Handelshögskolan vid Göteborgs Universitet
Institutionen för Informatik

Ett säkert Internet

Betalningsformer för säkra transaktioner över Internet

Författare: Anders Frånberg

Examensarbete I, 10p
Vårterminen - 00

Handledare: Mathias Klang

Sammanfattning

Detta examensarbetet behandlar olika betalningsformer för elektronisk handel på Internet och fokuserar på säkerheten kring detta ämne.

Elektronisk handel på Internet är fortfarande en relativt ny företeelse som snabbt sprider ut sig. Det har blivit allt vanligare att företag erbjuder sina kunder att handla via Internet och även att betala sina inköp över Internet. Det vanligaste sättet att betala över Internet är med kontokort och eftersom det kan vara riskfyllt att lämna ut sitt kontokortnummer på Internet behöver dessa kontokortstransaktioner skyddas mot eventuella avlyssningar.

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

- Vilka krav bör man kunna ställa för att en E-handelsplats skall betraktas som säker?
- Vilka betalningsformer finns tillgängliga för att uppfylla dessa krav?
- Finns det någon elektronisk betalningsform som anses mer säker än någon annan?

De slutsatser jag kommit fram till är:

- De krav som ställs från de inblandade är att betalningen skall vara säker för avlyssning, handlare och kund skall kunna identifiera varandra samt för att inte köpare och säljare ska kunna förneka att de beställt en vara respektive tagit emot betalning, måste transaktionen kunna bevisas av motparten vid en eventuell tvist.
- De betalningsformer som uppfyller dessa krav är smarta kort och SET. Jag anser inte att SSL uppfyller kravet att en transaktion skall kunna bevisas.
- Av de elektroniska betalningssätt jag har undersökt uppfyller smarta kort och SET dessa krav, men att den allra säkraste betalningsformen är SET.

Innehållsförteckning

1. Inledning

1.1 Bakgrund

Idag kan man utnyttja många olika slags tjänster på Internet. I och med att fler och fler privatpersoner börjar använda Internet blir det en intressant marknadsplats för företag som vill sälja produkter och tjänster. Samtidigt ökar intresset för att handla hemifrån. Jämfört med att gå till butiken är det ofta både billigare och enklare att köpa t ex böcker, skivor och livsmedel via Internet. Här finns även ett avgörande samband: ett säkert betalningssystem stimulerar naturligtvis till ökad E-handel.

Elektronisk handel är en relativt ny företeelse och har ännu inte slagit igenom i lika stor utsträckning som Internet i övrigt. En bidragande anledning till detta är den osäkerhet människor känner inför handel via elektronisk väg. Att direkt i samband med beställning betala för varor eller tjänster på elektronisk väg, d v s att debitera kontot direkt, ställer mycket höga krav på säkerheten, då det innebär att kontokortnummer eller motsvarande information skickas över Internet. Bekväma, snabba och framförallt säkra betalningssystem är en förutsättning för att Internet skall kunna växa som elektronisk marknadsplats.

I den här uppsatsen skall jag behandla olika tre olika betalningsformer för säkra elektroniska transaktioner över Internet. Dessa är SSL, SET och smarta kort. Anledningen till att jag valt just dessa är att de två förstnämnda är mest vanliga i dagens E-handel och smarta kort ser jag som en framtida lösning om den får rätt genomslag bland de olika aktörerna på marknaden.

1.2 Syfte

Syftet med denna uppsats är skapa förståelse för vilka krav på säkerhet de olika aktörerna ställer på en elektronisk marknadsplats samt belysa tre tekniker som uppfyller dessa. Slutligen skall jag presentera en betalningsform som jag tycker tillgodoser dessa krav allra bäst.

1.3 Problemställning

Internet har idag blivit ett kommunikationsmedel som allt fler människor använder dagligen och möjligheterna till olika användningsområden på Internet är naturligtvis stora. Ett populärt uttryck är att med Internet har man hela världen i sitt hem, och min uppfattning är att det faktiskt ligger en hel del sanning i det.

Från att bara vara en informationskälla eller ett sätt att kommunicera har Internet nu blivit en plats att betala sina räkningar och göra affärer. Detta sker med elektroniska transaktioner över Internet och dagligen gör banker, företag och privatpersoner transaktioner på ofantliga belopp, utan att vare sig se eller ta i pengarna rent fysiskt.

Detta ställer höga krav på säkerheten om Internet skall fortsätta vara en global elektronisk handelsplats. Det finns en mängd olika tekniker som anses mer eller mindre säkra i dagens E-handel och hela tiden dyker det upp nya ”säkra” tekniker.

De problemställningar jag skall utreda är:
Vilka krav bör man kunna ställa för att E-handelsplats skall betraktas som säker?
Vilka betalningsformer uppfyller dessa krav?

Finns det någon elektronisk betalningsform som anses mer säker än någon annan?

Jag kommer successivt att behandla de mest aktuella teknikerna som bäst kan garantera säkra transaktioner över Internet.

1.4 Avgränsningar

Problematiken inom datasäkerhet är stor och en avgränsning i området måste därför ske. Avgränsning har därför gjorts till att endast gälla datoriserade tekniker för att säkerställa säkra elektroniska transaktioner över Internet. Fokus ligger då på själva transaktionen över Internet där kryptering dominerar. Således kommer jag inte att behandla brandväggar och liknade säkerhetslösningar som kan förhindra obehörig insyn i t ex dataregister.

Vidare tar jag inte upp hur säkerheten fungerar inom organisationen. Att det är viktigt för ett företag att ha klara riktlinjer för den interna säkerheten har givetvis lika stor betydelse för hur den skyddar sig mot externa hot. T ex med behörighetsnivåer, lösenordshantering, externa inloggningar på företagets server och liknande.

1.5 Disposition

Kapitel 1 Inledningen innehåller en bakgrund till uppsatsen, syfte, problemställning och avgränsningar.

Kapitel 2 Metodkapitlet består av de metoder som finns tillgängliga och vilka jag valt. Vidare motiverar jag min val som jag använt mig av under förberedelserna inför studien och vid genomförandet av undersökningen.

Kapitel 3 Här behandlar jag vilka krav som ställs på en E-handelsplats för att den skall kunna betraktas som säker.

Kapitel 4 Detta kapitel behandlar tre huvudtyper av krypomekanismer. Jag förklarar skillnaden mellan de olika typerna samt ger exempel på kända algoritmer och redovisar vilka nyckellängder de tillämpar.

Kapitel 5 Kapitlet redovisar två av de vanligaste standarderna som används för att skydda kontokortstransaktioner över Internet, SET och SSL. Jag behandlar även digitala certifikat och signaturer som har ett starkt samband med kontokortstransaktioner.

Kapitel 6 Detta kapitel förklarar ingående vad smarta kort är, hur de fungerar samt vilka olika typer av smarta kort som finns. Jag tar även upp för- och nackdelar med smarta kort.

Kapitel 7 Här har jag presenterat de tre intervjuerna jag gjort.

Kapitel 8 Kapitlet är en analys av de olika betalningssätten över Internet. Jag analyserar betalning med SSL, SET och med smarta kort.

Kapitel 9 I detta kapitel håller jag en diskussion om ämnet jag skrivit om. Här diskuterar jag även lite om framtiden.

Kapitel 10 Här presenteras mina slutsatser på de problemställningar jag har från kapitel 1.

Kapitel 11 En översikt av det material jag baserat mitt arbete på. Här finns även mina respondenter presenterade.

Kapitel 12 Bilaga I. Underlaget för mina telefonintervjuer.

2. Metod

Vid undersökning av ett problem finns det ett antal olika tillvägagångssätt att använda sig av, både vad gäller insamling och bearbetning av data. Den undersökningsmetod som väljs, påverkas i stor utsträckning av mängden tillgänglig information om problemet och syftet med undersökningen. Vidare kan resurser som står till ditt förfogande vara en avgörande faktor. Exempel på sådana faktorer kan vara tid, pengar och personal. Det är därför av största vikt att undersökaren funderar 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 samt förbereda tillvägagångssättet avseende anskaffning av annan önskad information.

2.1 Möjliga metoder

Metoder som brukar användas för att samla in data är enkäter, intervjuer, samt direkt observation. En annan vanlig metod är att använda sig av befintlig data - litteraturstudier[1]. När inte det eftersökta materialet finns sedan tidigare, väljs vanligtvis att göra en undersökning med hjälp av enkäter, intervjuer eller direkt observation[2]. 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.

Det är vanligt att i en given primärdataundersökning använda sig av en kombination av olika metoder[3]. 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.

2.1.1 Enkäter

En enkätundersökning beskrivs som att ett, vanligen slumpmässigt urval av personer eller företag får ett frågeformulär att fylla i och skicka tillbaka[4]. 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 huvudtaget att svara på frågorna och att det kan ta lång tid att få in svaren.

2.1.2 Intervjuer

Även intervjuer kan beskrivas 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

[1] Patel, P & B, Davidsson Forskningsmetodikens grunder 1994
[2] K. Dahmström, Från datainsamling till rapport 1991
[3] Ibid
[4] Ibid

uppstår oklarheter i frågorna kan det redas ut direkt, men det är i allmänhet kostsamt och tar förhållandevis lång tid att genomföra.

Ett snabbare sätt att få kontakt med respondenterna är att göra en telefonintervju[5]. 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.

2.1.3 Direkt observation

Direkt observation 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.

2.1.4 Litteraturstudier

De vanligaste källorna att hämta kunskap ur är böcker, artiklar och rapporter[6], vilka vanligen hittas i biblioteken. Att basera sina studier på tidigare arbeten kallas att göra en litteratur-studie. 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.

En fördel med att använda redan insamlade data är att det blir billigare än att själv samla in all data[7]. 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.

En nackdel som är vanligt förekommande, är att syftet med den ursprungliga undersökningen var ett annat än det som undersökaren nu tänker använda det till[8]. 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. 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.

[5] K. Dahmström, Från datainsamling till rapport 1991
[6] Patel, P & B, Davidsson Forskningsmetodikens grunder 1994
[7] K. Dahmström, Från datainsamling till rapport 1991
[8] Ibid

2.2 Metoder för bearbetning av data

När undersökaren har all den data han önskar är det dags att bearbeta och strukturera materialet. Det finns två olika inriktningar för hur undersökaren väljer att bearbeta den insamlade materialet, nämligen kvantitativ bearbetning och kvalitativ bearbetning[9]. 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.

2.2.1 Kvantitativ bearbetning

Kvantitativt inriktad forskning använder sig av statistiska bearbetnings- och analysmetoder[10]. 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.

2.2.2 Kvalitativ bearbetning

Denna typ av analysmetod syftar till att skaffa en annan och djupare kunskap än den fragmentariska kunskap som ofta erhålls när kvantitativa metoder används[11]. Ambitionen är 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.
En annan aspekt som skiljer denna metod från den kvantitativa är 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.

2.3 Val av metod

Naturligtvis är det ideala att välja den metod som, med 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 sett är besöksintervjuer den mest resurskrävande metoden för att samla information[12]. Därför är den metoden inget alternativ för ett arbete där en mycket begränsad tid står till förfogande, utan där kan det i stället vara lämpligt med en telefonintervju.

[9] Patel, P & B, Davidsson Forskningsmetodikens grunder 1994
[10] Ibid
[11] Ibid
[12] K. Dahmström, Från datainsamling till rapport 1991

2.3.1 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, elektronisk handel och de säkerhetstekniker som idag finns tillgängliga. 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 med betoning på säkerhet är aktuella och populära ämnen har det inte varit några som helst problem att få tag på material. Problemet är snarare det motsatta: Att sålla i den uppsjö av information som finns, för att erhålla den typ av material som är lämplig för detta arbete. Eftersom området hela tiden präglas av förnyelse och förbättring har det istället varit svårt att skaffa sig information för att kunna bedöma vilken teknik som f n är den mest aktuella.
De informationskällor som jag kommer att använda mig av är universitetsbiblioteket i Göteborg och bibliotek för Högskolan i Halmstad, där jag funnit både böcker i ämnet och tidigare examensarbeten inom samma ämne. Jag kommer också att använda mig av rapporter, samt artiklar i olika tidningar såsom Computer Sweden, Internetguiden och Nätverk & Kommunikation. Jag har också haft stor nytta av Internet, där jag funnit många artiklar och rapporter inom mitt problemområde.

Även om arbetet i huvudsak bygger på litteraturstudier erfordras ett visst inslag av egen insamlad information -- primärdata. Det som förefaller mest lämpligt med hänsyn tagen till den begränsade tiden, är telefonintervjuer. En telefonintervju ger stora möjligheter att ställa detaljerade 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 vilka säkerhetstekniker och tillämpningar som IT-företag använder sig av idag. Vidare ville jag få svar på vilka krav de ställer på säkerheten vid elektroniska betalningar, samt vad de anser om de olika formerna av digitala betalningssätt. Syftet är att få svar på min problemställning om vilket betalningssätt som bedöms som säkrast.

2.3.2 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 två sakkunniga personer inom IT-säkerhetsbranschen, 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 rena statistiska uppgifter.

En metod som jag anser som mindre lämplig för min undersökning är metoden för direkt observation. I mitt tycke lämpar sig den metoden bättre för statistiska undersökningar, där

undersökaren vill ha fram ett stort antal observationer av någon företeelse för att på ett tillförlitligare sätt kunna grunda sina värderingar och antaganden på.
Jag anser inte heller att den kvantitativa metoden för databearbetning är lämplig för mitt arbete, då den synes vara mest lämpad för att analysera sifferuppgifter. Enligt min uppfattning skulle den metoden kunna vara mest lämpad att använda tillsammans med metoden för direkt observation.

2.4 Plan över arbetet

Det fortsatta arbetet kommer att bedrivas på så sätt att jag kommer att genomföra telefonintervjuer med tre IT-företag med inriktning mot IT-säkerhet. Detta i syfte att reda ut vilka säkerhetstekniker som gäller idag samt vilka krav och önskemål som ställs på säkerheten vid 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 7.

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 analysen att presenteras separat i kapitel 8.

3. Säkerhetsfunktioner

Många ger uttryck för behov av att kunna skicka känslig information via nät för tele- och datakommunikation. Företag, myndigheter och enskilda utövar ett allt starkare tryck på leverantörer av IT-produkter och operatörer av nättjänster att kunna genomföra elektroniska affärer, elektronisk ärendehantering och service, distansarbete, kommunikation mellan privatpersoner etc, på ett säkert sätt, både inom och utanför Sverige.

All kommunikation över Internet är i grunden osäker eftersom Internet är byggt med öppenhet som det primära målet. Näten är flexibla, samtidigt som de gör det möjligt att t.ex. avlyssna meddelanden och skicka meddelanden i andras namn. Användare kan alltså inte förvänta sig att öppna och allmänna nät är säkra och måste därför själva vidta åtgärder för att skydda sin information och därmed också kunna få säkerhet hela vägen från avsändare till mottagare. Detta innebär att det behövs skydd på olika nivåer i en säkerhetsarkitektur. På tillämpnings-nivån krävs textskydd, och det är den nivån som oftast diskuteras när frågor om digitala signaturer och kryptering kommer upp.
Säkerhetsfunktioner bygger i de allra flesta fall på någon användning av krypteringsteknik.

De säkerhetsfunktioner som krävs bygger på identifiering, signering och kryptering och är fundamentala. Det finns huvudsakligen tre säkerhetstjänster som är intressanta när vi talar om elektroniskt informationsutbyte, nämligen:

- **Autentisering**, verifiering av att sändare och mottagare verkligen är de som de utger sig för att vara.
- **Konfidentialitet**, att ingen obehörigt kan ta del av informationsinnehållet som överförs.
- **Signaturer**, att varken sändare eller mottagare kan förneka att de har sänt eller tagit emot viss information.

3.1 Autentisering

Autentisering sker antingen med hjälp av användarnamn och lösenord eller med certifikat och digitala signaturer. Autentisering med hjälp av användarnamn och lösenord är en dålig metod, främst eftersom de flesta har svårt att komma ihåg sitt lösenord och bevarar det uppskrivet på en lapp nära datamaskinen. Därtill kan lösenord lätt brytas om de baserar sig på vanliga ord, och de kräver att servern upprätthåller ett lösenordsregister. För att förbättra säkerheten används sällan lösenordsregister utan kontrollsummeregister, där kontrollsummorna av lösenorden förvaras.

För att autentiseringen skall vara säker, måste olika procedurer utföras i en noga uttänkt ordning. Det finns protokoll som sköter om att autentiseringen sker på rätt sätt. Två av de mera använda är SSL och SET. Dessa två protokoll kommer att redovisas i kapitel 5.

I den ”riktiga” världen brukar vi människor ofta identifiera oss med våra pass, körkort, ID-kort eller liknade. Motsvarigheten i den ”elektroniska” världen heter elektroniska ID-kort och kan vara i form av ett smart kort, och dessa behandlar jag i kapitel 6. Med smarta kort kan autentiseringen ske på ett säkert sätt även i den ”elektroniska” världen.

De nya smarta korten som använder sig av PKI (se 6.3.4), är ett annat sätt att säkerställa autentisering. Smarta kort använder sig av en tredje part (CA) som garanterar att de inblandade är det de utgör sig för att vara (se avsnitt 5.3).

3.2 Konfidentialitet

När information transporteras över Internet via webbkommunikation eller e-post mellan två personer, måste denna information skyddas. Den befintliga teknik som används idag är baserad på kryptering och finns exempelvis i dagens HTTPS-servrar på Internet. HTTPS använder sig av SSL-protokollet (se avsnitt 5.1). Enligt tidningen Nätverk och kommunikation har den Finska staten emellertid ett projekt med elektroniska ID-kort på stark framfart och detta kort har ett inbyggt integritetsskydd som kan få ett bredare genomslag[13].

3.3 Signaturer

Dessa signaturer gör att du vet vem som skickat ett visst dokument samt säkerställer att dess innehåll inte har ändrats. Detta är nödvändigt för att kunna hantera juridiskt bindande avtal via Internet, och kräver förutom den tekniska säkerheten även en tillämpbar lagstiftning[14]. Kravet på signering är viktigt för båda parter i en transaktion därför om kunden aldrig har signerat sitt köp kan någon verklig (fysisk) identifiering göras, och säljaren har därför ingen möjlighet att kräva någon betalning.

Dessa tre olika säkerhetstjänster fungerar som krav för att en E-handelsplats skall betecknas som säker. Det finns givetvis olika tekniker för att uppfylla varje specifikt krav och dessa kommer jag att redovisa i de efterföljande avsnitten.

[13] Gustafsson, J. Digital Identitet i Finland. Nätverk & Kommunikation 000125
[14] Ibid

4. Kryptering

För att möjliggöra säkra elektroniska transaktioner via Internet måste vissa säkerhets-åtgärder vidtas. Den kanske vanligaste åtgärden är att kryptera meddelandet innan det sänds.

De flesta protokoll bygger på kryptering, vilket innebär att all information som utväxlas mellan handlare och konsument skyddas med nycklar för att inga obehöriga skall få tillfälle att läsa eller ändra informationen. En nyckel är en serie siffror och tecken som används till att kryptera information. Istället för att ange antalet nycklar brukar man ange nyckellängden. Den enhet som nyckellängden anges i brukar kallas bitar. För varje tillkommande bit fördubblas antalet möjliga nycklar och därmed tiden för att pröva sig fram till rätt nyckel[15]. Tio bitar betyder ungefär tusen nycklar, 20 bitar ca en miljon. Med andra ord, ju längre nycklar, desto säkrare kryptering. I dag arbetar moderna datorer mycket snabbt varför antalet nycklar måste därför uppgå till totalt sett ofantliga mängder.

När mottagaren får meddelandet måste denne dekryptera det för att åter se meddelandet i dess ursprungliga klartext. Kryptering utgör ett gränsskydd ur sekretessynpunkt. Ett krypterat meddelande kan inte läsas av obehöriga och det går inte heller att modifiera det på något ”intelligent” sätt[16] utan att ha tillgång till eller att lyckas med att hitta rätt nyckel.

Ett problem i sammanhanget är att det inte går att bevisa att en algoritm är bra, utan egentligen bara att den inte är dålig på något känt sätt. Detta gör att olika standarder och tillämpningar inte bör vara bundna till en viss algoritm, utan det ska vara enkelt att välja vilken algoritm som ska användas och att byta ut en algoritm som börjar visa sig tveksam.

I varje verksamhet måste det finnas ett program för vilka åtgärder som måste vidtas om en algoritm blir tveksam eller om en central eller lokal krypto nyckel röjs. För att förhindra detta bör man arbeta med regelbundna nyckelbyten eller använda längre nycklar. Längre nycklar påverkar dessvärre prestandan på krypteringen, vilket blir kännbart om de används för elektroniska transaktioner över Internet.

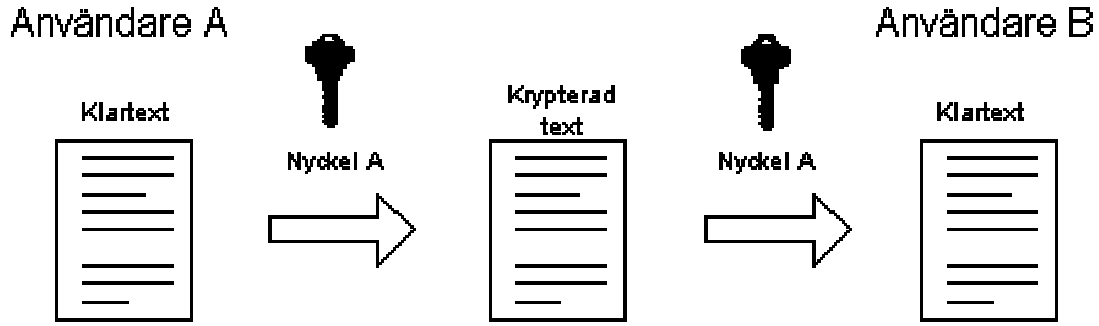
I detta avsnitt beskrivs tre huvudtyper av kryptomekanismer:
- Symmetrisk kryptering
- Asymmetrisk kryptering
- Envägskryptering (hash-funktioner).

Alla krypteringsmetoder bygger på minst en hemlighet, en krypteringsnyckel, som delas mellan parterna. Säkerheten vid kryptering är helt beroende på att nyckeln är hemlig, och inte kommer i orätta händer eller enkelt kan forceras. Därför är processen avseende nyckel-generering, nyckelhantering och nyckelutbyte lika viktigt som hur starkt själva kryptot är[17]. Detta är något som ofta förbises. Många gånger kan det vara svårt att forcera själva kryptot, medan det kan finnas ganska enkla sätt att få tag på nyckeln. Den kanske till och med ligger lagrad i klartext hos användaren.

[15] Ur regeringens skrivelse till riksdagen Skr. 1998/99:116 ang kryptografi, Bilaga 2
[16] Säkerhetsarkitekturer SIG security 1998
[17] Ibid

4.1 Symmetriska krypteringsalgoritmer

Symmetrisk kryptering är baserad på att kryptering och dekryptering utförs med samma nyckel. Algoritmerna används för volymkryptering av data eller dataströmmar. När avsändaren vill sända ett skyddat meddelande krypterar han den oskyddade informationen till kryptotext med den hemliga nyckeln. Mottagaren dekrypterar kryptotexten till klartext med hjälp av samma hemliga nyckel. En nackdel med symmetrisk kryptering är att man måste hålla sig med lika många nycklar som det finns personer som man vill kommunicera säkert med, ett problem som, åtminstone delvis, löses med asymmetrisk kryptering. Fördelar är dess snabbhet och det är även vanligt att ha ett stort antal möjliga nycklar. De symmetriska nyckelalgoritmerna kan delas upp i två kategorier: block och ström. Strömalgoritmer krypterar ”byte by byte”, medan blockalgoritmer krypterar ett datablock i taget.



Figur 1. Den symmetriska krypteringen[18].

Data Encryption Standard (DES) introducerades under 70-talet och är idag en standard i de flesta länder och används främst inom finansiella verksamheter. DES används dock inte längre av den amerikanska staten, som avvaktar på att den nya standarden, AES (American Encryption Standard), skall fastställas[19]. AES måste självklart vara säkrare än dagens DES, vilket den blir genom att bland annat använda nycklar på upp till 256 bitar. Tanken är att den nya algoritmen ska kunna användas under de kommande 30 åren eller kanske längre[20].

DES är ett blockkrypto som använder 64-bitars datablock med en 56-bitars nyckel. Detta gör den relativt enkel att knäcka för stora aktörer på marknaden med tillgång till kraftfulla datorer eller med specialdesignad hårdvara. DES anses emellertid fortfarande vara stark nog för att hindra de flesta ”hackers” och andra som försöker göra intrång. SSH Communications Security antyder dock att DES börjar bli för svag, och rekommenderar systemdesigners att bortse från DES i framtiden.

Just för DES finns ingen möjlighet att förlänga nyckeln med en bit i taget–det skulle kräva att man skriver om hela systemet från grunden. Men varianten Triple DES har i praktiken en 112 bitars nyckel, vilket med god marginal klarar dagens krav[21].
3DES är baserad på att den använder DES tre gånger. Oftast brukar 3DES krypteras efter följande sekvens: kryptering-dekryptering-kryptering, där olika nycklar används för

[18] källa: www.itkommissionen.se
[19] Lotsson A. Standardkryptot knäckt för länge sen. CS 991129
[20] Ricknäs, M. Öppenhet nyckeln till ny krypteringsstandard. CS 000413
[21] Ibid

respektive krypteringsprocess. Många anser att 3DES-algoritmen är mycket säkrare än den vanliga DES[22].

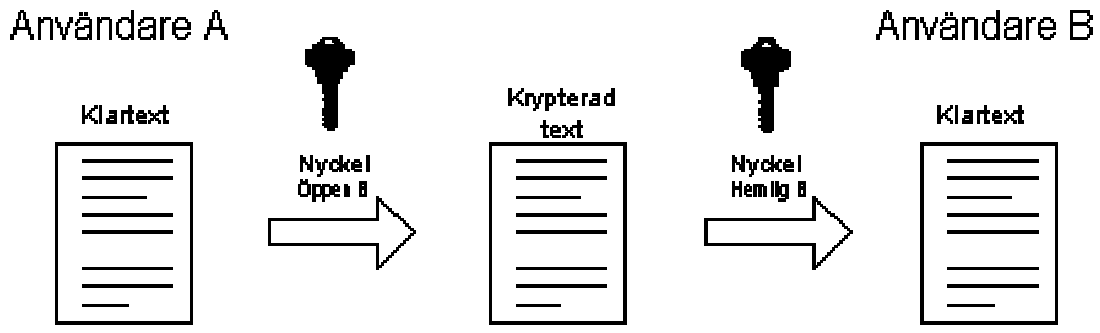
Blowfish är en algoritm utvecklad av Bruce Schneier. Blowfish är ett block-krypto och som symmetrisk krypteringsalgoritm är den snabb och kompakt. Blowfish är optimerad för 32- eller 64-bitarsprocessorer och tillåter en variabel nyckellängd upp till 448 bitar[23]. I skrivande stund har inga kända attacker gjorts mot Blowfish[24].

International Data Encryption Algorithm (IDEA) är utvecklad i Schweiz och använder sig av en 128 bitars nyckel och anses vara mycket säker[25]. Det är en relativt ny algoritm och har därför inte blivit utsatt för några riktigt seriösa attacker där någon försökt knäcka den. Eftersom den använder sig av en 128 bitars nyckel kan man visserligen förvänta sig att den är säker, men jag tycker ändå att den har mycket kvar att bevisa.

RC4 är en chiffer designad av RSA Data Security (Samma företag som designat RSA-algoritmen). Algoritmen var från början en affärshemlighet, tills någon okänd publicerade dess källkod på UseNet News. Algoritmen är mycket snabb och dess säkerhet är i skrivande stund okänd eftersom inga kända attacker har publicerats. Detta kan möjligen bero på att den fortfarande är ganska okänd. SSH tror att RC4 kan ha används i vissa applikationer p g a sin goda prestanda. RC4 kan dessutom anta nycklar av godtycklig storlek[26]. USA:s myndighet har godkänt export av denna algoritm med en nyckellängd av 40 bitar. Men en nyckellängd av denna storlek kan relativt enkelt knäckas av amatörer och illvilliga kriminella, varför den skall användas med längre nycklar för att betraktas som säker.

4.2 Asymmetriska krypteringsalgoritmer

Asymmetrisk kryptering, även kallad Public-key-kryptering (PKK), karaktäriseras av att man använder sig av olika nycklar för kryptering och dekryptering. En öppen publik nyckel och en privat, hemlig nyckel. Public-key-kryptering kan användas för utbyte av hemliga nycklar och/eller kryptering och dekryptering. PKK kan även utföra digitala signaturer och säkra transmissioner.



Figur 2. Den asymmetriska krypteringen[27]

[22] http://www.ssh.fi/tech/crypto/algorithms.html
[23] Säkerhetsarkitekturer SIG security 1998
[24] http://www.ssh.fi/tech/crypto/algorithms.html
[25] Ibid
[26] Ibid
[27] källa: www.itkommissionen.se

I princip fungerar det så att det finns ett par av samhörande krypteringsnycklar, där den ena offentliggörs, den publika nyckeln och den andra, den privata, förblir hemlig och endast känd av användaren, dvs nyckelägaren. Detta kan utnyttjas på två olika sätt beroende på om krypteringsnyckeln eller dekrypteringsnyckeln görs publik; Om den publika nyckeln är offentlig, kan vem som helst skicka ett skyddat meddelande till nyckelägaren. Det är endast denne som kan dekryptera och därmed läsa det skyddade meddelandet.

RSA[28] är den mest använda asymmetriska algoritmen. RSA använder Public-Private Key (PPK) kryptografi och kan vara av varierande nyckellängd, men idag rekommenderar de flesta en nyckellängd på 1024 bitar eller mer[29]. Detta är lite beroende på den implementation som skall användas.

I dagsläget har ingen ännu lyckats knäcka 1024 bitars RSA, och anses av många vara den säkraste krypteringstekniken[30]. Men jag vill även poängtera att det beror lite på vilka resurser som används när någon vill knäcka ett krypto. Detta bekräftar Bruce Schneider, som är författare till standardverket Applied Cryptography. Han menar att med rätt resurser kan alla krypto knäckas inom en viss tid och tar som exempel 512 bitars RSA, som med rätt teknik kan knäckas på en vecka. Den teknik han åsyftar här användes när DES-algoritmen, som tidigare var officiell standard i USA, knäcktes[31].

Digital Signature Standard (DSS) har utvecklats av National Security Agency, NSA. DSS är baserad på Digital Signature Algorithm, DSA. Även om DSA tillåter nycklar av variabel längd, tillåts endast nycklar mellan 512 och 1024 bitar under DSS. Som det är specificerat, kan DSS endast användas för digitala signaturer, även om det är möjligt att använda DSA-implementationer även för kryptering[32]. Dess design har emellertid inte blivit publicerad, och många användare har hittat potentiella problem med den. De problem som SSH anger är att den läcker data och kan avslöja sin hemliga nyckel om någon händelsevis råkar signera två olika meddelanden med samma slumpade tal.

Elliptic curve public key cryptosystems (ECC) är ett kryptosystem som blir allt vanligare. Tidigare har problemet varit att de är långsamma att arbeta med, men med dagens moderna datorer har den blivit alltmer tacksam att exekvera. Den anses vara godtyckligt säker men har än så länge inte funnit samma stöd som t ex RSA[33].

4.3 Envägskryptering

Med hjälp av envägs hash-funktioner kan man åstadkomma ett integritetsskydd för filer. Detta går till så att man utgående från informationen i filen beräknar en kontrollsumma, även kallat fingeravtryck, med hjälp av hash-funktionen. Filen kan ha vilket storlek som helst medan kontrollsumman har en fix längd. Kontrollsumman lagras på ett säkert ställe där den inte kan modifieras. Om man sedan vill kontrollera att filen inte har ändrats beräknas kontrollsumman ytterligare en gång och jämförs med den lagrade varianten. Om de två är lika är det ytterst sannolikt att filen inte har ändrats, eftersom hash-algoritmen har egenskapen att i princip varje

[28] Efter dess uppfinnare Rivest, Shamir och Adleman.
[29] http://www.ssh.fi/tech/crypto/protocols.html#ssl
[30] Electronic Commerce, E. Turban 1999. s.84
[31] Lotsson A. RSA-kryptot knäckt. CS Artikelarkiv 990913
[32] Säkerhetsarkitekturer SIG security 1998
[33] http://www.ssh.fi/tech/crypto/algorithms.html

ändring i filen medför att hash-värdet ändras[34]. Det skall alltså inte finnas två olika filer som ger samma hash-värde. Denna egenskap kallas att algoritmen är kollisionsfri och fungerar som ett slags signering att informationen inte har ändrats eller modifierats.

Message Digest Algorithm (MD5) är en hash-algoritm, och även den är utvecklad av RSA Data Security. Den kan användas för att envägskryptera vilken filstorlek som helst till en 128 bitars nyckel[35]. MD5 används över hela världen och SSH anser att algoritmen är väldigt säker.

Secure Hash Algorithm (SHA) är en kryptografisk hash-algoritm och utvecklad på beställning av USA:s regering. Den kan användas för att envägskryptera vilken filstorlek som helst till en 160 bitars nyckel[36]. Många anser den vara mycket bra trots att det är en relativt ny algoritm.

4.4 Moores lag för kryptering

Processorernas kapacitet fördubblas i princip var artonde månad. Det lär oss Moores lag som har gällt i över trettio år. Det innebär att tiden som krävs för att knäcka ett krypterat meddelande halveras på arton månader.
Bruce Schneier menar att man kan säga att det finns en Moores lag för kryptering.
Detta innebär att man regelbundet måste förlänga nycklarna. En tumregel är att varje extra bit i nyckeln gör att det tar dubbelt så lång tid att knäcka kryptot. Detta gäller för symmetrisk kryptering, till exempel DES och Bruce Schneiers egen algoritm Blowfish. För asymmetrisk kryptering, som RSA, är matematiken annorlunda.
”Man kan säga att om man förlänger nyckeln med åtta bitar så tar det tre gånger så lång tid”[37], menar Bruce Schneier.

[34] Säkerhetsarkitekturer SIG security 1998
[35] http://www.ssh.fi/tech/crypto/algorithms.html
[36] Ibid
[37] Lotsson, A. Tryggheten med kryptering en farlig illusion. CS 991104

5. Säkerhetsprotokoll

Ordet standard har många olika betydelser. I detta kapitel använder jag ordet standard synonymt med ordet protokoll. Protokoll är en uppsättning regler för hur datorer skall kunna kommunicera med varandra, d v s för att datorernas applikationer skall kunna kommunicera med varandra.

Standarderna SET och SSL

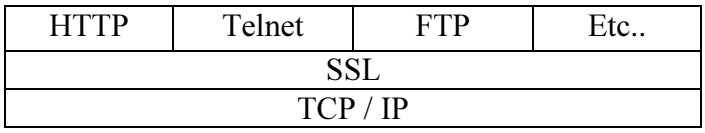
De två vanligaste standarderna idag för att skydda kontokorttransaktioner över öppna nätverk som Internet är SSL, Secure Socket Layer, och SET, Secure Electronic Transaction. I detta kapitel beskriver jag dessa två standarder, både tekniskt och praktiskt samt skillnaderna mellan dem.

5.1 SSL, Secure Socket Layer

SSL-standarden, som är utvecklad av Netscape, kom som en av de tidigaste standarderna för säkra transaktioner över Internet. SSL är ett protokoll som används för att verifiera identiteten hos en klient och en server samt etablera en krypterad förbindelse mellan dem. SSL är inte utformad speciellt för betalningstransaktioner[38], utan är främst utvecklad för att skydda kommunikationen mellan två kommunicerande applikationer över Internet.

SSL är idag den vanligaste standarden för överföring av kontokortnummer över Internet och finns installerad i alla stora tillverkares webbläsare (Netscape & Explorer).
Orsaken till detta beror till stor del på att SSL kom som en av de första standarderna på marknaden och att det har inneburit en förhållandevis snabb uppbyggnad av en bred kompetens inom området.

Säkerhetsprotokollet SSL är ett lager som kan skjutas in mellan ett vanligt nätverksprotokoll som TCP[39], och applikationslagret (se figur 3). Exempel på sådana applikationslager är HTTP[40], FTP[41] eller Telnet[42].



Figur 3. Secure Socket Layer

SSL använder sig av en kryptering som är baserad på 40, 56, 128 eller 168 bitar. SSL innebär att kommunikationen sker genom en krypterad förbindelse – tunnel – mellan klient och server[43].

[38] Johansson, R. *Krypteringsteknik – nyckeln till säkerhet*?
[39] TCP (Transport Control Protocol) - Det vanligaste transportprotokollet på Internet
[40] HTTP (Hyper Text Transport Protocol) - Webtrafiken använder detta protokoll.
[41] FTP (File Transfer Protocol) – Protokoll för överföring av filer över Internet
[42] Telnet – Terminalhantering och inloggning över nätverk.
[43] http://www.set-guide.com/

Eftersom man vill att trafiken över Internet skall ske snabbt är det viktigt att kryptering och dekryptering inte ger några prestandaförluster. Detta är en anledning till varför Netscape ville använda sig av symmetrisk kryptering under en SSL-session. För att uppnå detta och samtidigt erhålla en hög säkerhet utnyttjar man de asymmetriska krypteringen som en mekanism för att på ett säkert sätt distribuera en symmetrisk sessionsnyckel[44].

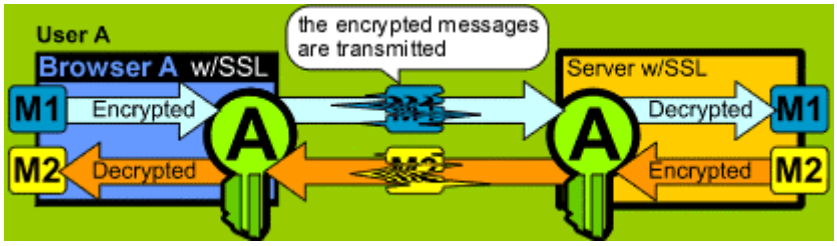
5.1.1 Funktionaliteten hos SSL

Vid en verifiering sänder klienten sin offentliga nyckel till servern. Servern sänder tillbaka ett meddelande till klienten som använder sin privata nyckel för att kryptera meddelandet. Meddelandet sänds tillbaka till servern, som använder klientens offentliga nyckel för att dekryptera meddelandet. Om detta meddelande överensstämmer med det som tidigare blev sänt har verifieringen fullbordats[45].

[44] Säkerhetsarkitekturer, SIG 1998
[45] http://www.ssl.com/n_privacyB.htm

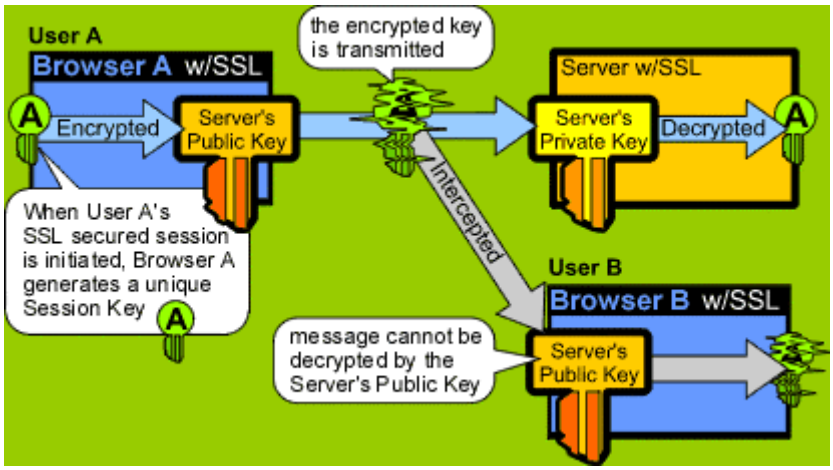
5.1.2 Kryptering i SSL

Som jag tidigare nämnt är de symmetriska algoritmerna snabbare jämfört med de asymmetriska. För att transporten av informationen skall bli så snabb som möjligt utnyttjar SSL de symmetriska algoritmerna. Vanliga symmetriska algoritmer för denna typ av transport är DES, IDEA, och 3DES (se kapitel 4.) De symmetriska algoritmerna används endast för överföring av information över Internet (se figur 4).



Figur 4. Transportering av information med symmetrisk kryptering[46].

De symmetriska algoritmerna må vara snabba, men de anses inte vara tillräckligt säkra för att användas för elektronisk handel. Anledningen till detta är att de använder samma nyckel för kryptering som dekryptering. Lösningen är att man istället använder sig av den asymmetriska krypteringstekniken för nyckelhanteringen (se figur 5).



Figur 5. Hantering av den privata nyckeln med asymmetrisk kryptering[47].

[46] källa: http://www.ssl.com
[47] Ibid

5.2 SET, Secure Electronic Transaction

I detta avsnitt går jag djupare in på vad SET är och hur det fungerar i praktiken. Vidare kommer jag även beskriva hur det är uppbyggt med hjälp av kontrollsummehantering och digitala identitetshandlingar. Jag berör SETs framtid och vad som talar emot att SET slår igenom som betalningssystem.

För att lösa problemet med säkerheten vid betalning på Internet har ett antal kontokortsföretag och banker gått samman och enats om att något måste göras.
VISA och MasterCard har bildat ett samägt bolag, SET Secure Electronic Transaction LLC, även kallat SETco. Bolaget bildades i syfte att driva utvecklingen av SET-standarden vidare, och idag har även American Express anslutit sig till standarden[48]. Tillstånden för att utfärda SET- certifikat ges av SETco som är samordnare av certifikaten[49]. I Sverige är det bankerna som beviljar företagen att få certifikat för SET-försäljning.

SET har under hösten 1998 introducerats på marknaden, efter en tids tester i ett pilotprojekt. Bakom projektet står enligt Visa (1996) kortföretagen Visa och MasterCard, ett antal banker däribland fyra svenska, samt företagen Microsoft, Netscape, GTE, Communications Corp., SAIC, Terisa System, VeriSign och IBM. SET bygger på den redan befintliga infrastrukturen för kreditkortstransaktioner, som har byggts ut för att stödja betalningar via Internet.

Standarden är en s k teknisk specifikation som är öppen för alla aktörer som vill bygga sin produktutveckling på SET.
Syftet med standarden är att kunna verifiera, godkänna och skydda handlare, konsument och bank när en kontokortbetalning genomförs på Internet. Genom kryptering garanteras och skyddas konsumentens och handlarens identitet samt den betalningsinformation som skickas mellan dem[50].

SET-standarden är designad för att skapa säkerhet för *alla* inblandade parter. Tack vare att en tredje part är inblandad och att avancerad kryptering används, kan systemet sägas vara lika säkert eller kanske ännu säkrare än vanliga kontokortbetalningar. Till skillnad från betalning i affärer med kontokort får handlaren inte tillgång till kundens namnunderskrift.

5.2.1 Funktionaliteten hos SET

För att SET skall fungera krävs det att kunden har en programvara, en sk ”digital plånbok”. Denna programvara finns oftast att ladda ner på bankens hemsida och måste sedan installeras på den egna hårddisken. Programmet identifierar sedan vilken webbläsare som finns installerad och identifiering och aktivering av betalprogrammet sker från bankens hemsida. Varje kund väljer sitt eget användarnamn och lösenord som används för att aktivera den digitala plånboken. Information om de olika kontokort som kunden har tänkt att använda för betalning över Internet, samt typ av kort, kortnummer, kredit- eller betalkort, kortets giltighetsdatum samt språk som skall användas vid senare betalning anges. För att använda SET vid inköp krävs att kunden får ett certifikat som hämtas genom att ange sitt användar-ID.

[48] Johansson, R. *Krypteringsteknik – nyckeln till säkerhet*?
[49] www.setco.com
[50] Johansson, R. *Krypteringsteknik – nyckeln till säkerhet*?

Registreringen är klar på några minuter och certifikatet läggs automatiskt in i betalprogrammet.

I princip fungerar SET-betalningen som en vanlig kontokortsbetalning i vilken butik som helst. Plastkortet ersätts med ett sk. certifikat som är ett elektroniskt kort. Istället för den vanliga namnteckningen skickas en elektronisk signatur. Denna krypterade signatur fungerar därmed som en garanti för att jag är jag.

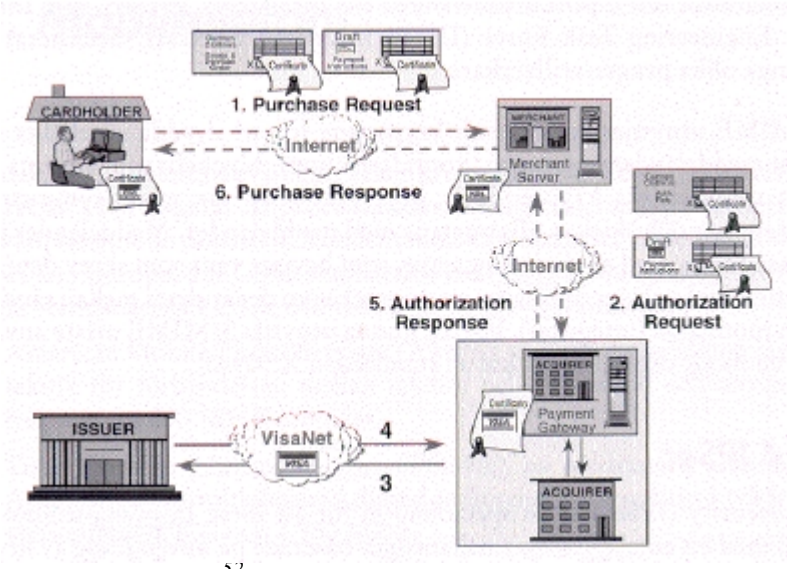
SET kombinerar digitala signaturer och kryptering för att skydda konfidentialitet och integritet samt för att verifiera ursprunget hos meddelandet. Krypteringen i SET bygger på en kombination av de båda krypteringsteknikerna DES och RSA. DES är av 56-bitars nyckellängd och RSA av 1024-bitar. Säkerheten är mycket hög tack vare kombinationen av flera säkerhetslösningar, men gör systemet kostsamt vilket leder till höga transaktionskostnader[51].

Med SET-standarden skickas aldrig kundens kontokortnummer över Internet. Standarden skiljer konsument och handlare åt vad gäller all kontokortinformation. Istället för att skicka kontokortnumret direkt till handlaren, som i sin tur skickar denna information vidare till en bank, går istället informationen direkt till banken. Banken utfärdar dels en bekräftelse till handlaren att pengar finns på kontot och dels utför betalningen från detta. På det här sättet undviks problemet med att oseriösa handlare får tag i kontokortnumret.
SET-standarden definierar betalningsprocessens alla steg (se 5.2.2) och meddelar vilken information som skall sändas mellan de olika inblandade parterna. Dessa parter är kontokortinnehavaren, banken som utfärdat kortet (emissionsbanken), handlaren, handlarens bank (förvärvsbanken) och det aktuella kontokortföretaget (ex VISA). SET uppfyller alla de tre säkerhetsaspekterna; autentisering, konfidentialitet och signering.

Dessutom ingår även identifiering av konsumentens och handlarens auktoriteter. Konsumenten kan via den tredje parten, d v s banken, få reda på om handlaren är registrerad hos denne och på så sätt få ett ”kvitto” på att handlaren är äkta och den som den utger sig för att vara. Handlaren får i sin tur information om att konsumenten är registrerad kontokortsinnehavare och att denne har tillräckligt med pengar för att kunna betala.

[51] Wigblad, R & Åhlgren, K. Elektronisk handel i små och medelstora företag

5.2.2 Betalningsprocessen med SET



Figur 6. Betalningsprocessen med SET[52]

1. Kunden skickar sin beställning till E-handelsbutiken och butikens certifikat skickas från butiken till kunden. Certifikatet krypteras när det skickas från butiken och dekrypteras när kunden tar emot det. Certifikatet kontrolleras av kundens digitala plånbok för att fastställa om butiken som tar ens kontokort är en legitim butik. Därefter skickas kundens egna certifikat till butiken i krypterad form av den digitala plånboken. Detta för att butiken skall kunna se att kunden är den han påstår sig vara. Den digitala plånboken är den programvara som kunden behöver för att kunna utföra SET-transaktioner.

2. Butiken skickar iväg en förfrågan, en auktorisation, som går via Payment Gateway (bankens Internetserver), som dekrypterar förfrågan och omvandlar transaktionen från SET-format till vanligt bankformat. Förfrågan skickas sedan till insamlaren Cekab, som bankerna även använder för alla vanliga traditionella kortköp som utförs i fysiska butiker.

3. Cekab skickar förfrågan vidare till kortutgivande bank. Banken gör då ett antal säkerhetskontroller för att kontrollera om kortet får lov att handla.

4. Förfrågan skickas tillbaka samma väg, från banken till Cekab och Payment Gateway.

5. Payment Gateway översätter förfrågan tillbaka till SET-format från bankformat, och skickar tillbaka den till butiken. Butiken får då en bekräftelse på att transaktionen är OK.

6. Butiken svarar kunden att beställningen går bra. Sedan skickas själva köpet, transaktionen, i väg till Payment Gateway, Cekab och den kortutgivande banken.

[52] Johansson, R. *Krypteringsteknik – nyckeln till säkerhet*? s.25

5.3 Digitala certifikat och digitala signaturer

I SET-standarden används så kallade digitala certifikat och digitala signaturer.
För att alla parter i en kontokortstransaktion skall kunna identifieras utfärdas digitala certifikat till alla parter som är inblandade i transaktionen. Certifikaten ger parterna en garanterad identitet. Både kontokortsinnehavarens och handlarens certifikat utfärdas av banken. Vid varje transaktion skickas certifikaten över Internet för att verifiera konsumenten, säljaren och banken. Konsumentens certifikat är bundet till dennes kontokortnummer och kan likställas med ett vanligt kontokort. Ett digitalt certifikat kan ses som ett elektroniskt ID-kort. Certifikatet är konsumentens bevis på att kontokortet är känt av kontokortsföretaget och därmed får konsumenten möjlighet att handla på Internet hos de handlare som är SET-certifierade.

Ett certifikat kan i sin tur definieras som ett elektroniskt dokument som:

- Identifierar den utfärdade certifieringsorganisationen.
- Identifierar, eller bestyrker en egenskap hos den certifierade signaturens upphovsman.
- Innehåller upphovsmannens publika nyckel.
- Signerats digitalt av den utfärdande certifieringsorganisationen (I SET:s fall är det banken som utfärdar dessa certifikat.

Antag att jag vill skicka ett sekretessbelagt meddelande. När jag krypterar mitt meddelande, är min avsikt att det endast är innehavaren av den privata nyckeln som skall kunna läsa det. Här måste jag vara övertygad om att den publika nyckel jag har, verkligen tillhör nyckelägaren. För att lösa administrationen av nyckelutbyten behövs en oberoende instans eller myndighet som användarna har förtroende för, och med vars hjälp man kan verifiera, eller certifiera, att man verkligen har rätt nyckel. En sådan instans kallas CA (eng. Certifikate Authority).
CA lagrar persondata om alla användare samt deras publika nycklar på ett sätt som gör det möjligt att bli övertygad om att en viss användare verkligen är ägare till en viss publik nyckel. En CA kan hantera nycklar för ett företag, en viss region eller kanske ett helt land. Men för att kunna använda asymmetrisk kryptering mellan olika länder eller regioner upprättar man ytterligare en CA, på en högre nivå, som certifierar att olika CA-instanser kan auktoriseras att verifiera kryptonycklar. På detta sätt kan man bygga upp en hierarkisk certifieringsstruktur, som utöver CA-instanser kan kompletteras med andra tjänster inom området nyckelhantering och digitala signaturer.
Man har då skapat en Public key Infrastructure (PKI). En infrastruktur för nyckelhantering som innebär att kommunikationen mellan två parter garanteras av en tredje (CA). Rent tekniskt inkluderar PKI både kryptering och autentisering.

En digital signatur är en teknik som baseras på kryptering och används för identifikation, och signering. För att generera signaturen krävs tillgång till den privata nyckeln, men för att läsa signaturen och verifiera autenticiteten krävs endast den publika nyckeln. Den digitala signaturen motsvarar en handskriven signatur på ett papper, fast på elektronisk väg. Den används för att säkerställa vem som skickat ett elektroniskt meddelande, d v s att kontokortsinnehavaren är den person som han eller hon utger sig att vara. Med den digitala signaturen kan också informationens integritet kontrolleras genom att det går att se om meddelandet ändrats på vägen mellan avsändaren och mottagaren[53].

[53] Johansson, R. *Krypteringsteknik – nyckeln till säkerhet*?

5.4 Framtiden för SET

Världen har sedan Internets genombrott haft behov av en enhetlig standard för betalningar över Internet. Elektronisk handel blir mer och mer vanlig, och på grund av detta har SET tagits fram. SET är en storsatsning från kortföretagen Visa och Mastercard i samarbete med flera företag samt ett antal banker däribland fyra svenska (Handelsbanken, Föreningssparbanken, Postgirot Bank och SE-banken).
Jag anser att SET är en standard som har vad som krävs säkerhetsmässigt för att säkra betalningar över Internet.

Förutom att SET är ett säkert sätt att utföra betalningar över Internet, har SET Visa och MasterCard som grundare vilka är stora kortföretag som redan är väl etablerade på den globala marknaden. Det är viktigt att SET etableras hos allmänheten snarast, annars finns det stor risk att något annan elektronisk betalning tar över. Antingen en ny betalningsrutin eller att de befintliga, som SSL, drar ifrån ytterligare.

5.5 Vad talar emot SET?

Enligt Rönn (1999) har endast 1500 köp med SET genomförts, vilket kan jämföras med bankernas satsade kapital på ca 3 miljarder kronor, detta innebär en kostnad på en miljon kronor per köp med SET[54]. Dessa siffror talar sitt tydliga språk att SET fortfarande är för dyrt för handlarna och för krångligt för användarna för ett verkligt genombrott. Onlinehandel till konsumenter bedrivs fortfarande i för liten utsträckning för att det skall vara värt de stora investeringar som krävs för införande av SET på en E-handelsplats.

Nackdelar med SET är att den inte lämpar sig för transaktioner på mindre belopp då administrationskostnaderna är ganska höga. Vidare kan investeringskostnaden för hård- och mjukvara bli relativt hög, då handlaren kan behöva investera i t ex databaser. Dessutom tillkommer en viss kostnad för varje transaktion som skall betalas till banken, precis som med vanliga kontokortsbetalningar. En annan nackdel är att det inte går att utföra person-till-person-betalningar då mottagaren måste vara auktoriserad handlare av kontokortföretag eller bank.

SSL-standarden är etablerad och mycket använd, vilket innebär att tillgängligheten är stor, vilket inte kan sägas om SET ännu, eftersom antalet handlare och konsumenter är lägre jämfört med SSL. En fördel med SET är att det är en global standard som flera större aktörer, bl a Visa, MasterCard, Netscape, IBM och Microsoft, står bakom. Detta medför att standarden har goda chanser att få en stor utbredning samt att både konsumenter och handlare ges möjlighet att handla och sälja varor och tjänster över hela värden. Att just dessa aktörer är involverade kommer förmodligen också att öka förtroendet för Internethandeln vilken tidigare mötts med stor skepsis.

Som jag tidigare behandlat är det i en affärssituation på Internet viktigt för både köpare och säljare att kunna identifiera varandra. För köparen är det 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

[54] Rönn, J. SET-fiaskot: en miljon kronor per transaktion. 1999

beställt eller tagit emot varan eller tjänsten. Detta är alltså ett problem främst för butikerna och kunderna, medan bankerna inte drabbas om tvistemål skulle uppstå (SSL).

Med andra ord är det butikerna och kunderna som tar de största riskerna, medan bankerna endast drabbas om det blir problem med avlyssning av kommunikationerna (SET). 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, eftersom det är där som de största riskerna kan identifieras. 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 kostnaden för att införa SET ligger mellan 200 000 - 250 000 kr[55].

[55] Sjögren, N. Riskfritt handla med kort på Internet CS artikelarkiv 98

6. Vad är ett smart kort?

Aktiva kort eller smarta kort som de även kallas har redan funnits en tid. Jag kommer att använda begreppet smarta kort.

Det var redan 1974 som fransmannen Roland Morena uppfann och tog patent på det första kortet. Detta gjorde att fransmännen tidigt visade ett intresse för användningen av de smarta korten. 1985 började man i Frankrike sälja telefonkort som då var den första och största tillämpningen. Varje år säljs det cirka 120 miljoner telefonkort i så väl Frankrike som i Tyskland. Fransmännen var även de som först började använda de smarta korten inom bankväsendet. Eftersom fransmännen både uppfann och är flitiga användare av korten har det blivit naturligt att de flest stora kortföretagen finns just i Frankrike.

Telefonkort är idag den största tillämpningen av tekniken och på andra plats kommer de smarta bankkorten som började användas 1992. Nu för tiden används korten till många olika saker, exempelvis som identitets- och tjänstekort.
En framtida användning av smarta kort vid identifiering av användare i samband med elektroniska transaktioner kan därför komma att vara en tänkbar lösning för att ytterligare förstärka säkerheten.

Smarta kort är en delmängd av de Integrated Circuit (IC) kort som finns tillgängliga på marknaden[56]. De har ungefär samma storlek som ett vanligt kreditkort och kan grovt delas in i tre olika typer av kort; IC-minneskort, smarta kort och superaktiva kort. Det som skiljer dessa typer åt är bland annat att IC-minneskort saknar processor, vilket de övriga har. Superaktiva kort, även kallade displaykort, har exempelvis tangentbord och display, vilket de andra typerna inte har.

6.1 Är smarta kort tillräckligt säkert för Elektronisk handel?

Skall man tro på företaget iD2, som är ledande i frågor om smarta kort är svaret på frågan: Ja, men det gäller inte alla smarta kort. Det finns olika typer av smarta kort som nästan ser identiska ut, men har helt olika säkerhetsfunktioner.

6.2 Smarta korts säkerhetsfunktioner

Vad är det som gör att det smarta kortet är säkert? Några faktorer enligt Bergdahl (1995) är:

- alla funktioner vad gäller säkerhet och kontroll tar kortet själv hand om
- all kommunikation sker via mikroprocessorn, vilket hindrar obehöriga att komma åt den hemliga information som finns lagrad i kortet
- när en transaktion äger rum ges endast den information ut som är nödvändig för transaktionen.

För att förvissa sig om att systemet är säkert måste kortläsaren ha möjlighet att validera data.

[56] Bergdahl, T. (1995), Smarta kort - teknik och tillämpning i USA

Detta görs genom att kortläsaren utför en igenkänningsprocess innan den accepterar information från det smarta kortet[57]. Den kräver att det smarta kortet skall bevisa att kortet är äkta och tillhör systemet. Igenkänning av smarta kort kan göras på flera olika sätt och det kallas normalt för "smartcard authentication".

Då smarta kort tillåter uppdatering av data via kortläsaren, bör det smarta kortet i sin tur utföra igenkänningstest av kortläsaren innan uppdateringen börjar. Denna omvända igenkänningsmetod kallas normalt för "cross-authentication" och det smarta kortet tar endast emot information då alla säkerhetskriterier är uppfyllda.

De smarta korten och deras chip är konstruerade för att förhindra förfalskning, kopiering, avlyssning eller återgivning av innehållet i den kommunikationen som sker mellan kortets chip och de tillämpningar som kortet nyttjas av[58]. Försök att forcera kortets inbyggda säkerhet leder till att funktionerna förstörs eller blockeras.

Smarta kort har tre olika säkerhetsfunktioner; identifiering, igenkänning och digital signatur.

6.2.1 Identifiering

Själva identifieringsprocessen innehåller tre byggblock:

1. något som en person har (innehav) t ex ett smart kort.
2. något som en person vet (kunskap) t ex lösenord.
3. någonting om personen i fråga (egenskap) t ex ett fingeravtryck.

Dessa tre byggblock kan kombineras för att höja säkerheten[59].
Alla tre används endast om säkerhetsrisken är stor. Det normala är att endast de två översta används. Den tredje kräver biometrisk teknik, t ex genom hornhinnan, vilket både är kostsamt och tekniskt avancerat.

Smarta korts uppgift vid identifieringen är att verifiera kortinnehavarens identitet i ett informationssystem, dvs användaren ska vara den hon/han utger sig för att vara. Kortinnehavarens elektroniska identitet döljs i en unik, skyddad "sträng" som inte kan ändras. Vissheten om att kortet är knutet till en enda person garanteras av ett certifieringsorgan, Certification Authority (CA) och dokumenteras i ett individuellt certifikat.

Kortanvändningen sker tillsammans med ett personligt lösenord som endast kortinnehavaren skall känna till. Lösenordet kan vara i form av en Person Identification Number (PIN) kod. Denna slås in på kortläsaren som sedan skickar koden till kortet. Detta utgör en säkerhetsrisk om inte kortläsaren krypterar PIN-koden innan den skickas. För att detta skall vara effektivt måste olika krypteringsnycklar användas vid varje tillfälle. När kortet har tagit emot koden, jämför chipet på kortet koden med den kod som finns lagrad i minnet. Om dessa två koder stämmer överens är användarens identitet verifierad. En klarsignal skickas sedan till

[57] Bergdahl, T. (1995), Smarta kort - teknik och tillämpning i USA
[58] Toppledarforum, (1996), Remissutgåva av Säkrare IT i offentlig sektor
[59] Bergdahl, T. (1995), Smarta kort - teknik och tillämpning i USA

kortläsaren och det ges tillgång till vissa filer i kortet samt att transaktionen kan fortsätta. Om den inslagna PIN-koden inte stämmer överens med den lagrade, ges det normalt två försök till att slå in den rätta koden. Om samtliga försök misslyckas kan kortet låsa sig, antingen mjukt eller hårt. Mjuk låsning innebär att kortets leverantör kan öppna det igen. Hård låsning innebär att kortet är oanvändbart för all framtid och innehavaren måste införskaffa sig ett nytt.

6.2.2 Igenkänning av smarta kort med hjälp av kryptering

Det finns olika metoder som ett smart kort kan bevisa sin systemtillhörighet med. Som tidigare nämnts kallas dessa generellt för "smartcard authentication" eller igenkänning av smarta kort. Det finns för- och nackdelar med de olika metoderna för igenkänning. De bör granskas utifrån minst fem aspekter[60]:

1. hur enkelt är det att implementera metoden?
2. hur avancerad mikroprocessor kräver metoden?
3. hur mycket kraft kräver styrning och övervakning av systemet?
4. vilken sårbarhetsgrad är acceptabel med tanke på exempelvis bedrägeri?
5. hur tidskrävande är igenkänningsprocessen?

De tre första aspekterna har att göra med kostnad, den fjärde har att göra med systemintegriteten och den femte avser kundtillfredsställelse.

Kryptering är ett effektivt sätt att bevisa systemtillhörighet utan att avslöja identifikationens särdrag, men det krävs ett system för att distribuera krypteringsnycklarna. För att kunna kryptera och dekryptera måste krypteringsnycklar finnas och dessa måste distribueras. Smarta kort kan användas för att lokalt skapa krypteringsnycklar för att kryptera information och det finns olika sätt att skapa krypteringsnycklar. Det enklaste och snabbaste sättet är att använda symmetriska algoritmer och den mest använda och kända är DES (se avsnitt.4.1) Enkelt beskrivet fungerar den på följande sätt;

Ett slumptal skickas till både kort och mottagare, algoritmen skapar sedan lokalt två identiska nycklar som används för kryptering och dekryptering av informationen. Det krävs alltså att nyckeln är känd på båda ställena för att det ska fungera.

För ännu bättre säkerhet kan två olika nycklar skapas, en för kryptering och en för dekryptering. Då använder man sig av asymmetrisk kryptering. Den mest använda och säkraste algoritmen är RSA (se avsnitt 4.2).

6.2.3 Digital signatur

Som jag nämnt tidigare används digitala signaturer för att säkerställa och knyta digitalt lagrad data till en viss person. Detta motsvarar den vanliga handskrivna signaturen och har som syfte att upprätthålla juridisk hållbarhet av digitala handlingar. Digitala signaturer kan skapas och information kan på så sätt säkras med hjälp av smarta kort.

Det smarta kortet kan användas för att signera elektroniska handlingar och skydda

[60] Bergdahl, T. (1995), Smarta kort - teknik och tillämpning i USA

innehållet från att bli ändrat. Det går inte att redigera eller ändra i existerande handlingar utan att signera, vilket går att spåra precis som om handlingarna vore signerade på vanligt handskrivet sätt.

För digitala signaturer används asymmetriska algoritmer, t ex RSA[61].
Informationen signeras med en privat signaturnyckel och mottagaren kan med en publik verifikationsnyckel verifiera och känna igen avsändaren.

6.3 Typer av smarta kort

Ett flertal av de typer av smarta kort som finns är inte anpassade för elektronisk handel. För att ha så säkra E-handelstransaktioner som möjligt måste korten uppfylla två fundamentala säkerhetskrav, autentisering (se avsnitt 3.1) och signaturer (se avsnitt 3.3)[62].

Smarta kort består av ett chip (processor och/eller minne), en kontaktyta och har utseendet som ett litet plastkort enligt gällande ISO-standard (ISO 7810 – 54x85x0.8 mm)[63]. Chip som enbart använder sig av processorer kräver någon form mjukvara. Denna mjukvara kallas ”mask” och agerar som kortets operativ system. Det är möjligt att programmera kortet och exekvera data och det är detta som gör kortet aktivt/smart. Kortet kan även innehålla någon form av minne, exempelvis ROM och RAM, som endast kan nås av mikroprocessorn. I skrivande stund rekommenderas minst 4 KB EEPROM. Detta ger en hög säkerhet med avseende på åtkomsten av den lagrade information.
De chip som finns i de smarta korten kan skilja sig åt mellan olika tillverkare. Detta beror på att varje tillverkare har egna unika tekniker. Några av de mest kända tillverkarna av smarta kort är; Gemplus, Schlumberger, Oberthur, Siemens, Giesecke & Devrient, Setec och Bull.

Kombinationen av ett inbyggt chip samt en mjukvara, är det grundläggande för tillverkning av smarta kort.

Generellt så brukar de flesta typer av smarta kort ha någon form av skrivskydd, men det finns även kort som inte har detta. Vidare är det även viktigt att kortet kan utföra säker bearbetning av data (nycklarna) inuti sitt chip. Detta för att omöjliggöra kopiering av signaturerna under transportering. Trots att signaturer är krypterade räcker det inte för att det skall vara helt säkert[64], menar ID2. ID2 betonar här, för att uppfylla digitala signaturer är det en nödvändighet att signaturprocessen sker inuti det smarta kortets chip.
Smarta kort kan delas upp i tre huvudkategorier:

- Memory Cards
- Symmetric Cryptoprocessor Cards (Symmetrisk krypteringsteknik)
- PKI smart cards (iD2´s benämning på ”Asymmetric cryptoprocessor cards”), (Asymmetrisk krypteringsteknik)

[61] http://www.id2.se/whitepapers/smartcards.asp
[62] Ibid
[63] Ibid
[64] Ibid

Vilken krypteringsteknik?

Anledningen till att de kryptografiska korten delats upp i två olika kategorier beror på att de skiljer sig åt när det handlar om autentisering och signaturer. Processorn i chip:et som utför den symmetriska krypteringen kan emellertid utrustas med mjukvara (mask) för att utföra den asymmetriska krypteringen. De nuvarande smarta korten med PKI (Public key Infrastructure) behöver inte denna mjukvara eftersom kortet redan är utrustat med en processor som klarar av den asymmetriska krypteringen. Oftast används den asymmetriska krypteringsalgoritmen RSA med 1024 bitars nycklar, som idag är en av de absolut säkraste.

Företaget iD2 poängterar att korten finns i flera olika modeller och att många av dem inte är utformade och optimerade för att använda RSA-kryptering. ID2 pekar på flera fall där det finns lösningar som endast är utformade till att lagra de nycklar som skall krypteras.

I nästa avsnitt kommer jag att behandla de tre ovanstående huvudkategorierna för smarta kort.

6.3.1 Memory Cards

Fortsättningsvis kommer jag att benämna memory cards som minneskort.

Minneskort kan genom sitt minne verifiera en användare genom en eller flera PIN-koder. En nackdel med minneskorten är att de inte kan skydda den lagrade information som finns i minnet. En jämförelse kan göras med vanliga disketter, med den skillnaden att minneskortet har mindre lagringskapacitet. Vidare är minneskortets läsare mindre komplicerad och billigare jämfört med en diskettenhet, och passar sig bättre i olika miljöer då den praktiskt taget är mobil.

Att associera minneskort med smarta kort känns inte helt naturligt eftersom kortet är begränsat till att endast lagra information. När minneskortet har verifierat en användare med rätt angiven PIN-kod, har han/hon fri tillgång till den lagrade informationen. Om inte informationen är skrivskyddad kan en verifierad användare modifiera data som kanske borde vara skyddad. Eftersom vissa användare skall ha möjlighet att ändra sådan information krävs ofta ytterligare en PIN-kod, vilket gör minneskortet starkt begränsat.

Således tycker jag inte att minneskort erbjuder tillfredsställande säkerhet för att säkerställa signaturer.

6.3.2 Symmetriska krypteringskort

De symmetrisk smarta krypteringskorten erbjuder en annorlunda struktur för hur stor tillgång av information som kan tillåtas. Tillgången till information kan begränsas till att bara vara läsbar och inte skrivbar och i omvänd ordning kan tillgången på informationen verifieras av ditt kort. Åtkomsten till filer kan skyddas av ett eller flera lösenord (PIN) och verifieras vid rätt angiven PIN-kod. PIN-koden är skrivbar (för att du skall kunna ändra ditt lösenord).

Då kortet använder sig av kryptering är det möjligt att skicka information mellan två parter utan att en tredje part får tillgång till det material som skickas.

Den symmetriska krypteringstekniken arbetar snabbt, och jämfört med den asymmetriska krypteringen är den märkbart snabbare. Det är dess stora fördel. Men att använda sig av symmetrisk kryptering medför vissa nackdelar. T.ex. blir utfärdandet av nycklar praktiskt taget omöjligt eftersom krypteringen bygger på samma nyckel, både för kryptering och dekryptering av den skyddande informationen. Detta leder med största sannolikhet till att förtroendet för denna typ av säkerhetsteknik blir låg, och i förlängningen kan detta bidra till att ingen vågar använda sig av systemet och utnyttja elektronisk handel som många kanske skulle önska.

6.3.3 Smarta kort som använder PKI

Det stora skillnaden mellan PKI-kortet och det symmetriska krypteringskortet är att PKI använder sig av en säkrare, asymmetrisk kryptering. Krypteringen utförs med den idag ännu icke knäckta 1024 nycklars RSA-algoritmen, och finns inbäddat i kortets chip. Kortet kan även använda sig av båda krypteringsteknikerna. Som jag beskrev tidigare kan åtkomsten av filer styras i alla riktningar.

Eftersom RSA betraktas som en av de mest pålitliga och säkraste krypteringsalgoritmerna, uppfyller PKI-kortet två av de grundläggande säkerhetsaspekterna, autentisering och signaturer[65]. ID2 menar att PKI-kortet erbjuder en helt ny säkerhetsnivå eftersom informationen på kortet varken går att komma åt eller kopiera. Jag anser även att smarta kort med PKI uppfyller kravet på konfidentialitet eftersom 1024-bitars RSA näst intill omöjliggör en eventuell avlyssning.

PKI-kortet är utrustat med ett eget operativsystem vars uppgift är att skydda nycklarna från obehöriga. Dessa nycklar kan inte läsas, ändras eller tas bort av någon, inte ens användaren av kortet om inte en PIN-kod anges. Denna PIN-kod kan, precis som med de övriga korten, ändras av användaren.

PKI är inte en produkt utan flera. Det inbegriper produkter för autentisering och kryptering. Kort kan man säga att det finns tre olika sorters produkter i PKI. Klienten (Kund), servern (Säljare) och den som ger ut certifikat (CA)[66].

6.4 Fördelar med smarta kort

Det finns många fördelar med smarta kort. Säkerheten för de smarta korten är bättre än magnetkortet eftersom informationen som kortet innehåller är skyddat. Vidare krävs det även ett lösenord som identifiering av användaren för att få tillgång till informationen och dessutom är kortet svårt att förfalska. Naturligtvis beror säkerheten mycket på innehavaren av kortet. Om användaren har bra kontroll och uppsikt på kortet, blir systemet säkrare och bättre. Kortets lilla och smidiga storlek är ytterligare en fördel.

Ökad säkerhet och säker identifiering av användare är en av de största fördelarna med smarta kort[67]. Jag anser att det smarta kortet ökar informationssäkerheten vid elektroniska transaktioner ochhanteringen i känsliga register. Det ger en enklare administration och gör det möjligt att kunna arbeta bl a hemifrån.

[65] http://www.id2.se/whitepapers/smartcards.asp
[66] Jakobsson H. PKI kan ge säkrare närhandel. CS artikelarkiv 000510
[67] Sundström, M. (1996), Hur används aktiva kort i offentlig förvaltning

Eftersom smarta kort kan användas för flera olika ändamål, exempelvis legitimation och inpasseringskontroll, upplevs det som praktiskt, lätthanterligt och som ersättare till komplicerade nyckelsystem. Smarta kort ger även en säker identifiering och behörighetskontroll av användare till allmänna terminaler och egna persondatorer.

Jag tror även att användningssättet är en fördel eftersom det påminner väldigt mycket om hur bank- och telefonkort används. De flesta personer har använt ett bank- eller telefonkort någon gång och är därför förtrolig med handhavandet av kortet. Detta anser jag bör minska så kallade handhavande fel som kan orsaka säkerhetsbrister i ett informationssystem.

6.5 Nackdelar med smarta kort

Den tekniska aspekten, exempelvis vad kortet kan klara av, kan vara svårt för gemene man att förstå[68]. Vanligt förekommande är att användaren endast nyttjar en bråkdel av de möjligheter och finesser som de tekniska apparaterna har att erbjuda. Detta gäller även smarta kort. En annan nackdel är bristen på en enhetlig standard, vilket ställer till problem när kortet ska användas i ett öppet system.

Ett problem som uppkommer vid införandet, är bristen på gemensamma tekniska plattformar och höga kostnader för licenser.

6.6 Informationssäkerhet inom E-handel med hjälp av smarta kort

Den nya tekniken med smarta kort som identifikationsmedel kan åtgärda många av de säkerhetsbrister som finns i dagens elektroniska transaktioner.

De smarta korten erbjuder väldigt hög säkerhet, samtidigt som det är en lösning som håller en lång tid framöver även om det kortsiktigt kan uppfattas som begränsande[69]. Smarta kort som använder PKI löser problemen med identifiering på ett säkert och smidigt sätt eftersom den infrastruktur med CA:s som tredje part garanterar säker identifiering av två parter.

[68] Bergdahl, T. (1995), Smarta kort - teknik och tillämpning i USA
[69] SIG Security – Säkerhetsarkitekturer 1998

7. Empiri

I detta kapitel kommer jag att återge mina intervjuer samt analysera dessa med avseende på problemställningen. Jag kommer att försöka generalisera företagens svar tillsammans och likaså kommer jag att kategorisera svaren i olika huvudfrågor som framgår av kapitel-indelningen nedan. Vilka de olika respondenterna är, har jag redovisat i avsnitt 11.1.

7.1 Företagens uppfattning om säkerheten på Internet

Alla företagen är rörande överens om att säkerheten på Internet kan bli bättre. Detta är väl ingen överraskning i sig eftersom Internet bygger på en protokollstandard, Ipv4, som helt saknar säkerhetsfunktioner. Det primära målet för Internet är öppenhet, så Internet i sig själv har ingen inbyggd säkerhet menade en respondent C. Vidare menade en annan respondent, A, att det alltid finns ”buggar”[70] i de program som används, stora som små, och att dessa är en säkerhetsrisk i sig eftersom de kan utnyttjas för en ev. attack. Respondent A menar att missar i programdesign och implementation av system samt programvara är andra säkerhetshål som företag har svårt att skydda sig mot, eftersom ingen vet att dessa problem existerar.

Respondent B tyckte att autentiseringen kunde göras mycket bättre, dvs att verifiering av att sändare och mottagare är de som de utger sig för att vara. En tänkbar lösning på detta tyckte respondenten är engångslösen. Som exempel tog respondenten upp Föreningssparbankens lösenordsgenerator. Den kräver att du har en personlig pin-kod som du anger och allt eftersom du, t ex klickar dig igenom en betalning, får du ett antal siffror som skall knappas in i generatorn, och detta leder sedan fram till ett unikt engångslösen för en specifik betalning. Eftersom jag själv använder denna typ av generator har jag tillräcklig kunskap att hålla med respondenten om att detta är en bra lösning för att säkra autentiseringen på ett bra sätt. En nackdel med denna generator är att den i mitt tycke fortfarande är lite för klumpig att bära med sig. Men som utvecklingen sett ut de senaste åren bör det enligt min uppfattning komma bättre format på denna, mycket funktionsdugliga lösenordsgenerator, inom en snar framtid.

De flesta uppfattningar är främst fokuserade på den information som finns lagrad i ett system och det är egentligen här som de största problemen även återfinns. När en transaktion utförs och transporteras över Internet via en E-handelsplats är den oftast krypterad med ett flertal kombinerade algoritmer, och detta anses vara väldigt säkert. Respondent A menade att företagen måste börja ”tänka hela vägen”. Vad han syftar på är att ta emot och lagra kunddata, informationen om sina kunder, på ett säkert sätt. Att inte bara fokusera på själva överföringen utan säkra upp sina system för hela processen, både före, under, och speciellt efter att en transaktion slutförts. Detta tycker jag är mycket viktigt och glädjande att företag tänker på, särskilt för utpräglade E-handelsbolag som endast har sin verksamhet på Internet. Den information som dessa företag lagrar om sina kunder är totalt sett värt så mycket och dessa data utgör ju grunden för hela verksamheten. Utan den har företaget ingen verksamhet längre och därmed, ingen ”business”.
Vidare kan en attack mot företag som endast finns på Internet innebära slutet då redan befintliga relationer är mycket värdefulla eftersom det blir lättare, snabbare och därmed billigare att betjäna befintliga kunder. I förlängningen kan detta visa sig vara helt avgörande för ett företags existens då det i många fall kan vara upp till 5-6 gånger så hög kostnad att

[70] källa: www.sunet.se. En oönskad och oväntad egenskap hos ett program eller hårdvara, speciellt om den egenskapen orsakar funktionsstörningar.

värva och betjäna en ny kund[71]. Detta tycker jag understryker vikten av att säkra upp sina kunddatabaser från attacker och insyn.

7.2 Krav på en säker E-handelsplats

Respondent C listade 5 saker som han tyckte var relevanta ur ett kundperspektiv:

1) Att det finns en policy för vad företaget gör med dina registrerade uppgifter, det vill säga att det klart framgår om man riskerar att hamna även i andra register.
2) Att informationen jag skickar om mig själv/mitt företag är krypterad
3) Att man kan garantera att den information jag skickar inte kan förvanskas under kommunikationen
4) Att man kan garantera att de uppgifter som finns om mig är adekvat skyddade mot intrång
5) Att webbplatsen är tillgänglig när det passar mig

Dessa krav anger respondent C sett ur ett kundperspektiv. Alltså vilka krav kunder ställer som krav när de gör en beställning på en E-handelsplats. Vidare nämner samma respondent att det i vissa fall kan vara nödvändigt med stark tvåfaktor autentisering som t ex Safeword eller SecurID. De är två autentiseringsverktyg som jag inte kommer att behandla i denna uppsats men som enligt respondent C är bra verktyg för att erhålla en säker autentisering.

Tillgängligheten för en webplats är en annan viktig faktor som förekommer på krav-specifikationer från beställande kunder. Respondent A menar att tillgängligheten är mycket viktig för en E-handelsplats eftersom du riskerar att få en negativ inställning från dina kunder om ditt system inte är tillgängligtnär kunderna vill utnyttja det. I förlängningen skadar detta naturligtvis din verksamhet. Som exempel tog respondent A det nu aktuella Love-letter viruset. Flera av de företag som hade samma ingångskanaler mot Internet för både mail och E-handelssystem tvingades att helt stänga av sin uppkoppling mot Internet eftersom viruset angrep mailservern. Samma respondent tyckte då istället att ett E-handelsföretag borde införa två separata ingångar till respektive server. En för det enskilda E-handelssystem och en annan för mailserver och den övriga åtkomsten för Internet. På så sätt menade respondent A att trots att man fått sina system angripna av någon form av attack kunde man ändå sköta sina affärer på Internet, och inte förlora marknadsandelar och därmed ”business”.

7.3 Tekniker för att säkra en E-handelsplats

Alla respondenter var rörande överens att de allra flesta krypteringsalgoritmerna ger ett tillräckligt skydd om nyckellängden för den aktuella algoritmen är tillräcklig lång. RSA är en väl använd algoritm när man talar om säkra överföringar. Denna algoritm anser både respondent A och B vara lämplig för just detta ändamål. Den nyckellängd som idag är mest vedertagen är av 1024 bitars längd, men även 2048 bitar förekommer menar respondent B. Nackdelen med sådana nyckellängder är att prestandan på överföringen bli långsammare. Idag finns det förvisso effektiva accelerationer för att snabba på krypteringsprocessen.

SSL är det mest använda protokollet när man gör elektroniska transaktioner över Internet. Detta innebär ofta att det finns ett övervägande stöd för de mest använda algoritmerna, som t ex RSA och DES. Respondent B menade att anledningen till detta var att dessa algoritmer

[71] Internet i marknadsföringen & marknadskommunikationen, Studentlitteratur 1995.

ofta ses som standard varför det ofta blir enklare att använda sig av samma algoritmer när man tvingas göra förändringar i säkerhetsarkitekturen, t ex när man ska öka på nyckellängder. Ofta använder man sig av en kombination av algoritmer när man skall kryptera en elektronisk överföring av information. PKI är en sådan teknik som använder sig av kombinerade krypteringsalgoritmer. Den använder sig av en symmetrisk algoritm för kryptering av informationen, p g a sin prestanda, och en asymmetrisk för nyckelhanteringen, för att den är säkrare. PKI även har CA som garant för de olika parterna.

Respondenterna A & B anger DES som den mest använda symmetriska och RSA för den mest asymmetrisk använda krypteringsalgoritmen. Men de poängterar även att detta inte beror på att de är bäst, utan snarare för att de används mest och stödjs därför i de flesta system.

Respondent B uppmuntrade även till frekventa byten av nycklar. Anledningen till detta är att det ger en högre säkerhet då det inte är bra att ha samma ”session nyckel” under en lång period. Ju längre du använder dig av samma nyckel desto större blir chansen att någon forcerar den. Respondent B förespråkade ett frekvent nyckelbyte på c:a 6-7h, och själva nyckelbytet kräver heller inte något större ingrepp utan görs relativt snabbt.

Men respondent A uppmuntrar även till användning av andra krypteringsalgoritmer. Exempel på en sådan algoritm är den relativt nya ECC. Även ECC finns i olika nyckellängder men respondent A menar att den är snabbare eftersom den använder sig av mindre nycklar. Respondenten menade att ECC med en 256 bitars nyckellängd kunde garantera samma säkerhet som RSA då RSA använde sig av en nyckellängd på 1024 bitar. Vidare menade han att det betraktas som en nackdel om en algoritm inte har några års ”erfarenhet” i branschen. Jag kan ha förståelse för detta resonemang eftersom en ny algoritm inte kan bevisa sin säkerhet om den inte blivit utsatt för någon som försökt knäcka den. Därför finner jag mig tveksam till ECC´s säkerhet då den i skrivande stund inte riktigt blivit utsatt för några attacker.

På frågan om SET, som jag anser vara en av de mest säkra teknikerna för att säkra elektroniska transaktioner, fick jag lite vaga svar om varför den inte används i större utsträckning. Respondent A tror att det är en kostnadsfråga för vissa företag och att det är, som han uttryckte det; ”enklare att åka med det man har". Detta har jag förståelse för, eftersom många företag idag har byggt sina E-handelsplatser på en SSL-infrastruktur, är det helt enkelt för dyrt att ändra protokollstandard.

7.4 Framtida säkerhetslösningar

Det råder lite delade meningar bland de respondenter jag intervjuat på frågan om framtida säkerhetslösningar. Något jag inte är direkt förvånad över då det naturligtvis är svårt att spekulera i en sådan bransch som hela tiden präglas av nya tekniker och anmärkningsvärda upptäckter.
Respondent A tror att framtiden ligger hos kryptering. Att starkare algoritmer med varierande nyckellängder kommer att dominera E-handel i framtiden.
Respondent B spekulerade att biometriska produkter kommer vara vanligt förekommande inom en snar framtid. Biometriska produkter använder kroppen som ditt autentiseringslösen, och redan idag finns det system som använder dina fingrar som verifiering. Kommande lösningar är genom horhinnan och sk. bodyscan.

8. Analys

I denna analys skall jag jämföra säkerheten hos de olika elektroniska betalningssätten som jag behandlat i denna uppsats. Detta görs utifrån de tre säkerhetsfunktioner som jag behandlade i kapitel 3;

- **Autentisering**, verifiering av att sändare och mottagare är de som de utger sig för att vara.
- **Konfidentialitet**, att ingen obehörig kan ta del av informationsinnehållet som överförs.
- **Signering** , att varken sändare eller mottagare kan förneka att de har sänt eller tagit emot viss information.

Jag skall dessutom jämföra fördelar och nackdelar för de säkerhetstekniker jag behandlat i denna examensuppsats. Detta skall så småningom leda fram till svaret på mina problemställningar om vilka betalningsformer som bäst uppfyller dessa krav och slutligen skall jag presentera en betalningsform som jag anser vara allra bäst.
Då det finns vissa skillnader i hur säkerhetskraven uppfylls mellan olika typer av betalningar som kan göras med kort, kommer de att redovisas var för sig.

8.1 SSL

Denna typ av betalning uppfyller både kraven på autentisering och konfidentialitet, eftersom de tillämpar kryptering med SSL. Eftersom kunden aldrig signerar sitt köp kan någon verklig (fysisk) identifiering göras, och säljaren har ingen möjlighet att kräva någon betalning. Således innebär detta att SSL inte uppfyller kravet på signering eftersom kunden aldrig signerar sina köp.

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 (SET). 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.

8.2 Smarta kort

Smarta kort uppfyller samtliga krav på autentisering, konfidentialitet och signering då de är krypterade med RSA-algoritmer. Speciellt smarta kort som använder sig av PKI, där en tredje part, CA, agerar som garant vid identifieringen av två parter. 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.

Vidare kan man fråga sig om inte de smarta korten innehåller för mycket information? I framtiden är det ingen omöjlighet att vi får se ett enda kort ersätta alla de kort som folk idag har i sina plånböcker. Ett smart kort kopplat till olika banker, personlig information etc. Sådan personlig information kan t ex vara var du bor, yrke, ålder samt blodgrupp. Men hur kan man

vara säker på att du endast lämnar ifrån dig den information som är nödvändig för just den händelsen, t ex en betalning? Hur vet man att detta inte missbrukas?

8.3 SET

Genom förfarandet som beskrivits i kapitel 5.2.2 uppfylls samtliga de krav på autentisering, konfidentialitet och signering 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. 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.

9. 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 elektroniska betalningssätt uppfyller de inblandades krav på säkerhet.
Om det är något alternativ som förefaller något mindre säkert så är det i så fall kontokortsbetalning med SSL, där butiken tar en viss risk eftersom kunden kan hävda att han inte har köpt något.

I övrigt anser jag att det inte finns speciellt mycket att anmärka på säkerheten på de betalningssätt jag behandlat. Vid samtliga typer av betalningstransaktioner används någon form av kryptering, och används rätt nyckellängder ger de enligt min åsikt 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 över Internet. Barrett säger att det är teoretiskt möjligt, men väldigt svårt[72].

Dock angav jag i min problemställning att jag skulle presentera ett betalningssätt som skulle vara bättre än övriga. Det alternativ som framstår som säkrast är utan tvekan SET. Jag anser att det inte finns något skäl att misstro de andra alternativen, men om något skall framhållas blir det trots allt SET. 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[73].

I avsnitt 5.5 tyckte jag att bankernas avsikter med SET kanske kunde ifrågasättas, och detta påstående har jag funnit stöd för bland flera källor, bl a i en intervju med Jon Karlung, vd för Bahnhof Internet (som är en Internetoperatör som bl a erbjuder företag e-posttjänster, egen domän etc.). 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 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[74].

Säkerheten är en faktor som i hög grad påverkar utvecklingen av den elektroniska handeln. Men kanske vore det mer korrekt att säga att det är gemene mans uppfattning om säkerhet som påverkar utvecklingen. Jag tror nämligen att den skepsis mot elektroniska betalningsmedel som är ganska utbredd bland folk i allmänhet, är omotiverad. Vidare tror jag att mycket handlar om hur media vinklar och framställer elektronisk handel. Om en tidning vill skapa rubriker så är naturligtvis skrämselpropaganda effektivt.

[72] Byttner, K-J. Säkerhetsexpert: Riskerna med webhandel överdrivna. CS artikelarkiv 990322.
[73] Sjögren, N. Riskfritt handla med kort på Internet CS artikelarkiv 98
[74] Lotsson, A. SET-standarden behövs inte. CS artikelarkiv 98

Dessutom tycker jag att det är anmärkningsvärt att det ofta är E-handelsbutikerna 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.

Angående 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 (SSL, och smarta kort) mycket väl uppfyller alla krav på säkerhet som rimligen kan ställas. För SSL råder det dock fortfarande problem med en riktig signering eftersom kunden aldrig signerar sina köp kan någon verklig (fysisk) identifiering göras, och säljaren har därför ingen möjlighet att kräva någon betalning.

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 E-handelsbutiker har börjat tröttna på att vänta på att SET skall bli allmänt använt[75].

Anledningen till att många E-handelsplatser tvekar till att installera SET är förmodligen därför att 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.

9.1 Framtiden

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, 1999) 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 E-handelsbutikerna väntar på, aldrig kommer.

Vidare skriver Fredholm (1998) att det kommer bli allt viktigare att synas på Internet via en webbplats[76]. 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 exempelvis telefonkatalogens gula sidor.
Lika viktigt som att synas på Internet är det också att marknadsföra sin Internetplats, att ha en riktigt genomarbetad Ebusiness-plan med reklam på lämpliga ställen, skapa en ömsesidig kontakt och ett förtroende gentemot sina kunder.

[75] Ottosson, M. Webhandlare misströstar om SET-standarden. CS artikelarkiv 990218.
[76] Fredholm. P. Elektronisk handel – Status och trender. Teldok, Telematik 2001 Rapport 121. 1998

Jag tror att det bara är en fråga om tid innan det stora genombrottet kommer för elektronisk handel. När folk i allmänhet har vant sig vid detta nya sätt att göra inköp kommer de förmodligen inte att tycka det är konstigare att handla på Internet än att handla via exempelvis 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 som finns idag för elektroniska betalningar. 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 att 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 med låg omsättning.

Min uppfattning är att om inte SET marknadsförs och blir billigare att installera inom kort så kommer branschen fortsättningsvis att se sig om efter andra -- och billigare -- alternativ.

Vidare kan man fråga sig om det inte är dags att införa en bestämd säkerhetsnivå som kan freda sig mot de flesta attackerna. Kan någon part ha rätt att kräva att en E-handelsplats uppfyller en bestämd säkerhetsnivå? Konsumenterna kanske?
Men om det skall bli en lagstiftning är det givetvis regeringen som måste agera. Om regeringen bestämmer sig för att införa en säkerhetströskel för de E-handelsplatser som finns i Sverige, tror jag att detta kan skapa en seriösare syn på E-handel. Även om många har goda avsikter på Internet finns det tyvärr en del som har andra, inte fullt så goda avsikter. Jag tror att en lagstiftning kan få många oseriösa E-handlare att avstå en sådan satsning eftersom en bra säkerhet trots allt kostar pengar. Förhoppningsvis för mycket för den oseriöse.

En klar risk med detta är naturligtvis att en sådan kostnad likväl kan få den seriöse att avstå och att det istället kan bli ett för stort hinder för många.
Detta är förstås ett problem men jag tror ändå idén om en lagstiftning om säkerhet är tillämpbar inom området för E-handel.

10. Slutsatser

Sammanfattningsvis ser mina resultat ut så här: Min första problemställning var vilka krav på säkerhet som bör ställas för att en E-handelsplats skall betraktas som säker. 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 (konfidentialitet), handlare och kund skall kunna identifiera varandra (autentisering) samt för att inte köpare och säljare ska kunna förneka att de beställt en vara respektive tagit emot betalning, måste transaktionen kunna bevisas av motparten vid en eventuell tvist (signatur).

Den andra problemställningen var att se vilka betalningsformer som uppfyller dessa krav. För att komma fram till svaret använde jag mig av både litteraturstudier och intervjuer. Resultatet jag slutligen kommit fram till är att de betalningsformer bäst uppfyller dessa krav är SET och smarta kort. Dock anser jag inte att SSL uppfyller kravet på signering. Eftersom kunden aldrig har signerat sitt köp kan någon verklig (fysisk) identifiering göras, och säljaren har därför ingen möjlighet att kräva någon betalning.

Den tredje 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 av de elektroniska betalningssätten jag undersökt är det smarta kort och SET som allra bäst uppfyller kraven, men att den allra säkraste betalningsformen är SET.

10.1 Uppslag till fortsatt arbete

Eftersom säkerhet och 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 säkerheten fungerar inom organisationen. Att det är viktigt för ett företag att ha klara riktlinjer för den interna säkerheten har givetvis lika stor betydelse som hur den skyddar sig mot externa hot. T ex med behörighetsnivåer, lösenordshantering, externa inloggningar på företagets server och liknande. Det skulle kunna ske antingen som litteraturstudie, eller ännu hellre ute på ett företag som just står i begrepp att utarbeta eller att se över sina riktlinjer för den egna organisationen.

Det borde kunna ge en god inblick i och förståelse för företagens villkor och var svårigheterna och problemen för företagen ligger. Jag tror att mycket kan göras där, om det kan utredas vilka behov företagen har.

11. Referenser

Böcker

Bergdahl, T. Smarta kort - teknik och tillämpning i USA 1995

Dahmström, D. Från datainsamling till rapport 1991

Efraim Turban. Electronic Commerce, 1999.

Jakobsson, P. Internet i marknadsföringen & marknadskommunikationen
Studentlitteratur 1995.

Patel, P & B, Davidsson Forskningsmetodikens grunder 1994

Rönn, J. SET-fiaskot: en miljon kronor per transaktion. 1999

Sundström, M. Hur används aktiva kort i offentlig förvaltning 1996

SIG Security. Säkerhetsarkitekturer 1998

Toppledarforum, Remissutgåva av Säkrare IT i offentlig sektor 1996

Wigblad, R & Åhlgren, K. Elektronisk handel i små och medelstora företag.
(En antologi medåtta resultatrapporter). Högskolan i Örebro 1998

Artiklar

Byttner, K-J. Säkerhetsexpert: Riskerna med webhandel överdrivna. CS artikelarkiv 990322.

Gustafsson, J. Digital Identitet i Finland. Nätverk & Kommunikation 000125

Lotsson A. RSA-kryptot knäckt. CS Artikelarkiv 990913

Lotsson A. Standardkryptot knäckt för länge sen. CS artikelarkiv 991126

Lotsson, A. SET-standarden behövs inte. CS artikelarkiv 98

Lotsson, A. Tryggheten med kryptering en farlig illusion. CS 991104

Ottosson, M. Webhandlare misströstar om SET-standarden. CS artikelarkiv 990218.

Ricknäs, M. Öppenhet nyckeln till ny krypteringsstandard. CS 000413

Sjögren, N. Riskfritt handla med kort på Internet CS artikelarkiv 98

Rapporter

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

Johansson, Rikard, *Krypteringsteknik – nyckeln till säkerhet*?. (Utlandsrapport från Sveriges tekniska attachéer. USA; 9817).

Ur regeringens skrivelse till riksdagen Skr. 1998/99:116 ang kryptografi, Bilaga 2

Websidor

http://www.id2.se/whitepapers/smartcards.asp

http://www.setco.com

http://www.set-guide.com/

http://www.ssh.fi/tech/crypto/algorithms.html

http://www.ssh.fi/tech/crypto/protocols.html#ssl

http://www.ssl.com

http://www.ssl.com/n_privacyB.htm

11.1 Intervjuer

Respondent A

Robert Malmgren - Robert Malmgren AB
Konsult som driver ett eget företag inom säkerhetslösningar.
2000-05-18

Respondent B
Ulf Holmqvist - Protect Data AB
Produktspecialist inom VPN och PKI.
2000-05-19

Respondent C
Per Albinsson - Atremo AB
Atremo AB arbetar som en IT-säkerhetspartner inom området säker kommunikation. Fokus är säkra internetförbindelser - brandväggar, VPN-lösningar och antivirus.
Per Albinsson arbetar som projektledare.
2000-05-18

11.2 Intervjufrågor

1. Namn och befattning.
2. Berätta om företaget och vilka Dina arbetsuppgifter är?
3. Vilken är Din uppfattning om säkerheten på Internet?
4. Vilka krav ställer Ni på en säker E-handelsplats?
5. Vilka tekniker anser Ni uppfyller dessas krav?
6. Vilka används mest frekvent?
7. Hur upplever Ni problematiken med att hålla en säker E-handelsplats och samtidigt ha en hög funktionalitet?
8. Vilka säkerhetstekniker tror Du kommer att dominera E-handel om c:a 2år?
9. Har du något övrigt att tillägga?