 Med Meddelandekvittens avses en kvittens på att ett EDI-meddelande nått fram till mottagande parts EDI-system på där angiven Kommunikationsadress, och där har genomgått syntaxkontroller.

2.11.4 Med Affärskvittens avses en kvittens på att ett EDI-meddelande nått fram till mottagande parts Affärssystem, och där har genomgått kontroller av datainnehåll.

2.11.5 Med Positiv kvittens avses en kvittens sänd av part som mottagit Utväxlingsfil, Överföring eller EDI-meddelande och som innebär att inga formella fel har upptäckts i Utväxlingsfilen, Överföringen eller EDI-meddelandet vid kontroller som utförts fram till tidpunkten för sändningen av kvittensen.

2.11.6 Med Negativ Kvittens avses en kvittens sänd av part som mottagit Utväxlingsfil, Överföring eller EDI-meddelande och som innebär att formellt fel har upptäckts i Utväxlingsfilen, Överföringen eller EDI-meddelandet och att vidare behandling av densamma har avbrutits.

3. Informationssystem

3.1 Respektive part svarar för att parten har tillgång till Informationssystem som möjliggör avtalad Utväxling av EDI-meddelanden. Gränssnitten för de Kommunikationssystem som parterna använder ska specificeras i Tekniska Bilagan.

3.2 Respektive part ska vid driftsättning och fortlöpande under avtalstiden genom tester och andra åtgärder tillförsäkra att det egna Informationssystemet uppfyller kraven enligt EDI-avtalet. Vardera parten svarar för sina egna kostnader under EDI-avtalet, om inte annat avtalas.

3.3 Part har rätt att på egen bekostnad och på eget ansvar anlita tredje man för att utföra Utväxling av EDI-meddelanden, bearbetning, lagring eller annan åtgärd avseende EDI-meddelanden. Om parterna anlitar samma VAN-leverantör eller annan tredje man och fråga uppkommer om ansvar för viss åtgärd som den tredje mannen vidtagit eller underlåtit bär den part, för vars räkning åtgärden vidtagits eller skulle ha vidtagits, ansvaret gentemot den andra parten.

3.4 Part som avser ändra delar av sitt Informationssystem på sätt som kan förväntas påverka Utväxling av EDI-meddelanden, ska meddela motparten om detta iså god tid att parterna gemensamt kan genomföra erforderliga tester för att säkerställa att Utväxling av EDI-meddelanden kan ske på avtalat sätt även efter ändringen.

4. Utväxling av EDI-meddelanden

4.1 Om part finner att ett meddelande inte kan utväxlas med EDI, eller om förvanskning upptäckts i ett EDI-meddelande, ska motparten omedelbart meddelas. Parten får därefter sända informationen enligt reservrutin som anges i Tekniska Bilagan eller enligt annat förfarande som i förväg avtalats mellan parterna. Om part använder reservrutin ska parterna, efter det att felet avhjälpts, gemensamt besluta om och utföra erforderliga tester innan ordinarie Utväxling av EDI-meddelanden återupptas.

4.2 Part som tar emot ett EDI-meddelande ska behandla och bearbeta EDI-meddelandet utan dröjsmål under de tider som anges för EDI-systemens öppethållande i Tekniska Bilagan.

5. Utväxlingslogg

5.1 Vardera parten ska som en del av sitt Informationssystem föra en Utväxlingslogg enligt medan

5.2 Utväxlingsloggen ska vara konstruerad så att det är möjligt att under avtalad tid återskapa och göra om bearbetningar av Överföringar samt ge underlag för att bedöma EDI-meddelandens status i respektive parts Informationssystem.

5.3 Loggning i Utväxlingslogg ska ske som en del av respektive parts EDI-system.

5.4 Vid tvist eller felsituationer har part rätt att på begäran få utdrag ur andra partens Utväxlingslogg avseende den gemensamma EDI-trafiken. Utdrag ska tillhandahållas i för mottagaren läsbar form och utan kostnad för denne.

6. Mottagningsbekräftelser och andra kvittenser

6.1 Om mottagningsbekräftelse överenskommits i Tekniska Bilagan ska mottagande part efter mottagandet sända Mottagningsbekräftelse till den andra parten i enlighet med de regler som avtalats i Tekniska Bilagan. Motsvarande ska gälla för andra kvittenser. Mottagningsbekräftelser och andra kvittenser ska sändas av part som tar emot EDI-meddelande i den utsträckning och inom de tidsfrister som anges i Tekniska Bilagan.

6.2 Parterna har i den Tekniska Bilagan avtalat omfattningen av de kontroller avseende Utväxlingsfilen, Överföringen respektive EDI- meddelandet som part ska genomföra innan parten sänder Positiv kvittens.

6.3 Sändande av Negativ kvittens medför att ansvaret för att utväxling sker kvarstår på den part som sänt Utväxlingsfilen, Överföringen eller EDI-meddelandet.

7. EDI-meddelandens bindande verkan

7.1 Om Affärsavtalet kräver att information lämnas skriftligen, anses detta krav uppfyllt genom Utväxling av EDI-meddelande enligt EDI-avtalet. I förhållande mellan parterna gäller detsamma även vid krav på skriftlighet i lag eller annan författning.

7.2 Ett EDI-meddelande ska, om inte annat visas, anses sänt av sändande part när den Överföring som EDI-meddelandet ingår i har loggats som sänt enligt sändande parts Utväxlingslogg eller, om EDI-meddelande sänts via parts VAN-leverantör, enligt Utväxlingslogg som förs hos VAN-leverantören.

7.3 Ett EDI-meddelande ska, om inte annat visas, anses ha kommit mottagande part tillhanda när den Överföring som EDI-meddelandet ingår i har loggats som mottagen i avtalat format enligt mottagande parts – eller, om mottagande part anlitar en VAN-leverantör, dennes – Utväxlingslogg. Om det avtalats i Tekniska Bilagan att Utväxlingskvittenser ska sändas, gäller istället att avsändande part står risken intill dess Positiv Utväxlingskvittens sänts av mottagande part eller dennes VAN-leverantör.

7.4 Sändande part står risken för att de EDI-meddelanden som ingår i en Överföring förloras, försenas eller förvanskas vid Överföringen intill dess Överföringen loggats som mottagen i avtalat format i mottagande parts – eller, om mottagande part anlitar en VAN-leverantör, dennes – Utväxlingslogg. Om det avtalats i Tekniska Bilagan att Utväxlingskvittenser ska sändas, gäller istället att avsändande part står risken intill dess Positiv Utväxlingskvittens sänts av mottagande part står risken intill dess Positiv Utväxlingskvittens sänts av mottagande part eller dennes VAN-leverantör.

7.5 EDI-meddelande som sänds av part i enlighet med EDI-avtalet ska anses vara behörigen sänt och bindande för sändande part såvida inte denne kan visa att EDI-meddelandet obehörigen sänts och att motparten hade eller borde haft kännedom om detta.

7.6 Om part sänder EDI-meddelande (sändande part), för vilket Mottagningsbekräftelse ska sändas av mottagande part, och Mottagningsbekräftelse inte kommit sändande part tillhanda inom överenskommen tidsfrist, får sändande part återkalla det aktuella EDI-meddelandet varefter detta meddelande inte har någon bindande verkan. Sådan återkallelse ska sändas utan dröjsmål efter utgången av tidsfristen för sändande av Mottagningsbekräftelse. Återkallelse ska ske per e-post eller telefax, såvida det inte i Tekniska Bilagan specificeras ett särskilt förfarande för detta. Om sändande part inte återkallar EDI-meddelande utan dröjsmål efter utgången av tidsfristen för sändande av Mottagningsbekräftelse, är EDI-meddelandet bindande för sändande part på samma sätt som om Mottagningsbekräftelse sänts och mottagits.

8. Avvikande information

Om avvikelse föreligger mellan innehållet i EDI-meddelande som utväxlats mellan parterna och motsvarande information lämnad på papper eller på annat medium, gäller EDI-meddelandet såvida det inte är uppenbart att sändande part avsett, att den information som lämnats på annat medium ska ha företräde.

9. Säkerhet

Parterna ska införa och underhålla procedurer och teknik för att skydda EDI-meddelanden och Utväxlingslogg mot obehörig tillgång, förvanskning, förlust av information och annan skada. Den närmare utformningen av dessa rutiner framgår av Tekniska Bilagan.

10. Sekretess

10.1 Information som part erhåller genom informationsutbytet enligt EDI-avtalet ska hanteras enligt de sekretessregler som framgår av Affärsavtalet. Om part anlitar VAN-leverantör eller annan tredje man för att utföra åtgärd som avses i punkt 3.3, ska parten tillse att tredje mannen är bunden av sekretess i motsvarande mån.

10.2 Är information hos part att anse som allmän handling, ska för denna part vad som sägs i lag om allmänna handlingars offentlighet respektive sekretess tillämpas.

10.3 Tar part emot EDI-meddelande som kommer från sändande part och som uppenbart är avsett för annan, är mottagande part skyldig att omedelbart meddela sändande part om detta och radera EDI-meddelandet, dock inte ur Utväxlingsloggen.

11. Ansvar

11.1 Parts ansvar för egen och av part anlitad VAN-leverantör eller annan tredje mas försummelse enligt EDI-avtalet ska i första hand regleras enligt bestämmelserna i Affärsavtalet.

11.2 Part har rätt att på egen bekostnad genom oberoende revisor kontrollera at motparten uppfyller sina förpliktelser enligt EDI-avtalet. Den part som anlitar VAN-leverantör ska tillse att även VAN-leverantören är skyldig att tillåta kontroll enligt denna punkt.

12. Force majeure m m

12.1 Beträffande parts ansvar vid force majeure gäller de regler som följer av Affärsavtalet. Punkt 12.2 nedan ska dock tillämpas.

12.2 Om fullgörande av EDI-avtalet omöjliggörs eller blir orimligt betungande för part i anledning av myndighets beslut eller nytillkommande lagstiftning, ska parter-

na på den drabbade partens begäran uppta förhandlingar om de ändringar av EDI-avtalet som föranleds av de ändrade förhållandena.

13. Avtalstid

13.1 När Affärsavtalet upphör att gälla upphör även EDI-avtalet att gälla utan uppsägning. Finns fler Affärsavtal upphör EDI-avtalet att gälla utan uppsägning alla Affärsavtalen upphört att gälla.

13.2 Om parterna särskilt upprättat ett skriftligt EDI-avtal och Affärsavtalet/Affärsavtalen gäller på obestämd tid, får vardera parten när som helst skriftligen säga upp EDI-avtalet till upphörande med tre (3) månaders uppsägningstid.

13.3 Om parterna särskilt upprättat ett skriftligt EDI-avtal får part skriftligen säga upp EDI-avtalet till omedelbart upphörande om motparten har gjort sig skyldig till väsentligt avtalsbrott och inte vidtar rättelse inom trettio (30) dagar från det att han mottagit skriftlig begäran därom.

13.4 Åtaganden som rör bevarande av Utväxlingsloggen, utlämnande av meddelanden ur Utväxlingsloggen samt sekretess ska under alla förhållanden äga fortsatt giltighet även efter det att EDI-avtalet i övrigt har upphört att gälla.

14. Ändringar och tillägg

14.1 Ändringar av och tillägg till dessa Allmänna Bestämmelser ska, för att vara gällande, vara skriftliga och undertecknade av behöriga företrädare för parterna.

14.2 Tekniska Bilagan kan komma att förändras under avtalstiden. Ändringar i Tekniska Bilagan ska vara skriftliga.

15. Tillämpning i lag och tvistelösning

15.1 Vid tvist med anledning av EDI-avtalet ska, om parterna särskilt upprättat ett skriftligt EDI-avtal, EDI-avtalet tolkas och tillämpas enslig svensk rätt och tvisten löses av svensk allmän svensk domstol.

15.2 Om parterna inte särskilt upprättat något skriftligt EDI-avtal, ska Affärsavtalets regler om tillämplig lag och sättet för tvistlösning tillämpas vid tvist med anledning av EDI-avtalet. framgår inte annat av Affärsavtalet ska EDI-avtalet tolkas och tillämpas enligt svensk rätt och tvisten lösas av svensk allmän domstol.