**Handelshögskolan vid**
**Göteborgs universitet**

Institutionen för informatik

# EDI – Electronic Data Interchange
# -ur ett säkerhetsmässigt perspektiv och en juridisk synvinkel

## Sammanfattning:

Syftet med detta arbete är att försöka utforska vilka säkerhetsaspekter som bör användas vid EDI. Finns det idag teknisk och juridisk säkerhet, för att två näringsidkare kan använda sig av EDI på ett tillfredsställande sätt? Jag skall även försöka att förklara hur EDI är uppbyggt och utforska vilka nackdelar samt fördelar det finns med detta förfarande. Mitt tillvägagångssätt har mestadels bestått av litteraturstudier. I uppsatsen har jag förklarat några speciellt utvalda säkerhetsmetoder som jag själv valt ut efter eget initiativ t ex Message Authentication Code och digitala signaturer. Uppsatsen behandlar även symmetriska och asymmetriska krypterings algoritmer som jag bedömer som grundläggande för att få ett tillförlitligt skydd vid elektroniska transaktioner. För att utforska huruvida det går att utföra EDI rent juridiskt har jag använt mig av relevant kurslitteratur, EDI-avtal 96 samt aktuella SOU:er och propositioner. EDI är utbytet av relevanta juridiska dokument mellan två eller flera handelsparters datorer på applikationsnivå. Med hjälp av EDI kan ett företag bl a effektivisera dokumenthanteringen, automatisera informationsflödet samt öka produktiviteten och flexibiliteten i företaget. Eftersom det inte finns några formkrav och avtal för viljeförklaringar är avtal och transaktioner som sluts elektroniskt accepterade juridiskt under förutsättning att inga juridiska problem uppkommer. Rent säkerhetsmässigt är digital signatur en av flera tekniker som finns för att underlätta EDI handeln mellan näringsidkare.

Examensarbete 1, 10 poäng
VT 1999
**Författare**: Darko Pintaric
**Handledare**: Faramarz Agahi

# INNEHÅLLSFÖRTECKNING

# 1. INLEDNING

I denna uppsats skall jag skriva om EDI ur ett säkerhetsmässigt perspektiv och en juridiskt synvinkel, eftersom jag finner dessa båda ämnen intressanta och spännande. Varför just EDI kan man kanske fråga sig. Vi lever i ett samhälle som hela tiden förändras snabbt speciellt när det gäller vår tekniska utveckling. Eftersom fler människor har upptäckt internet för att söka efter information eller handla ifrån ser jag EDI som ett ämne i tiden. Speciellt då vi börjat använda internet för att t e x betala räkningar, köpa kurslitteratur eller handla aktier. Företag har upptäckt denna värld och ser nya fördelar m h a internet, dels för att marknadsföra sig dels för att handla med både leverantörer som kunder effektivare och snabbare. Samtidigt finns det stora kostnadsfördelar för de handelsföretag och näringsidkare som använder sig av EDI eller någon form av elektronisk handel. Som jag ser det kan företag spara stora pengar på att införa ett EDI system för handel med företag som man kontinuerligt gör affärer med.

## 1.2 Syfte

Mitt syfte med detta arbete är att försöka utforska vilka säkerhetsaspekter som bör användas vid EDI, då handelsparter vill genomföra elektroniska transaktioner mellan varandra på ett säkert sätt. Finns det idag teknisk säkerhet, för att två näringsidkare kan använda sig av EDI på ett tillfredsställande sätt? Jag skall även försöka att förklara hur EDI är uppbyggt och utforska vilka nackdelar samt fördelar det finns med detta förfarande. Med anledning av det som sagts ovan vore det därför även intressant att utforska hur det juridiska förhåller sig då företag ingår t ex avtal med varandra. Jag skall försöka att utforska den allmänna uppfattningen om hur förfarandet kan lösas med hjälp av EDI och vilka juridiska hjälpmedel som behövs för att elektroniska transaktioner skall kunna fungera tillfredsställande med hjälp av EDI eller elektronisk handel.

## 1.3 Metod

Mitt tillvägagångssätt består mestadels av litteraturstudier men även av två intervjuer samt relevant information från internet. I uppsatsen har jag förklarat några speciellt utvalda säkerhetsmetoder som jag själv selekterat ut. Dessa kan vara intressanta för att eventuellt lösa de frågeställningar som jag tagit upp i mitt syfte.
De säkerhetslösningar som jag valt är MAC (Message Authentication Code), digitala signaturer, äkthetsbevis (Message origin authentication), sekvenskontroll (Message sequence integrity) och äktheten i ett meddelandes innehåll (Message content integrity). I samband med dessa förklaras även symmetriska och asymmetriska krypterings algoritmer som jag bedömer som grundläggande för att få ett tillförlitligt skydd vid elektroniska transaktioner. För att utforska huruvida det går att utföra EDI rent juridiskt har jag använt mig av relevant kurslitteratur, EDI-avtal 96,

UNCITRAL(United Nations Commission on Internatinal Trade Law) s modell lag för elektronisk handel samt aktuella SOU:er och propositioner.

## 1.4 Avgränsning

Jag har avgränsat mig till säkerhetsrutiner som MAC (Message Authentication Code), digitala signaturer, äkthetsbevis (Message origin authentication), sekvenskontroll (Message sequence integrity) och äktheten i ett meddelandes innehåll (Message content integrity). Arbetet vänder sig i första hand till näringsidkare och inte mot privatpersoner. Avgränsningen består även av en inblick i ämnet avtal och vilka handelsrättsliga krav som krävs vid denna typ av handel och om det är möjligt trots denna papperslösa handel att bedriva affärsverksamhet och ändå skyddas av lagen. Eftersom både elektronisk handel och EDI är verktyg som inriktar sig mot handel är det naturligt att utforska just avtals mekanismen och dess funktion vid EDI.

Uppsatsen vänder sig till medstuderande vid informatik institutionen samt näringsidkare och personer som har intresse av att veta mer om EDI.

## 1.5 Disposition

Kapitel 1 börjar med syftet med uppsatsen, tillvägagångssättet och hur jag valt att avgränsa mig.

I kapitel 2 beskrivs allmänt bakgrunden för dagens internet, elektroniska handeln och EDI. Detta för att senare naturligt förklara själva EDI-kommunikationen med dess kännetecken samt fördelar och nackdelar. Sedan kommer en del som handlar om VAN som är lite som ”spindeln i nätet” när det gäller EDI och elektronisk handel efter detta avsnitt tas de allmänna juridiska och avtalsrättsliga aspekterna upp för att se om denna typ av handel är möjlig.

Kapitel 3 är ett säkerhetskapitel där författaren försöker att utreda vilka säkerhetsaspekter som kan vara användbara vid EDI och hur de fungerar. Dessa förankras sedan som eventuella lösningar för de tekniska problem som kan uppkomma vid elektronisk handel och EDI.

Slutligen så finns en diskussions och slutsats del i kapitel 4 där jag försöker att knyta samman de olika problemställningarna till ett slutligt resultat. Här diskuteras även själv kritik och framtida forsknings områden.

# 2. EDI – ELECTRONIC DATA INTERCHANGE
**- ur ett säkerhetsmässigt perspektiv och ur en juridisk synvinkel**

I detta kapitel förklaras till en början bakgrunden till internet för att läsaren skall förstå uppbyggnaden och den massiva tillväxten idag. Detta är viktigt för att förstå sättet att kommunicera med hjälp av EDI men även för att förstå de fördelar och nackdelar som senare utforskas i underkapitlet som handlar om EDI-kommunikation. I detta kapitel försöker jag även visa nyttan med EDI och hur EDI förhåller sig till EDIFACT standarden och tvärtom. I efterföljande underkapitel försöker jag knyta ihop själva EDI-meddelandet som skickas med hjälp av EDIFACT standarden via ett VAN till sändarens handelspart. De följande tre underkapitlen som heter allmänna juridiska aspekter, avtalsrättsliga aspekter och EDI-avtal 96 utreder hur det juridiska förhåller sig med denna typen av elektroniska transaktioner. Kapitlen tar upp aktuella lagrum och de krav som måste vara uppfyllda för att elektroniska transaktioner och därmed EDI skall bli giltiga.

## 2.1 Bakgrund

I början av 1960-talet påbörjades under ledning av ARPA, ett forskningsprojekt numera DARPA, inom den amerikanska försvarsindustrin med paketförmedlande nät (packet switching). Denna teknik har än idag stor betydelse för datorkommunikationen däribland internet. ARPA växte så småningom under 60-talet till ett 50-tal värddatorer och då var NCP det protokoll som användes. Det fanns dock ändå relativt tidigt en vision att skapa ett internet där alla nät i världen var sammankopplade till ett öppet nät oavsett arkitektur.

Genom ARPANET sammankopplades universitet, forskare, myndigheter etc under 70-talet så att de kunde utbyta både filer och elektronisk post. Mot slutet av 70-talet lanserades och implementerades TCP/IP som det officiella ARPANET protokollet. TCP/IP – protokollets uppgift var att binda ihop olika tekniker och nät till ett enda stort öppet nät. De sammankopplade datorerna adresseras med IP och använder TCP som överföringsprotokoll. I och med detta var grunden också lagd för dagens närmast obegränsade tillväxt.

Den viktigaste uppfinningen för dagens internet, som togs fram av CERN 1989-1992, var WWW eller även kallat ”Webben”. Webben skapades som en reaktion mot svårigheterna att hålla reda på alla adresser på internet. Tanken var att man skulle kunna förflytta sig mellan både dokument och hemsidor med hjälp av så kallade hypertext – länkar. Dessa hypertext – länkar har i och för sig funnits i dokument länge, men den nya idén var att länka mellan dokumentet och datorerna. Det vill säga få applikationsprogrammet (webläsaren) och nätet att föra vidare länkanrop och hämta dokument från andra hemsidor. Samtidigt skapades också HTTP ett transportprotokoll, men även ett sk sidbeskrivningsspråk, ett kodsystem för att formatera dokument för internet, HTML. Detta gjorde det möjligt för en marknad med bl a Netscape Navigator och MS Explorer [Berti 1995, Borg&Jonson1994].

Internet är som beskrivits uppbyggt av en mängd sammankopplade nätverk.
Ett centralt begrepp för att förklara detta är backbones. Dessa utgör ryggraden eller stommen i Internet, genom att de binder samman flera nätverk. Oftast är ryggrads-näten uppbyggda av höghastighetsförbindelser. Ryggradsnäten i det svenska universitetsnätet SUNET består av förbindelser med en överföringshastighet på 34 Mbps. Vilket innebär att 34 miljoner bitar kan överföras varje sekund. De som ansluter sina nätverk till ett ryggradsnät betalar de företag som driver ryggradsnätet ungefär på samma sätt som när man betalar Telia eller motsvarande operatör för att koppla in sin telefon på telenätet.

Näten på internet använder sk routers för att ansluta sig till varandra. En router håller reda på var de olika datorerna och delnäten på Internet finns. När nätverk av olika typer ansluter sig till varandra används bryggor för anslutningen. En brygga kan översätta mellan olika protokoll om det behövs [Borg&Jonson 1994]. Det finns ingen internationell organisation som sköter eller äger internet. I likhet med telefonernas internationella nätverk finns det däremot standardiserings organisationer som definierar de regler, eller protokoll som måste följas vid anslutning till nätverket. Dessa protokoll utarbetas främst av the Internet Architecture Board (IAB) och the Internet Engineering Task Force (IETF). Alla protokoll är öppna och allmänna för att vem som helst skall kunna utveckla programvara som bygger på dessa.
Eftersom internet inte ägs av någon enskild, är den allra största delen av information som är tillgänglig gratis för användarna. Detta till skillnad från de större databaserna där det kostar att erhålla information [Winberg 1997].

Sverige är ett av världens mest datoriserade samhällen. Datorerna har blivit länkar i ett globalt system för bl a information och kommunikation. Användningen av modern informationsteknik har bidragit till en ökad internationalisering. Datorerna annan teknisk utrustning och det allmänna telefonnätet erbjuder utrymme för att överföra, behandla eller lagra data som representerar elektroniska meddelanden. Ett elektroniskt meddelande är inte enbart text utan det kan också vara ljud och bilder såväl rörliga som fasta [SOU 1996:40, Prop 1995/96:125].

Elektronisk handel är ett begrepp som idag används flitigt. Genom elektronisk handel kan företag internationalisera sig och därmed har samverkan mellan företagen globaliserats. I och med detta har marknaden för handel gjort det möjligt för samarbete och konkurrens på en internationell marknadsplats. Där den geografiska placeringen idag inte har lika stor betydelse som förut, detta med hjälp av Internet [Toppledarforum 1997].

Elektronisk handel har ur ett IT perspektiv många olika ämnesområden som är viktiga. För att elektronisk handel och IT skall fungera på ett bra sätt är det viktigt att ett företags kommunikation blir mer applikationsorienterat så att det täcker hela affärscykeln. När detta gjorts ges stora fördelar. Samtidigt krävs det att kommunikationen ökar i leverantörsleden, vilket gör de elektroniska transaktionerna nödvändiga. Till sist krävs det en gemensam anslutning till standarder för att den elektroniska handeln skall fungera tillfredsställande utan problem [Chesher&Kaura 1998].

Definitionen av (EDI) Electronic Data Interchange (elektronisk data överföring) är utbytandet av juridiskt relevanta dokument mellan två företag/organisationers datorer på applikationsnivå. Vilket även innebär automatisk bearbetning och tolkning hos motpartens interna informationssystem. Skillnaden mellan EDI och elektronisk kommunikation är att användningen sker på olika sätt. Vid EDI kommunicerar datasystem med varandra på ett sätt som har blivit bestämt i förväg. När det gäller elektronisk kommunikation är det däremot individer som kommunicerar i en oftast fri textform [Dykert & Lindberg 1996].

## 2.2 EDI – kommunikation

För att EDI skall ske mellan två handelsparter, måste parterna på något sätt vara uppkopplade gentemot varandra. Uppkopplingen kan vara i direkt eller indirekt form. Vid direkt form eller (point to point) sker kommunikationen direkt från avsändarens dator till mottagarens dator. Direkt EDI kommunikation kan ske genom en uppringd linje/krets eller en reserverad linje/krets. Kommunikationen sker genom den publika telefonväxeln och så länge parterna utväxlar data är förbindelsen öppen. Men så fort någon part slutar sända och läger på luren bryts uppkopplingen. Vid en reserverad linje är uppkopplingen konstant. Vem som helst av parterna kan när som helst sända data till respektive handelspartner genom en speciell förutbestämd dialog som parterna har kommit överens om. Här behövs ingen uppringning för att börja sända eftersom linjen/kretsen alltid är ledig. Denna typen av uppkoppling är att föredra då transaktionerna är volym och tids känsliga. Direkt uppkoppling krävs dock, eftersom det ökar tillgängligheten då företaget har många handelspartners vilket leder till många olika kommunikations protokoll och tids zoner [Colberg mfl 1995].

Vid indirekt EDI uppkoppling, används oftast VAN för att ge de kommunikations egenskaper som krävs, expertis och teknik är nödvändigt för att kommunicera elektroniskt. Grundfunktionerna för VAN är att ta emot, lagra och skicka elektroniska meddelanden. I detta fall fungerar VAN som en elektronisk brevlåda.

Nyttan med EDI är bl a en ökad och effektivare verksamhet för företaget vilket leder till minskning av arbetsuppgifter och fel. Då företaget minskar de administrativa kostnaderna med hjälp av EDI kan man koncentrera sig på förbättrad kundservice och en ökad respons mot kunderna [SWEPRO 1992, Sokol 1995].

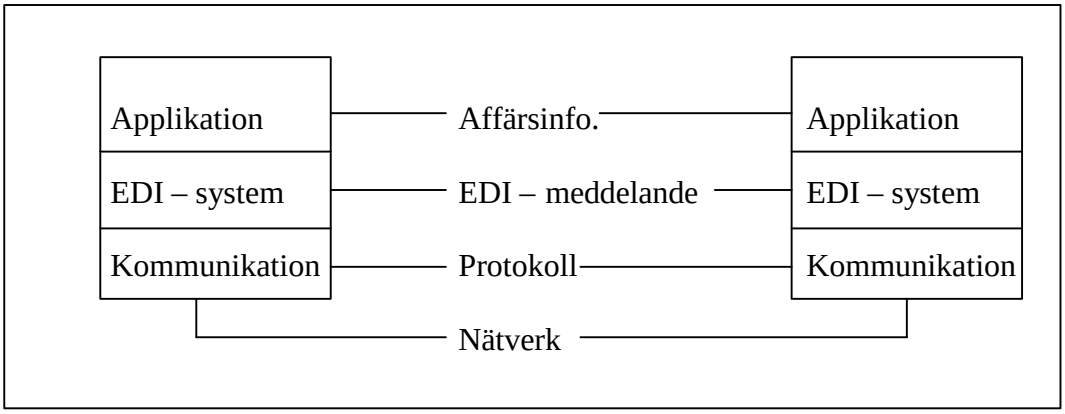



Fig 1. EDI – konceptet

Ofta blandas tyvärr EDI och EDIFACT samman då man pratar om elektronisk handel. För att förtydliga dessa båda begrepp skall dessa förklaras kort.

- **EDIFACT** - står för Electronic Data Interchange For Administration, Commerce and Transport. Det är en standard som definierar elektroniska dokument och EDI– meddelanden, till uppbyggnad och informationsinnehåll. Denna standard är också en av flera som används hos Volvo Information Technology i Europa. EDIFACT – standarden är en samling regelverk och kataloger där standardiserade meddelanden används inom många olika ämnesområden. Rollen som EDIFACT har är att ta fram branschlösningar för den snabba EDI utvecklingen. EDIFACT standarden säger inte hur ett elektroniskt meddelande skall transporteras mellan två system. Inte heller hur det skall implementeras med företagens interna informationssystem eller vilken typ av säkerhet som skall tillämpas [Jansson 1997, Sokol 1995].

- **EDI** - innebär att affärssystem som t ex order-, lager-, fakturerings- eller ekonomisystem kan utbyta information direkt från en dator till en annan dator på t ex två olika företag med en uppkoppling mot varandra [Jansson].

EDI – kännetecknas av:[Chesher & Kaura 1998, Sokol 1995]

- Strukturerade meddelanden/dokument i standardiserande elektroniska format
- Inter-Enterprise (eng)
- Applikation till Applikation
- Affärsdokument
- Dataformat standards som körs av användarna

Fig. 2 EDI - kännetecken

Detta visar att EDIFACT standarden enbart är en delmängd av t ex EDI, som i sin tur är en delmängd av tekniker som tillämpas vid elektronisk handel. Bilden nedan belyser att dessa olika delmängder slutligen är till för att förbättra ett företags handelsprocedurer elektroniskt [Fredholm 1997].

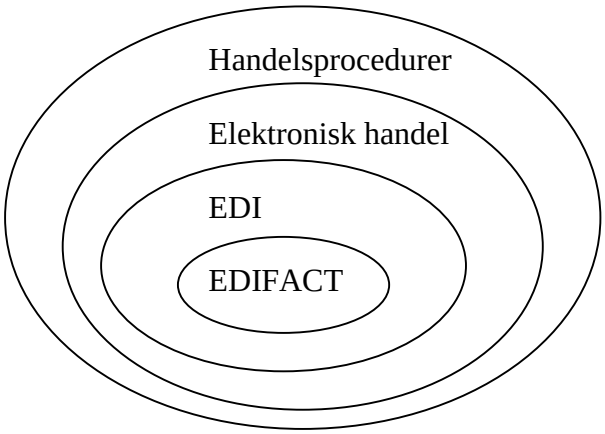



Fig 3. EDIFACT är en del av EDI – konceptet.

Med hjälp av EDI kan ett företag effektivisera dokumenthanteringen och det registrerade informationsflödet automatiseras. En stor fördel med EDI är att data endast behöver behandlas vid en arbetsstation. Elektroniska order hanteras snabbt och enkelt vilket gör JIT (Just In Time) möjligt [Goldman 1995].

Den information som kommer via EDI behandlas direkt och automatiskt utan att en handläggare tar sig an ärendet. Idag är EDIFACT den internationella standarden för EDI runt om i världen. Standarden är godkänd av bl a FN och ISO [Fredholm 1997].

Då EDI motsvarar dessa kännetecken nedan kan man få stora effektivitets och rationaliseringsfördelar [Sokol 1995]:

- Överföring av strukturerad information elektroniskt
- Kommunikation mellan datorer/applikationssystem utan mänskligt ingripande
- Användning av kommunikationsstandard och att meddelanden är strikta och absoluta
- Säkerhetskrav på informationskvalitet och behörighetsskydd samt att tillgänglighet tillgodoses
- Juridisk acceptans för de ekonomiska transaktionerna (genom avtal och lagstiftning)
- Parter kommunicerar med varandra (multilaterala avtal)

De nackdelarna som kan uppkomma med EDI är allt ifrån sociala till tekniska problem [Fredholm 1997].

- Skepsis om att använda Internet vid handel, eftersom många tvivlar på bl a säkerhet och diskretion
- Säkerheten måste lösas, så att den kan hanteras enklare och att man kan känna sig säkrare vid handel på nätet
- Eftersom arbetet på många områden blir mer automaticerade finns risken att personal kommer att bli utan arbete, men detta kan leda till att företaget kan öka sina kund kontakter avsevärt
- Ny teknik i ett företag innebär att ny kompetens krävs
- Fortfarande är EDI en ganska så stor initial kostnad för företagen, men EDI tekniken har blivit allt mer standardiserad

EDI används idag som ett stängt system mellan de företag som är uppkopplade mot varandra. För näringsidkare är EDI ett relativt säkert sätt att göra elektroniska affärer. Säkerhetsaspekten blir dock svårare att bibehålla om EDI i framtiden börjar användas på Internet. Om olika parter vill använda EDI ingås ett ramavtal mellan dessa för att på detta sätt undvika onödiga juridiska tvister. Därför krävs det att parterna känner varandra någorlunda bra innan ett ramavtal upprättas och företaget börjar att använda EDI i sina transaktioner [Winberg 1997].

För många företag har EDI blivit lite av en överlevnadsfråga. En EDI implementering kan komma att gynna företag både såväl taktiskt som strategiskt. Fördelarna med en EDI implementering kan komma att minska kostnaden på sålda varor samt öka produktiviteten och flexibilitet för olika beteendemönster på marknaden.
Andra fördelar kan även vara att minska fördröjningen i leverantörleden och öka konsumentlojaliteten [Chesher&Kaura 1998]. Flertal företag i olika branscher ställer EDI som krav gentemot leverantörer och kunder, däribland Volvo Information Technology. Annars finns risken till sämre affärsvillkor då den ena parten trots sin EDI – teknik blir tvungen att använda manuella rutiner [Fredholm 1997].

Då EDI används som teknik för kommunikation måste informationen omvandlas från tillämpningssystemen till standardiserade EDI – meddelanden. Dessa skall senare tolkas av mottagarens datasystem. Informationen skall sedan omvandlas till EDI – format. Detta kan ske genom en speciell typ av programvara kallad EDI – konverterare [Dykert & Lindberg 1997].

## 2.3 VAN [Colberg mfl 1995, Sokol 1995]

Med ett VAN (Value Added Network) sker alla transaktioner till en tredje part. VANs handhar en mängd tjänster som tillgodoser deras kunders behov att skicka elektroniska transaktioner till en mängd handelsparter precis när de vill. Systemet är uppbyggt ungefär som postens central sortering. Ett skickat meddelande överförs till mottagarens brevlåda vid centraldatorn, där det kan hämtas när som helst av mottagaren genom att ringa upp VAN och ladda hem den överförda informationen.

Om det finns flera handelsparter som är uppkopplade flera olika VANs kan meddelanden skickas mellan de olika nätverken. De flesta VANs erbjuder nätverk som är världsomfattande, detta för att EDI användare skall kunna handla på internationell basis.

En VAN kund handhar en enda uppkopplad linje mellan sig själv och VANs närmaste punkt vanligtvis genom ett lokalt telefon samtal. VAN levererar standardiserade EDI transaktioner som t ex ANSI ASC X12 eller UN/EDIFACT meddelanden till de tänkta mottagarna. Den som skall skicka meddelandet kan kommunicera med VAN när det passar och VAN i sin tur levererar meddelandet/transaktionen till sk elektroniska brevlådor. Varje brevlåda handhar olika specifika meddelanden med data, transaktioner från flera kunder kan samlas i samma brevlåda.

Mottagaren kan när han vill hämta EDI data från VAN som finns lagrat i dess brevlåda. Eftersom leverantören och mottagaren av EDI data har egna kommunikationslinjer kan VAN agera som en säkerhets buffert.

Då leverantören och mottagaren aldrig har en direkt kontakt mellan varandra, innebär detta också att VAN inte behöver ge ”support” av t ex datakommunikations protokoll eller hastighet som baseras på handelsparternas skicklighet. Andra viktiga saker att peka på när det gäller VAN, är att ett föravtal mellan handelsparter tillkommer. Varje EDI part måste godkänna handelsrelationen innan användandet börjar med VAN. Sändaren och mottagaren meddelar VAN att transaktioner mellan sändare och mottagare är godkända. VAN kontrollerar även att transaktionerna överensstämmer med EDI-standards.

## 2.4 Allmänna juridiska aspekter

Ur juridisk synvinkel är EDI en ny företeelse. Olika typer av pappersdokument har traditionellt sett varit bärare av olika funktioner. Detta innebär att lagtexter mm har ofta direkt eller indirekt hänvisat till pappersdokumenten. Sådana hänvisningar till traditionella utgör mestadels effektiva rättsliga hinder mot en övergång till EDI. Exempel på några hinder är kravet på egenhändig undertecknad handling, arkivering eller bevarande av pappersdokument. Huvudregeln är dock att det inte får finnas några direkta juridiska hinder mot användningen av EDI vid handel mellan två parter, annat än vid speciella tillfällen som fastighetsköp eller liknande. I SOU 1996:40 har det presenterats en rad förändringar vilket kommer att underlätta EDI-kommunikationen. Den grundläggande lagstiftningen för handel är avtalslagen från 1915. SOU 1996:40 kommer fram till att nuvarande lagstiftning bör kunna fungera även vid elektronisk handel. Detta eftersom avtalslagen inte ställer några krav på skriftform då två eller flera parter kommunicerar med varandra. Ett avtal kan träffas både muntligt eller på annat sätt t ex med EDI. Affärsparterna kan själva komma överens om vilka avtal som skall gälla mellan dem och när de skall träffas. Detta eftersom avtalslagen till stora delar kan avtalas bort av parterna i en affärssituation [Ramberg 1996].

Det finns många olika juridiska aspekter som man måste tänka på när det gäller EDI. De problem som kan uppstå vid elektronisk handel kan bl a vara, kravet på skriftlighet, egenhändig namnteckning eller att information och det traditionella pappersdokumentet lagras som nämnts ovan.

Det finns inga formkrav och avtal för viljeförklaringar, därför är avtal som sluts elektroniskt eller muntligt giltiga på samma sätt som skriftliga kontrakt.
EDI transaktioner anses accepterade rent juridiskt om det inte föreligger några juridiska problem [SWEPRO 1992].

När det gäller egenhändig namnteckning föreligger inte något sådant problem enligt civilrättsliga avtal eftersom parterna själva får välja form för hur avtal skall ingås. Avtal slutna på elektroniskt sätt är lika giltiga som skriftliga dokument. En stor skillnad föreligger dock när det gäller bevisvärde och bevismöjligheter. Andra problem kan även bestå av legala krav som inte tar formen av en rättshandling, t ex kravet på god offentlighetsstruktur d v s offentlighetsprincipen och rätten att ta del av allmänna handlingar. Om inte kraven uppfylls uppstår ett sk legalt problem [Dykert & Lindberg 1996].

Vid pappersdokument är informationen låst till dokumentet. Förändringar eller tillägg kan upptäckas på originaldokumentet. Den låsta informationen är låst till en individ via namnteckningen. Dessa funktioner kan uppfyllas med ett elektroniskt dokument med hjälp av olika tekniker. Av SOU 1989:20 framgår att teknik som digitala signaturer och vissa elektroniska sigill som dels verifierar innehållet, dels identifierar utställaren och låser denne till det verifierade innehållet i dokumentet.
Enbart ett lösenords baserat system räcker inte som skydd för att uppgifter på ett elektroniskt dokument skall vara säkra. Det krävs någon form av elektronisk teknik för att lösa detta problem, eventuellt någon av de presenterade teknikerna ovan [SOU 1996:40].

Eftersom det idag inte finns några generella lagregler eller vägledande rättsfall om EDI – transaktioners giltighet, torde den bästa juridiska förutsägbarheten skapas av sk EDI– avtal och UNCITRALs (United Nations Commission on Internatinal Trade Law) Modell lag för elektronisk handel.

## 2.5 Avtalsrättsliga aspekter

Avtalsrekvisiten vid EDI användning berörs inte på något sätt då ett avtal ingås elektroniskt. Det finns inga hinder eller skillnader när det gäller avtalsrekvisiten trots att anbud och accept tillkommer antingen via EDI eller elektronisk handel. Elektroniska avtal kan slutas på många olika sätt. Avtal kan uppstå då köpare gentemot säljare kommunicerar elektroniskt och har ingått ett EDI-avtal, men även då parternas datasystem automatiskt kommunicerar trots att ett EDI – avtal inte slutits [SOU 1996:40].

För att ett meddelande skall anses ha kommit motkontrahenten tillhanda krävs det inte att man tagit del av meddelandet utan att han har fått tillfälle att ta del av det.

Då det gäller ett elektroniskt meddelande bör det enligt IT – utredningen ha kommit mottagaren tillhanda då meddelandet överförts till adressatens informationssystem t ex mottagarens elektroniska adress. Skulle mottagaren ha en brevlåda på en server skall meddelandet enligt IT – utredningen anses ha kommit mottagaren tillhanda då det nått brevlådan. Var serven är placerad geografiskt har dock ingen betydelse rent juridiskt, samma ståndpunkt återfinns hos IT – utredningens SOU 1996:40.

Tyvärr kan olika tekniska fel uppkomma vid elektronisk kommunikation, som kan leda till att meddelandet inte alls eller först senare kan läsas. Enligt IT – utredningen bör meddelandet anses ha kommit mottagaren tillhanda först då det kan göras läsbart för denne. Sker elektronisk kommunikation vid direkt uppkoppling mellan parterna skall denna situation anses som muntlig kommunikation. Skulle ett anbud ges, krävs det att anbudstagaren direkt accepterar anbudet om ingen acceptfrist givits, för att anbudet skall gälla. Det avgörande blir således huruvida kommunikationen sker i direkt eller indirekt form [Dykert & Lindberg 1996].

Enligt 40§ Avtalslagen går vissa meddelanden på mottagarens risk. Parterna som utväxlat anbud och accept via elektronisk post, är enligt IT – utredningen ändamålsenlig och torde omfattas av 40§ Avtalslagen. Men frågan får dock lösas med praxis i framtiden. Inom näringslivet är det sedan länge accepterat att skicka meddelanden per fax vilket idag anses ändamålsenligt. Jag tror därför att det inte dröjer länge innan IT – utredningens synpunkter inkluderas i den ovan nämnda paragrafen eller inom andra lagar och betydelsefulla avtal.

Avtalslagen tar även upp bestämmelser om att anbud och accept alltid är bindande för parterna och kan återkallas till dess mottagaren tagit del av anbudet eller accepten. Har ett anbud kommit mottagaren tillhanda bör anbudsgivaren enligt IT – utredningen kunna återkalla detta fram till dess att mottagarens EDI – system har behandlat detta. Skickas återkallelsen i form av ett EDI-meddelande förutsätter detta att systemen är konstruerade så att återkallelsen hinner förhindra verkställigheten av anbudet. Återkallelsen kan dock skickas som ett särskilt meddelande via t ex fax eller e-mail. För att det skall få effekt måste det ha kommit honom tillhanda senast samtidigt som anbudstagaren tar del av anbudet.

Om parterna blir oense vid EDI-kommunikation kommer av naturliga skäl bevisfrågor att uppkomma. För att domstolarna skall kunna acceptera både äkthet, innehåll och uppgifter om utställare kommer det att ställas stora krav på elektroniska dokument för att de skall få juridisk acceptans. Det gör att säkerhetsfrågor och juridiska frågor är mycket nära sammankopplade [SITO 1996].

Det finns vissa krav som bör ställas på system som används för ekonomiska transaktioner:

- Transaktioner och åtgärder måste dokumenteras så att de kan användas som bevis. Vilket innebär att de även måste kunna förklaras på ett begripligt sätt.
- Man måste kunna följa de enskilda transaktionerna i ett tidsperspektiv
- Man måste säkerhetställa vem som gjort en viss transaktion och att det meddelande som avsänts haft det innehåll som avsändaren avsett.

## 2.6 EDI – Avtal 96

EDI – avtal 96 har utarbetats av Toppledarforum och Svenska IT-företagens Organisation (SITO) i samarbete med EAN Sverige och EDIS. Det är baserat på internationella modellavtal som har anpassats till svenska förhållanden inklusive avtalslagen. Den generella avsikten med ett EDI-avtal är att reglera form och teknik för utväxlande av EDI - meddelanden samt hur risken för sådana meddelanden skall fördelas mellan avtalsparterna. Parterna kan därför använda det för att reglera vad som ska gälla när de ingår köpeavtal med hjälp av EDI.

De parter som vill använda sig av EDI bör ingå ett sk EDI-avtal med varandra för att få bästa tänkbara juridiska förutsägbarhet. EDI – avtalet är ett dokument som reglerar kommunikation inom ramen för det kommersiella avtalet och SFTI[1]. Avtalet består av olika delar bl a avtalet i sig, allmänna villkor och en teknisk del.

De viktigaste punkterna i ett EDI-avtal bör omfattas av:

- Avtalsvillkor – klar göra vilken typ av meddelanden som får utväxlas av EDI-systemet (t ex enbart EDIFACT – meddelanden)
- Mottagningsbekräftelse – för att ange tidsfrister och inbringa hög säkerhet
- Tillämplig lag och forum – klargöra ansvarsfördelning och gällande lagrum
- Teknik – säkerhetsbestämmelser t ex elektroniska signaturer

EDI – avtal kan jämföras med några affärsavtal. För det första ett ramavtal vilket innebär avtal om att parterna har ett kommersiellt förhållande. Det vill säga att köparen får avropa produkter eller tjänster samt att leverantören skall leverera beställd produkt/tjänst. Ramavtalet innehåller normalt mycket av de kommersiella villkoren för dessa avrop [Adlercreutz 1995].

För det andra ett avrop där det enskilda köpeavtalet grundar sig på ramavtalet. Avrop sker genom utväxlande av EDI – meddelanden på ett sätt som anges i EDI - avtalet. Men de kommersiella villkoren styrs av ramavtalet samt avropet i sig. Själva avropet innehåller normalt de kommersiella villkoren som är unika för den specifika transaktionen t ex avtal och leveranstid.

Hur skiljer sig då EDI – avtalet gentemot dessa två ovan. Ett EDI – avtal är ett avtal om formen för utväxlande av meddelanden mellan parterna och vilken rättslig betydelse sådana meddelanden skall ha. EDI – avtalet innehåller normalt inga kommersiella villkor för köp eller leverans av produkter eller tjänster.

**Sammanfattningsvis** har det i detta kapitel beskrivits och utforskats huruvida EDI fungerar med hjälp av EDIFACT standard samt dess fördelar, nackdelar och funktion med hjälp av VAN. Men även under vilka förutsättningar två handelsparter på ett effektivt och snabbt sätt kan göra ekonomiska transaktioner mellan varandra med juridisk acceptans.

[1] SFTI är ett regelverk för EDI-kommunikation i den offentliga sektorn, här finns olika specifikationer samlade.

# 3. SÄKERHET

I detta kapitel utreds några olika säkerhetsmetoder hur de fungerar och deras uppbyggnad. En betydande del av detta kapitel tar upp säkerhetsmetoden digitala signaturer. Här visas dess uppbyggnad med asymmetrisk algoritm och symmetrisk algoritm och vad som kännetecknar dem samt beräkningen av den digitala signaturen mm. I slutet av detta kapitel presenteras några potentiella tekniska problem som kan uppkomma med EDI transaktioner och potentiella lösnings förslag.

## 3.1 Kryptering [Sokol 1995, Egen källa 1996]

För att hindra obehöriga att läsa information kan man förvanska texten så att den endast kan återskapas av den som är behörig. Man kan genom att kryptera klartext få sk kryptotext. Vi en kryptering behövs förutom ursprungsinformationen ytterligare två saker, en matematisk krypteringsalgoritm och en krypteringsnyckel.

En krypteringsalgoritm är en beskrivning av hur klartext skall förvanskas till kryptotext. Det finns olika krypteringsalgoritmer, men för att få två parter att kommunicera med varandra krävs det en överenskommelse om vilken algoritm som skall användas. Förutom själva algoritmen måste de också komma överens om de olika krypteringsnycklarna. Då en part har kännedom om både algoritm och nyckel kan denne återskapa klartext från kryptotext.

Själva krypteringen görs genom att ursprungsinformationen behandlas av både den matematiska krypteringsalgoritmen och krypteringsnyckeln, varvid ursprungsinformationen erhåller ett nytt utseende. Om samma ursprungsinformation bearbetas med samma krypteringsalgoritm, men med en annan krypteringsnyckel får ursprungsinformationen ytterligare ett annat utseende. Då informationen skall återställas i sitt ursprungliga skick genomförs samma operation, fast i omvänd ordning, vilket brukar benämnas dekryptering.

Om informationen skall överföras i krypterad form mellan sändare och mottagare, förutsätter det alltså att sändare och mottagare använder samma krypteringsalgoritm och krypteringsnyckel (symmetrisk kryptering) eller samma krypteringsalgoritm med matchande nyckelpar (asymmetrisk kryptering).

## 3.2 Message Authentication Code [Colberg 1995, Sokol 1995]

En annorlunda metod för att skydda integriteten av överförd information är autenticering av meddelanden (MAC = Message Authentication Code). Vid MAC är informationen autentisk i dess original form, men vid överföring läggs en extra data sträng till i meddelandet som skall överföras, en sk MAC. Under MAC processen läggs en algoritm med data i slutet av meddelandet som skall skickas.

Mottagaren konfirmerar autensiteten och integriteten av meddelandet genom att öppna MAC med den medskickade nyckeln.

Om samma MAC mottagits av mottagaren innebär detta att:

1. Informationen/meddelandet kommit från någon som ägt den nödvändiga nyckeln *och*
2. Att informationen inte har förändrats

Om inte MAC värdena matchar det MAC som mottagits kan mottagaren bortse från det som skickats eller be sändaren att göra ett nytt försök.

### **3.2.1 Nyckeln** [Sokol 1995, Colberg 1995]

Den viktigaste faktorn vid dekryptering och autenticering, är nyckeln. Det finns tre typer av nycklar:

- Master key (lagrings nyckel) – används vid kryptering av de andra nycklarna. Den finns inne i den konstanta hårdvaruenheten, där även DES algoritmen (Data Encryption Standard) finns.

- KEK (Key Encrypting Keys = krypterings nyckeln) – används av en handelspart för att tillhandahålla en kryptografisk relation med en annan handelspart.

- Data keys (data nyckel) – används för kryptera, dekryptera och tillför MAC specifika data meddelanden.

När två handelsparter har upprättat en KEK förbindelse kan de använda KEK för att säkert utbyta KEK eller data nycklar mellan dem.

Om någon part vill utbyta det krypterade eller autenticerade datameddelandet till ytterligare en part, krävs det att båda använder samma hemliga datanyckel. Den gemensamma nyckeln är vad som krävs för att systemet skall fungera. Men för att hela krypteringen och autenticerings processen skall fungera måste säkerheten kring KEK nyckeln var hög.

Huvudmålet för intrång är data nyckeln. Det bästa skyddet är att använda en enda datanyckel vid ett enstaka tillfälle, antingen kryptering eller autenticering men inte bägge.

## 3.3 Digitala signaturer

Begreppet digitala signaturer har blivit allt vanligt förekommande vid säkerhetsdiskussioner inom EDI. Tekniken med digitala signaturer fungerar enligt public-key-konceptet vilket innebär att den signerade handelsparten får ett nyckelpar. Den ena nyckeln är publik och den andra är privat. Den digitala signaturen är en kryptografisk kontrollsumma och den är främst tänkt att ersätta namnunderskrifter då man går från papper till EDI. Med den digitala signaturen kan man tillföra ett personligt attribut till ett EDI-meddelande. Det personliga attributet ger, förutom säker identifiering av avsändaren, också skydd mot förändringar av utväxlande meddelanden liksom skydd mot att utställaren förnekar avsändning av meddelandet. Om kravet finns på att mottagaren skall kvittera ankommande meddelanden, kan en digital signatur även tillföras kvittensen, som tillsammans med referenser och ursprunglig digital signatur, utgör ett skydd mot förnekande av mottagning [Goldman 1995, Hultmark 1998 ].

### 3.3.1 Hur beräknas den digitala signaturen? [Goldman 1995, Egen källa 1996]

En digital signatur beräknas genom att man komprimerar ett meddelande till ett tal. Detta tal krypteras sedan med hjälp av en användares hemliga nyckel (personligt attribut) enligt en förvald algoritm. Algoritmer kan vara av symmetrisk eller asymmetrisk typ.

Det krypterade resultatet skall utgöra ett unikt värde för varje kombination av enskilt meddelande och personligt attribut. Det kan därför vara lämpligt att alltid se till att datum och tid ingår i beräkningen. För att uppnå högsta möjliga säkerhet måste den hemliga nyckeln vara okänd och otillgänglig för alla obehöriga. Ofta används ett aktivt kort som bärare av den hemliga nyckeln, där den är oåtkomlig för såväl obehöriga som användaren själv. Dessutom bör meddelandets komprimerande värde vara relativt stort.

För att verifiera en digital signatur hämtar mottagaren ut den digitala signaturen ur meddelandet, komprimerar meddelandet på samma sätt som avsändaren och kan därefter verifiera signaturen med hjälp av avsändarens hemliga nyckel (detta om en symmetrisk metod används) eller avsändarens publika nyckel (om asymmetrisk metod används). Om den publika nyckeln stämmer kan mottagaren känna sig relativt säker på att dokumentet är intakt och kommer från sändaren av den privata nyckeln.

De delar som bör tas med då digital signatur skall beräknas översiktligt är:

- att den digitala signaturen beräknas på data i EDIFACT-format
- att alla tecken mellan två givna segmentpositioner i meddelandet skall ingå i beräkningen

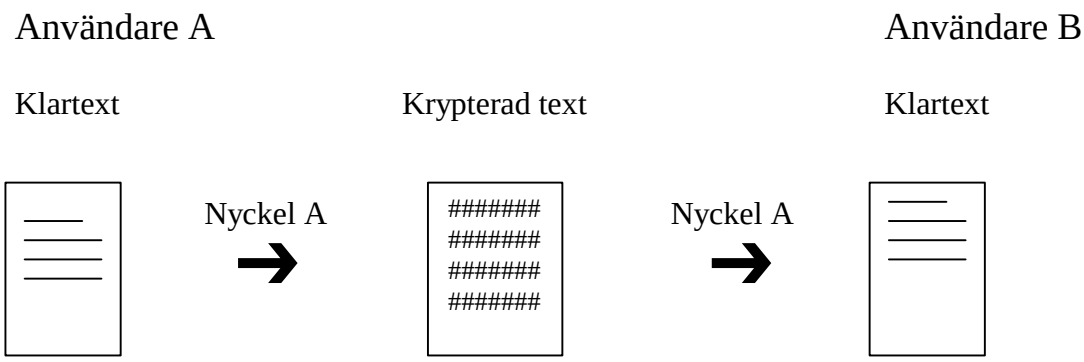
### 3.3.2 Algoritmer [Egen källa 1996, Hultmark 1998, Goldman 1995]

Det finns två typer av algoritmer, **symmetriska** och **asymmetriska**. Vid symmetrisk kryptering används samma krypteringsnyckel vid kryptering och dekryptering. Detta innebär att mottagare och avsändare på förhand måste ha erhållit samma krypteringsnyckel. Ofta använder två handelsparter en för just deras förhållande specifik nyckel. När någon av parterna vill kommunicera med en tredje part så används en annan nyckel. Vid en sådan struktur behövs en unik krypteringsnyckel för varje kommunicerande par. Detta innebär att behovet av stora krav på rutiner för nyckeladministration när antalet kommunicerande par är väldigt stort. Men å andra sidan medför en sådan nyckelhantering att krypteringen indirekt fungerar som autentisering av motparten.

Kända symmetriska krypteringssystem är DES, Trippel DES och IDEA. Flera symmetriska algoritmer är mycket snabba och kan därför användas på stora mängder information. Det krävs mindre datorkapacitet att kryptera samma informationsmängd med ett symmetriskt krypteringssystem än ett asymmetriskt. Därmed kan de lättare göras snabba, även vid realisering i programvara. En nackdel är att nyckeladministrationen och nyckelhanteringen blir väldigt omfattande och kräver mycket arbete.

Kännetecknande för symmetrisk algoritm är:

- att båda parterna använder samma (hemliga) nyckel vid skapande av resp verifiering av digital signatur
- bra prestanda
- vedertagen och etablerad sedan många år tillbaka
- många befintliga produkter och implementeringar




Figur 1. Symmetrisk kryptering

Vid asymmetrisk kryptering används samma krypteringsalgoritm men med olika krypteringsnycklar vid kryptering och dekryptering. De asymmetriska krypteringsalgoritmerna är utformade med ett nyckelpar där den ena nyckeln är publik och den andra är privat. De asymmetriska krypteringsalgoritmerna har den egenskapen att då information krypteras med den ena nyckeln kan den endast

dekrypteras till sin ursprungliga form med den andra nyckeln. Informationen kan med andra ord inte krypteras och dekrypteras med en och samma nyckel.

Den publika nyckeln är tillgänglig för alla som önskar att använda den, medan den privata nyckeln är tillgänglig enbart för nyckelinnehavaren. Detta innebär att i den fall krypterad information skall överföras, kan en godtycklig avsändare kryptera informationen med mottagarens öppna nyckel som vem som helst har tillgång till. Avsändaren vet då att endast den avsedda mottagaren och ingen annan kan dekryptera informationen med sin privata nyckel. Detta innebär att vem som helst kan ha tillgång till en användares publika nyckel, medan användaren är den enda som får ha tillgång till den privata nyckel.

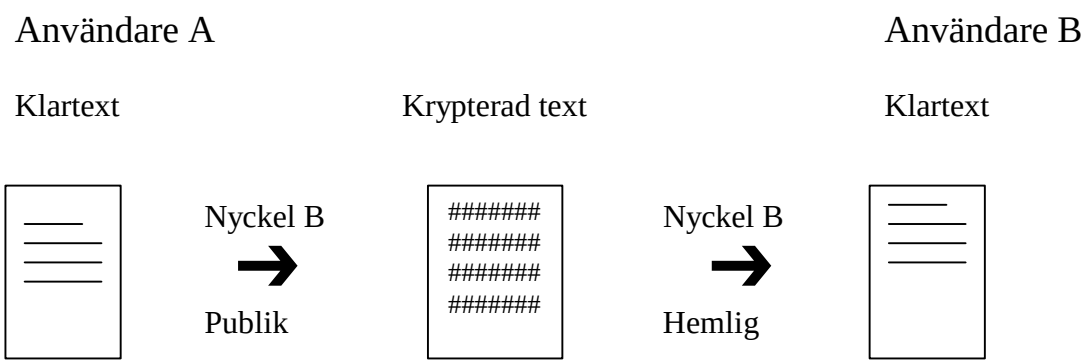
I den publika delen av ett asymmetriskt nyckelpar tillförs ytterligare information som t ex användarens identitet, giltighetstid, typ av algoritm och utställare. Detta förses med en digital signatur av någon man litar på. I denna process skapas en signerad bindning mellan t ex en person och en nyckel, denna informationsmängd brukar ibland kallas för certifikat. Certifikat förvaras på olika sätt t ex i en elektronisk katalog, i den egna datorn eller på ett aktivt kort, certifikaten delges dem som behöver tillgång till aktuell öppen nyckel på ett enkelt sätt.

Fördelen med asymmetriska krypteringssystem är alltså att det löser problem som har med överföring av nycklar att göra. Sändare och mottagare behöver inte på förhand få tillgång till samma nyckel, eftersom den som vill kommunicera med en specifik användare kan hämta dennes öppna nyckel i en elektronisk katalog eller få tillgång till den på annat sätt. På detta sätt förenklas nyckeldistributionen väsentligt. Alla måste kunna verifiera certifikatutställaren d v s den som signerar någons nycklar. Digitala signatur krävs för att bindningen mellan den publika nyckeln och dess innehavare skall kunna säkerställas. Detta kan åstadkommas genom att den öppna nyckeln för certifikatutställaren i förväg delges alla på ett säkert sätt.

Nackdelen med asymmetriska krypteringssystem är att de är beräkningsintensiva. Det krävs mer datorkapacitet att kryptera en informationsmängd med ett asymmetriskt krypteringssystem än med ett symmetriskt. Det är därför inte sannolikt att den asymmetriska metoden används för hela informationsmängden om den är av någon storlek, utan bara för att skydda överföringen av en symmetrisk nyckel. Med hjälp av den öppna nyckeln kan en för kommunikationen skapad symmetrisk sessionsnyckel krypteras och därmed ges en säker överföring. Detta förfarande kombinerar fördelarna hos den symmetriska och den asymmetriska tekniken. Exempel på asymmetriska krypteringsalgoritmer är RSA, Diffie-Hellman/ElGamal och epiliptiska kurvbaserade system.

Kännetecknande för asymmetrisk algoritm är:

- nycklar förekommer i par, den ena är hemlig och den andra är öppen
- endast en part har tillgång till den hemliga nyckeln
- verifiering görs med hjälp av den öppna nyckeln
- öppen nyckel kan distribueras och hanteras utan speciella säkerhetsåtgärder, men det kan behövas en mekanism som garanterar nyckelns partstillhörighet
- den algoritm som rekommenderas av EDIFACT och som är allmänt vedertagen som framtidsstandard.




Figur 2. Asymmetrisk kryptering

**3.3.3 Nyckeladministration** [Goldman 1995, Egen källa 1996]

För att skapa och verifiera digitala signaturer, förändringsskydd och krypterade meddelanden krävs tillgång till nycklar. För att hantera egna och samarbetsparters nycklar måste varje part bygga upp en nyckeladministration där bl a nycklar kan läggas upp, gamla nycklar raderas och personer eller parter ges vald behörighet.

Nyckeladministrationen och nycklarna skall enbart vara åtkomliga för behöriga personer.

Symmetrisk algoritm:

Vid användning av symmetrisk algoritm måste såväl avsändare som mottagare använda sig av samma nyckel. Detta medför att parterna, före start av kommunikation måste utbyta nycklar med varandra. Såväl utbytet av nycklar som lagringen och åtkomst av nycklar måste ske på ett säkert sätt för att behålla trovärdigheten och bevisvärdet i säkerhetsfunktionerna.

I takt med att allt fler parter kommunicerar med varandra kommer administrationen av nycklar att öka avsevärt och bli omfattande, komplext och dyrt.

Asymmetrisk algoritm:

Vid användningen av asymmetrisk algoritm behöver varje användare enbart administrera son egen hemliga nyckel. För verifiering av data används partens öppna (publika) nyckel, varför enbart en nyckel per part behöver administreras. Denna nyckel kan hanteras öppet, d v s utan säkerhetskontroller och utan insynsskydd.

### 3.3.4 Filter och intern teckenrepresentation [Sokol 1995, Egen källa 1996]

Då matematiska algoritmer används för att beräkna värdena för digitala signaturer och förändringsskydd (MAC) uppstår två praktiska problem:

1. Resultatet av beräkningen baseras ofta på binär representation av data, vilket medför att resultatet blir beroende av vilken teckenrepresentation som används. Avsändaren och mottagaren måste därför vara överens om vald teckenrepresentation liksom hantering av insignifikanta tecken.

2. Då resultatet av beräkningen är en slumpmässig bisträng kan problem förorsakas vid överföringen (t ex för kommunikationsprotokollet) eller för mottagande EDI-system. Detta löser man genom att resultatet är reversibelt avbildat/filtrerat till en godkänd teckenrepresentation. För att markera slutet på avbildningen kan speciella avslutningstecken användas t ex en skiftsekvens (escape).

### 3.3.5 Rättsliga hinder

De rättsliga hindren anser många idag är en ökad internationell handel via internet. Efter EU-kommissionens grönbok om digitala signaturer hösten 1997 kom diskussionen igång och idag finns ett lagförslag. Grundtanken är att göra digitala signaturer internationellt erkända med ett juridiskt regelverk för kedjor av CA (Certification Authorities). Direktivet innebär sammanfattningsvis att inget obligatoriskt krav av CA införs, däremot tillåts nationella ackrediteringssystem att växa fram, men villkoren får inte diskriminera andra medlemsstater. CA:s tillåts enbart i den offentliga sektorn. Digitala signaturer får inte betraktas som ogiltiga enbart p g a att de är digitala, digitala och handskrivna signaturer jämställs både civilrättsligt och som bevis i rättegång [Hultmark 1998].

Under vecka 16, antog EU ett direktiv som likställer elektroniska signaturer med handskrivna signaturer. Direktivet väntas bli start för ett legalt regelverk för elektroniska signaturer och därmed främja utvecklingen av EDI och elektronisk handel. Till en början skall direktivet först gå igenom en andra läsning i EU-parlamentet innan telekomministrarna i höst kan ta ett formellt beslut. En svensk lag om elektroniska signaturer kommer till riksdagen i början av nästa år [Computer Sweden 26 april nr 43].

CA som ger ut kvalificerade certifikat svarar för att uppgifterna om nyckelinnehavare är korrekta och att utfärdande nyckelpar hör ihop. De certifikat som är utfärdade utanför EU är lika giltiga om de uppfyller direktivkraven och har ackrediterats i något EU-land eller en CA inom EU går i god för certifikatet. CA får dock enbart inhämta persondata från vederbörande personligen[EU direktivet].

## 3.4 Message origin authentication [SITO 1996, Egen källa 1996]

Message origin authentication (äkthetsbevis) visar upphovsmannens identitet av meddelandet som skickats. Eftersom ett äkthetsbevis är begränsat utan bevis om äktheten i meddelandet, ger äkthetsbeviset försäkran att meddelandet inte har ändrats. Äkthetsbevis kan ske genom två olika metoder, ett äkthetsbevis eller ett bevis om äktheten i meddelandet. Äkthetsbeviset möjliggör identiteten av den som avsänt meddelandet och detta bekräftas med ett kvitto. Asymmetriskt kryptering används vid detta förfarande.

I kontrollen av äkthetsbevis finns en digital signatur inkluderad i meddelandet. Upphovsmannen beräknar signaturen till en funktion i hela meddelandet. Om meddelandet är krypterat beräknas signaturen som en funktion av den krypterade massan. Men identiteten av upphovsmannen kan konfirmeras utan att hela meddelandet ses. Om signaturen är beräknad från det fullständiga meddelandet, ger äkthetsbeviset en funktion där även icke förnekbarhet av ursprung inkluderas. Detta skyddar mottagaren av ett meddelande. Denna funktion ges ej om signaturen beräknas på ett krypterat meddelande. Upphovsmannen kan inte förneka att han skickat ett okrypterat meddelande, men kan däremot förneka att innehållet i ett krypterat inte är det samma som innehållet i ett vanligt okrypterat dokument.

Äkthetsbeviset beräknas genom upphovsmannens privata nyckel. Funktionen har inga restriktioner av upphovsmannen när det gäller vilken typ av asymmetrisk algoritm som används. Mottagaren av meddelandet kan kontrollera signaturen genom att använda upphovsmannens publika nyckel. Denna kan finnas med i meddelandet eller fås på annan väg.

Den andra metoden för äkthetsbevis är äktheten i ett meddelandes innehåll. Denna metod tillåter en kontroll av integriteten hos upphovsmannen av mottagaren men också av kuriren till meddelandet. Denna kontroll ges en gång till varje mottagare med asymmetrisk eller symmetrisk kryptering.

Upphovsmannen kan antingen välja symmetrisk eller asymmetrisk beräkning. Om upphovsmannen använder en symmetrisk algoritm, används en symmetrisk krypterad nyckel av upphovsmannen vid beräkningen, men även hos mottagaren för att kontrollera beräkningssumman. Denna nyckel kan överföras i en meddelandets krypterade data eller på annat förutbestämt sätt.. Eftersom både upphovsman och mottagare delar denna nyckel, kan ingen dekryptera meddelandet. Om äktheten i ett meddelande innehåll beräknas med en asymmetrisk krypterings algoritm, används upphovsmannens privata nyckel för att möjliggöra beräkningen. Mottagaren kontrollerar äktheten med upphovsmannens publika nyckel. Denna kan överföras med meddelandet eller på annat sätt. Detta under förutsättning att upphovsmannen inte överför kontrollsumman i den krypterade delen av meddelandet.

## 3.5 Message Content Integrity och Message sequence integrity [SITO 1996]

Content integrity (äktheten i ett meddelandes innehåll) är meningslöst att använda om inte message origin integrity används. Denna service ger användaren bevis för att innehållet i en transaktion inte har manipulerats. Content integrity i sig självt kontrollerar originalet av ett meddelande, men meddelandet kan ha skickats av en bedragare.

Message sequence integrity (sekvensskydd) skyddar bl a mot kopiering, tillägg och förstörelse av data från det ursprungliga meddelandet. För att spåra försvunna meddelanden kan användaren inkludera ett sekvensnummer som mottagaren kan kontrollera då han får meddelandet. Avsändaren kan även begära konfirmering av mottagande meddelande. För att upptäcka kopierade meddelanden med tillägg kan användaren inkludera ett sekvensnummer som mottagaren kan kontrollera. Avsändaren kan även inkludera en sk tidstämpel som mottagaren kontrollerar.

Då sekvensnummer används måste man ha bestämt hur dessa skall användas. Tidstämpeln produceras av sändarens system. Det är härifrån som originaliteten bestäms och kontrollen utförs.

## 3.6 Tekniska problem och eventuella lösningar

En EDI – lösning måste innefatta vissa säkerhetsaspekter. Detta för att affärshändelserna måste kunna spåras i varje behandlingsled. Det är ett krav som betingas av både lagstiftning och affärsmässighet. I ett EDI – avtal som ingås mellan två parter som idkar handel via EDI är säkerheten en viktig del. Har man många handelsparter ökar givetvis riskerna och därmed behovet av systematiskt säkerhetstänkande.

I en handelssituation är de vanligaste meddelanden beställning, orderbekräftelse, leveransavisering, leveransgodkännande, faktura och betalningen. Beroende på bransch, produkt, pris mm kan kraven på säkerhet variera. Ett meddelande som alltid kräver säkerhet är betalningsuppdraget. Att göra en elektronisk betalning utan en säkerhetslösning är som att skriva ut en check med blyerts, utan underskrift och skicka den som vykort med frimärke. Detta sker nästan aldrig, men vi skickar dock information okrypterad i våra nätverk.

När vi skickar en beställning på varor vill vi ha garantier för att hela beställningen fullföljs. Vi vill ha garanti för att:

1. Ett beställningsmeddelande inte förvanskas och att sekvensen följer förväntad ordning

2. Innehållet i beställningen inte förvanskas under sändning

3. Ingen annan skickar en beställning i vårt namn, avsiktligt eller oavsiktligt

4. Vår leverantör ska kunna vara säker på att det verkligen är vi som är beställare och vi inte kan neka till beställningen

5. Vår leverantör inte ska kunna neka till att han/hon mottagit vår beställning

6. Vår beställning inte skall kunna läsas av obehöriga

De tekniska lösningarna mot dessa garantier eller potentiella hot kan eventuellt lösas på nedanstående sätt:

1. *Sekvensen mellan transaktioner bryts* – detta inkluderar att transaktioner tappas bort under transport från avsändare till mottagare. Den innefattar också att meddelanden inte kommer mottagaren tillhanda i kronologisk ordning. Vilket leder till att en transaktion blir obegripligt i sammanhanget. Hotet möjliggörs av duplicering, tillägg, utplånande eller repetition av transaktionen.

   *Eventuell teknisk lösning,* sekvensnummer, som hanteras genom EDI-konverteraren. EDIFACT:s syntax har uppgifter i början och slutet av varje meddelande och överföring som tillåter kontroll genom sekvensnummer och ”räknare”. Avsändaren kan begära och kontrollera ett erkännande. Säkerhetsfunktionen sekvensskydd utförs med antingen meddelandet AUTACK (Secure Authentification And Acknowledgement Message) eller de särskilda säkerhetssegment som kan placeras i början och slutet av ett meddelande.

2. *Meddelandets innehåll förvanskas* – den här typen av förvanskning innefattar att ett eller flera informationsbärande grunder i meddelandet förvanskats under transporten från avsändare till mottagare. En typ av förvanskning är att vissa informationsbärande grunder helt försvinner. Detta kan bero på tekniska faktorer eller direkt manipulation av t ex belopp, konto eller tidpunkt. Möjligheten finns även att förvanskningen kan vara avsiktlig eller oavsiktlig.

   *Eventuell teknisk lösning,* kryptografisk algoritm, (digital signatur). Förverkligas med hjälp av ett kontrollvärde som beräknas på en informationsmängd med en algoritm och en privat nyckel med syfte att upptäcka förändringar. En kryptografisk kontrollsumma som hör till en informationsmängd kan beräknas då den skapas eller då den lagras och verifieras. Vid användning av informationsmängden kan summan beräknas och jämföras med den ursprungliga.

3. *Meddelande anländer från avsändare som utger sig för att vara någon annan* – den här typen av händelse innebär att någon avsändare avsiktligt eller oavsiktligt försöker att framstår för mottagaren som någon annan.

   *Eventuell teknisk lösning,* inkludera ett MAC (Message Authentication Code) och en digital signatur i det överförda meddelandet. Digital signatur är en omvandling av ett meddelande på ett sätt som endast avsändaren kan utföra. Men som även tillåter mottagaren att kontrollera meddelandets äkthet, innehåll och avsändarens

identitet. Digital signatur kan genomföras på informationsobjekt i digital form med avsändarens privata nyckel och kontrolleras med den publika nyckeln. En förutsättning är ett krypteringssystem med publika och hemliga nycklar.

4. *Avsändning av meddelande förnekas av avsändaren* – denna typ av handling innebär att avsändaren i efterhand förnekar att han avsänt ett visst meddelande medan mottagaren påstår att det mottagits.

   *Eventuell teknisk lösning,* digital signatur som inkluderas i det överförda dokumentet. Då ett meddelande ska knytas till en individ måste digital signatur bifogas meddelandet för att styrka avsändarens identitet. Det kan göras på många olika sätt.

5. *Mottagning av meddelande förnekas av mottagaren* – denna typ av handling innebär att mottagaren förnekar att ett meddelande mottagits medan avsändaren påstår att det avsänts. Det innebär inte att meddelandet försvunnit, men det kan ha gjort det; meddelandet kan felaktigt ha skickats till någon annan utan att denne upptäckt att det inte var avsett för honom.

   *Eventuell teknisk lösning,* mottagaren skickar en bekräftelse som bifogar en digital signatur. EDIFACT har utvecklat ett speciellt säkerhetsmeddelande AUTACK, som kan användas vid överföring av digitala signaturer.

6. *Meddelandets innehåll röjs för obehörig* – denna typ av händelser innebär att ett meddelande som innehåller information som är hemligt kunnat läsas och förstås av obehörig. Det kan bero på att det har skickats till fel part eller att en obehörig person hos den rätte parten fått tillgång till innehållet.

   *Eventuell teknisk lösning,* kryptering. Den kan förverkligas genom att meddelanden krypteras. Krypteringen kan göras med hjälp av symmetrisk algoritm baserad på en privat nyckel som sändare och mottagare känner till.

Utöver dessa skydd krävs det självklart en fysisk säkerheten hos respektive handelspart för att säkerhetställa tillgängligheten och den generella data säkerheten hos företagen.

**Sammanfattningsvis** så utforskas i detta kapitel en rad olika säkerhetsaspekter samt hur de fungerar t ex MAC och digitala signaturer. Något som är påfallande är att de olika säkerhetsaspekterna ofta är starkt kopplade till varandra för att utgöra ett effektivt skydd. I detta kapitel har även en rad olika tekniska problem tagits upp som har försökts lösas med hjälp de olika säkerhetsaspekterna som presenterats tidigare i kapitlet. Något som jag har kommit fram till i detta kapitel är att digital signatur har en stark roll för att EDI skall fungera rent tekniskt och juridiskt på ett tillfredsställande sätt.

# 4. DISKUSSIONER OCH SLUTSATSER

Som jag ser det är EDI men även elektronisk handel ännu i sitt inledningsskede. Alla aktörer är medvetna om att den elektroniska handeln kommer att få ett betydande inflytande i framtiden. Ett land med ofördelaktig lagstiftning kommer snabbt att hamna efter, med en försämrad konkurrenssituation som följd. Sverige ligger väl framme på grund av den offentliga sektorns initiativ till införande av elektronisk handel både på myndighetsnivå och inom näringslivet. Förhoppningsvis kommer detta att hjälpa Sverige till en tätposition i Europa inom den närmaste framtiden. Vi ser redan idag svenska företag som t ex Ericsson, som har en världsledande position med hjälp av bra produkter och teknik som ligger i tiden. För ett par månader sedan hade Ericsson ett seminarium med medlemmar från tidningen Aktiespararen. Under seminariet presenterades framtida produkter och utsikterna, vilket stärker mitt ställningstagande ovan.

Under arbetets gång har jag också kommit fram till att det i längden blir omöjligt att klara sig utan elektronisk handel och EDI. Användningen kommer att öka och när datorer blir var mans egendom, kommer vi säkert att få se någon form av elektronisk handel i hemmen. Detta gäller bl a i områden som distansarbete, livsmedelshandel, bankärenden mm. För företag kommer EDI att leda till mindre personalbehov i ADB sektorn. Men detta behöver inte leda till friställningar, vid en omorganisation skulle det exempelvis finnas mer resurser att satsa på den egentliga produktionen av både produkter och tjänster. När det gäller implementeringen av EDI inom företagsvärlden krävs det en stor kompetens. Denna kompetens finns, men det tar tid att lära ut kunskapen, framförallt i den snabba tekniska utveckling som råder idag.

Ur ett konkurrensperspektiv händer det mycket i och med användandet och införandet av EDI. Företag kan konkurrera mer jämställt med IT. Trots detta krävs det samarbetsrelationer när det t ex gäller lagerhållning, leverantörer, kunder och övriga handelspartners, för att inte tappa marknadsandelar. Risken med detta förfarande är att återförsäljarna blir bundna till en eller ett flertal leverantör. Det kan även vara kostsamt att byta leverantörer, om dessa använder olika EDI – standarder. På Volvo IT används olika standarder bl a EDIFACT och Odette för att kunna vara med på olika marknader och inte tappa marknadsandelar. Ett annat perspektiv är att fler företag kommer att kunna konkurrera på lika villkor. Företag i glest befolkade regioner kommer ha samma fördelar som företag i större städer. Detta förutsätter bra kommunikationer såväl inom telekommunikation som övrig struktur.

Världen vi lever i kommer att förändras dramatiskt över nästa årtionde. EDI:s roll i denna världen är inte klart definierad. EDI experterna har ett uppdrag att förklara för internetvärlden bl a vilka fördelar EDI kan medföra i Cyberspace. Det ligger en stor fara i att standardiseringsprocessen kommer att göras om. Därför måste EDI förklaras som den elektroniska handelns ryggrad. Vi kan använda de existerande EDI – standarderna tillsammans med Internet för att bl a uppnå de mål vi satt upp i våra EDI projekt. Internet och då speciellt WWW ger oss verktyg att bygga WWW – sidor där människor kan fatta beslut och där EDI – meddelanden inkluderas och applikationer kan behandla all data. Det är en viktig uppgift för EDI – organisationerna att verka för större medvetande av värdet med EDI standarder i telekommunikationsvärlden, mobila data , filmer och video, kabel-TV etc.

Många initiativ har tagits för att tillåta konsumenter att handla från hemmet, för att kunden skall kunna beställa vad som helst, var som helst och när som helst. Gränssnitt i gamla applikationer installerade i företag som levererar varor, kräver EDI standarder för att koppla dem samman i denna process. Många problem kvarstår att lösa. En stor uppgift är transaktionssäkerhet på internet. Vi kommer att behöva högt sofistikerade krypteringstekniker för att kunna erbjuda att betala för tjänster på elektronisk väg.
I Computer Sweden i april presenterade Siemens ett program ”Trustedmime” för kodning av meddelanden då man skickar e- post samtidigt som man undertecknar det digitalt. Programmet kan kryptera meddelandet med 128 bitar och klarar upp till 2048 bitars signaturer. Kanske är detta ett framtida program för både elektronisk handel och EDI ?

Dessutom antog EU vecka 16, ett direktiv som likställer elektroniska signaturer med handskrivna signaturer. Direktivet väntas bli en slags start för att etablera ett legalt regelverk för elektroniska signaturer och därmed främja utvecklingen av elektronisk handel. Men till en början skall direktivet först gå igenom en andra läsning i EU-parlamentet innan telekomministrarna i höst kan ta ett formellt beslut. En svensk lag om elektroniska signaturer kommer till riksdagen i början av nästa år, enligt Computer Sweden 26 april nr 43. Efter att ha arbetat med denna uppsats ser jag en stor potential för tekniken digital signatur. Den digitala signaturen ser jag som den bäst uppbyggda tekniken med såväl symmetrisk och asymmetrisk kryptering. Denna är enligt min mening den mest lämpade tekniken för att EDI skall fungera såväl elektroniskt som juridiskt. Framför allt så stärktes mitt ställningstagande då EU antog direktivet om digitala signaturer. Detta innebär även att avtalsmodellen modellen bör fungerar med EDI men även med elektronisk handel. Som jag bedömer det finns det inga problem att använda sig av EDI för att göra elektroniska överföringar mellan två eller flera näringsidkare juridiskt och med fullgod säkerhet. Tekniken finns idag, nu gäller det bara att komma igång på allvar.

Helt klart är, att EDI är här för att stanna och kommer drastiskt att förändra sättet att göra affärer i framtiden. Företag som inte inser EDI:s betydelse kan sätta hela sin existens på spel. Därför är det viktigt att företag förstår att EDI är oundvikligt om man vill överleva i framtiden. Det är hög tid att starta med EDI. De flesta företag ha provat EDI och fått erfarenhet av systemet. Nu kan företag inte längre ta sig tid att lära och göra misstag. Företagen måste agera fort helst redan innan år 2000, annars finns risken att de blir överkörda på informationsmotorvägen.

Den stora skillnaden mellan elektroniska avtalsslut och traditionella är enligt min mening att det går så fruktansvärt fort när det gäller kommunikationen mellan avtalsparterna. De stora frågetecknen är hur de juridiska problemen skall lösas så att de fungerar i en elektronisk miljö. För att bli juridiskt accepterat måste det elektroniska dokumentet uppfylla de krav som ställs på det pappers baserade dokumentet. Eftersom tekniken för detta i dag finns ser jag ingen anledning till att det elektroniska dokumentet ska vara ett sämre alternativ ur bevishänseende, snarare tvärtom.

Rent juridiskt saknas praxis för att sluta avtal elektronisk vilket kräver stor försiktighet. Med hjälp av t ex EDI – avtal kan parterna bestämma hur avtal på ett korrekt sätt ska slutas. Enligt min mening kommer EDI – avtal att finnas kvar så länge praxis inte vuxit fram. Antagligen kommer avtalet att användas under en mycket lång

tid framöver. En annan möjlighet finns i UNCITRAL:s Model Law on Electronic Commerce som har utarbetats av FN. Dessa två hjälpmedel är till en mycket stor fördel idag och kommer enligt min mening att förbli så tills elektronisk handel och EDI börjat att användas vardagligt. Inte förrän då tror jag att någon mer heltäckande lag nationellt kan tillkomma. Frågan är om detta överhuvudtaget behövs med tanke på vårt EU - medlemskap. Jag tror därför att det inte dröjer länge innan IT – utredningens synpunkter inkluderas i 40§ AvtL eller inom andra lagar och betydelsefulla avtal.

En annan risk är att organisationer blir för beroende av varandra när de kopplar ihop sig med hjälp av EDI. Flexibiliteten kan minskas och organisationen blir sårbar när företaget anpassar sig till några få leverantörer. Därmed är risken högre för att avsluta ett samarbete om det inte fungerar tillfredsställande.

## 4.1 Själv kritik och framtida forsknings möjligheter

Denna uppsats har i huvudsak skrivits efter diverse litteraturstudier. Jag skulle gärna ha sett mer information efter olika intervjuer, men dessa gick inte att boka in på den begränsade tid som uppsatsen skulle ha gjorts på. Mitt mål från början var att utforska huruvida bra EDIFACT standarden är och dess användbarhet vilket jag tyvärr inte hunnit med. Dessutom tycker jag det är tråkigt att jag inte hunnit att utforska fler säkerhetsaspekter och eventuellt komponerat ihop en egen lösning till vissa av de problemen som finns idag. Samtidigt skulle man kunna fördjupat sig i de säkerhetsaspekter som jag tagit upp i arbetet men det var aldrig mitt syfte från början. Trots detta känner jag att jag skulle gjort en fördjupning och selekterat ut andra delmoment i uppsatsen såhär efteråt. Tekniskt skulle jag även vilja fördjupa mig i själva implementeringen av EDI hos företag och utvecklingen ända tills handlingsförfarandet påbörjas med EDI men denna möjlighet kanske finns i framtiden.

Utöver detta finns det alltid en bredare aspekt på den juridiska biten vid elektronisk handel och EDI, tyvärr fanns inte den tiden att fördjupa sig i den juridiska delen som behandlar dagens snabba tekniska framfart när det gäller EDI och den juridiska säkerheten från implementering till användandet. Då skulle den röda tråden tappas. Eventuellt kan man gör allt detta i en framtida magisteruppsats.

# 5. KÄLLFÖRTECKNING

## 5.1 Publicerade källor

**Böcker:**

Adlercreutz A, *Avtalsrätt 1*, 10 uppl, Juristförlaget, Lund 1995, ISBN 91-544-0010-4

Berti V, *Datakommunikation*, Liber, Stockholm 1995, ISBN 91-634-0203-3

Borg, Jonson, *Internet @ Sverige*, 1994, Bonnier DataMedia, ISBN 91-644-0010-7

Chesher, Kaura, *Electronic Commerce and Business Communications*, Springer – Verlag Berlin Heidelberg New York 1998, ISBN 3-540-19930-6

Colberg T, Gardner NW, Horan K, McGinnis D, McLauchlin P, So Y-H, *The Price Waterhouse EDI Handbook*, Wiley & Sons 1995, ISBN 0-471-10753-0

Dykert, Lindberg, *Elektroniska affärer juridik och revision*, EDI-föreningen I Sverige, Stockholm 1996

Fredholm P, *Elektroniska affärer*, Studentlitteratur, Lund 1997, ISBN 91-44-00404-4

Goldman J, *Applied data communications*, John Wiley & Sons Inc 1995,

Handelsprocedurrådet SWEPRO, *EDI Affärskommunikation genom elektronisk datautväxling*, Stockholm 1992, ISBN 91-86418-12-2

Hultmark C, *Elektronisk handel och avtalsrätt*, uppl 1:1, Norstedts Juridik AB 1998, ISBN 91-39-20105-8

Jansson I, *Den elektroniska marknadsplatsen*, IRI-rapport 1997:1

Pålsson, *Elektronisk handel över Internet I*, Sveriges tekniska attachéer, 1998, ISBN 99-2585826-7

Ramberg J, *Allmän Avtalsrätt*, 4:e uppl, Juristförlaget, Stockholm 1996, ISBN 91-7508-728-7

SITO, *EDI för elektroniska affärer*, En polhem-rapport 1996, ISBN 9187186322

Sokol P, *EDI to Electronic commerce*, McGraw-Hill 1995, ISBN 0-07-059512-7

Toppledarforum, *Fördelar med elektronisk handel*, Statskontoret 1997, ISBN 91-7099-66366

Winberg G, *Elektroniska betalningssystem på Internet*, IRI-rapport 1997:3

Wiedersheim-Paul F, *Att utreda forska och rapportera*, Uppl 4:2, Ekonomiförlagen 1991, ISBN 91-21-60183-6

**Propositioner:**

*Proposition 1995/96:125*

**Statens offentliga utredningar:**

*SOU 1989:20*, Tullregisterlag mm, Finansdepartementet, Stockholm 1989, ISBN 91-38-10301-X

*SOU 1996:40*, Justitiedepartementet, Stockholm 1996, ISBN 91-38-20210-7

**Tidningsartiklar:**

Computer Sweden 26 April nr 43

**Övrig litteratur:**

Egen källa – *Datakommunikations kompendium*, kursen Datakommunikation fördjupning, Mälardalens Högskola 1996

## 5.2 Opublicerade källor

**Intervju:**

Norström Kristin, Volvo Information Technology AB, 1998-11-10, kl 0900