

**Elektronisk handel ur ett säkerhetsmässigt
perspektiv**

(HS-IDA-EA-99-404)

Susanne Andersson (a96susan@ida.his.se)

*Institutionen för datavetenskap
Högskolan i Skövde, Box 408
S-54128 Skövde, SWEDEN*

Examensarbete på det dataekonomiska programmet
under vårterminen 1999.

Handledare: Åsa Grehag

Elektronisk handel ur ett säkerhetsmässigt perspektiv

Examensrapport inlämnad av Susanne Andersson till Högskolan i Skövde, för Kandidatexamen (BSc) vid Institutionen för Datavetenskap.

99-06-10

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Sammanfattning

Elektronisk handel är på väg att bli allt vanligare. Detta examensarbete behandlar en av de två olika typerna av elektronisk handel, nämligen webhandeln. Den andra varianten är EDI. Webhandel är den elektroniska handel som bedrivs mellan företag och privatpersoner, till skillnad från EDI som är handel mellan två företag.

Det har blivit allt vanligare att företag kan erbjuda sina kunder att handla via Internet och även betala över Internet. Det finns några olika sätt att betala för sina inköp, nämligen med betalkort, att vara medlem i ett shoppingtorg eller att använda digital valuta. Det kan dock vara riskfyllt att lämna ut sitt kontokortnummer på Internet, eftersom en skicklig och oärlig person skulle kunna avlyssna transaktionen och sedan använda kontokortnumret för egna inköp.

Mitt examensarbete är ett försök att reda ut hur farligt det egentligen är att betala via Internet. De problemställningar som har utretts är :

- Vilka krav finns på säkerhet från de olika aktörerna på marknaden, d v s banker, webbutiker och kunder?
- Vilket av betalningssätten uppfyller säkerhetskraven i störst utsträckning?

De slutsatser jag har kommit fram till är:

- De krav på säkerhet som ställs från de inblandade är att betalningen skall vara säker för avlyssning, webbutik och kund skall kunna identifiera varandra samt kunden vill känna förtroende för att ingen information om hans köp hamnar i orätta händer.
- Vad gäller säkerheten i de olika betalningssätten så anser jag att samtliga elektroniska betalningssätt uppfyller kraven, men att den allra säkraste metoden är SET – Secure Electronic Transactions.

Innehållsförteckning

| | | |
|----------|--|-----------|
| 1 | Introduktion..... | 1 |
| 2 | Bakgrund | 3 |
| 2.1 | Historien om Internet | 3 |
| 2.1.1 | Att använda Internet | 5 |
| 2.1.2 | Möjligheterna med Internet | 7 |
| 2.2 | Elektronisk handel..... | 7 |
| 2.3 | Webhandel | 9 |
| 2.3.1 | Vem handlar | 9 |
| 2.3.2 | Vad handlas | 10 |
| 2.3.3 | EDI | 11 |
| 2.4 | Betalningsmedel vid webhandel | 12 |
| 2.4.1 | Betalkort | 12 |
| 2.4.2 | Medlemskap i shoppingtorg | 13 |
| 2.4.3 | Digital valuta | 14 |
| 2.5 | Risker vid elektronisk handel..... | 14 |
| 3 | Problembeskrivning | 16 |
| 3.1 | Problemställning..... | 16 |
| 3.2 | Avgränsning..... | 16 |
| 3.3 | Förväntat resultat | 17 |
| 4 | Metod..... | 18 |
| 4.1 | Möjliga metoder..... | 18 |
| 4.1.1 | Enkäter | 18 |
| 4.1.2 | Intervjuer | 19 |
| 4.1.3 | Direkt observation | 19 |
| 4.1.4 | Litteraturstudier | 20 |
| 4.2 | Metoder för bearbetning av data..... | 20 |
| 4.2.1 | Kvantitativ bearbetning | 21 |
| 4.2.2 | Kvalitativ bearbetning | 21 |
| 4.3 | Val av metod..... | 21 |
| 4.3.1 | Val av metod för datainsamling | 22 |
| 4.3.2 | Val av metod för bearbetning av data | 22 |
| 4.3.3 | Metoder som ej valts..... | 23 |
| 4.4 | Plan över arbetet | 23 |

| | |
|--|-----------|
| 5 Genomförande | 24 |
| 5.1 Problem med digitala betalningsmedel | 24 |
| 5.2 Aktörernas krav | 25 |
| 5.3 Sammanställning av risker och krav | 26 |
| 5.4 Säkerheten hos de olika betalningssätten | 27 |
| 5.4.1 Betalkort | 27 |
| 5.4.2 Medlemskap i shoppingtorg | 29 |
| 5.4.3 Digital valuta | 29 |
| 6 Analys | 31 |
| 6.1 Betalkort..... | 31 |
| 6.1.1 Konto/kreditkort..... | 31 |
| 6.1.2 Smarta kort..... | 31 |
| 6.1.3 SET | 32 |
| 6.2 Medlemskap i shoppingtorg | 32 |
| 6.3 Digital valuta..... | 32 |
| 6.4 Diskussion | 33 |
| 7 Resultat | 35 |
| 7.1 Diskussion | 36 |
| 8 Slutsatser | 37 |
| 9 Erfarenheter från arbetet | 38 |
| 9.1 Uppslag till fortsatt arbete | 39 |
| 10 Referenser | 40 |
| Bilaga 1 | |

1 Introduktion

Många företag erbjuder idag sina kunder att handla och betala via Internet. Det finns många olika sätt att betala sina inköp, och jag skall undersöka dessa och peka på för- respektive nackdelar med dem, samt hur säkra de olika alternativen är för kunden. Enligt Schmitz (1998) finns följande betalningsmedel:

- Postförskott
- Faktura/inbetalningskort
- Kontant
- Check/internationell bankcheck
- Betalkort
- Digital valuta
- Shoppingtorg (medlemskap)

Arbetet kommer i första hand att koncentreras på de betalningar som sker direkt via Internet, alltså med olika betalkort, digital valuta eller som medlem i ett shoppingtorg. De andra betalningssätten är mindre relevanta i detta sammanhang. Därför kommer dessa ej att behandlas ytterligare i detta examensarbete, då själva betalningen ej sker via Internet.

En traditionell betalning för varor köpta via Internet kräver att köparen postar en check, betalar en faktura eller går till posten och löser ut sitt paket mot postförskott. Detta förfarande har gjort att det tagit ganska lång tid att få sina varor och eftersom diverse olika avgifter tillkommer har det dessutom blivit ganska dyrt om köparen vill göra många småköp från olika webbutiker. Teknikens framsteg har nu gjort det möjligt att istället betala direkt hemma vid sin dator, antingen via konto/kreditkort eller digital valuta. Enligt Schmitz (1998) finns det dock inga svenska banker som erbjuder möjligheten använda digital valuta i Sverige än.

Enligt Fredholm (1998) finns det två typer av elektronisk handel – den som riktar sig till privatpersoner (webhandel) och den som riktar sig till företag (EDI). Detta arbete koncentreras uteslutande på webhandeln. I syfte att kartlägga denna handel har många undersökningar gjorts, av vilka några studerats här.

En av dessa undersökningar har gjorts av FSI (Föreningen för Samhälls- och informationsstudier). Den redovisas av Forsebäck (1998) och visar att den typiske Internetanvändaren är en 35-årig högavlönad man i ett storstadsområde. Samma undersökning visar också att andelen kvinnliga användare har ökat och nu utgör drygt en tredjedel. De varor och tjänster som handlas mest är böcker, CD-skivor, biljettbeställningar samt sexrelaterade tjänster.

1 Introduktion

Wallström (1998) redovisar en undersökning gjord av Computer Sweden som visar att knappt hälften av de svenska företagen bedriver någon form av handel via Internet. Ytterligare en fjärdedel av företagen planerar att införa det. Många av de tillfrågade personerna på företagen som deltog i undersökningen uppgav att det som avhåller dem från att satsa på elektronisk handel är säkerheten, och hela 61 % av de tillfrågade företagen anser att de behöver höja säkerheten i det egna företaget. Detta kan tjäna som en fingervisning om vikten av att granska denna fråga.

Enligt Schmitz (1998) finns inte alternativet med digital valuta tillgängligt via de svenska bankerna. Inte heller vill de svenska bankerna godkänna köp med betalkort över Internet. De webbutiker som ändå erbjuder sina kunder denna möjlighet har avtal med utländska banker (Westholm, 1998). Den enda form av kontokortsbetalning som svenska banker godkänner är vid medlemskap i shoppingtorg, där kundens identitet fastställs då medlemskapet inleds (Schmitz, 1998).

Vad är det då som gör att bankerna stretar emot på detta vis? Enligt Ottosson (1999) är det så att banken hittills inte har ansett att det funnits något betalningssätt som varit tillräckligt säkert, vare sig för kunden, butiken eller banken. Ett problem här är att bankerna och butikerna ofta har något skild syn på säkerheten. Banken vill alltid jobba med 100-procentig säkerhet medan butikerna alltid räknar med ett visst svinn.

Även butikerna har naturligtvis stort intresse av att det så fort som möjligt introduceras en lösning som garanterar säkerheten för samtliga inblandade parter. Ju längre det dröjer innan det sker ett genombrott för den elektroniska handeln, desto större summor går butikerna miste om. Detta kan leda till att vissa affärer avstår från en planerad satsning på handel via Internet, medan andra kanske får lägga ned sin verksamhet helt och hållet. Dessa problem leder fram till frågan om det i dagsläget finns något betalningssätt som uppfyller de krav på säkerhet som finns, och i så fall vilket av dem. Den frågeställningen ligger till grund för detta arbete.

Arbetet kommer härafter att presenteras i form av en bakgrund, där läsaren får en överblick över ämnet Internet och elektronisk handel. Där kommer viktiga termer och begrepp att introduceras för att skapa förståelse för kommande resonemang. Där ges också en redogörelse för de betalningsmetoder som finns och hur de tillämpas. Därefter följer ett kapitel där problemställningen presenteras mer detaljerat, vilket följs av en beskrivning av de metoder som finns för att bedriva en vetenskaplig undersökning. Där kommer också att redogöras för mitt val av metod för detta problem.

Sedan följer en redovisning för hur undersökningen genomförts, de erfarenheter som arbetsprocessen givit, samt en värdering och analys av det insamlade materialet. Slutligen kommer resultat och slutsatser att redogöras, vilka följs av uppslag till fortsatt arbete inom detta område.

2 Bakgrund

För att ge en överblick över Internet och alla dess förgreningar presenteras här hur Internet uppstod, samt vilka dess huvudsakliga syften var. Då det finns olika åsikter om de samband som finns mellan Internet, elektronisk kommunikation och elektronisk handel kommer det att klargöras vilken min uppfattning är.

Vidare kommer det att redogöras för de problem som dyker upp i samband med att en kund vill handla något i den elektroniska butiken.

2.1 Historien om Internet

En vag definition av Internet är helt enkelt att det är en mängd datorer sammankopplade i nätverk. Användarna behöver inte veta hur de är sammankopplade eller hur de kommunicerar med varandra – de behöver bara bry sig om att använda nätverket på bästa sätt (Makey, 1996).

Men vad är egentligen Internet? Hur uppstod det? Vilket var dess ursprungliga syfte? För att besvara dessa frågor har jag studerat Internets historia som författarna Lynch & Lundquist (1996) och Makey (1996) beskriver den.

Lynch & Lundquist (1996) beskriver ursprunget till Internet som ett projekt hos det amerikanska försvarsdepartementet. Det kallades Arpanet eller ARPAnet, eftersom det grundades av Advanced Research Projects Agency (ARPA). Arkitekturen hos Arpanet utvecklades under decenniet mellan 1959 och 1969 i ett samarbete mellan militären och ett flertal olika universitet och forskningsinstitut.

Det huvudsakliga syftet med Arpanet var att skapa ett distribuerat datorkommunikationssystem som skulle kunna stå emot ett militärt anfall, så att även om en del av systemet sattes ur funktion skulle resten av nätverket fortfarande fungera. Andra viktiga mål med Arpanet var enligt Lynch & Lundquist (1996):

- Olika datorer skulle ha möjlighet att utbyta information på ett enkelt sätt
- Att information automatiskt skulle omdirigeras runt de delar av nätverket som inte fungerade
- Ett mål som tillkom senare var att genom att använda Interface Message Processors (IMPs) bestående av många små nätverk så skulle endast en dator på en site (IMPn) behöva vara ansluten till Arpanet

Enligt Makey (1996) skulle Arpanets mål uppfyllas på följande sätt:

2 Bakgrund

- Det måste finnas många alternativa vägar för informationen att färdas om det blir nödvändigt. Detta underlättades genom strukturen av datornätverk inom större nätverk. Detta gav informationen som färdades i nätverket nästan obegränsade möjligheter till olika vägval om den skulle stöta på svårigheter längs en specifik rutt.
- Informationen som färdades i nätverket måste vara oberoende av infrastrukturen i nätverket. Varje dator i nätverket ansvarade för att adressera varje ”paket” av information, d v s det skulle tydligt framgå både ursprung (vem som skickat det), samt destination (vem som är mottagare). Paketet skulle sedan kunna dirigeras genom nätverket längs vilken rutt som helst tills det slutligen nådde sin destination.

Makey (1996) gör en liknelse mellan nätverket och en motorväg, där informationspaketen är fordon som trafikerar motorvägen. Motorvägen själv dirigerar fordonen/paketen till deras rätta destination med hjälp av trafiksignaler o s v, men är ovetande om paketens innehåll.

Under 1970-talet fick de universitet och andra institutioner som sysslade med försvarsrelaterad forskning tillåtelse att ansluta sig till Arpanet. 1975 fanns det ungefär 100 siter (Lynch & Lundquist, 1996).

Lynch & Lundquist (1996) berättar vidare att Arpanet från början designades på ett sådant sätt att informationen skulle färdas i ett specifikt format, Network Control Protocol (NCP). Ett protokoll är en uppsättning regler för utbyte av information mellan datorer, en sorts åtkomstkontroll (Beekman, 1994). Lynch & Lundquist (1996) påpekar att denna typ av protokoll innebar att datan som skulle skickas delades upp i bitar eller paket som adresserades med ursprung och destination, ungefär som ett brev. Paketet skickades sedan från en dator till en annan tills de nådde sin destination. Om något kom bort kunde det sändas igen från avsändaren. För att undvika att man återutsände meddelanden på detta sätt i onödan fick mottagaren bekräfta att han mottagit informationen.

Lynch & Lundquist (1996) berättar vidare att i slutet av 1970-talet hade Arpanet vuxit så mycket att NCP inte längre ansågs tillräckligt bra och man ändrade därför från NCP till ett nytt protokoll som kallades Transfer Control Protocol/Internet Protocol (TCP/IP). Fördelen med TCP/IP var att det tillät nästan obegränsad tillväxt av nätverket och att det var lätt att implementera på en mängd olika datorplattformar.

Nästa vändpunkt i Internets liv var enligt Makey (1996) i slutet av 1980-talet då National Science Foundation (NSF) beslöt av sammankoppla fem superdatorer som skulle kunna användas över hela USA. Detta motarbetades dock av amerikansk byråkrati och till slut blev grundarna tvungna att skapa ett eget nätverk. Detta nätverk kallades NSFNET och blev en stor succé. Det öppnades för kommersiell trafik under

2 Bakgrund

det tidiga 1990-talet. Det var då som det Internet vi känner idag verkligen startade och TCP/IP etablerades som standardprotokoll.

Enligt Lynch & Lundquist (1996) startades två andra nätverk, Usenet och BITNET, ungefär samtidigt med NSFNET. Dessa två nätverk var avsedda för allmänheten och byggde på att de skulle vara lätta att använda. Kopplingarna mellan alla dessa tre nätverk växte efterhand som folk ville utbyta email och annan information med varandra. Nya nätverk uppstod såsom CompuServe och America Online. Alla dessa nätverk tillsammans bildar vad vi idag kallar Internet. Det består av tusentals nätverk som är sammankopplade från kontinent till kontinent.

När Internet nämns i dagligt tal är det egentligen ofta World Wide Web (WWW) som avses. WWW kan beskrivas som ett lager ovanpå Internet som gör det enklare att komma åt informationen på Internet – WWW är ett nät som binder samman de enskilda dokumenten som finns därute (Ericsson, 1995). Enkelt uttryckt är WWW den del av Internet där websidorna finns.

WWW är den del av Internet som växer snabbast, men också den del som är mest sårbar och utsatt för attacker och intrång (Garfinkel & Spafford, 1997). Därför är säkerheten på WWW ett ständigt aktuellt ämne. Allteftersom det görs nya ansträngningar för att garantera säkerheten, så gör också de personer som försöker bryta sig in framsteg. Det är min uppfattning att det närmast har blivit en kapprustning mellan dessa parter.

2.1.1 Att använda Internet

För att läsaren skall få en bättre förståelse för problemområdet och för att förklara vissa termer och begrepp som kommer att användas i kommande resonemang följer här en kort beskrivning av den hård- och mjukvara som är nödvändig för att kunna använda Internet och därmed få tillgång till de elektroniska butikerna.

Hur gör den som vill ta del av allt det som finns på Internet? Vad behövs det för utrustning? För att kunna ”komma ut på nätet” (eller surfa som det populärt kallas) krävs viss hård- och mjukvara. En del måste användaren skaffa själv, annat finns installerat ute i nätverken.

Det som man behöver skaffa själv är till att börja med en dator. Utöver denna måste man också ha ett *modem*. Modemet kan vara antingen externt (en liten ”låda” bredvid datorn) eller internt (monterat på ett kretskort inne i datorn). Modemet är det som gör att datorn kan kommunicera med andra datorer. Det omvandlar datorns digitala signaler till analoga signaler som kan färdas på telefonledningarna. Vid den mottagande datorn finns också ett modem som återför signalerna till digitala signaler (Beekman, 1994). Ett alternativ till modem är en s.k. *fast anslutning*. Som namnet antyder innebär det att man ständigt ligger uppkopplad mot Internet. En sådan anslutning är således dyr och är alltså inget alternativ för hemmabruk (Arvidsson et al, 1995).

2 Bakgrund

När man köper en dator brukar man ofta få med en sorts mjukvara som kallas *webbrowser* eller *webläsare*, vilken också behövs för att kunna utnyttja Internet. Browsern är en mjukvara som gör så att användaren kan läsa *HTML*-kodade sidor på World Wide Web. Makey (1996) anger de två största på marknaden som Netscape vilka har Navigator och Communicator samt Microsoft som har Internet Explorer. Browsern kan visa information på olika sätt: vanlig text, grafiska bilder eller som länkar. När man klickar på en länk (visas vanligen i blått på websidan) talar man om för browsern att öppna ett nytt dokument eller flytta till en annan plats i det redan öppnade dokumentet.

HTML betyder HyperText Markup Language, vilket närmast kan översättas med "märkspråk för hypertext". Ericsson (1995) beskriver HTML som ett sorts "språk" som används för att publicera och läsa elektroniska dokument på Internet - "websidor". När en användare tittar på olika sidor på WWW så använder han browsern. För att browsern skall veta hur informationen på dessa sidor skall visas måste det finnas information i dokumenten som *markerar* vad som är t ex:

- En länk
- En bild
- En rubrik
- Fetstil

Texten i ett HTML-dokument innehåller alltså märken (*tags*) och det är dessa som gör att det som egentligen är en vanlig textfil blir ett hypermediadokument. Browsern hämtar textfilen med märken i, och tolkar sedan informationen, d v s lägger in länkar på rätt ställen, visar viss text som rubriker o s v (Ericsson, 1995).

Ute på Internet finns sedan andra komponenter som är nödvändiga. Ett exempel på detta är *routrar*. Som tidigare berättats färdas informationen i form av "paket" i nätverket. De dirigeras dit de skall med hjälp av routrar som tar emot paketen och skickar dem vidare till rätt adress. Routrarna bedömer vilken väg som är lämpligast för paketen att färdas mellan de olika datorerna (Gustavsson & Johansson et al, 1998).

För att få hjälp med att ta fram de dokument som användaren vill se behövs en *server*. Servern kan enligt Makey (1996) beskrivas som en s k värddator, alltså en specifik dator som är ansluten till Internet och har en egen unik *IP-adress*. Dess jobb är att invänta förfrågningar som sänds från browsers angående olika dokument. Servern hämtar dokumentet och skickar tillbaka det till browsern via *HTTP*. Enligt Makey (1996) vet servern vart den skall skicka dokumentet tack vare adressen som medföljde informationspaketet. HTTP betyder HyperText Transfer Protocol och är ett protokoll som anger reglerna som browsern måste följa för att begära data och som servern måste följa för att tillhandahålla densamma.

Makey (1996) påpekar också att en användare som ansluter till Internet oftast inte får någon egen, fast IP-adress utan blir tilldelad en temporär adress som varierar varje gång användaren ansluter till Internet. Adressen är ett nummer som kan se ut t ex så här: 193.10.176.19.

2.1.2 Möjligheterna med Internet

Möjligheterna till olika användningsområden på Internet är naturligtvis stora. Ett populärt uttryck är att med Internet har man hela världen i sitt eget hem, och min uppfattning är att det faktiskt ligger en hel del sanning i det.

Med hjälp av olika sök katalogtjänster kan Internet användas som ett stort uppslagsverk och det blir möjligt att söka efter företeelser eller personer som det kan vara intressant att veta mera om. En annan väldigt stark sida hos Internet är möjligheten att få aktuell information på ett enkelt sätt. Det är t ex möjligt att ta fram busstidtabellen eller läsa dagstidningarna via sin dator, istället för att gå till busstationen och hämta en tabell eller att prenumerera på en tidning. Det går att kommunicera med sina vänner och bekanta och skicka dokument till varandra via e-post istället för fax eller post. Det är också möjligt att sköta betalningar och handla i olika elektroniska butiker via Internet och det är just vad som kommer att undersökas i detta examensarbete.

Men allt som rör Internet är inte positivt. Eftersom alla användare kan välja att vara anonyma på Internet så är det svårt, för att inte säga omöjligt att spåra personer som ägnar sig åt olaglig verksamhet på Internet. Exempel på sådan olaglig verksamhet kan vara intrång i datasystem, stöld av känslig information, spridande av datavirus och liknande.

En annan aspekt är vad denna nya företeelse egentligen gör med oss som människor. Dels är det inte så ovanligt med ledvärk vid stillasittande arbete vid datorn, dels befarar jag att den elektroniska kommunikation som många människor ägnar sig åt, kan göra att vi avskärmar oss mer och mer från varandra och det verkliga samhället som finns omkring oss.

2.2 Elektronisk handel

Det finns olika uppfattningar om vilken innebörd man skall lägga i begreppet elektronisk handel. Holländer (1997) har i sitt examensarbete uppfattningen att elektronisk handel är ett samlingsbegrepp för olika typer av meddelandeutväxling, t ex EDI och Internet. Han stödjer sig på en definition som tagits fram av Toppledarforum, vilket är ett samarbete mellan statliga myndigheter som har till uppgift att effektivisera offentlig verksamhet genom ökad användning av IT. Definitionen av elektronisk handel lyder:

”Elektronisk handel avser bl a att manuella pappersrutiner såsom anbud, beställning, faktura ersätts med sina elektroniska motsvarigheter eller av elektroniska rutiner.”

2 Bakgrund

Denna definition instämmer jag i, men ofta kan begreppet elektronisk handel definieras olika beroende på vilken situation som avses. Fredholm (1998) skriver att det finns olika typer av elektronisk handel och de passar olika bra vid olika tillfällen. När två företag har ett affärsavtal med varandra, och där företagen kontinuerligt skickar en massa transaktioner, finns behov av att automatisera flödena. I andra fall där det är fråga om köp vid mer enstaka tillfällen krävs det en enklare och billigare teknik. Behovet av automatisering blir då inte lika stort.

Fredholm (1998) benämner dessa två olika varianter av elektronisk handel EDI och webhandel. Webhandeln är den elektroniska handel som det i allmänhet talas mest om och det är den som vänder sig till privatpersoner. Betydligt mer omfattande och avgörande för många företag är den elektroniska handel som sker mellan företagen, s k "business to business". Denna uppsats kommer huvudsakligen att koncentreras på den handel som riktar sig till privatpersoner (webhandel), men även ge en beskrivning av vad EDI är. Eftersom jag helt inriktat mig på webhandeln kommer jag att använda begreppet elektronisk handel som liktydigt med webhandel.



Fig 1. Elektronisk handel (Fredholm, 1998)

Både elektronisk kommunikation och elektronisk handel kan ju förekomma utanför Internet, men för den typ av elektronisk handel jag har valt att studera är Internet en förutsättning.

Wallström (1998) skriver om en undersökning som Computer Sweden har gjort med IT-ansvariga på 100 företag över hela Sverige inom olika branscher. Denna undersökning kom fram till att det är 44% av företagen som använder någon form av elektronisk handel. Av dessa är det hela 80% som går in för handel mellan företag, medan endast 20% satsar på konsumentrelaterad handel. Ytterligare 24% av de utfrågade planerar att satsa på elektronisk handel.

Säkerhetsfrågor spelar dock en stor roll. Hela 61% av företagen säger att de behöver höja säkerhetskraven i det egna företaget. Vissa går så långt att de anser att säkerheten kan avhålla dem från e-handelssatsningar. De vanligaste säkerhetsproblemen är virus, förlust av data, stöld av intern information eller affärshemligheter, manipulation av program, samt överföring av olagliga dokument och bedrägerier (Wallström, 1998).

De slutsatser som jag drar av dessa siffror är att den elektroniska handeln redan har tagit en stor del av den totala handeln och kommer att fortsätta att expandera. Stöttestenen är dock (enligt de utfrågade i ovan nämnda undersökning) att säkerheten ännu inte kan garanteras fullt ut, varken för webbutikerna eller för kunderna. För att

2 Bakgrund

den elektroniska handeln skall kunna få sitt riktiga genombrott krävs nya rutiner för att komma till rätta med dessa problem, vilket det för närvarande forskas intensivt omkring.

Naturligtvis kan det även finnas andra anledningar till att det förväntade genombrottet för den elektroniska handeln dröjer. En tänkbar orsak tror jag är att de flesta människor ogärna ändrar på sina rutiner. Om en kund är van att handla i en viss butik vill han inte gärna byta till en annan. Många kunder kan också tänkas uppleva att utbudet i de elektroniska butikerna inte är tillräckligt stort; det finns helt enkelt inte tillräckligt mycket att välja på. En annan tänkbar anledning tror jag kan vara att det detta till stor del är en generationsfråga. Många äldre kan ha svårt att till sig den nya tekniken och vill hellre att allt skall vara som det alltid har varit, medan ungdomar idag växer upp med datorer och Internet som en del i vardagen. De ungdomar som inte har tillgång till Internet hemma, har det oftast tillgängligt i skolan. Det ger naturligtvis en annan syn på tekniken än vad de äldre har som fått lära sig detta i vuxen ålder, eller som helt står utanför och inte har någon erfarenhet eller kunskap alls om vare sig datorer eller Internet.

2.3 Webhandel

Med webhandel avses den handel från Internetbutiker som privatpersoner kan ägna sig åt via datorn i hemmet, till skillnad från den handel som sker mellan företag. Enligt Wallström (1998) verkar det dock som om denna handel inte riktigt har fått fart ännu. Detta kan bero på att det ännu inte finns någon betalningsstandard som är helt accepterad av samtliga aktörer på marknaden. Enligt Wallström (1998) är SET – Secure Electronic Transaction - den standard som de flesta verkar hoppas mest på. Vad denna standard innebär kommer att diskuteras längre fram i arbetet.

2.3.1 Vem handlar

En undersökning som gjorts av FSI (Föreningen för Samhälls- och Informationsstudier) och som redovisas av Forsebäck (1998) har gett en bild av den typiske Internetanvändaren: En 35-årig man med relativt hög inkomst och boende i storstad. Emellertid bedöms andelen kvinnliga Internetanvändare ha stigit. Kvinnorna beräknas nu utgöra 37% av Internetanvändarna. Undersökningen har också kommit fram till att den typiske ”webshopparen” tillbringar betydligt fler timmar på Internet än den genomsnittlige Internetanvändaren. Forsebäck (1998) anser att det möjligen kan tolkas som att de grupper som flitigast använder sig av möjligheten att handla på Internet är de som använt sig av det under längst tid och skaffat sig erfarenheter. De yrkesgrupper som har någon anknytning till IT eller kommunikation är klart överrepresenterade när det gäller elektronisk handel.

Forsebäck (1998) gör vidare den bedömningen att den stora vinnaren på det tidiga 2000-talets elektroniska marknad kommer att vara konsumenten. Det gäller både de hushåll som ser till de tidsbesparingar som kan göras genom att handla via Internet och de som ser möjligheten att spara pengar genom att handla billigare på Internet. Helt

2 Bakgrund

följdriktigt konstaterar han också att när konsumenterna på allvar upptäcker möjligheterna att handla elektroniskt kommer de stora förlorarna att vara grossisterna.

2.3.2 Vad handlas

Enligt Forsebäck (1998) är den affärsverksamhet som länge dominerat webbandeln den sexrelaterade. 1997 överträffades den dock av handeln med aktier som den mest inkomstbringande på Internet (Sandén, 1998). Forsebäck (1998) anser därmed att det också är rimligt att anta att denna typ av sexrelaterad handel så småningom kommer att förlora en del av nyhetens behag, men det är också sannolikt att handel med andra varor och tjänster via Internet kommer att växa i sådan omfattning att sexhandeln kommer att framstå som relativt obetydlig.

Flera undersökningar gjorda av FSI pekar på att en av de tjänster som flest svenskar skulle vilja ha via Internet är tjänster som rör bankärenden (Segerlund, 1998). Övriga tjänster som enligt Segerlund (1998) intresserar Internetanvändarna är de nyttotjänster som finns tillgängliga, såsom att hämta information från myndigheter, beställa resebiljetter eller biljetter till diverse evenemang samt att beställa varor. Det som användarna sedan i själva verket utnyttjar Internet till kan skilja sig betydligt från ovanstående. Där upptäcker Forsebäck (1998) att det är handeln med varor som dominerar. Framförallt är det kurslitteratur som handlas elektroniskt, vilket knappast förvånar då högskolor och universitet relativt tidigt börjat utnyttja Internets möjligheter.

De varor som idag finns tillgängliga att handla på Internet visar på en ganska stor bredd på utbudet. Se detta exempel ur Forsebäcks (1998) rapport:

- **Dagligvaror**
 - Livsmedel
 - Hygienartiklar
 - Andra förbrukningsartiklar

- **Det specialiserade sortimentet**
 - Böcker
 - CD-skivor
 - Mjukvara
 - Blommor
 - Leksaker
 - Kläder
 - Sport- och fritidsartiklar
 - Antikviteter och frimärken
 - Särskilda livsmedel (exempelvis orientalisk mat, hälsokost, mat för husdjur)

- **Sällanköpsvaror**
 - Möbler
 - Vitvaror

2 Bakgrund

- Bostäder
- Bilar

De tjänster som förekommer är också de av skiftande karaktär (Forsbäck, 1998).

▪ Finansiella tjänster

- Traditionella banktjänster, överföring mellan konton e t c
- Rådgivning och handel med aktier och andra värdepapper
- Kreditupplysning
- Konsulttjänster
- Rese-, evenemangs- och hotellbokningar
- Speltjänster (både dataspel och tips, trav o dyl.)
- Kontaktförmedling
- Hemleveranser av färdiglagad mat
- Söktjänster i exempelvis mediaarkiv

2.3.3 EDI

EDI, Electronic Data Interchange, bygger enligt Fredholm (1998) på standardiserade elektroniska affärsdokument. Det används för att automatiskt kunna skicka och ta emot dessa dokument. Till skillnad från webhandeln, som vänder sig till privatpersoner, är EDI inriktat mot handel mellan företag och i stor utsträckning automatiserat. Det används ofta vid tät handel mellan två företag som har reglerat sin verksamhet genom affärsavtal. Denna hantering fanns redan på 1960-talet i USA för handel och transport - alltså före Internets tillkomst (Fredholm, 1998).

Kühn Pedersen (1990) beskriver användningsområdet för EDI som att utväxla olika typer av affärsdokument, såsom beställningar, orderbekräftelser och fakturor, via datorer istället för med posten. Den fördel som man direkt lägger märke till är att det går mycket fortare. Med elektronisk hjälp kan ett dokument förflyttas från ett land till ett annat på några få sekunder. Om man sparar tid så sparar man i allmänhet också pengar, vilket inte heller kan sägas vara någon nackdel. En annan fördel rör inmatningen av data, vilken endast sker en gång. Därefter flyttas datan elektroniskt. Detta minskar risken för att fel skall uppstå i samband med inmatningen. Ytterligare fördelar är att det blir ett långt mindre behov av manuella inmatningar eller kopiering av dokument. När datan väl är inmatad i det elektroniska formuläret har man stora möjligheter till att behandla och distribuera den (Kühn Pedersen, 1990).

Trots att EDI ger dessa uppenbara fördelar har det inte fullt slagit igenom, bortsett från vissa branscher t ex fordonsindustri. Fredholm (1998) anger som anledning till detta att EDI har varit komplext och dyrt att sätta i drift. Genombrottet har skett först i mitten av 1990-talet och beror till stor del på att standarden mognat och fått acceptans, samt att möjligheterna att använda EDI har byggts in i allt fler affärssystem på marknaden (Fredholm, 1998).

Som tidigare sagts kommer EDI inte att behandlas närmare, utan arbetet inriktas på den handel som sker företag – privatperson.

2.4 Betalningsmedel vid webhandel

Det finns många olika sätt att betala sina inköp från webbutikerna. Uppsatsen kommer att koncentreras på de alternativ där köparen betalar direkt vid sin dator och kommer alltså att utelämnas sådant som postförskott, checkar och fakturor/inbetalningskort. Allt eftersom ämnet har undersökts inför detta examensarbete har fler och fler betalningsmöjligheter upptäckts, som dock samtliga antingen bygger på idén om digital valuta eller någon form av betalkort (konto/kreditkort eller smarta kort).

De betalningssätt som jag kommer att undersöka blir

- Betalkort
- Medlemskap i shoppingtorg
- Digital valuta

Den första punkten innefattar också en ny betalningsstandard som håller på att införas i Sverige. Denna standard kallas SET vilket står för Secure Electronic Transaction. Lind (1999) berättar att denna nya teknik alltså bygger på kontokortsbetalning, men nyheten är att SET använder sig av digitala certifikat, d v s "virtuella kontokort". Det innebär att kortet finns lagrat på datorns hårddisk.

2.4.1 Betalkort

Med betalkort avses kreditkort, kontokort eller bankkort som exempelvis är anslutet till Visa, Mastercard eller annan likvärdig tjänst. Detta är det absolut vanligaste betalningssättet i den internationella Internetvärlden (Westholm, 1998).

Westholm (1998) beskriver betalningsproceduren på följande sätt. Köparen lämnar sitt kortnummer till webbutiken via ett formulär på butikens hemsida. Där har en säker förbindelse upprättats mellan köparens dator och företagets server. Till detta används vanligen SSL (Secure Sockets Layer), vilket är en krypteringsteknik som finns i de flesta webbservrar. Företaget måste också ha en säker förbindelse till en bank som skall ta ställning till om köpet skall godkännas eller inte. De svenska bankerna har hittills inte accepterat detta system, men det är ändå möjligt för svenska företag att utnyttja möjligheten, då med hjälp av utländska banker.

Vidare skriver Westholm (1998) att nu är dock SET på intågande, vilket kan bli startskottet för kontokortsbetalningar på den svenska delen av WWW. Detta är en ny teknik som lanseras av Visa, Mastercard, IBM, Netscape och Microsoft. SET är en öppen standard, vilket innebär att det är tillåtet för alla att använda den. SET använder sig av en krypteringsmetod som kallas RSA. Denna metod bygger på publika och privata nycklar. Den publika är tillgänglig för alla och gör att avsändarens identitet kan säkerställas eftersom det bara är denne som kan framställa "signaturen" med sin privata nyckel (Nilsson, 1996). Hur detta går till kommer att beskrivas utförligare i kapitel 5.4.1.

2 Bakgrund

När betalning sker med hjälp av SET så får aldrig affärsinnehavaren tillgång till kundens kreditkortsnummer, detta sänds krypterat till köparens bank. Sedan görs själva transaktionen upp mellan kundens och affärsinnehavarens banker. Ingen av dessa banker kan se vad som har köpts, det är endast kunden och affärsinnehavaren som har den informationen (Segerlund, 1998).

En annan variant av betalkort är s k *smarta kort* (smart cards). De ser ut ungefär som vanliga betalkort, men de lagrar information på ett chip (mikroprocessor) istället för på en magnetremsa som de konventionella korten gör. I jämförelse med de konventionella korten skiljer de sig på flera viktiga punkter (Garfinkel & Spafford, 1997).

- Smarta kort kan lagra betydligt mer information än de som har magnetremsa. Tack vare denna kapacitet kan smarta kort ha flera användningsområden.
- Smarta kort kan skyddas av lösenord.
- Smarta kort kan användas för att skapa *krypteringsnycklar*. Kortet kan då designas så att den publika nyckeln kan avläsas, medan den privata inte avslöjas. För att kunna läsa ett krypterat meddelande måste kortet befinna sig i användarens ägo. Detta garanterar att användarens privata nyckel inte har kopierats.

Ett exempel på ett smart kort är de telefonkort som numera används i så gott som alla telefonautomater.

2.4.2 Medlemskap i shoppingtorg

Ett medlemskap i ett shoppingtorg fungerar enligt Schmitz (1998) på så sätt att medlemmen blir tilldelad ett konto och ger shoppingtorget fullmakt att debitera detta konto. Därefter är det fritt fram att handla i de butiker som är anslutna till shoppingsystemet och betala via postgiro eller betalkort. Detta förfarande gör att alltså att konsumenten kan ta sig runt de bestämmelser som de svenska bankerna har mot att betala med kontokort. Även personer som inte är medlemmar i shoppingtorget, kan naturligtvis handla där. Betalningen sker då i stället via postgiro eller postförskott.

Forsebäck (1998) berättar i sin rapport att de shoppingtorg i Sverige som har blivit mest kända är Postens Torget och Telias Passagen, vilka båda är riktade till privatpersoner. Torget startade sin verksamhet i maj 1996 och blev snabbt en succé. Redan under hösten samma år hade Torget dagligen 50 000 besök. Utvecklingen har fortsatt i samma takt. I mars 1998 hade Torget 300 000 besök per dygn. Medlemskapet är gratis och ger varje kund ett eget användar-ID, som sedan kan användas vid all handel av varor och tjänster på Torget. Kunderna behöver alltså inte uppge numret på kontokortet när de skall betala. Medlemmarna erbjuds också egen e-postadress, hemsida och olika rabatter.

Fredholm (1998) beskriver en ny framtid för idén om shoppingtorg, nämligen att det nu börjar dyka upp marknadstorg som riktar sig både till företag och privatpersoner. De innehåller alltså både EDI och webhandel. En fördel som många företag anser att

2 Bakgrund

de får genom en gemensam marknadsplats är att en specialiserad part står för säkerheten, vilket medför mindre risk för intrång i de egna systemen (Fredholm, 1998).

2.4.3 Digital valuta

Digital valuta kan enligt Garfinkel & Spafford (1997) definieras som en elektronisk ersättning för kontanter. Det går att spara och överföra, men är omöjligt att förfälska. Det garanterar även köparens anonymitet, eftersom det inte går att spåra. En annan fördel gentemot kreditkort är att alla kan skaffa sig den digitala valutan, utan någon form av kreditprövning. Därmed ger den elektroniska butiken fler människor möjligheten att handla hos dem.

Fram till helt nyligen har två av de mest kända varianterna av digital valuta varit Ecash från holländska DigiCash och Cybercoin från amerikanska CyberCash. Nyhetstjänsten Paywatch (1998) skriver dock att nu har DigiCash gett upp i sina försök att få allmänheten att anamma det nya betalningssystemet. Då det förväntade genombrottet för den digitala valutan har låtit vänta på sig, håller nu DigiCash på att rekonstruera bolaget och förväntas arbeta vidare med den teknik som utvecklats, men inom andra områden än betalning.

Hur CyberCash fungerar beskriver Lynch & Lundquist (1996) på följande sätt. Köparen kan dels få kredit, dels handla kontant genom att pengarna dras från ett i förväg öppnat konto. Vid ett köp på kredit skickas en elektronisk faktura från butiken till kunden, som fyller i sitt kreditkortsnummer. CyberCash-programmet krypterar sedan numret och skickar tillbaka fakturan till butiken. Där verifieras den genom ytterligare ett nummer, krypteras och skickas sedan till banken. Väl framme på banken hanteras det hela precis som en vanlig kredittransaktion. Detta gör att butiken aldrig får reda på kundens kreditkortsnummer.

När det gäller kontant betalning så samverkar CyberCash enligt Lynch & Lundquist (1996) med banken på så sätt att det skapas s k pekare till de kontanter som finns på kundens bankkonto. Kunden avsätter alltså en viss summa till sitt CyberCashkonto i form av en deposition. CyberCash-kontot i sig innehåller alltså inga pengar, utan ”pekar” på pengar som finns på ett bankkonto. När en betalning skall verkställas från CyberCash-kontot flyttas ”pekaren” och pengarna som finns på bankkontot överförs till butikens bank.

2.5 Risker vid elektronisk handel

Men hur farligt är det egentligen att lämna ut sitt kontokortsnummer på Internet? Vad kan hända om det hamnar i orätta händer? Sjögren (1998) (som är reporter på datortidningen Computer Sweden) hävdar i en artikel att konsumenten i verkligheten inte riskerar någonting, även om kortnumret skulle missbrukas. Där framgår det nämligen att det vid all handel där kortet inte har presenterats fysiskt alltid är butiken som får stå för kostnaderna om kortinnehavaren bestrider köpet. Bankernas regler säger klart och tydligt att om någon har beställt varor med ett kreditkort och

2 Bakgrund

innehavaren av kortet sedan bestrider köpet, så kommer banken inte att betala ut några pengar till butiken. De kräver nämligen att kortet har visats upp tillsammans med legitimation och att kunden har signerat köpet för att garantera att butiken får sin betalning.

Sjögren (1998) fortsätter sitt resonemang med att konstatera att de som tar risken är butikerna och inte kunderna. Butikerna har alltså stort intresse av att det lanseras en ny lösning som gör att det går att komma förbi problemet med att identifiera vem det är som använder betalkortet. En sådan lösning är SET, som nämnts tidigare i arbetet. SET-tekniken löser problemen med identifikation med hjälp av digitala signaturer och stark kryptering.

Dock medför denna teknik även en del nya problem. Sjögren (1998) visar att det av många anses som krångligt och dyrt, vilket helt naturligt skrämmer bort småföretagen. Många ifrågasätter nu om SET är värt de stora summor som det kostar att införa. Dessutom har lanseringen av SET tagit avsevärt längre tid än planerat. Många webbutiker börjar nu tala om att tiden håller på att rinna ut för SET-projektet, då betydligt färre kunder än väntat har börjat använda SET.

3 Problembeskrivning

Mycket av den kritik som idag riktas mot den elektroniska handeln berör säkerheten vid transaktionerna. Det skriver bl a Pappinen (1999) och Wallström (1998) om. Då denna typ av handel är på väg att ta en betydande del av den totala handeln (Wallström, 1998) är det av stor vikt att kartlägga de risker som finns, samt att försöka reda ut vilket betalningssätt som är det säkraste.

De fördelar som finns med att handla elektroniskt kontra i en vanlig butik är många. Exempel på detta är som jag själv noterat att det ofta är billigare i webbutiken, kunden slipper gå ut när det är dåligt väder och kan dessutom i lugn och ro titta igenom butikens sortiment utan att bli störd av expediten. Ändå har det elektroniska alternativet inte riktigt slagit igenom, enligt Ottosson (1999). Många provar det någon gång utan att göra det till en vana. Andra provar inte över huvud taget, av olika anledningar. En vanlig anledning är att många människor inte tror att det är tillförlitligt att lämna ut sitt kontokortsnummer på Internet, berättar Sjögren (1998). Hon säger vidare att det dock aldrig är kunden själv som råkar illa ut om kortnumret skulle komma på avvägar, det är webbutiken som får stå för notan.

Ju längre det dröjer innan den elektroniska handeln får sitt genombrott, desto större summor går butikerna miste om. Det är alltså av stort intresse för webbutikerna att det tas fram en lösning som kan accepteras av både butik och kunder.

3.1 Problemställning

De problemställningar som kommer att undersökas i detta arbete är:

- Vilka krav på säkerhet finns från de olika aktörerna på marknaden, d v s banker, butiker och kunder?
- Vilket av de befintliga betalningssätten uppfyller dessa krav i störst utsträckning?

Genom att reda ut dessa frågor kommer förhoppningsvis även andra frågor att besvaras, exempelvis vad som krävs för att den elektroniska handeln skall få det genombrott på bred front som webhandlarna väntat så länge på. Det bör också framgå vilka förväntningar som finns från handlarnas sida och hur de föreställer sig att framtiden kommer att utveckla sig.

3.2 Avgränsning

Avsikten med detta arbete har varit att analysera säkerheten i de olika betalningssätt som står de svenska konsumenterna till buds för närvarande. Det kommer att göras genom att visa hur handelstransaktionerna går till vid de olika betalningssätten.

3 Problembeskrivning

De betalningssätt som kommer att analyseras är betalkort, digital valuta samt medlemskap i shoppingtorg. Detta för att det inte är relevant i detta sammanhang att analysera sådana betalningssätt som postgiro och postförskott. Vidare har jag valt att koncentrera arbetet mot den handel som berör företag – privatperson. Anledningen till detta är att arbetet annars skulle bli alltför omfattande.

De lagstiftningar som reglerar handeln i allmänhet ligger också utanför detta arbetes område.

3.3 Förväntat resultat

När det gäller analysen av betalningssätt förväntar jag mig att finna att den standard som de svenska bankerna och handlarna håller på att införa (SET) är den som är säkrast. Dessvärre verkar det finnas en del problem som återstår att lösa innan SET blir allmänt accepterat.

Vidare väntar jag mig att finna att det som krävs för att det skall bli ett genombrott för den elektroniska handeln är en bättre marknadsföring av SET, liknande den som gjorts när Cashkorten nyligen infördes på den svenska marknaden.

Jag har en misstanke om att en stor del av problematiken ligger i människors skepsis mot den nya tekniken. De anser helt enkelt inte att det är tillräckligt säkert att lämna ut sitt kontokortsnummer på Internet. Så länge det inte finns en standardteknik som samtliga aktörer på marknaden är nöjda med kommer genombrottet för elektronisk handel troligtvis att dröja.

4 Metod

Dahmström (1991) berättar att vid undersökning av ett problem finns det ett antal olika tillvägagångssätt att använda sig av, både vad gäller insamlandet av data och hur den sedan bearbetas. Vilken undersökningsmetod som väljs beror till stor del på hur mycket information som finns om problemområdet från början, men också vilket syftet är med undersökningen samt vilka resurser som står till förfogande, exempelvis i form av tid, pengar och personal. Därför bör undersökaren fundera igenom vad han önskar med sin undersökning, vilket syftet är, samt vilken information som finns att använda från början och vad han själv måste ta reda på. Därefter kan han börja samla in den information som finns och förbereda hur han ska skaffa annan önskad information.

4.1 Möjliga metoder

De metoder som finns för att samla in data är enligt Dahmström (1991) enkäter, intervjuer, samt direkt observation. Patel & Davidsson (1994) beskriver dessutom en metod för att använda sig av befintlig data - litteraturstudier. Dahmström (1991) skriver vidare att då det eftersökta materialet inte finns sedan tidigare, väljs vanligtvis att göra en undersökning med hjälp av enkäter, intervjuer eller direkt observation. Materialet samlas alltså in för första gången, d v s det görs en *primärdataundersökning*. Om alternativet att använda sig av befintlig data väljs, kan materialet antingen användas direkt eller efter ytterligare bearbetning; då görs en *sekundärdataundersökning*.

Dahmström (1991) påpekar att det är vanligt att använda sig av en kombination av olika metoder. Exempelvis kan det vid en postenkät bli nödvändigt att komplettera med en telefonintervju för att få svar från dem som inte skickat tillbaka frågeformuläret. En annan vanlig kombination är att utnyttja befintliga data tillsammans med nyinsamlat material.

4.1.1 Enkäter

Dahmström (1991) beskriver enkätundersökningen som att ett urval av personer eller företag får ett frågeformulär att fylla i och skicka tillbaka. Dessa formulär skickas vanligtvis med posten och kallas då *postenkät*. Fördelar med detta är bl a att det är en billig metod och att *respondenten* (den som besvarar frågorna) kan göra det när han har tid. Nackdelarna är att det finns risk för stort bortfall om respondenten inte anser sig ha tid över huvud taget att svara på frågorna och att det tar lång tid att få in svaren. Vis av egen erfarenhet tror jag det är nödvändigt att planera för att skicka ut ett flertal påminnelser för att få in ett acceptabelt antal svar, vilket gör att undersökningen tar ännu längre tid att genomföra.

Dahmström (1991) beskriver också alternativet att dela ut formulären direkt till de utvalda då alla i en bestämd grupp vid ett visst tillfälle skall utfrågas, t ex en skolklass. Då är det fråga om en *gruppenkät*. Detta alternativ ger den fördelen att många personer kan vara med i undersökningen samtidigt, vilket även gör att det är en billig

4 Metod

och snabb metod. Dock finns det risk för att respondenterna kan påverkas av sin gruppleddare och lämna svar som inte helt överensstämmer med deras egna åsikter. Dessutom kan inte alltid anonymiteten garanteras, vilket är viktigt vid ifyllandet av gruppenkäter.

En annan variant som Dahmström (1991) beskriver, är när besökande på en plats, t ex myndighet, sjukhus eller liknande, får en enkät att fylla i. Den kallas då *besöksenkät*. Det helt dominerande problemet här är risken för stort bortfall. Dessutom är det personalkrävande, då det behövs personal som hjälper till med att dela ut och samla in enkäter och pennor, svarar på frågor och annat.

Generellt är min personliga åsikt om enkäter att de inte ger så stora möjligheter att ställa detaljerade eller invecklade frågor, eftersom det finns risk att respondenten inte förstår frågan och därför inte besvarar den. Inte heller går det att ställa följdfrågor med utgångspunkt i svaret på en tidigare fråga, vilket gör att betydelsefull information kan gå till spillo.

4.1.2 Intervjuer

Dahmström (1991) beskriver även intervjuer som ett slumpvis urval av personer eller företag som skall besvara frågor. Om intervjuaren har gott om tid och vill ställa många och invecklade frågor kan han välja att göra en *besöksintervju*. Det går vanligen till så att intervjuaren efter överenskommelse söker upp respondenten t ex i hemmet eller på arbetsplatsen och sedan ställer frågor efter ett i förväg strukturerat frågeformulär. Det ger många fördelar, t ex om det uppstår oklarheter i frågorna kan det redas ut direkt, men det är i allmänhet dyrt och tar lång tid att genomföra.

Dahmström (1991) berättar att ett snabbare sätt att få kontakt med respondenterna är att göra en *telefonintervju*. I likhet med besöksintervjuerna har intervjuaren här möjlighet att reda ut oklarheter i frågorna direkt, men har inte möjlighet till alltför långa intervjuer med krångliga frågor. Dessutom är det risk för att svaren inte är speciellt väl genomtänkta, då miljön runt respondenten kan vara störande eller stressande.

4.1.3 Direkt observation

Detta beskriver Dahmström (1991) som en lämplig metod om undersökaren vill studera ett beteende eller vissa vanor samtidigt som han vill ha detaljerad information om dessa aktiviteter. De undersökta personerna skall här observeras av speciella "observatörer" som har till uppgift att registrera något beteende eller någon egenskap. Observationen kan antingen ske direkt (öppet) så att respondenten vet om att han är iakttagen, eller indirekt, så att han inte vet det. Det senare förekommer t ex i studier över mänskliga beteenden och grupprelationer.

Ett exempel på direkt observation kan vara att bestämma antalet besökande till ett museum eller till en myndighet.

4 Metod

Dahmström (1991) beskriver ett av problemen som kan uppstå i samband med direkt observation med hjälp av observatörer som att var och en av observatörerna bara hinner med ett visst antal observationer samtidigt. Om händelsen som skall observeras inte inträffar jämnt fördelat över tiden kan det få till följd att kvaliteten på materialet troligtvis blir olika vid olika tidpunkter.

4.1.4 Litteraturstudier

Patel & Davidsson (1994) anser att de vanligaste källorna att hämta kunskap ur är böcker, artiklar och rapporter, vilka vanligen hittas i biblioteken. Att basera sina studier på tidigare arbeten kallas att göra en litteraturstudie. I böcker kan undersökaren ofta finna olika teorier och modeller att basera sitt arbete på, och i artiklar finner han ofta de senaste rönen. De data som framkommer vid en sådan undersökning är sk sekundärdata. Det är enligt min åsikt en lämplig metod för att ge en bakgrund till det problemområde som undersökaren vill belysa.

Enligt Dahmström (1991) är en uppenbar fördel med att använda redan insamlade data att det blir billigare än att själv samla in all data. Dessutom är det möjligt att få tillgång till data från flera tidigare tidpunkter, vilket kan vara betydelsefullt exempelvis då det gäller att studera utvecklingen hos en viss företeelse under en längre tidsperiod, istället för att undersöka läget vid en viss tidpunkt.

De nackdelar som enligt Dahmström (1991) förekommer kan vara att syftet med den ursprungliga undersökningen var ett annat än det som undersökaren nu tänker använda det till. Det kan då ge en felaktig bild av den företeelse som undersöks. Dessutom finns en stor risk att undersökaren använder sig av inaktuella uppgifter i sin rapport, då utvecklingen går fort framåt inom många områden.

De källor som kan användas för att skaffa sig information kan exempelvis vara bibliotek, rapporter från myndigheter, tidningar och tidskrifter, samt olika föreningar. Ett annat alternativ är att söka på Internet efter den information som önskas. Jag tycker dock det är viktigt att undersökaren har i åtanke att om material från Internet skall användas kan han kanske inte alltid vara säker på tillförlitligheten, eftersom vem som helst kan publicera vad som helst på Internet. Därför är det i dessa fall extra viktigt att kontrollera vem som har skrivit texten eller givit ut artikeln. Vid tveksamhet kan det vara lämpligt att höra av sig till författaren eller organisationen som står bakom texten.

4.2 Metoder för bearbetning av data

När undersökaren har all den data han önskar är det dags att bearbeta och strukturera materialet. Patel & Davidsson(1994) berättar att det finns två olika inriktningar för hur undersökaren väljer att bearbeta den insamlade materialet, nämligen kvantitativ bearbetning och kvalitativ bearbetning. Ofta framställs dessa båda inriktningar som om de vore helt oförenliga, vilket Patel & Davidsson (1994) dock tillbakavisar. De menar

att huvuddelen av den forskning som bedrivs inom samhälls- och beteendevetenskapen idag befinner sig någonstans mellan dessa båda ytterligheter.

4.2.1 Kvantitativ bearbetning

Patel & Davidsson (1994) definierar kvantitativt inriktad forskning som sådan forskning som använder sig av statistiska bearbetnings- och analysmetoder. Något förenklat kan det uttryckas med att om undersökaren i första hand är intresserad av frågor som rör ”Var? Hur? Vilka är skillnaderna? Vilka är relationerna?” så bör statistiska bearbetnings- och analysmetoder användas. Dessa metoder används för att i siffror ge en beskrivning av det insamlade materialet, och på det sättet belysa forskningsproblemet, men kan också användas för att testa statistiska hypoteser. När denna metod används är det vanligt att undersökaren väntar med alla analyser av materialet tills all data är inhämtad.

4.2.2 Kvalitativ bearbetning

Patel & Davidsson (1994) beskriver syftet med denna typ av analysmetod som att skaffa en annan och djupare kunskap än den fragmentariska kunskap som ofta erhålls när kvantitativa metoder används. Ambitionen är här istället att analysera och försöka få förståelse för helheter, vilket ger en annan syn på problemet. Detta gör också att arbetet till stor del kan komma att präglas av den som genomfört undersökningen.

Enligt Patel & Davidsson (1994) är en annan aspekt som skiljer denna metod från den kvantitativa att undersökaren här gärna genomför kontinuerliga analyser genom hela arbetet, vilket är mycket praktiskt eftersom det annars är lätt att glömma bort någon viktig tanke som dykt upp under arbetets gång. Ytterligare en fördel med denna metod är att de löpande analyserna kan ge uppslag till nya idéer om hur det fortsatta arbetet skall bedrivas.

4.3 Val av metod

Enligt Dahmström (1991) är det ideala att välja den metod som, givet de befintliga resurserna, kan ge data av så hög kvalitet som möjligt. Det kan dock vara svårt att avgöra, så det finns några tumregler att ta till. Ofta väljs en huvudinsamlingsmetod som sedan kan kombineras med andra alternativ för att täcka bortfallet. Exempelvis kan telefonintervjuer vara ett bra komplement till postenkäter som inte blivit besvarade. Generellt gäller enligt Dahmström (1991) att besöksintervjuer är den mest resurskrävande metoden för att samla information. Därför är den metoden inget alternativ för ett arbete där en mycket begränsad tid som står till buds, utan där kan det i stället vara lämpligt med en telefonintervju.

4.3.1 Val av metod för datainsamling

I valet mellan att använda sig av primär- eller sekundärdata får tidsramarna styra till stor del. Därför är valet att huvudsakligen använda sekundärdata inte svårt. Sekundärdatan har jag redan använt i stor utsträckning, för att erhålla en bred överblick över området Internet och elektronisk handel. I synnerhet i början av arbetet försökte jag samla på mig så mycket information som möjligt från många olika källor, eftersom det var viktigt att utforska området och belysa det från många olika håll. Dessa sekundärdata har sedan legat till grund för den fortsatta undersökningen.

Eftersom både Internet och elektronisk handel är aktuella och populära ämnen har det inte varit några som helst problem att få tag på material. Problemet är snarare det motsatta: Att sälla i den uppsjö av information som finns, för att erhålla den typ av material som är lämpligt för detta arbete. De informationskällor som jag kommer att använda mig av är Högskolebiblioteket, där jag funnit både böcker i ämnet och tidigare examensarbeten inom samma ämne. Jag kommer också att använda mig av rapporter som jag har beställt från organisationen Teldok, samt artiklar i olika tidningar såsom Computer Sweden och Internetguiden. Jag har också haft stor nytta av Internet, där jag funnit många artiklar och rapporter inom mitt problemområde.

Även ett arbete som huvudsakligen bygger på litteraturstudier behöver dock ett visst inslag av egen insamlad information – primärdata. Det som förefaller mest lämpligt med tanke på den begränsade tiden är telefonintervjuer. En telefonintervju ger stora möjligheter att ställa detaljerade och invecklade frågor, eftersom det går att förtydliga sig direkt om det skulle behövas. Dessutom kan intervjuaren ställa följdfrågor, vilket är viktigt när det gäller att få fram motiveringar till varför/varför inte respondenten tycker på ett visst sätt. Den primärdata jag behöver är information om vad olika banker, webbutiker och privatpersoner har för krav på säkerheten vid elektroniska betalningar, samt vad de anser om de olika formerna av digitala betalningssätt. Detta för att få svar på min problemställning om vilket betalningsätt som skall anses som det säkraste för alla inblandade parter.

4.3.2 Val av metod för bearbetning av data

När det gäller metoder för bearbetning av erhållen data kommer jag att använda mig av den kvalitativa inriktningen, vilket förefaller vara det lämpligaste alternativet. Anledningen till detta är att jag anser att det inte finns resurser för att göra en statistisk undersökning med ett stort antal intervjuade personer. Jag väljer då istället att intervjua ett fåtal sakkunniga personer på banker och webbutiker, för att sedan kunna analysera det material jag erhållit.

Även det material som jag samlat in via andra källor – sekundärdatan – lämpar sig bättre att analysera på ett kvalitativt sätt än kvantitativt, eftersom det till stor del är vanlig text det handlar om och inte så mycket statistiska uppgifter.

4.3.3 Metoder som ej valts

En metod som jag inte anser som lämplig för min undersökning är metoden för direkt observation. I mitt tycke lämpar den sig bättre för statistiska undersökningar, där undersökaren vill ha fram ett stort antal observationer av någon företeelse att grunda sina värderingar och antaganden på.

Inte heller anser jag att den kvantitativa metoden för databearbetning är lämplig för mitt arbete, då den verkar bättre lämpad för att analysera sifferuppgifter. Enligt min uppfattning skulle den kunna vara lämplig att använda tillsammans med metoden för direkt observation.

4.4 Plan över arbetet

Det fortsatta arbetet kommer att bedrivas på så sätt att jag kommer att genomföra ett fåtal intervjuer med banker, webbutiker och kunder i syfte att reda ut respektive aktörs krav och önskemål om säkerheten i elektroniska betalningar. Detta kommer vid behov att kompletteras med ytterligare litteraturstudier för att förtydliga respondenternas svar och förklara vissa tekniska begrepp för läsaren. Allt detta kommer att presenteras i kapitel 5.

Parallellt med detta arbete kommer arbetet att analyseras kontinuerligt, vilket är en av grundstenarna i den kvalitativa inriktningen på databearbetning. För att få en bättre överblick över arbetet och inte riskera att sammanblanda analysen med presentationen av materialet kommer dock analysen att presenteras separat i kapitel 6.

5 Genomförande

I de digitala betalningssätt som existerar idag finns vissa riskmoment inblandade. Det jag vill utreda med mitt arbete är vilka dessa risker är, var de finns, hur man kan skydda sig mot dem och vilket betalningssätt som har lyckats bäst med att eliminera dessa risker.

I det första skedet skall jag reda ut vilka riskerna är i respektive betalningsmedel, dels genom litteraturstudier, och dels genom intervjuer med sakkunniga inom området. Detta kommer sedan att ligga till grund för den fortsatta undersökningen av de säkerhetskrav som ställs på digitala betalningsmedel. Är riskerna godtagbara utifrån de krav som finns eller är säkerhetskraven så höga att inga betalningsmedel egentligen kan accepteras? Dessa frågeställningar skall slutligen leda mig fram till om det går att urskilja något digitalt betalningsmedel som bättre än övriga kan uppfylla de ställda kraven.

I detta kapitel kommer jag att presentera materialet som jag fått fram genom intervjuer och litteraturstudier. Analysen av materialet kommer att grundas på vad jag får fram i detta kapitel och den kommer att presenteras i kapitel 6.

5.1 Problem med digitala betalningsmedel

Internet är ett öppet nätverk vilket innebär att vem som helst har tillgång till det. Då det inte finns någon kontrollfunktion som förhindrar olagligheter, är det fullt möjligt för en skicklig person att avlyssna en förbindelse och eventuellt snappa upp ett kreditkortsnummer, eller t o m ändra på den data som överförs. Den person som har för avsikt att handla i en webbutik vill också vara säker på att det verkligen är den avsedda butiken han gör affärer med, och inte en skojare. Dessutom vill nog många kunder inte att deras köpvanor kommer till allmän kännedom. Dessa problem är enligt många källor, t ex Lind (1999), de allvarligaste.

De huvudsakliga problemen vid webhandel är enligt exempelvis Lind (1999) alltså dessa tre:

- Dataintegritet
- Identifikation
- Förtroende

Dataintegritet innebär enligt Westholm (1998) att kunna lita på att ingen kan komma åt eller ändra på den data som sänds från en part till en annan. Lind (1999) tar också upp problemet, men kallar det för avlyssningsrisk, vilket bättre beskriver vad det handlar om. Möjligheten finns ju, även om den är liten, att någon avlyssnar överföringen och kommer åt ett kontokortsnummer, som sedan kan användas olagligt. Problem med avlyssning kan drabba såväl butiker och kunder, som banker.

Westholm (1998) anser vidare att det i en affärssituation på Internet är viktigt att säljare och köpare är säkra på att de kan *identifiera* varandra. För köparen är det

5 Genomförande

viktigt att veta att han betalar till den riktige säljaren och inte till en bedragare. På samma sätt vill säljaren vara säker på vem han har att göra med, eftersom köparen efter att ha genomfört köpet kan hävda att han varken har beställt eller tagit emot vara eller tjänst. Detta är alltså ett problem främst för butikerna och kunderna, medan bankerna inte drabbas om tvistemål skulle uppstå.

Avslutningsvis tar Westholm (1998) upp problemet med *förtroende*. Kunder vill inte gärna att de data som överförs vid ett köp skall hamna i orätta händer. Detta gäller såväl kontoinformation som information om köpbeteende (t ex vilka varor en person brukar handla). Kunderna vill kunna känna förtroende för att ingen utomstående person eller organisation tar del av deras köpvanor. Icke krypterade Internetförbindelser är mycket osäkra och det är fullt möjligt för en oärlig och kunnig person att avlyssna kommunikationerna. Detta problem är egentligen av samma typ som problemet med avlyssning (dataintegritet), men här speglas också en annan sida, nämligen den att ingen utomstående skall kunna ta del av andras köpvanor, för att sedan kunna utnyttja det i sina egna syften.

Om dessa tre olika problemområden sammanställs framträder bilden av att det är butikerna och kunderna som tar de flesta riskerna, medan bankerna endast drabbas om det blir problem med avlyssning av kommunikationerna. Ändå är det främst bankerna som driver på utvecklingen av nya och säkrare betalningssystem, såsom SET-systemet. Butikerna är ju annars den grupp som borde vara mest utsatt, då det är de som tar de största riskerna. Om butikerna ändå tycker att säkerheten är tillräcklig, varför finns det då ett behov av att införa SET-systemet? Det kanske finns anledning av ifrågasätta bankernas avsikter med SET, då det är relativt dyrt för en butik att införa systemet. Sjögren (1998) berättar att butikerna får investera mellan 200 000 - 250 000 kr för att kunna erbjuda sina kunder SET-betalningar.

5.2 Aktörernas krav

För att klargöra om de problem som redovisats i avsnittet ovan sammanfaller med aktörernas krav på säkerhet har jag intervjuat en webbutik och en kund. Någon sakkunnig person från bankvärlden hade tyvärr inte tillfälle att delta i undersökningen, men jag anser att bankernas krav ändå kan fastställas utifrån de artiklar och rapporter jag har tillgång till.

Jag har valt att intervjua en medarbetare på en webbutik som säljer CD-skivor. Han uppger att den betalningsform som är vanligast bland butikens svenska kunder fortfarande är att betala mot faktura, men att kontokortsanvändningen håller på att öka. I andra länder, t ex England och Frankrike används kontokort betydligt oftare av kunderna. Butikens kontokortslösning går via ett franskt företag som heter Kleline. Säkerheten vid Klelinebetalningar bygger på två principer:

- Den första principen bygger på förutsättningen att all överföring av konfidentiell information måste vara helt säker. Vid betalning on-line passerar kontokortnummer aldrig över Internet, utan detta sker endast en gång: När kunden första gången ansluter till Kleline. Endast Kleline känner till kort- och kontouppgifter om köpare

5 Genomförande

respektive säljare. Den överförda informationen är i båda riktningarna skyddad genom mycket hård kryptering - RSA-kryptering (tas upp i kapitel 5.4)

- Den andra principen är att de inblandade aktörerna måste identifieras och verifieras. Både butik och kund finns registrerade hos Kleline, vilket försäkras köparen om att butiken verkligen existerar, samtidigt som butiken garanteras att medel för betalning finns.

Respondenten uppger att då alla transaktioner sker via säkra servrar och inga kortuppgifter lagras, är den säkerhet som Kleline erbjuder fullt tillräcklig för webbutiken. Detta tolkar jag som att företaget anser att kraven på dataintegritet och identifikation är de viktigaste. Dock upptäcker jag vid en närmare granskning av Klelinesystemet att det även uppfyller behovet av förtroende från kunden genom att butiken aldrig får någon kontoinformation om kunden.

På min fråga om vilket betalningsmedel de ansåg vara säkrast blev svaret att för kunden är det säkraste att använda sig av faktura, eftersom de då kan handla på kredit. Dock säger respondenten senare att om man skall se det ur rent säkerhetsmässigt perspektiv så är det absolut säkraste alternativet SET. Fakturabetalning skulle vara mest fördelaktigt då kunden får kredit, men han lägger inga säkerhetsmässiga aspekter i det. Ur butikens perspektiv ansåg respondenten att kontokortbetalning var att föredra, eftersom butiken då är garanterad betalning. Även här anser han SET som det överlägset säkraste alternativet.

Jag tog även tillfället i akt att ställa några frågor till respondenten som kund istället för som representant för en webbutik. På frågan om vilket betalningsalternativ han själv föredrar att använda sig av när han handlar på Internet blev svaret kontokort. Han anser det som mycket smidigare än faktura, eftersom en faktura lätt kan glömmas bort och det då tillkommer påminnelseavgifter. Vidare anser han riskerna med webhandel som rejält överdrivna, och att man väldigt sällan hör talas om reella incidenter med kontokortsbedrägerier. Han tror att det till stor del har handlat om en mediafluga, men att den allmänna uppfattningen om att det är väldigt farligt att handla med kontokort på Internet, kommer att förändras avsevärt i framtiden.

5.3 Sammanställning av risker och krav

De säkerhetskrav som ställs från butikerna sammanfaller enligt de intervjuer jag gjort med de risker som beskrivits i avsnitt 5.1; alltså ett betalningssystem skall vara säkert för identifikation och avlyssning. Det skall helst också uppfylla kundernas önskemål om att deras köpvanor inte skall hamna utanför den webbutik där de handlar, men det anses inte vara så fullt så viktigt som de övriga kraven.

5.4 Säkerheten hos de olika betalningssätten

Utifrån de tre krav som jag nu har lyckats urskilja skall jag härnäst gå djupare in på de olika betalningsmedel som skall studeras, nämligen betalkorten (där också SET inkluderas), shoppingtorgen och den digitala valutan. Avsikten är nu att utröna hur de digitala betalningssätten försöker uppfylla säkerhetskraven.

5.4.1 Betalkort

Kontokort/kreditkort

Vid betalning med ett vanligt kontokort eller kreditkort uppfylls kravet på dataintegritet, då SSL-protokollet förser parterna med en tillförlitlig förbindelse (Westholm, 1999). Som tidigare nämnts om SSL så betyder det Secure Sockets Layer och det är en krypteringsmetod som används bl a för att skydda viktig information som skickas via Internet. På så sätt förhindras att obehöriga läser kreditkortsinformation eller läser dokument. Lövgren (1998) berättar att denna teknik används både för att förhindra avlyssning och för att säkerställa identifiering. Vid kryptering används en nyckel och en mer eller mindre komplicerad algoritm som förvränger data.

Därmed anser Lövgren (1998) att kraven på dataintegritet och identifikation bör anses vara uppfyllda av vanliga kontokortbetalningar. Förtroendeproblemet är inte helt uppfyllt, men krypteringen är ett försök att lösa det. En krypterad förbindelse kan inte avlyssnas utan svårigheter och därmed borde människor bli mindre rädda för att lämna ut sitt kontokortnummer.

Smarta kort

Innehavaren laddar ned pengar till kortet, som sedan kan användas tillsammans med en speciell kortläsare för att betala inköpen som gjorts på Internet. Wallgren (1998) anger att kortet innehåller en elektronisk signatur som skall lösa ett av de grundläggande problemen, nämligen att kunna säkerställa identifieringen och bevisa att jag är jag. Dessa kort är krypterade med den sk RSA-algoritmen, som har fått sitt namn efter sina upptäckares initialer (Rivest, Shamir, Adelman). Lövgren (1998) berättar att det inom krypteringsvärlden i allmänhet talas om tre olika typer av nycklar:

- Hemlig nyckel, där bara sändaren och mottagaren känner till nyckeln
- Privat nyckel, där endast nyckelns ägare känner till den
- Publik nyckel, där alla som vill kan komma åt nyckeln

Lövgren (1998) återger vidare att med sk *symmetriska krypteringsalgoritmer* används samma nyckel för kryptering och *dekryptering* (att återställa datan till sin ursprungliga form). Nyckeln måste då alltså vara hemlig och känd endast av de personer som skall ha tillgång till meddelandet. Den vanligaste symmetriska algoritmen heter DES (Data Encryption Standard). Den utvecklades på 1970-talet och anses idag vara för svag.

5 Genomförande

Lövgren (1998) uppger att för cirka 20 år sedan utvecklades de första *assymmetriska algoritmerna*. De kräver två nycklar: en publik nyckel som används för kryptering och en privat nyckel som används för dekryptering. Den assymmetriska algoritmen som är vanligast förekommande är just RSA-algoritmen. Ett exempel på hur det kan fungera :

Person A vill skicka ett krypterat meddelande till person B. Då måste A kryptera meddelandet med B:s publika nyckel (som ju alla har tillgång till). Meddelandet är nu krypterat och kan inte läsas av någon annan än B. För att B skall kunna dekryptera meddelandet måste han använda sin privata nyckel.

Dock skriver nyhetstjänsten Paywatch (1998) att de smarta korten inte längre är säkra. Där berättas att en grupp forskare i San Fransisco har presenterat en metod för att läsa informationen från smarta kort. Metoden sägs bygga på mätningar av den elektriska aktiviteten i kortet, vilka sedan analyseras med statistiska metoder för att finna exempelvis koder och privata krypteringsnycklar. Proceduren sägs ta några timmar att genomföra och en av forskarna - Paul Kocher, vd för Chryptography Research - hävdar att de ännu inte hittat något kort som de inte lyckats knäcka. Tillförlitligheten i detta uttalande kanske kan ifrågasättas då företaget Chryptography Research tillverkar mjukvara, som exempelvis motmedel mot denna typ av intrång på smarta kort, vilket gör att deras uttalande kanske inte skall tas på fullaste allvar.

En ny typ av smart kort som är anslutet till SET är under uppbyggnad, berättar Hultgren (1999). Han berättar att inom fyra-fem år räknar industrin med att de flesta persondatorer kommer att vara utrustade med smartkortsläsare, vilket då kommer att öka användningen av den typen av betalning.

SET

Som tidigare berättats använder sig SET av krypteringsmetoden RSA, som bygger på användningen av två olika krypteringsnycklar, den publika och den privata. Innan köpare och säljare kan börja använda sig av SET måste vissa förberedelser göras. Hultgren (1999) beskriver förloppet på följande sätt.

- Kunden måste ansöka hos sin bank om att få ett kortcertifikat, och via bankens websida hämta en elektronisk plånbok, som är ett tillägsprogram till kundens webläsare. Plånbokens syfte är att skydda kortcertifikatet.
- Webbutiken får ett motsvarande certifikat av sin bank, och de behöver också ett tillägsprogram till sitt system.

När detta är klart är det möjligt att handla. Förloppet ser då ut så här:

- Kunden besöker webbutiken och fyller sin shoppingkorg med varor. När han är klar väljer han alternativet "Köp med kontokort".
- Webbutiken skickar sitt certifikat till kunden. Det dekrypteras och kontrolleras av kundens elektroniska plånbok för att fastställa att butiken är en legitim butik.
- Den elektroniska plånboken skickar sedan över kundens certifikat till butiken så att den kan kontrollera att kunden är den som han påstår sig vara. Butiken kan dock

5 Genomförande

inte se alla uppgifter som kunden skickar, eftersom det finns två delar i betalningsordern: en krypterad och en okrypterad. I den okrypterade finns uppgifter om namn, adress osv, medan det i den krypterade finns kortinformation. Det sistnämnda kan butiken alltså inte se.

- Webbutiken skickar därefter vidare betalningsordern till sin bank. Där översätts betalningsordern till en vanlig kontokortstransaktion, som slussas in i det befintliga kontokortssystemet. Nu uppträder transaktionen precis som om kunden köpt en vara i en verklig butik.
- Transaktionen skickas sedan till kundens bank som kontrollerar att det finns pengar på kontot. Ett svar skickas tillbaka till webbutiken, som nu kan leverera varorna.
- När varan är levererad skickas en ny transaktion då den verkliga betalningen sker. I förra steget reserverades endast pengarna på kundens konto. Själva betalningen sker alltid först då varan har levererats.

5.4.2 Medlemskap i shoppingtorg

Genom att bli medlem i shoppingtorg kommer kunden undan de risker som finns i samband med vanliga kontokortsbetalningar. Schmitz (1998) berättar att kunden då i förväg har undertecknat en fullmakt och skickat in till torget via den ”vanliga” posten. Denna fullmakt ger torget rättighet att debitera kontot, och eftersom numret aldrig vid något tillfälle lämnas ut på Internet är det därefter riskfritt att använda kortet. Kunden behöver vid köp bara uppge ett lösenord och sedan är betalningen klar. Fullmakten anses ersätta den underskrift som det svenska regelverket kräver.

5.4.3 Digital valuta

Denna form av betalning brukar även kallas mikrodebiteringar, då dess främsta styrka är dess lämplighet att användas vid mindre betalningar (Pappinen, 1999). Detta beroende på att det blir tämligen oekonomiskt att betala små inköp via kontokort. Eftersom det företag som jag intervjuade använde sig av Klebox från franska Kleline, så har jag valt att studera denna digitala valuta närmare. Det finns flera varianter, exempelvis Cybercoin från Cybercash, som kanske är mer känd än Kleline.

När kunden väl har skaffat sin Klebox är det mycket enkelt att använda den. Att ansluta sig till Klebox går till på följande sätt (<http://www.kleline.com>, 1999):

- Det första kunden måste göra är att ladda hem och installera Klebox-programvaran från Klelines websida.
- Därefter får kunden registrera sig hos Kleline genom att fylla i ett formulär. Detta är första och enda gången som kunden behöver uppge numret på det kredit- eller kontokort som han vill ansluta till sin Klebox. Överföringen av numret skyddas genom kryptering.

5 Genomförande

- Kleline tilldelar sedan kunden ett Kleboxnummer. Kunden kan sedan använda detta nummer och dess lösenord för att göra köp och utföra säkra betalningar på Internet.

Att använda sig av den digitala valutan är sedan lika enkelt:

- När kunden vill betala med sin Klebox är det bara att klicka på Klebox-ikonen och använda sitt lösenord för att identifiera sig
- Därefter får kunden klicka på betalningssymbolen som finns på websidan hos alla butiker som är anslutna till systemet.
- För att avsluta köpet måste kunden använda sin digitala signatur (lösenordet) för att signera kvittot som han erhåller av butiken. Därefter är köpet och betalningen klara.

Kunden kan även på ett enkelt sätt fylla på sin "elektroniska plånbok" från det konto som är anslutet till Kleboxen, eller lägga till ytterligare konton till Kleboxen.

Exempel på områden där digital valuta är vanligt är där kunden kan betala för att läsa en viss artikel i ett nyhetsarkiv, lyssna på en låt, siter som har dataspel on-line där kunden kan betala för varje gång han spelar, eller att inhandla enstaka CD-skivor (Engholm, 1997).

I Sverige har dock inte alternativet digital valuta slagit igenom ännu. Om en webbutik vill erbjuda sina kunder möjligheten att betala med digital valuta får de använda sig av en utländsk bank, eftersom inga svenska banker stöder detta alternativ. De butiker som erbjuder kunderna Klebox t ex , använder sig av en fransk bank, Groupe Paribas, för att förmedla transaktionen.

6 Analys

I denna analys skall jag jämföra säkerheten hos de olika elektroniska betalningssätten utifrån de krav som ställts från banker, butiker och kunder. Jag skall dessutom jämföra fördelar och nackdelar hos dem. Detta skall så småningom leda fram till svaret på min problemställning om vilken elektronisk betalningsform i de svenska webbutikerna som är säkrast.

6.1 Betalkort

Då det finns vissa skillnader i hur säkerhetskraven uppfylls mellan de olika typer av betalningar som kan göras med kort, kommer de att redovisas var för sig.

6.1.1 Konto/kreditkort

Denna typ av betalning uppfyller både kraven på dataintegritet och identifikation, eftersom de tillämpar kryptering med SSL. Därmed anser jag att även önskemålet från kunderna om förtroende är uppfyllt, eftersom en krypterad förbindelse inte kan avlyssnas utan svårighet.

Den främsta fördelen med att använda sig av ett vanligt bankkort tycker jag är enkelheten. Kunden behöver inte göra några extra arrangemang i form av att ladda hem en elektronisk plånbok eller att i förväg ansöka om medlemskap och fylla i en fullmakt för webbutiken, för att kunna använda kreditkortet på Internet. Det enda kunden behöver göra är att uppge sitt kortnummer och därmed kan han göra sina inköp snabbt, vilket uppmuntrar till impulsköp på ett annat sätt än om kunden i förväg måste fylla i en fullmakt till butiken.

En stor nackdel med detta system är att säljaren inte har något underlag för att kräva betalning för de varor och tjänster som har beställts. Han får betalt i samband med att köpet genomförs, men sedan kan kunden reklamera sitt köp. Eftersom kunden aldrig har signerat sitt köp kan någon verklig (fysisk) identifiering inte göras, och säljaren har ingen möjlighet att kräva någon betalning.

6.1.2 Smarta kort

Smarta kort uppfyller samtliga krav på dataintegritet, identifikation och förtroende då de är krypterade med RSA-algoritmer. Dess fördelar är att det är ett enkelt och snabbt sätt att betala. Den största nackdelen är enligt min uppfattning att det kräver en kortläsare, vilket ännu inte är ett särskilt vanligt tillbehör hos datoranvändare.

6.1.3 SET

Genom förfarandet som beskrivits i kapitel 5.4.1 uppfylls samtliga de krav på identifikation och dataintegritet som ställs från de inblandade, eftersom det är en metod som bygger på stark kryptering med RSA-algoritmer. Dessutom tillgodoser SET kundernas önskemål om att kunna lita på att ingen information om deras köpbeteende sprids på ett otillbörligt vis, eftersom endast butiken (och inte banken) får kännedom om vad kunden köper. På samma sätt är det bara banken som får veta kundens kontouppgifter, butiken får aldrig denna information.

Detta är i mitt tycke den säkraste betalningsformen och den kommer troligtvis att bli standard för Internetbetalningar inom några år. Dess nackdel är att det är dyrt för butikerna att installera, vilket kan medföra att om butikerna tvekar att införa denna teknik, så kommer inte heller kunderna att vilja använda sig av den.

6.2 Medlemskap i shoppingtorg

Jag anser att denna betalningsform uppfyller de krav som ställs på dataintegritet, men däremot är det mer osäkert angående identifikationen. Om någon lyckas ta reda på mitt lösenord till torgetkontot så är det sedan fritt fram att handla, utan att butiken på torget anar oråd. Dessutom måste kunden här göra extraarrangemang innan han kan börja handla på sitt konto. Det är visserligen säkert, men ur webbutikernas synvinkel tror jag att det hämmar köplusten lite hos kunderna eftersom detta förfarande inte uppmuntrar till några impulsköp.

Genom att inga kontouppgifter vid något tillfälle skickas över Internet, garanteras kunden att ingen utomstående får information om vare sig kontonummer eller inhandlade varor. Det är ett enkelt och säkert sätt att handla på Internet när förberedelserna är avklarade. En nackdel kan vara att det endast finns ett begränsat antal affärer på torget, vilket inte uppmuntrar till impulsköp. Det kan ju vara bra ur kundens synpunkt, men knappast ur butikens. En annan sak som kan hämma köplusten är just de förberedelser som gör metoden så säker: Att skriva på en fullmakt som skall skickas in till torget och som sedan tillåter kunden att handla i butikerna på torget.

6.3 Digital valuta

Då även Kleline använder sig av kryptering med olika nycklar får detta betalningssätt anses ha hög säkerhet och uppfylla kraven på dataintegritet och identifikation. Även kundernas önskemål om att kunna känna förtroende för att informationen inte sprids anser jag uppfylls, då de elektroniska kontanterna är helt anonyma och inte kan spåras (Garfinkel & Spafford, 1997). Banken vet alltså inte vad kunden köper och webbutiken har inga kontouppgifter om kunden.

Den främsta fördelen med detta betalningsalternativ är att det lämpar sig väl att använda vid små betalningar, eftersom det inte tillkommer några extra avgifter. Tyvärr är det ännu inte så många butiker i Sverige som kan erbjuda sina kunder detta

alternativ. Ett skäl till det tror jag kan vara att de i så fall skulle bli tvungna att anlita en utländsk bank, eftersom inga svenska banker idag kan erbjuda denna möjlighet för webbutikerna.

6.4 Diskussion

Punkterna ovan ger nu en översikt av de olika alternativens säkerhet tillsammans med deras olika för- respektive nackdelar. Jag anser att det nu framgår ganska tydligt att samtliga de elektroniska betalningssätten uppfyller de inblandades krav på säkerhet. Om det är något alternativ som förefaller något mindre säkert så är det i så fall kontokortsbetalning utan SET, där butiken tar en viss risk eftersom kunden kan hävda att han inte har köpt något. Dessutom kan medlemskap i shoppingtorg vara något osäkert, om lösenordet skulle hamna på avvägar. Då kan vem som helst handla på mitt konto utan att butiken anar att något är fel. Men om kunden inte skriver upp eller lämnar ut sitt lösenord på annat sätt, anser jag att medlemskap i shoppingtorg är ett mycket bra betalningssätt eftersom inga kontouppgifter lämnas ut på Internet någon gång.

I övrigt anser jag att det inte finns speciellt mycket att anmärka på vad gäller säkerheten. Vid samtliga typer av betalningstransaktioner används någon form av kryptering, vilket enligt min åsikt ger en fullt tillfredsställande säkerhet. Min uppfattning stöds av flera artiklar, bl a skriver Byttner (1999) att en säkerhetsexpert vid namn Neil Barrett anser att riskerna med webhandel är kraftigt överdrivna. Barrett vill, som han uttrycker det, avliva ett antal myter, bl a den att hackare skulle kunna få tag i kreditkortsnummer vid korttransaktioner. Barrett säger att det är teoretiskt möjligt, men väldigt svårt, vilket är samma åsikter som den person jag intervjuade på webbutiken gav uttryck för.

Dock angav jag i min problemställning att jag skulle presentera ett betalningssätt som skulle vara bättre än övriga. Det alternativ som framstår som det ojämförligt säkraste är utan tvekan SET. Jag anser inte att det finns något skäl att misstro de andra alternativen, men om något skall framhållas blir det trots allt SET, inte minst p g a att detta troligen kommer att bli standard som betalningsmedel på Internet. Säkerheten i SET-betalningar är mer än nog tillfredsställande, och vill man vara drastisk skulle man kunna säga att det är överdrivet säkert.

Det som skulle kunna anföras emot SET är de stora kostnader som installationen medför för butikerna. Dessutom har det dröjt väldigt länge att komma igång med lanseringen, vilket har gjort att många butiker börjat dra öronen åt sig och istället se sig om efter andra och billigare alternativ (Sjögren, 1998).

I kapitel 5.1 gav jag luft åt åsikten att bankernas avsikter med SET kanske kunde ifrågasättas och detta påstående har jag funnit stöd för bland flera källor. Lotsson (1998) intervjuar Jon Karlung, vd för Bahnhof Internet (som är en Internetoperatör som bl a erbjuder företag e-posttjänster, egen domän och webhotell). I denna intervju framkommer det att Karlung anser att riskerna med att handla över Internet är en mytbildning och att SET egentligen inte behövs. Enligt Karlung är anledningen till att

6 Analys

SET införs att bankerna vill skaffa sig monopol på Internetbetalningar. Han drar paralleller till hur Microsoft vill tvinga människor att använda webbläsaren Explorer genom att bygga in den i operativsystemet, och med SET påstår han att bankerna nu vill göra samma sak - införa en standard för att skaffa sig monopol.

7 Resultat

De resultat jag har kommit fram till under arbetets gång stämmer ganska väl överens med vad jag förväntade mig från början. Säkerheten är en faktor som i hög grad påverkar utvecklingen av den elektroniska handeln. Kanske vore det mer korrekt att säga att gemene mans uppfattning om säkerhet är det som påverkar utvecklingen. Jag tror nämligen att den skepsis mot elektroniska betalningsmedel som är ganska utbredd bland folk i allmänhet, är omotiverad. Jag anser också att min uppfattning stöds av flera källor, bl a respondenten från min intervju. Han uppgav att :

”säkerhetsrisken är rejält överdriven. Väldigt sällan hör man talas om reella kontokortsbedrägerier. Det är oftast tredjehandsinformation. Sådan riskerar alltid att förvrängas. Mycket har det handlat om en mediafluga, tror jag. Det är alltid tacksamt att ropa varningar för trollen, även om få har sett dem.”

Min uppfattning är att det här resonemanget stämmer ganska väl med verkligheten. Om en tidning vill skapa rubriker så är naturligtvis skrämpropaganda effektivt. Dessutom tycker jag att det är anmärkningsvärt att det ofta är webbutikerna själva som tycker att säkerhetsriskerna är överdrivna, då det är de som skulle råka illa ut om något skulle inträffa. Det anser jag borgar för att deras åsikt verkligen är ärligt menad. Annars skulle det ju kunna ligga nära till hands att misstänka att: ”Självklart säger de att det är ofarligt, annars får de ju inte sälja något”. Men det resonemanget faller ju, då det som sagt är butikerna själva som drabbas om något går fel. Det resultat som jag själv har kommit fram till i mitt arbete – att samtliga elektroniska betalningssätt är säkra – anser jag också stöder min teori om att rädslan för att handla på Internet är obefogad.

Vad gäller säkerheten hos de olika betalningssätten kan jag bara konstatera att mina förväntningar infriades. Om man vill vara helgarderad mot värsta tänkbara händelser så är SET det allra säkraste som finns idag. Dock anser jag att även de andra elektroniska betalningssätten (betalkort utan SET, medlemskap i shoppingtorg samt digital valuta) mycket väl uppfyller alla krav på säkerhet som rimligen kan ställas. För mig ligger tanken ganska nära till hands att den allmänna misstänksamhet som råder mot elektroniska betalningsmedel har utnyttjats för att skapa en efterfrågan på en ny produkt – SET. Människor inbillas helt enkelt att tro att SET är något som de måste skaffa om de vill känna sig säkra.

Naturligtvis är SET väldigt säkert, det är odiskutabelt. Men det finns trots allt en nackdel som jag tidigare berört och det är det faktum att det har tagit alldeles för lång tid att introducera detta nya begrepp. Både kunder och webbutiker har börjat tröttna på att vänta på att SET skall bli allmänt använt (Ottosson, 1998). Många intervjuade webbutiker anser att tiden nu håller på att rinna ut för SET-projektet, eftersom marknaden blir alltmer splittrad av alla de olika nya tekniker som ständigt dyker upp. Anledningen till att många webbutiker tvekar till att installera SET är det är en dyr investering. För kunden är det kostnadsfritt att installera mjukvaran, men om inte butikerna använder SET så är det ju ingen idé att kunden gör det heller.

7.1 Diskussion

Att förutspå hur framtiden kommer att se ut för den elektroniska handeln är förmodligen en omöjlig uppgift, men många av de källor jag använt mig av (bl a Ottosson, 1998) är överens om att det krävs en gemensam standard för betalningar via Internet som kunderna vågar lita på. Annars är det stor risk för att det verkliga genombrottet som webbutikerna väntar på, aldrig kommer.

Fredholm (1998) har en intressant teori om hur framtiden kommer att gestalta sig. Han skriver att idag är trenden att olika tekniska lösningar håller på att växa samman. För ett företag som skall börja med elektronisk handel finns två huvudalternativ – EDI och webhandel. Med EDI får företaget i hög grad automatiserade lösningar som skapar mycket rationella flöden mellan två företag, men detta har den nackdelen att det medför stora kostnader att upprätthålla dessa flöden. Fredholm (1998) berättar att dessa två typer av elektronisk handel nu tenderar att växa ihop. Han skriver vidare att idag är det endast ett fåtal företag i Sverige som knutit samman de bägge koncepten, men att det inom ca tre år kommer att vara en självklarhet att göra på det sättet.

Fredholm (1998) har ytterligare några kloka ord som jag vill återge. Han säger att det kommer att bli allt viktigare att synas på Internet via en webbplats. Jag kan bara instämma i detta och jag tror att det för många är lika naturligt idag att leta efter produkter eller leverantörer på webben som det förut har varit att leta i Gula Sidorna. Lika viktigt som att synas på Internet är det också att marknadsföra sin Internetplats, med reklam på lämpliga ställen eller att få andra att göra länkar till den egna websidan.

Jag tror att det bara är en fråga om tid innan det stora genombrottet kommer för webhandeln. När folk i allmänhet har vant sig vid detta nya sätt att handla kommer de förmodligen inte tycka det är konstigare att handla på Internet än att handla på postorder. Dessutom instämmer jag med dem som säger att det behövs en gemensam betalningsstandard. Där tror jag mycket på SET, som uppenbarligen är den säkraste metoden för elektroniska betalningar som finns idag. Men som jag tidigare sagt, så har det tagit väldigt lång tid att lansera denna teknik. Vad som måste ske nu för att rädda SET är en kraftfull marknadsföring så butiker och kunder får upp ögonen för det. Kanske borde bankerna heller inte vara så angelägna om att snabbt få tillbaka de stora investeringar de gjort i SET, utan se det hela lite mer långsiktigt. Bankernas brådska att snabbt få in pengarna gör nämligen att det blir väldigt dyrt för butikerna att ansluta sig till betalningssystemet. De summor det handlar om är ca 200 000 – 250 000 kr, vilket är mycket för en liten butik som inte omsätter några stora summor.

Ottosson (1998) antyder ju att det nu är ”fem i tolv” för SET, med den betydelsen att om det inte kommer igång verkligt fort så kommer branschen att se sig om efter andra – och billigare – alternativ. Ottosson (1998) skriver vidare att alla inblandade är överens om att SET är en väl fungerande teknik och att en lösning som bygger på betalkort är bra. Men problemet kvarstår: Antalet kunder och webbutiker är för lågt.

8 Slutsatser

Sammanfattningsvis ser mina resultat ut så här:

Min första problemställning var vilka krav på säkerhet som finns från de olika inblandade aktörerna på marknaden, alltså banker, webbutiker och kunder. För att ta reda på detta använde jag mig både av intervjuer och litteraturstudier. Svaret som jag kommit fram till är att: betalningen skall vara säker för avlyssning, webbutik och kund skall kunna identifiera varandra samt kunden vill känna förtroende för att ingen information om hans köp hamnar någonstans där den inte hör hemma.

Den andra problemställningen var vilket av de elektroniska betalningssätten som uppfyller kraven i störst utsträckning. För att få ett svar på denna problemställning har jag jämfört säkerheten hos de olika betalningssätten och även jämfört deras för- respektive nackdelar. Det jag kommit fram till är att alla de elektroniska betalningssätt jag har undersökt uppfyller kraven, men att den allra säkraste betalningsformen är SET.

9 Erfarenheter från arbetet

Att välja ämne för examensarbetet var svårt. Jag ville skriva om något som är aktuellt och som jag kan ha nytta av i framtiden att kunna mycket om. Dessutom måste det vara intressant och roligt, så att jag inte skulle tröttna på att arbeta med det en hel termin. Så småningom föll valet på elektronisk handel, mest för att det är något som det talas väldigt mycket om nu. Eftersom jag inte hade så stora kunskaper i detta ämne innan jag startade, så har jag fått lägga ner mycket tid på att ta fram bakgrundsmaterial och själv skaffa mig grundläggande kunskaper och förståelse inom ämnet.

Efterhand som kunskaperna ökade, så ökade också vetgirigheten. Men 20 veckor är inte så mycket som man kan tro i början. Tiden räcker inte till för att fördjupa sig i allt som finns inom ämnet, så det blev nödvändigt att göra avgränsningar för att hinna färdigt med arbetet i tid. För att verkligen få tiden att räcka till, tror jag att det är viktigt att i ett tidigt skede göra en plan över sitt arbete och sedan försöka hålla sig till den i största möjliga mån. Och det är verkligen lärorikt och nyttigt att själv vara tvungen att ta ansvar för att arbetet blir utfört, vilket ställer stora krav på självdisciplin. Däremot har det varit litet besvärligt när det varit idétorka och jag saknat en arbetskamrat att pröva idéer på, och som kan komma med nya tankar när man själv kört fast. Min handledare har dock hela tiden varit verkligt engagerad och kommit med synpunkter och förslag på allt jag gjort.

I början av terminen verkade uppgiften väldigt stor, hur skulle jag kunna komma på så mycket att skriva om? Efterhand upptäckte jag att det inte var det som var problemet, utan det svåra var att jag hela tiden hittade så mycket som jag ville ha med att jag blev tvungen att begränsa mig. Nya frågor och tankar har hela tiden dykt upp och det har varit lätt att hamna på stickspår. Det finns nästan obegränsade möjligheter till fördjupningar inom ämnet elektronisk handel.

En viktig erfarenhet som jag dragit av arbetet är att i mycket god tid kontakta personer för intervjuer om man vill vara säker på att få någon intervju över huvud taget. Jag är medveten om att en brist i mitt arbete är att jag bara har gjort två intervjuer, vilket inte är så mycket att basera hela arbetet på. Men det tycks som det rent allmänt är svårt att få människor att ta sig tid till att ställa upp på intervjuer. Kanske kan det vara så att företag i allmänhet har mer att göra under våren och därför inte har tid med att svara på frågor från studenter.

Jag tycker ändå att jag fick användbara svar, som dels ledde mig in på nya tankar, dels befäste vad jag från början antagit. Jag har försökt att närma mig problemställningen på ett objektivt sätt och vara beredd att ändra de uppfattningar som jag hade från början. Min ambition har också varit att utöver de formulerade problemställningarna kunna diskutera om framtiden för den elektroniska handeln och vad som behövs för att det skall bli ett allmänt accepterat och vanligt sätt att handla på.

Arbetet har varit intressant och givande och gett mersmak på elektronisk handel. Det vore väldigt roligt att på något sätt få utveckla detta i någon form ute i arbetslivet, t ex att hjälpa företag att starta upp och utveckla sin elektroniska handel.

9.1 Uppslag till fortsatt arbete

Eftersom elektronisk handel är ett mycket omfattande ämne finns det näst intill outtömliga möjligheter till nya arbeten inom området. Ett förslag som känns som en naturlig fortsättning på mitt examensarbete är att utreda hur den elektroniska handeln fungerar ur företagets perspektiv. Exempel på hur arbetet skulle kunna bedrivas är att man studerar hur det går till att starta upp en ren webbutik, eller hur en ”vanlig” affär kan gå till väga för att komplettera sin försäljning med försäljning på Internet. Det skulle kunna ske antingen som litteraturstudie, eller ännu hellre ute på ett företag som just står i begrepp att genomföra detta.

Det borde kunna ge en god inblick i och förståelse för företagets villkor och var svårigheterna och problemen för företagen ligger. Jag tror att mycket kan göras där, om det kan utredas vilka behov företagen har. Det är ju trots allt de som måste våga satsa om det skall bli någon framtid för den elektroniska handeln.

10 Referenser

Arvidsson, S, Ek, J, Liljegren, J (1995) *Lättpocket om Internet*. Upplands-Väsby: Pagina Förlags AB.

Beekman, G (1994) *Computer Currents – Navigating Tomorrow's Technology*. Redwood City: The Benjamin/Cummings Publishing Company.

Byttner, K-J (1999) Säkerhetsexpert: Riskerna med webhandel överdrivna. *Computer Sweden*, 1999-03-22.

Engholm, A (1997) Mikrobetalningar blir störst. *Computer Sweden*, Nr 60.

Ericsson, M (1995) *Internet och HTML – Kompendium i informationsteknologi*. Universitetet i Linköping, Institutionen för datavetenskap.

Forsebäck, L (1998) Cybershoppare, intermediärer & digitala handelsmän. Teldok, *Telematik 2001*, Rapport 120.

Fredholm, P (1998) Elektronisk handel – Status och trender. Teldok, *Telematik 2001*, Rapport 121.

Garfinkel, S & Spafford, G (1997) *Web Security & Commerce*. O'Reilly & Associates, Inc.

Gustavsson & Johansson, P & Johansson, M (1998) Grundläggande begrepp för teknikplattformar. Högskolan i Skövde, Institutionen för datavetenskap.

Holländer, N (1997) *Elektronisk handel – Aspekter runt lag, säkerhet och Ecash*. Examensarbete, Institutionen för datavetenskap, Högskolan i Skövde (HS-IDA-EA-97-310)

<http://www.kleline.com> 1999-04-06

Kühn Pedersen, M (1990) *EDI i virksomheden*. Köpenhamn: Teknisk Forlag A/S.

Lynch, D & Lundquist, L (1996) *Digital Money – the New Era of Internet Commerce*. John Wiley & Sons, Inc.

10 Referenser

- Lind, S (1999) Säkrare handel på nätet. *Dagens Nyheter*, 99-01-25
- Lotsson, A (1998) "SET-standarden behövs inte". *Computer Sweden*, Nr 7.
- Lövgren, P (1997) Bankerna säkrar näthandeln. *MikroDatorn* 97-04-10
- Lövgren, P (1998) Kryptering är ett måste för säkert skydd. *MikroDatorn*, 98-03-05
- Makey, P (1996) *The Corporate Intranet/Internet – Strategies and Technologies*. Hesse: Butler Publishing Ltd.
- Nilsson, Å (1996) Säker näthandel i Sverige 1997. *Computer Sweden*, Nr 65.
- Ottosson, M (1999) Webbutvecklare misströstar om set-standarden. *Computer Sweden*, 1999-02-18
- Pappinen, L (1997) Elektroniska betalningar. <http://www.pagina.se>. 1999-04-24
- Patel, R & Davidsson, B (1994) *Forskningsmetodikens grunder – Att planera, genomföra och rapportera en undersökning*. Lund: Studentlitteratur.
- Paywatch (1998) *DigiCash kastar in handduken*. <http://www.paywatch.sisu.se/tu/news.htm>. 1999-02-17.
- Sandén, W (1998) Nätet som marknadsplats – de svenska pionjäreerna. Teldok, *Telematik 2001*, Rapport 123.
- Schmitz, B (1998) Så betalar du i webbutiken. *Internetguiden*, Nr 10, sid 16 – 19.
- Segerlund, C-Ö (1998) Välfärd via nätet? Teldok, *Telematik 2001*, Rapport 124.
- Sjögren, N (1998) Riskfritt handla med kort på Internet. *Computer Sweden*, Nr 39.
- Wallström, M (1998) Kraftigt genombrott för e-handel. *Computer Sweden*, Nr 104.
- Westholm, M (1998). <http://www.webhandel.nu>. 1999-02-26

10 Referenser