Institutionen för Informatik
Göteborgs Universitet

Magisteruppsats 20p vt98

Säker Elektronisk Transaktion

Sammanfattning

Den elektroniska handeln på Internet växer i en mycket snabb takt. Men många kunder känner fortfarande tveksamhet över hur säkert det är att handla över Internet. Säker Elektronisk Transaktion eller SET som det kallas i dagligt tal är en ny teknisk standard för kontokortsbetalningar över nätet. I och med att det är många stora världsledande företag så som Visa, MasterCard, Microsoft, IBM och Netscape som ligger bakom framtagandet av SET, så kommer SET i framtiden att vara det dominerande betalsystemet för Internethandeln. De involverade företagen försöker med alla medel att få SET att bli en de de facto standard vilket har gjort att de lämnat alla tekniska specifikationer öppna så att andra företag själva kan utveckla egna applikationer.

Av: Ergun Tuna

Innehållsförteckning

1 Inledning

Handel över Internet har blivit en väldigt populär företeelse. Nu håller man på att utveckla system så att man skall kunna betala över Internet. Och detta är en väldigt ny företeelse. Man tror att det kommer att öka avsevärt under de närmaste åren. Enligt marknadsundersökningsföretaget Killen & Associates väntas omsättningen uppgå till mellan 7 och 9 miljarder dollar år 2000, där de flesta av dessa inköp kommer att ligga under 10 dollar. Det vanligaste sättet att handla över Internet fram till idag var att beställa varan för att sedan betala på det traditionella sättet.

Det finns en rad olika metoder för hur handel över Internet kan ske. Vissa är bra medan andra är mindre bra. Det jag skall ta upp i min uppsats är kontokorts användningen över Internet med hjälp av SET-standarden. I en snar framtid så tror man att betalningar över Internet kommer att öka radikalt. För tillfället så är man lite skeptiskt till hur säkert det är att handla över Internet. Men skulle systemet vinna kundernas förtroende så skulle det innebära ett stort genombrott. Vem skulle inte vilja betala sina räkningar hemifrån istället för att gå till posten eller banken? Största frågan är egentligen hur säkert SET är. I denna uppsats så skall jag försöka att svara på denna fråga.

SET-pilotprojektet startades under hösten 1996 med kontoorganisationen Visa tillsammans med banker som finns över hela världen. Under Visas regi så deltar ett fyrtiotal banker över 16 europeiska länder i ett pilotprojekt sedan oktober 1996. Detta är den europeiska piloten som genomförs i Europa. Bankerna som deltar från Sverige är Handelsbanken, Postgirot, S-E-Banken och Sparbanken. Pilottesten inleddes under januari 1998, och det skall lanseras senare i år då man räknar med att systemet skall ha utvecklats klart för kortinnehavare, banker och handlare. MasterCard och Visa har tillsammans tagit fram en symbol som betecknar säkra betalningar över Internet och den symbolen kommer att läggas ut på den sidan som det är säkert att handla från.

SET-standarden skapar nya möjligheter till att betala sina räkningar. Varför skall man gå till banken eller posten när du kan göra det hemifrån? I och med Internets framtåg så ökar intresset för elektronisk handel från de flesta aktörer som är inblandade i varor eller tjänster i marknaden. Det har varit många olika företag som har ställt sig i kö för att vara med i SET-pilotprojektet som ger plats för runt 30 säljställen. Jag tror att konsumenterna kommer att känna större förtroende för systemet, vilket i sin tur kommer att leda till fler och större transaktioner. För närvarande så är det inte stora summor som läggs ut, men snart kan man tänka sig att köparen lägger ut en stor summa i form av ett t ex inköp av ett hus. Med hjälp av SET så skall kortinnehavare och handlare kunna utföra transaktioner över Internet lika säkert och enkelt som om att betala med eller ta emot kort i butiker. I och med att köpet sker inom ramen för SET, så vet både säljaren och köparen att betalningen sker säkert och korrekt, precis som vid ett vanligt kortköp. Med tanke på de garantier SET ger så kommer troligen den elektroniska handeln att ta fart under det kommande året.

1.2 Vad är SET ?

Det pågår ett projekt som kallas för SET, Secure Electronic Transaction (Säker Elektronisk Transaktion). Fyra banker har inlett ett samarbete med varandra för att införa SET standarden.

Om en person eller ett företag som är en Visakortskund hos en av dessa fyra banker så kan man köpa eller sälja varor från vilken del av världen som helst förutsett att denne använder sig av SET-systemet.

Flera företag har samarbetat under de senaste åren för att komma fram med en standard, och detta blev slutligen känt som SET. Det är meningen att det skall användas till att på ett säkert sätt betala räkningar över öppna nätverk så som Internet. SET är en branschstandard som MasterCard och Visa har tagit fram med hjälp av en rad data- och IT-företag, däribland Netscape, IBM, och Microsoft.

Med SET så möjliggörs det att man kan ange kontonumret när man handlar men det är ändå säkert att ge ut sitt eget kontonummer därför att systemet bygger på kryptering. Tekniken bygger på att två parter, Visakortsinnehavaren och försäljningsstället, byter nycklar - en serie siffror och tecken - som krävs för att koda och avkoda meddelande. Det går inte att läsa meddelanden utan dessa nycklar. Meningen är den att med hjälp av SET så skall informationen behandlas konfidentiellt, så att både kontokortsinnehavaren och handlaren är den man säger sig vara och att kunden kan godkänna sina köp precis som man gör det idag.

Anledningen till att man krypterar är att för den som kan så är det ganska smärtfritt att avlyssna ett meddelande och se vad det står på det. Men med hjälp av SET-standarden så krypteras meddelandet när man skickar det och avkodas när man tar emot och öppnar meddelandet. Den information som skickas skyddas med nycklar, så att inga obehöriga kommer åt att läsa eller ändra på informationen. Själva krypteringen sker i flera led, både i bankens, säljföretagets och kontokortsinnehavarens datorer. Med ett sk digitalt certifikat skickas kontonumret i krypterad form över Internet, där det digitala certifikatet kopplas till det aktuella Visa-kortet vid en SET-transaktion. Detta kallas för ett virtuellt kontokort, och är speciellt skapade för varje part i det elektroniska handelssystemet. Varje kortinnehavare och säljföretag får ett eget digitalt certifikat från banken. Båda parter måste ha ett certifikat innan de kan köpa eller sälja. Precis som ett kontokortsköp i en butik där man skriver sin namnteckning, så finns det en digital signatur som visar att kontokortsinnehavaren är den person de utger sig för att vara.

Rent användningsmässigt så fungerar det ungefär som vid en kontokortstransaktion, med skillnaden att man använder sig av digitala certifikat i samtliga led. Som jag har nämnt tidigare så menas ett digitalt certifikat att det är ett virtuellt Visakort istället för ett fysiskt. Banken vet inte vad det är som är inköpt men de vet vem det är som har gjort inköpet. Säkerhetsmässigt är detta bra därför att allt är krypterat och säkrat i alla led. Vill man vara med och handla via SET så måste man söka det digitala certifikaten hos sin bank. När man ansöker om ett kontokort i framtiden så kommer detta troligtvis att utfärdas både i form av en plastbricka och som ett digitalt certifikat om man så önskar. Verisign som är underleverantören till Visa kontrollerar alla ansökningar som kommer in och ger sedan ut certifikaten. Om man därefter vill handla så laddar man ner SETs färdiga mjukvaruprogram till sin dator. Skulle man jämföra vanliga kontokort med certifikaten så skulle man se att innehållet skulle vara likadan plus att certifikaten har digitala nycklar. I en handlares digitala certifikat innehålls information om handlaren, förbindelser med banken och certifikatets utfärdare samt handlarens nycklar. För att någon som helst information skall kodas, transporteras och avkodas så måste de digitala certifikaten godkännas i båda parternas datorer.

Här följer en kort beskrivning av vilka processer som sker när man handlar över Internet med SET.

1. Man besöker den plats på nätet som man vill handla från och fyller sin shoppingkorg. När man är klar så klickar på knappen ”köp med kontokort”.
2. Ett certifikat skickas från butiken till kunden. När certifikatet skickas från butiken så krypteras det och när man tar emot det så dekrypteras det och kontrolleras av kundens elektroniska plånbok för att fastställa om butiken är en legitim butik som tar ens kontokort.
3. Nu skickas kundens eget certifikat till butiken i krypterad form av den elektroniska plånboken så att butiken skall se ifall jag är den jag påstår mig att vara. Men butiken kan inte se alla uppgifter som man har skickat. Betalningsordern innehåller två delar: en okrypterad och en krypterad. I den okrypterade finns det uppgifter om namn, adress osv. Medan i den krypterade så finns din egen kortinformation.
4. Betalningsordern skickas vidare av butiken till butikens egen bank. Bankens betalningsport tar emot transaktionen. Denna betalningsport översätter betalningsordern och slussar in det i det befintliga kontokortssystemet. Nu finns det ingen skillnad mot att om man hade köpt en vara från en verklig butik.
5. Nu skickas transaktionen via bankernas clearingsystem till min egen bank som ser efter om jag har pengar på kontot. Ett svar skickas till butiken som nu kan leverera varan.
6. Efter det att varan är levererad så skickas det en ny transaktion då det är nu den verkliga betalningen sker. I steg 5 så reserverades endast pengarna på ditt konto. Den riktiga betalningen sker alltid först då varan har levererats.

1.3 Problemdefinition

Konsumenterna har hittills varit tveksamma till elektronisk handel. Folk har inte litat på det nya betalningssättet utan de har gjort sina betalningar på de traditionella sättet. Inte nog med att företag har tagit fram nya och säkra system utan de måste också ändra konsumenternas attityder gentemot den nya tekniken. SET är ny standard som har tagits fram av stora företag för elektronisk handel över nätet. Det är alltid svårt att ändra en persons attityd om någonting, men den här uppsatsen syftar till att visa att det är säkert att göra transaktioner med SET.

1.4 Syfte

Syftet med uppsatsen är dels att ge en liten överblick över ett par av de vanligaste kontokorts systemen som finns och dels att ge en mer noggrann inblick över den nya standarden SET. Dessutom så vill jag få fram att SET är en säker källa på att göra transaktioner över nätet. T ex så är krypteringen lika stark som hos det man använder i militären. Det stora debattämnet är fortfarande hur säkert det är att handla på Internet. Med denna uppsats så vill jag visa att det är minst lika säkert som när man handlar i en butik med hjälp av kontokort.

1.5 Avgränsning

Jag kommer att avgränsa mig till att behandla och beskriva SET. Men för att få lite inblick och se vad skillnaderna och likheterna är så skall jag beskriva lite kort av ett par av alla systemen och modellerna som finns. Men jag kommer inte att behandla t ex den matematik som ligger till

grund för krypteringen i de olika system utan de kommer bara att nämnas och beskrivas i korta drag.

1.6 Insamling av data

De företag som erbjuder betalsystem över Internet har ganska stora resurser på nätet i form av WWW-sidor, där man bl a kan hämta dokumentation för de olika betalsystemen. För att få kunskap och åsikter från de personer som jobbar med SET i det dagliga arbetet, så har gjort intervjuer via telefon och e-post. Jag hittade de personer som intervjuades via nätet. Först fick jag ta kontakt via telefon och frågade ifall det gick bra att intervjua dem. Alla de fyra personer som intervjuades var villiga att ställa upp, men tyvärr så fick jag inte svar från två personer. Frågorna skickades via e-post och de fick svara i lugn och rå, men en nackdel kan vara att det blir svårt att ställa motfrågor för att förtydliga respondentens svar, detta kunde emellertid lösas med att man kunde ringa upp respondenten för att ställa följdfrågor. De frågor som ställdes är både lite tekniska och generella.

Den data som jag har samlat från Internet har mestadels varit från de företag och banker som har varit inblandade i framtagandet av systemet. I och med det så kan jag känna mig ganska säker på att informationen är tillförlitligt. Det bästa hade varit att intervjua personerna ansikte mot ansikte, men i och med att alla kontakter som jag hittade var utanför Göteborg så fick jag hålla mig till telefon och e-post. När man sökte på SET så fick man så många träffar att det inte är möjligt att gå igenom alla. Man fick göra sitt bästa med att sålla bort ”oviktig” information.

2 Elektronisk handel

Handel över Internet beräknas att växa kraftigt under de närmaste åren. Hittills så har det funnits lite enklare sorter av handel i form av att man t ex har beställt en bok men betalningen har inte skett på Internet utan man fick göra det på det traditionella sättet. Nu håller man på med att utveckla system så att man skall kunna betala över Internet.

Betalningssystem med kontokort över Internet kan delas in i tre delar:

- Överföring av okrypterad kontokortsinformation till handlaren
- Överföring av krypterad kontokortsinformation till handlaren
- Överföring av krypterad kontokortsinformation eller kortkod till en tredje part som handhar transaktionen

2.1.1 Överföring av okrypterad kontokortsinformation till handlaren

Man skickar sitt kontokorts nummer tillsammans med den information som man får fylla i via ett ifyllningsformulär eller med e-post till handlaren över nätet. Om man handlar via den här metoden så kommer man förr eller senare att råka illa ut, därför att bristen på säkerhet är väldigt stor. En tredje part kan ta upp informationen och sedan missbruka den. Och skulle man få hem en räkning på flera tusenlappar och inser att du inte har köpt de varorna så lär det inte bli en trevlig överraskning. Därför skall man vara väldigt försiktig när man skickar känslig information på Internet.

2.1.2 Överföring av krypterad kontokortsinformation till handlaren

Informationen krypteras innan den skickas iväg på nätet. Denna företeelse försvårar för obehöriga att komma över informationen. Fast det finns inga garantier för att handlaren som får ta del av informationen inte missbrukar det.

2.1.3 Överföring av krypterad kontokortsinformation eller kortkod till en tredje part som handhar transaktionen

Här kan man låta en tredje part att sköta betalningarna. Denne tar hand om transaktionen och sköter själv kontakten med banken samt informerar handlaren om köpet kan godkännas eller inte. Här får handlaren bara den information som behövs för att leverera varan och får således inte ta del av kontokortsinformationen. Man kan skapa en viss anonymitet i form av att handlaren inte behöver veta vem konsumenten är och banken kan inte se vad som köpts.

Nedan så finns en kort beskrivning av andra befintliga system som finns. Anledningen till att jag har tagit med är att man skall kunna se hur de olika systemen är uppbyggda och vilka likheter/skillnader som finns.

2.2.1 SSL

SSL (Secure Sockets Layer) är ett säkerhetsprotokoll som Netscape har utvecklat för säker överföring av data mellan två parter. Det protokoll som SSL använder ligger mellan transportprotokollet (ex TCP) och applikationsprotokollet (HTTP, Telnet, NNTP eller FTP). Först skall man mellan två parter komma överens om en gemensam hemlig nyckel, samt identifiering av varandra, som sker med RSA publik nyckelkryptering. För att säkra överföringen så används en rad krypteringstekniker, såsom RC2, RC4, IDEA, DES, trippel DES och MD5.

Den 24 juni 1997 så tillät USAs regering export av 128-bitars krypteringsnyckel för Netscape och Microsoft. I och med detta så finns den tillgänglig i SSL protokollet som bl a är inbyggt i respektives webläsare. Denna nya nyckeln ökar säkerheten avsevärt jämfört med tidigare då man ”endast” hade en nyckellängd på 40-bitar. Utanför USA får den nya nyckeln endast användas vid kommunikationen mellan kunder och certifierade banker. När systemet känner av att det är en godkänd användare, m h a digitala certifikat, så kopplas den högre säkerheten på och används sedan under hela kontakten. Om man saknar certifikatet så används 40-bitars nyckeln.

2.2.2 SIPS (CyberCash)

CyberCash har deltagit i utformningen av SET, vilket gör att deras eget system i stor utsträckning liknar SET. CyberCash har dessutom tänkt att i framtiden implementera SET i sitt system. Det betalningssystem som CyberCash använder sig av kallas för SIPS (Secure Internet Payment Service). Man kan säga att systemet fungerar som en förbindelseagent med servrar som länkar till det nätverk som används av banker för elektroniska transaktioner. För att kunna göra transaktioner med CyberCash så krävs det att handlaren installerar programmet ”Cash Register” som går att använda på de flesta webservers. Kunden bör också skaffa sig en elektronisk plånbok. Man kan ladda ner dessa två program som finns tillgängliga gratis på nätet från CyberCashs hemsida. När kunden installerar den elektroniska plånboken skapas det en privat och en publik RSA nyckel för kunden. Genom att kunden trycker på betalknappen på en handlares hemsida när denne vill köpa något, så startas kundens plånbok automatiskt. Där kan kunden välja vilken betalningsmetod som skall användas, kontokort, check eller kontanter. Efter det att kunden har bekräftat köpet så signerar och krypterar kundens programvara betalningsordern samt annan information, t ex kontokortnummer, om det behövs. Handlaren tar emot ordern och kontrollerar att uppgifterna stämmer, men handlaren kan inte se kundens kontoinformation. En debiteringsorder läggs sedan till av handlaren som krypteras och signeras av dennes privata nyckel, och allt detta skickas till en CyberCash server som är kopplad till det vanliga banknätet. Servern dekrypterar informationen och kontrollerar att det är äkta och det skickar betalningsordern vidare till banken om allt är okej. Ett meddelande kommer till handlaren om att affären kommer att genomföras och kunden kan då få sin vara av handlaren. En likhet mellan SET och CyberCash är att bägge systemen använder sig av DES- och RSA-kyptografi för att skydda informationen.

2.2.3 Verifone

Verifone har ett system för handlare på Internet som används tillsammans med Microsoft Merchant Server. Verifone har deltagit i testerna av SET och de använder sig av SET-specifikationen och RSA publik nyckelkryptering i sitt system. För att en kund skall kunna handla över Internet så får man gå till en sida på nätet som tillhandahåller betalning med Verifone. Kundens kontokortsnummer och orderinformation krypteras med den SSL-teknik som finns inbyggd i webläsaren innan det skickas iväg till handlaren och dess programvara som heter vPOS. Denna lägger till en krypterad behörighetsbegären och skickar allt vidare med SET till en bank som dekrypterar informationen och bekräftar att uppgifterna är riktiga. Om allt är okej så krypterar banken uppgifterna igen och skickar tillbaka dem till handlaren tillsammans med ett godkännande. Ett digitalt kvitto skapas av handlarens VPOS program, där kvittot skickas till kunden och affären avslutas.

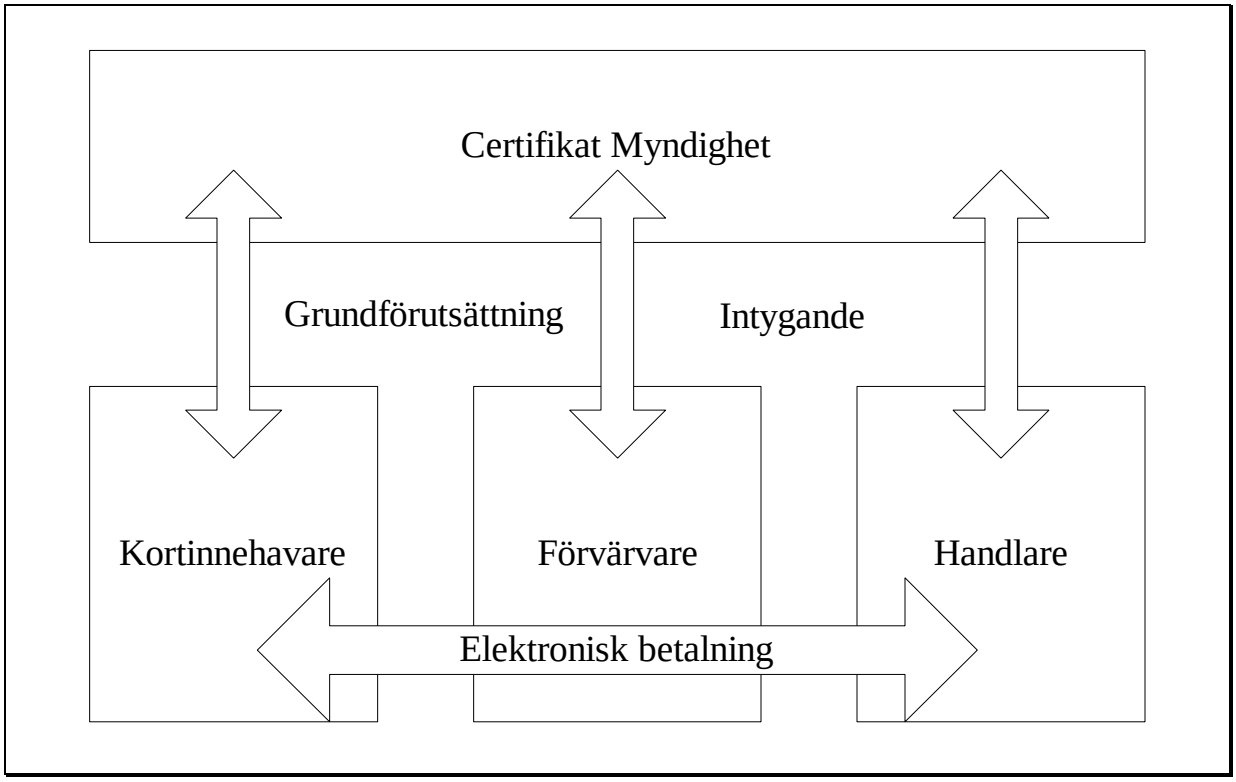
Med hjälp av sin webläsare så kan kunden göra betalningar utan att behöva installera några andra program. Man har dock nyligen kommit fram med en elektronisk plånbok, vWallet, som kan användas, till att lagra information om bl a kontokortsnummer och tidigare köp, på kundens dator. En markant skillnad från det tidigare är att med vWallet så krypteras de känsliga uppgifterna med SET även mellan kundens dator och handlarens server.

Det är inte lämpligt att göra mikrobetalningar med tanke på det kostnader som tillkommer. En likhet med SET är den att det inte går att överföra pengar mellan två privatpersoner.

3 Säker Elektronisk Transaktion - SET

3.1 Omfattning

I den elektroniska handelsomgivningen, så har nya möjligheter för handlare att sköta affärer dykt upp beroende på den växande utsättandet och åtkomsten av konsumenter för information angående deras produkt och service. Konsumenter kommer att vara kapabla att handla, komma åt information, och betala för varorna och servicen. Till skillnad från ansikte-mot-ansikte eller brev order/telefon order transaktion, så påbörjas elektroniska behandlingar av betalningar med kortinnehavaren snarare än handlaren eller förvärvaren. Med dessa nya möjligheter, så kommer det att vara nya utmaningar som behövs hanteras för att underlätta betalningar via elektronisk handel på ett säkert sätt. Figur 1 här nedan beskriver SET-betalnings system deltagare och deras interaktioner.



Figur 1: Betalningssystem deltagare

Elektronisk handel kommer i normala fall att fortgå från följande faser. SET stödjer tre av dessa faser: a) betalnings bemyndigande och transport, b) bekräftande och förfrågning, c) handelsman återbetalning.

- Titta och handla
- Handel och artikel selektion
- Förhandling och beställning
- Betalnings selektion
- SET -> Betalnings bemyndigande och transport
- SET -> Bekräftande och förfrågning
- Leverans av varor

- SET -> Handelsman återbetalning

SETs förhållande med de andra faserna av den elektroniska handelsmodellen beskrivs i följande tabell. SET fokuserar på faserna 5, 6, 7, och 8.

FAS	BESKRIVNING
1	Kortinnehavaren tittar efter artiklar. Detta kan åstadkommas på ett antal sätt, så som: • användning av en browser för att titta på en on-line katalog i en handlares WWW-sida • genom att titta på en katalog i en CD-ROM som har anskaffats av handlaren, eller • genom att titta på en pappers katalog.
2	Kortinnehavaren väljer de artiklar som skall köpas från en handlare.
3	Det överlämnas en orderformulär som innehåller en lista av artiklarna, deras priser, och en total pris som inkluderar frakt, hantering, och skatt, till kortinnehavaren. Denna orderformulär kan levereras elektroniskt från handlarens server eller så skapas det på kortinnehavarens dator genom den elektroniska handelsmjukvaran.
4	Kortinnehavaren väljer vilka medel som skall användas vid betalning. SET fokuserar på fallet när ett betalningskort väljs.
5	Kortinnehavaren skickar en komplett order tillsammans med vilka medel som skall användas till handlaren. I SET, så signeras ordern och betalningsinstruktioner digitalt av kortinnehavare som innehar ett certifikat.
6	Handlaren kräver ett betalningsbemyndigande från kortinnehavarens finansiella institution via förvärvaren. Om bemyndigandet lyckas, så kan handlaren skicka en bekräftelse av ordern till SET.
7	Handlaren skickar iväg varorna eller utför den service som stod skriven i ordern.
8	Handlaren begär betalning från kortinnehavarens finansiella institution via förvärvaren.

3.2 Affärs kraven

De sju affärs kraven för SET är:

1. Skapa konfidentiella betalningsinformationer och göra det möjligt för konfidentiella order informationer som är vidarebefordrade tillsammans med betalningsinformationer.
2. Försäkra integriteten av alla vidarebefordrade data..
3. Garantera äktheten så att en kortinnehavare är en legitimerad användare av en betalningskortskonto.
4. Garantera äktheten så att en handlare kan acceptera betalningskortstransaktioner genom sina relationer med en förvärvad finansiell institut.
5. Försäkra så att den bästa säkerhetsmetoden och systemdesigner används för att skydda alla legitimerade inblandade i en elektronisk handelstransaktion.
6. Skapa ett protokoll som varken beror på transportsäkerhetsmekanismen eller förhindrar användningen av den.
7. Underlätta och uppmuntra inbördes opebariteten bland mjukvara och de personer som förser oss med nätverk.

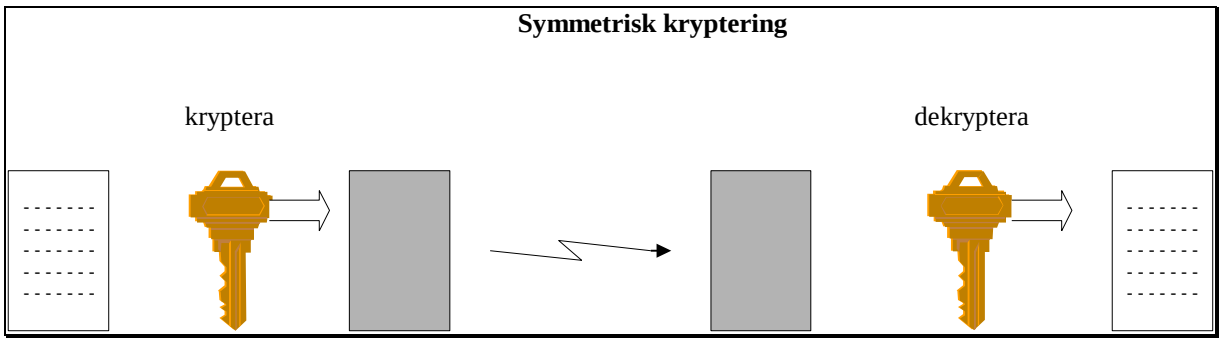
3.3 Överföringskanaler

I den symmetriska krypterinsmetoden så krävs det tillgång till två kanaler, en säker kanal där lösenorder överförs och en osäker kanal där data överförs. I praktiken överförs lösenordet via ett telefonsamtal (om det nu kan kallas för en säker kanal) medan själva data överförs på Internet. Detta är inte särskilt praktiskt för elektronsik handel. I den asymmetriska krypteringsmetoden så skickas både lösenordet och data på en enda kanal. Det kanske låter som en mindre lyckad idé, men är möjligt tack vare att varje användare har två nycklar (lösenord): en privat och en offentlig. I och med detta så behöver man inte en säker kanal för att överföra lösenord, och det betyder att asymmetrisk kryptering är lämplig för elektronisk handel.

3.4 Kryptografi

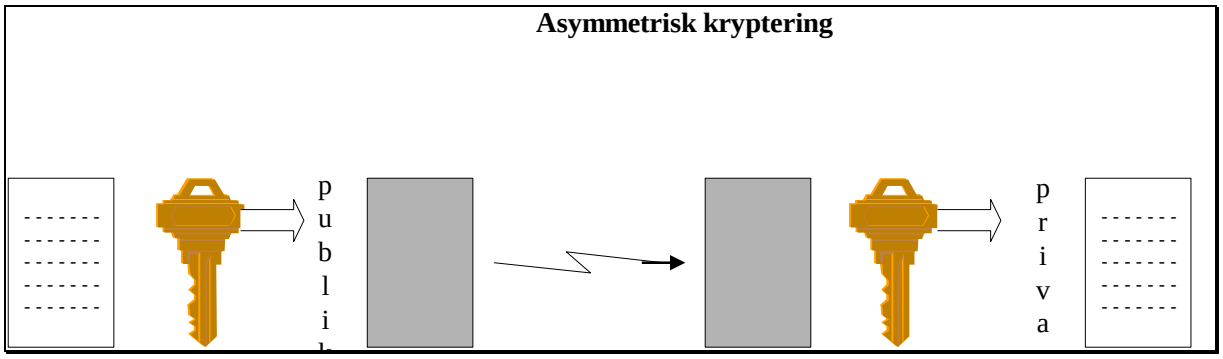
Ett meddelande krypteras med hjälp av en nyckel i ett krypterad system. Den resulterande chiffertexten skickas till en mottagare där den dekrypteras med hjälp av en nyckel för att producera det ursprungliga meddelandet. Det finns två primära krypteringsmetoder som används idag: symmetrisk kryptering och asymmetrisk kryptering. SET använder sig av båda metoderna i sin krypterings process.

Symmetrisk kryptering använder samma nyckel för kryptering och dekryptering av meddelandet. I och med detta så måste sändaren och mottagaren dela på en hemlig nyckel när ett meddelande skickas. En välkänd symmetrisk kryptografisk algoritm är Data Encryption Standard (DES), som används av finansiella institutioner för krypteringen av personliga identifikationsnummer.



Figur 3a: Symmetrisk kryptering

Asymmetrisk kryptering använder två nycklar: en nyckel för att kryptera meddelandet och en nyckel för att dekryptera meddelandet. De två nycklarna är matematiskt beroende av varandra på så sätt att det meddelandet som krypteras kan bara dekrypteras med den andra nyckeln. Varje användare har två nycklar: en publik nyckel och en privat nyckel. Användaren distribuerar den publika nyckeln. I och med relationen mellan dessa två nycklar, så kan användaren och någon som tar emot den publika nyckeln vara säker på att den data som är krypterad och skickad med den publika nyckeln kan bara dekrypteras när användaren använder sig av sin privata nykel. Men denna försäkran erhålls bara ifall användaren försäkrar sig om att den privata nyckeln inte har avslöjats för någon annan. Därför så borde bägge nycklarna genereras av användaren. Den mest kända publik-nyckel kryptografiska algoritmen är RSA.



Figur 3b: Asymmetrisk kryptering

Hemlig-nyckel kryptografi är opraktiskt för utbyte av meddelanden med en stor grupp av okända korrespondenter över ett publikt nätverk. För att en handlare skall sköta sina transaktioner säkert med miljoner andra Internet användare, så krävs det att varje konsument skulle behöva en tydlig nyckel tilldelad av handlaren och vidarebefordra den över en separat säker kanal. Å andra sidan så kan man med hjälp av den publika-nyckel krypteringen, se till att en och samma handlare skulle kunna skapa publik/privat nyckelparen och publicera den publika-nyckeln så att man tillåter någon konsument att skicka ett säkert meddelande till den handlaren.

3.4.1 Användning av symmetriska nyckeln

SET beror på kryptografi för att försäkra att ett meddelande blir konfidentiell. I SET, så kommer meddelandedata att krypteras med användning av en slumpmässig genererad symmetriskt krypterad nyckel. Denna nyckel, i sin tur, kommer att krypteras med användning av meddelandemottagarens publika nyckel. Detta refereras till som ”digital plånbok” av meddelandet och sänds till mottagaren tillsammans med det krypterade meddelandet. Efter det att man har tagit emot den digitala plånboken, så dekrypterar mottagaren det genom att använda sig av sin egen privata nyckel för att erhålla det slumpmässigt genererade symmetriska nyckeln och använder sedan den symmetriska nyckeln för att låsa upp det originella meddelandet.

3.4.2 Behov av en tillförlitlig tredje part

Innan bägge parterna kan använda sig av asymmetrisk kryptografi för att uträtta affärer, så vill båda parterna vara säkra på att den andra parten är äkta. Innan Kalle accepterar ett meddelande med Evas digitala signatur, så vill han vara säker på att den publika nyckeln tillhör Eva och inte någon som utger sig att vara Eva. Ett sätt att vara säker på att den publika nyckeln tillhör Eva är att ta emot meddelandet över en säker kanal direkt från Eva. Hursomhelst, i det flesta situationerna så är denna lösning opraktiskt.

Ett alternativ till säker överföring av nyckeln är att använda sig av en tillförlitlig tredje part för att bestyrka att den publika nyckeln tillhör Eva. En sådan part är känd som en certifikat-myndighet. Certifikatmyndigheten verifierar Evas fordran enligt dess publicerade hållning. Till exempel, en certifikatmyndighet kunde förse certifikat som skulle kunna erbjuda en hög säkerhet av personlig identitet för att uträtta affärs transaktioner; denna certifikatmyndighet

kan komma att kräva Eva till att presentera ett körkort eller pass till en offentlig notarie innan ett certifikat utfärdas. När väl Eva har skaffat bevis för hennes identitet, så skapar certifikatmyndigheten ett meddelande som innehåller Evas namn och hennes publika nyckel. Detta meddelande, känd som ett certifikat, är digitalt signerat av certifikatmyndigheten. Det innehåller ägare identifikationsinformation, och en kopia av en av ägarens publika nycklar (”nyckel utväxling” eller ”signatur”). För att utnyttja den största fördelen, så borde certifikatmyndighetens publika nyckel vara känd till så många personer som möjligt. Följaktligen, genom att lita på en enda nyckel, så kan en hel hierarki etableras där man kan hitta en hög grad av förtroende.

Eftersom SET användarna har två nyckelpar, så har de också två certifikat. Bägge certifikaten skapas och signeras samtidigt av certifikatmyndigheten.

3.4.3 Certifikatmyndighetens funktioner

Det primära funktionerna för certifikatmyndigheten är att:

- ta emot registreringsbegäran
- bearbeta och godkänna/avvisa begäran
- utfärda certifikat

Process flödet beskriver dessa funktioner så som om de var utförda av en enda enhet, men de kan faktiskt utföras av en till tre enheter. Betalningskortsorganisationer (så som Visa och MasterCard) och individuella finansiella institutioner kommer att granska deras affärs behov för dessa funktioner för att välja en lösning för implementation. Den valda lösningen kan vara så att man implementerar en singel-server som förser certifikatmyndighetens funktioner eller multipla servers som distribuerar utförandet.

Följande lista föreslår några möjliga arrangemang med variationer på distribuering:

- Ett företag som utfärdar ägarkort kan utföra alla tre stegen för sina kortinnehavare.
- En finansiell institution kan ta emot, utföra, och godkänna certifikat önskemål för sina kortinnehavare eller handlare, och vidarebefordra informationen till lämpliga betalningskortsorganisationer för att utfärda certifikaten.
- En oberoende registreringsmyndighet som utför certifikat för betalningskortsapplikationer för multipla betalningskortsorganisationer kan ta emot certifikat begäran och vidarebefordra de till en lämplig finansiell institution för utförandet; den finansiella institutionen vidarebefordrar godkända begäran till betalningskortsorganisationer för att utfärda certifikaten.

Dessa scenarios föreslår några möjliga arrangemang. Betalningskortsorganisationer och finansiella institutioner kommer att välja en lämplig lösning baserade på deras individuella affärsbehov.

3.4.4 Användning av meddelandesammandrag

När man kombinerar nycklarna med meddelandesammandrag, så tillåts man att använda privata nyckeln för digitalt signering av meddelanden. Ett meddelande sammandrag är ett värde genererad för ett meddelande (eller ett dokument) som är unikt för just det meddelandet. [1] Ett meddelande sammandrag genereras genom att meddelandet passerar genom en en-vägs kryptografisk funktion; vilket, en som inte kan reserveras. När ett sammandrag av ett meddelande krypteras genom användning av sändarens privata nyckel och är fäst till det originella meddelandet, så är resultatet känt som den digitala signaturen av meddelandet. Mottagaren av den digitala signaturen kan vara säker på att meddelandet verkligen kom från sändaren. Och, därför att en förändring av ett enda tecken i meddelandet ändrar meddelandesammandragen på ett oförutsägbart sätt, så kan mottagaren vara säker på att meddelandet inte var ändrat efter det att meddelandesammandraget genererades.

[1] Algoritmen som används av SET genererar 160-bit meddelandesammandrag. Algoritmen är sådan att ifall man ändrar en enda liten bit i meddelandet så förändras, på genomsnitt, hälften av biten i meddelande sammandraget. I stora drag, så är oddsen till att två meddelanden kommer att ha samma meddelande sammandrag är en på 1000,000,000,000,000,000,000,000,000,000,000,000,000,000. Det är okänsligt uträknat att generera två olika meddelanden som har samma meddelandesammandrag.

3.4.5 Dubbla signaturer

SET introducerar en ny applikation av digitala signaturer, nämligen dubbla signaturer. För att förstå nödvändigheten för detta nya koncept, så kan man tänka sig följande scenario: Kalle vill sända ett erbjudande till Eva för att köpa en sak och han vill också skicka ett berättigande till sin bank för att skicka pengarna om Eva accepterar erbjudandet, men Kalle vill inte att banken skall se villkoret i erbjudandet och han vill heller inte att Eva skall se hans konto-information. Vidare, så vill Kalle bara länka ihop erbjudandet med transaktionen så att pengarna skickas bara om Eva accepterar erbjudandet. Kalle uppnår allt detta genom att digitalt signera bägge meddelandena med en signatur som skapar en dubbel signatur.

En dubbel signatur genereras genom att skapa en sammanfattning av bägge meddelandena, där båda är sammanlänkade, och därefter så beräknas meddelandesammandragen och detta krypteras med undertecknarens privata signatursnyckel. Undertecknaren måste inkludera meddelandesammandragen av det andra meddelandet för att mottagaren skall kunna verifiera den dubbla signaturen. En mottagare av endera meddelande kan kontrollera dess legitimitet genom att generera meddelandesammandrag av dess kopia av meddelandet, sammanlänkade med sammanfattningen av det andra meddelandet och beräkna meddelandesammandragen av resultatet. Om det nya genererade sammanfattningen stämmer överens med det dekrypterade dubbla signaturen, så kan mottagaren lita på att meddelandet är legitimt.

Om Eva accepterar Kalles erbjudande, så kan hon sända ett meddelande till banken genom att ange sitt godkännande inkluderat med meddelandesammandragen av erbjudandet. Banken kan verifiera äktheten av Kalles överföringsberättigande och försäkra för att godkännandet är för samma erbjudande genom att använda dess sammanfattning av godkännandet och meddelandesammandragen som är presenterad av Eva för att kontrollera giltigheten hos den dubbla signaturen. Alltså kan banken kontrollera äktheten av erbjudandet gentemot den dubbla signaturen, men däremot så kan banken inte se villkoren i erbjudandet.

Inom SET så används dubbla signaturer till att länka ett ordermeddelande som skickas till en handlare tillsammans med köpinstruktioner som innehåller kontoinformation som är skickad till förvärvaren. När handlaren sänder en berättigandebegäran till förvärvaren, så inkluderas

betalningsinstruktioner som är skickad till de av kortinnehavaren och meddelande sammandrag av orderinformationen. Förvärvaren använder meddelandesammandragen från handlaren och beräknar meddelandesammandragen av betalningsinstruktionen för att kontrollera den dubbla signaturen.

3.5.1 Certifikat för kortinnehavare

Kortinnehavarecertifikat fungerar som en elektronisk representation av ett betalningskort. I och med att de signeras digitalt av ett finansiellt institut, så kan de inte ändras av en tredje part och de kan endast genereras av ett finansiellt institut. Ett kortinnehavarecertifikat innehåller inte kontonumret och utgångsdatumet. Istället så är kontoinformationen och ett hemligt värde känt bara av kortinnehavarens mjukvara som är kodad med hjälp av en en-vägs hash algoritm. Om kontonumret, utgångsdatumet, och det hemliga värdet är kända, så kan länken till certifikatet bevisas, men informationen kan inte erhållas genom titta på certifikatet. Inom SET-protokollet, så förser kortinnehavaren kontoinformationen och det hemliga värdet till betalningsporten där länken verifieras.

Ett certifikat utfärdas till kortinnehavaren bara när kortinnehavarens utfärdande finansiella institut godkänner det. Genom att begära ett certifikat, så har en kortinnehavare indikerat avsikten på att utföra handel via elektroniska medel. Denna certifikat överförs till handlaren med begäran av att köpa tillsammans med krypterad betalningsinformation. På kvittot på kortinnehavarenscertifikat, så kan en handlare vara säker på att det minst är så att kontonumret har validerats av kort utfärdande finansiella institutet eller dess agent.

3.5.2 Certifikat för handlare

Ett certifikat för handlare fungerar som en elektronisk ersättare för avdragsbilden av en betalningsstämpel som man kan se i en affärs skyltfönster. Avdragsbilden i sig själv är en representation som visar att handlaren har en relation med ett finansiellt institut som tillåter stämpeln som finns på betalningskortet. Med ett betalningskortsstämpel så menar jag t ex att kortorganisationen Visa har sitt speciella type-logo (märke). Därför att de är signerade digitalt av handlarens finansiella institut, så kan handlarens certifikat inte ändras av en tredje part och det kan bara genereras av ett finansiellt institut.

En förvärvare är ett finansiellt institut som upprättar ett konto med en handlare och genomför bemyndigande av betalningskort och betalningar. Dessa certifikat har blivit godkända av den förvärvade finansiella institutet och denna förser försäkran på så sätt att handlaren har en giltig överenskommelse med en förvärvare. En handlare måste minst ha ett par certifikat för att medverka i SET-miljön, men det kan vara multipla certifikat par per handlare. En handlare kommer att ha ett par certifikat för varje stämpel som finns på betalningskortet som den accepterar.

3.5.3 Certifikat för betalningsporten (Payment gateway)

Certifikat för en betalningsport erhålls av en förvärvare eller deras centrala enhet för systemen som behandlar berättigande och fångar meddelanden. Betalningsportens krypterings nyckel,

som kortinnehavaren får från detta certifikatet (krypteringsnyckeln följer med certifikatet), används till att skydda kortinnehavarens kontoinformation.

3.5.4 Certifikat för förvärvare

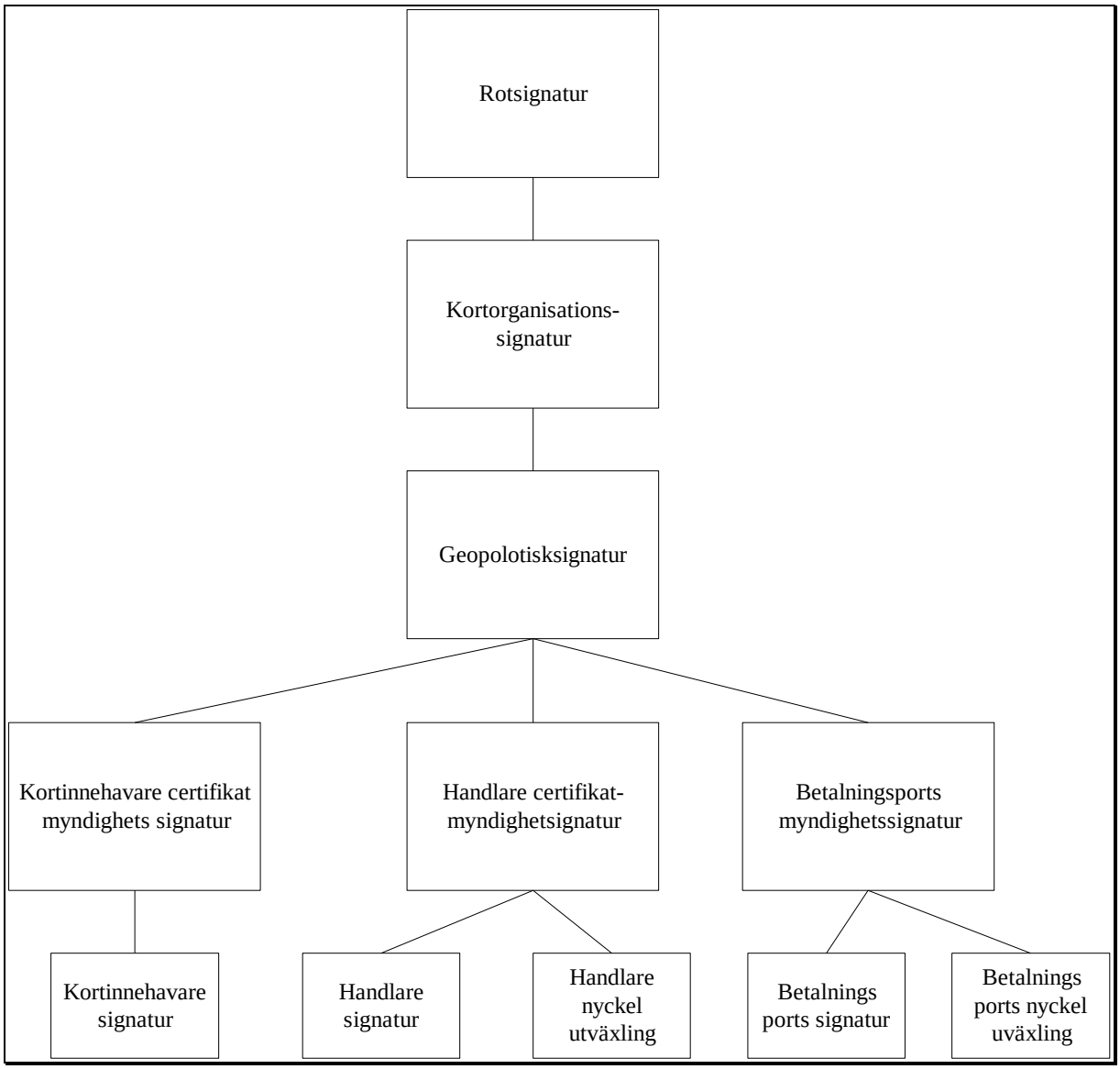
En förvärvare måste ha ett certifikat för att driva en certifikatmyndighet som kan acceptera och genomföra certifikat begäran direkt från handlare över publika och privata nätverk. De förvärvare som väljer att ha en certifikatbegäran för ett betalningskortsstämpel för egen skull kommer inte att behöva certifikat därför att de håller inte på med att bearbeta SET-meddelanden.

3.5.5 Utfärdande certifikat

En utfärdare måste ha ett certifikat för att driva en certifikatmyndighet som kan acceptera och genomföra certifikat begäran direkt från kortinnehavare över publika och privata nätverk. Utfärdaren som väljer att ha en certifikatbegäran för ett betalningskortsstämpel för egen skull kommer inte att behöva certifikat därför att de håller inte på med att bearbeta SET-meddelanden.

3.5.6 Hierarki av förtroende

SET-certifikat verifieras genom en hierarki av förtroende. Varje certifikat är länkad till signatur certifikatet av enheten som har signerat det digitalt. Genom att följa förtroende trädet till en part som man kan lita på, så kan man försäkra sig om att certifikatet är giltigt. Ett exempel kan vara att en kortinnehavares certifikat är länkat till det certifikat som tillhör utfärdaren. Utfärdarens certifikat är länkat tillbaka till en rotnyckel genom kortorganisationens certifikat. Den publika signaturnyckeln av roten är känd för alla SET-mjukvaruprogram och kan användas till att verifiera varje certifikat. Följande figur illustrerar en hierarki av förtroende.



Figur 3c: Hierarki av förtroende

3.5.7 Rotnyckeln

Rotnyckeln distribueras i ett eget-signerat certifikat. Detta rotnyckel certifikat kommer att vara tillgängligt till mjukvaruförsäljare för att inkludera med deras mjukvara. Mjukvaran kan konfirmera att den har en giltig rotnyckel genom att sända en begäran till certifikat-myndigheten som innehåller en hash av rotnyckel certifikatet. Om mjukvaran inte har ett giltig rotcertifikat, så kommer certifikatmyndigheten att skicka ett i gensvar.

Notera att i denna extremt ovanliga situation där mjukvarans rotnyckel är ogiltig, så måste användaren (kortinnehavaren eller handlaren) mata in en sträng som motsvarar hashen av certifikatet. Denna bekräftelsehash måste erhållas från en tillförlitlig källa, så som en kortinnehavarens finansiella institution.

När rotnyckeln genereras, så genereras också en ersättningsnyckel. Ersättningsnyckeln sparas undan på ett säkert ställe framtill det att det kommer till användning. Det egen-signerade rot-certifikatet och hashen av ersättningsnyckeln distribueras tillsammans. Mjukvaran kommer att meddelas om ersättandet genom ett meddelande som innehåller egen-signerat certifikat av ersättningsroten och hashen av den nästa ersättningsrotnyckeln. Mjukvaran validerar ersättningsrotnyckeln genom att räkna dess hash och jämför detta med hashen av ersättnings nyckeln som finns i rotcertifikatet.

3.6.1 Registrering av kortinnehavare

Figur 3d som finns på nästa sida ger en överblick av kortinnehavare registrerings processen, genom att visa dess sju grundläggande steg. Varje steg beskrivs sedan noggrant.

Kortinnehavare måste registreras hos en certifikatmyndighet innan de kan sända SET-meddelanden till en handlare. För att sända ett SET-meddelande till certifikatmyndigheten, så måste kortinnehavaren ha en kopia av certifikat myndighetens ”nyckel-utväxlings” nyckel, som finns i certifikatmyndighetens nyckel-utväxlingscertifikat.

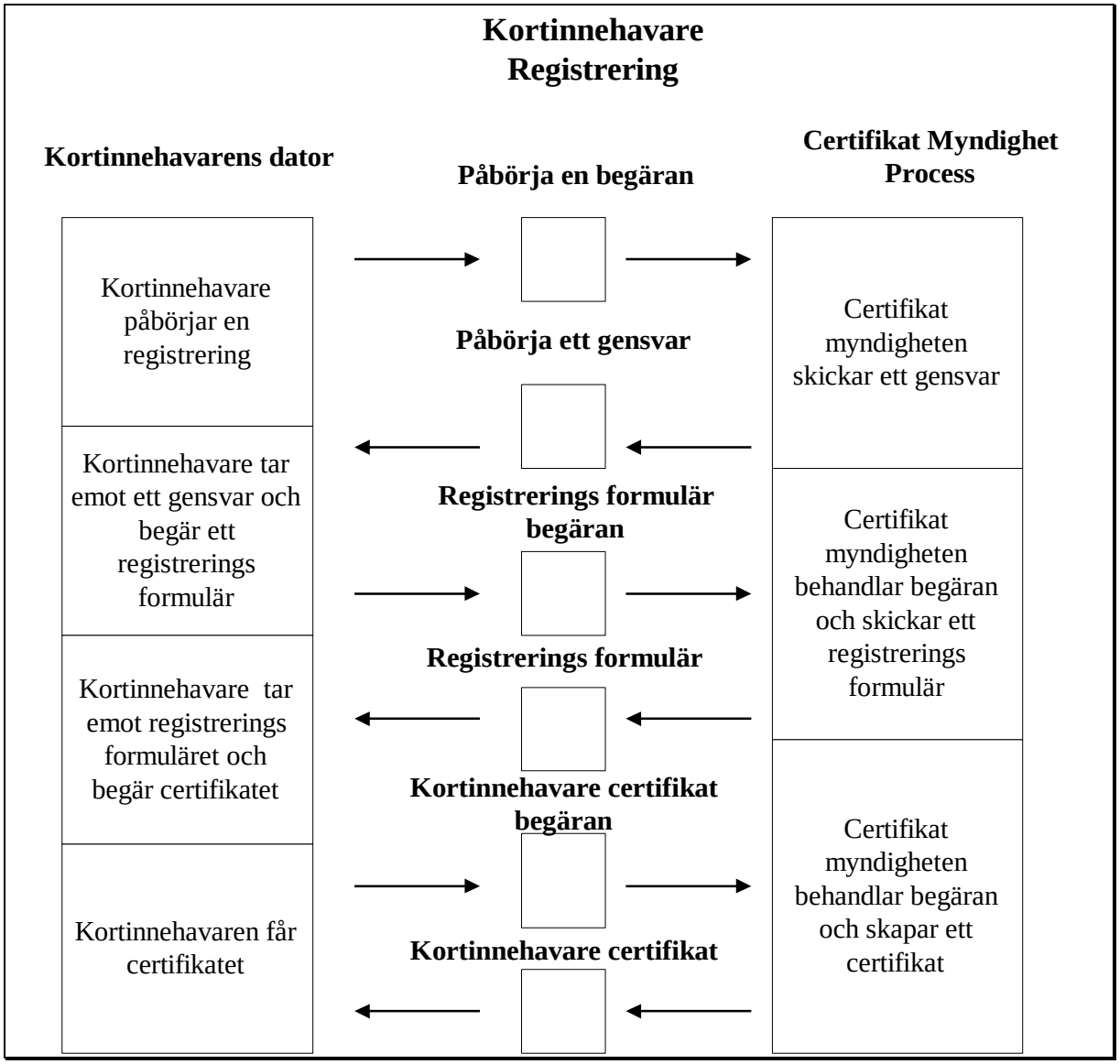
Kortinnehavaren behöver också en kopia av registreringsformuläret från kortinnehavarens finansiella institution. För att certifikatmyndigheten skall kunna ge ut registreringsformuläret, så måste kortinnehavarens mjukvara identifiera utfärdande finansiella institution till certifikatmyndigheten. För att erhålla registreringsformuläret så krävs det två utbyten mellan kortinnehavarens mjukvara och certifikatmyndigheten. Registrerings processen börjar när kortinnehavarens mjukvara begär en kopia av certifikatmyndighetens nyckel-utväxlings-certifikat. När certifikatmyndigheten tar emot en begäran, så överförs dess certifikat till kortinnehavaren. Certifikatmyndighetens dekrypteringsnyckel förser kortinnehavarens mjukvara med den information som är nödvändig för att skydda betalningkorts kontonummer i registreringsformuläret. Kortinnehavarens mjukvara verifierar certifikatmyndighetens certifikat genom att följa förtroendekedjan till rotnyckeln. Mjukvaran måste lagra certifikatmyndighetens certifikat för att använda den senare i registrerings processen.

Kortinnehavarens mjukvara skapar en begäran om ett registreringsformulär. Efter detta så genererar mjukvaran en slumpmässig symmetrisk krypteringsnyckel. Den använder denna slumpmässig genererade nyckeln för att kryptera begäran om registreringsformuläret. Denna slumpmässiga nyckel krypteras sedan tillsammans med kontonumret till den digitala plånboken genom att använda certifikatmyndighetens publika nyckel-utväxlingsnyckel. Tillslut, så överför mjukvaran alla dessa komponenter till certifikatmyndigheten.

Kortinnehavarens mjukvara:

- verifierar certifikatmyndighetens certifikat genom att följa förtroendekedjan till rot- nyckeln
- lagrar certifikatmyndighetens certifikat för att använda det senare i registrerings processen
- skapar en begäran om ett registreringsformulär
- genererar en slumpmässig symmetrisk krypteringsnyckel
- använder den slumpmässiga nyckeln för att dekryptera begärandet om registrerings-formuläret
- krypterar den slumpmässiga nyckeln tillsammans med kontonumret till den digitala plånboken genom att använda certifikatmyndighetens publika nyckel-utväxlingsnyckel

- överför alla dessa komponenter till certifikatmyndigheten



Figur 3d: Kortinnehavare registrering

Certifikatmyndigheten identifierar kortinnehavarens finansiella institution (genom att använda de första 6 till elva numren av kontonumret) och väljer en lämplig registrerings-formulär. Det signerar det digitalt och returnerar denna registreringsformulär till kortinnehavaren. I vissa fall, så kan det hända att certifikatmyndigheten inte har en kopia av registreringsformuläret men kan informera kortinnehavarens mjukvara var formuläret kan erhållas.

När certifikatmyndigheten får en begäran från en kortinnehavare, så dekrypteras den digitala plånboken för att erhålla den symmetriska krypteringsnyckeln, kontoinformationen, och det slumpmässigt genererade numret av kortinnehavarens mjukvara. Mjukvaran använder den symmetriska nyckeln till att dekryptera registreringsbegärandet. Det använder sedan signatur-nyckeln i meddelandet för att försäkra att önskemålet var signerat genom att använda motsvarande privata signaturnyckeln. Om signaturen är verifierad, så fortsätter meddelande

processen; annars, så avslås meddelandet och ett lämpligt meddelande skickas till kortinnehavaren.

Sedan så måste certifikatmyndigheten verifiera informationen från registreringsönskemålet genom att använda kortinnehavarens kontoinformation.

Om informationen i registreringsönskemålet är verifierad, så utfärdas det ett certifikat. Först, så genereras ett slumpmässigt nummer av certifikatmyndigheten kombinerat med det slumpmässiga numret som är skapat av kortinnehavarens mjukvara för att generera ett hemligt värde. Det hemliga värdet används för att skydda kontoinformationen i kortinnehavarens certifikat. Kontonumret, utgångsdatumet, och det hemliga värdet kodas genom att använda en en-vägs hash algoritm. Resultatet av hash algoritmen placeras in i kortinnehavarens certifikat. Om kontonumret, utgångs datumet, och det hemliga värdet är kända, så kan länken till certifikatet bevisas, men informationen kan inte erhållas genom att titta på certifikatet.

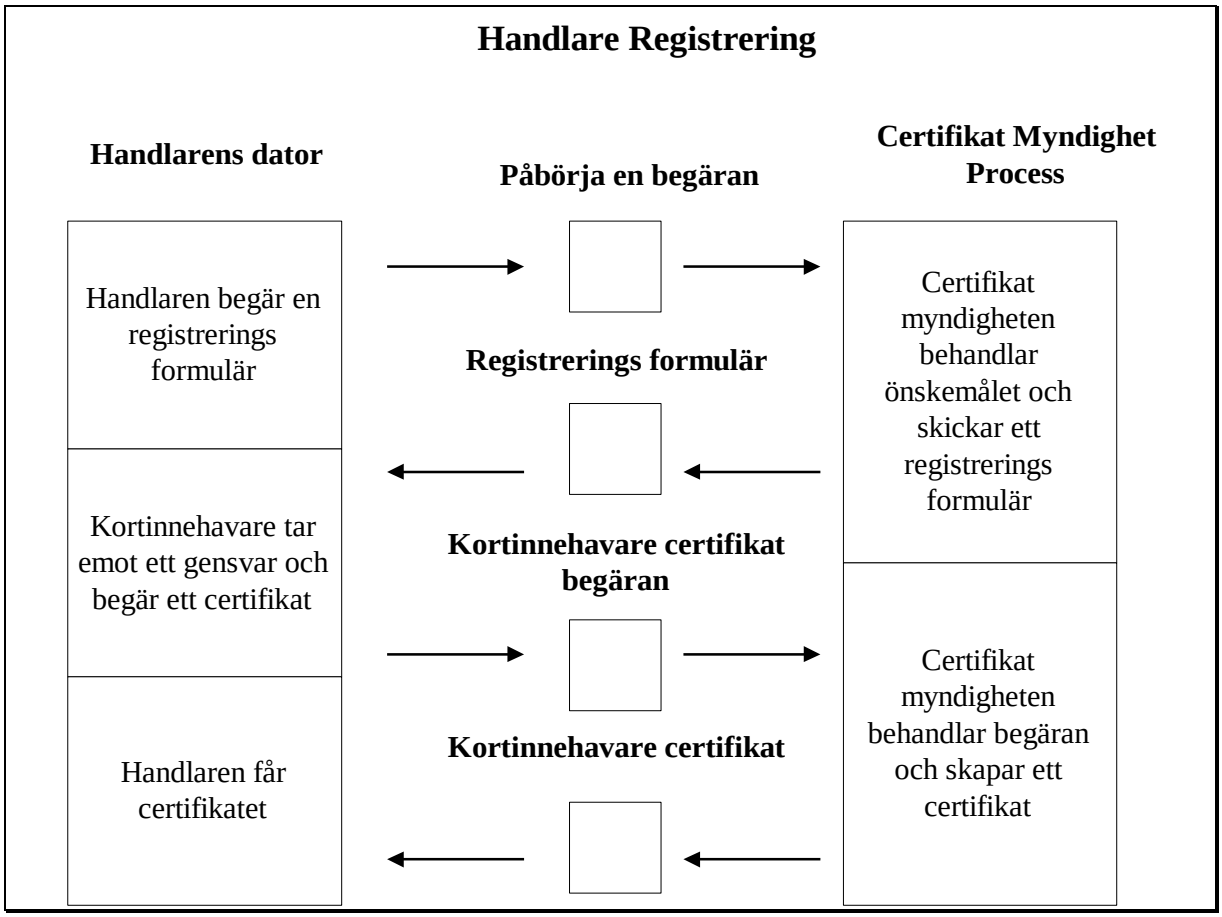
Sedan skapas och signeras kortinnehavarens certifikat digitalt av certifikatmyndigheten. Giltighetstiden av certifikatet kommer att bestämmas av certifikatmyndighetens policy; där det oftast är så att utgångsdatumet blir samma som utgångsdatumet på kortet, men det kan vara så att det går ut tidigare.

Ett meddelande som innehåller det slumpmässiga numret genererat av certifikatmyndigheten och annan information genereras och krypteras sedan genom att använda symmetriska nyckeln som skickades av kortinnehavarens mjukvara i registreringsmeddelandet. Meddelandet vidarebefordras sedan till kortinnehavaren.

När kortinnehavarens mjukvara tar emot gensvaret från certifikatmyndigheten, så verifieras certifikatet genom att följa förtroendekedjan till rotnyckeln. Mjukvaran sparar sedan certifikatet i kortinnehavarens dator för att använda det senare i framtida transaktioner. Sedan, så dekrypterar kortinnehavarens mjukvara registreringsgensvaret genom att använda den symmetriska krypteringsnyckeln som är skickat till certifikatmyndigheten i registrerings-meddelandet. Mjukvaran kombinerar det slumpmässiga numret som returnerades av certifikat-myndigheten med det värde som är skickades i registreringsmeddelandet för att bestämma det hemliga värdet. Mjukvaran sparar sedan det hemliga värdet för att använda det med certifikatet. Försäljarna av kortinnehavarens mjukvara kommer att försäkra att certifikatet med relaterad information är sparad på ett sådant sätt att det hindrar obehörig åtkomst.

3.6.2 Registrering av handlare

Figur 3e ger en överblick av processen för handlareregistrering, genom att visa dess fem grundläggande steg. Sedan följer det en mer detaljerad beskrivning av varje steg.



Figur 3e: Handlarregistrering

Handlare måste registrera sig hos en certifikatmyndighet innan de kan ta emot SET-betalningsinstruktioner från kortinnehavare eller SET-transaktionsprocesser genom en betalningsport. För att skicka SET-meddelanden till certifikatmyndigheten, så måste handlaren ha en kopia av certifikat myndighetens publika nyckel-utväxlingsnyckel, som finns i certifikatmyndighetens nyckel-utväxlingscertifikat. Handlaren behöver också en kopia av registreringsfomuläret från handlarens finansiella institution. Registrerings processen börjar när handlarens mjukvara begär en kopia av certifikatmyndighetens nyckel-utväxlingscertifikat och en lämplig registreringsformulär.

Certifikatmyndigheten identifierar handlarens finansiella institution och väljer ut ett lämpligt registreringsformulär. Myndigheten returnerar registreringsformuläret tillsammans med en kopia av sitt eget nyckel-utväxlingscertifikat till handlaren. Handlarens mjukvara verifierar certifikat myndighetens certifikat genom att följa förtroendekedjan till rotnyckeln, och lagrar certifikatmyndighetenscertifikat för att använda det senare i registreringsprocessen. När mjukvaran har en kopia av certifikatmyndighetens nyckel-utväxlingscertifikat, så kan handlaren registrera sig för att acceptera SET-betalningsinstruktioner och göra SET-transaktioner. Handlaren måste ha relationer med en förvärvare som gör SET-transaktioner innan en certifikat begäran kan genomföras.

Handlaren behöver två publika/privata nyckelpar för att använda SET: nyckel-utväxling och signatur. Handlarens mjukvara genererar dessa nyckelpar om de inte existerar sedan tidigare. För att registrera, så fyller handlaren i registreringsformuläret på skärmen med information så

som handlarens namn, adress, och ID. Handlarens mjukvara tar denna registreringsinformation och kombinerar med de publika nycklarna i ett registrerings-meddelande. Mjukvaran signerar sedan registreringsmeddelandet digitalt. Sedan, genererar mjukvaran en slumpmässig symmetrisk krypteringsnyckel. Denna slumpmässiga nyckel används för att kryptera meddelandet. Den slumpmässiga nyckeln krypteras sedan in i den digitala plånboken genom att använda certifikatmyndighetens publika nyckel-utväxlings-nyckel. Slutligen, så vidarebefordrar mjukvaran alla dessa komponenter till certifikat-myndigheten.

När certifikatmyndigheten får handlarens begäran, så dekrypteras den digitala plånboken för att erhålla symmetriska krypteringsnyckeln, som används för att dekryptera registrerings-önskemålet. Det använder sedan signatur nyckeln för att försäkra att önskemålet var signerat genom att använda privata signaturnyckeln. Om signaturen är verifierad, så fortsätter meddelande processen; annars, så avvisas meddelandet och ett lämpligt meddelande gensvar returneras till handlaren.

Sedan, så måste certifikatmyndigheten verifiera informationen i registreringsbegärandet genom att behandla den kända informationen om handlaren. Om informationen i registrerings önskemålet är verifierad, så skapas och signeras handlarens certifikat digitalt av certifikat-myndigheten. Giltighetstiden av dessa certifikat bestäms av certifikatmyndighetens policy; där det ofta är så att det kommer att motsvara utgångs datumet av handlarens kontrakt med förvaren, men det kan vara så att det går ut tidigare. Certifikaten krypteras genom att använda en ny slumpmässig genererad symmetrisk nyckel, som i sin tur krypteras genom att använda handlarens publika nyckel-utväxlingsnyckel. Gensvaret vidarebefordras sedan vidare till handlaren.

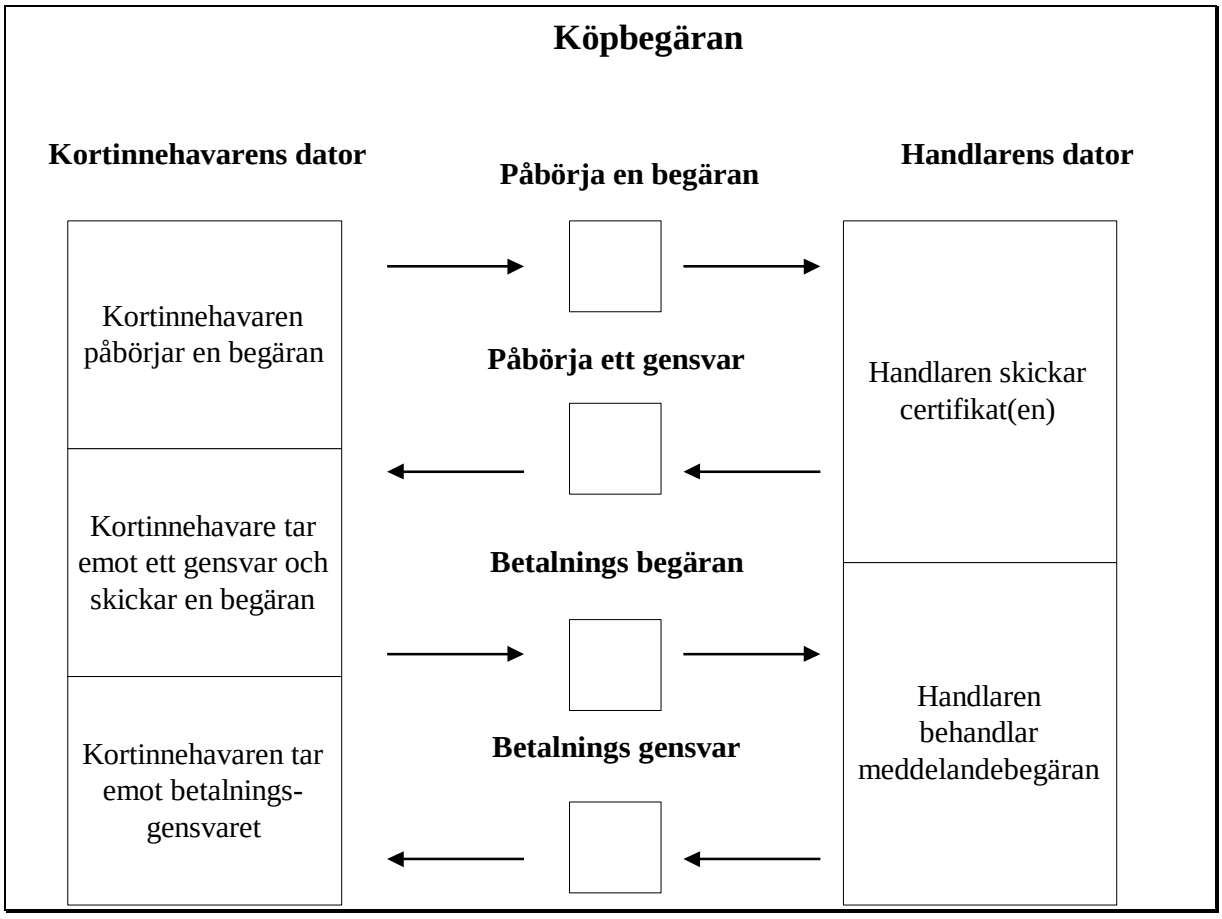
När handlarens mjukvara tar emot gensvaret från certifikatmyndigheten, så dekrypteras den digitala plånboken för att erhålla den symmetriska krypteringsnyckeln. Det använder symmetriska nyckeln till dekryptera registreringsgensvaret som innehåller handlarens certifikat. Efter det att handlarens mjukvara verifierar certifikaten genom att följa förtroende-kedjan till rotnyckeln, så sparas certifikaten på handlarens dator för att använda det i en framtida elektroniska handelstransaktioner.

3.6.3 Köpbegäran

Figur 3f på nästa sida ger en överblick över betalnings begäran av en kortinnehavares order-process, genom att visa dess fem grundläggande steg. Stegen beskrivs sedan mer noggrant.

SET-protokollet är inkapslat efter det att kortinnehavaren har blivit klar med att titta, välja, och beställa. Innan detta flöde påbörjas, så får kortinnehavaren en komplett orderformulär och godkänner dess innehåll och villkor, så som antal avbetalningar om handlaren gör en räkning för avbetalnings transaktionerna. Som tillägande, så kommer kortinnehavaren att välja ett betalningskort som hjälpmedel för att betala.

För att en kortinnehavare skall kunna skicka SET-meddelanden till en handlare, så måste kortinnehavaren ha en kopia av betalningports nyckel-utväxlingsnyckel. SET-order processen påbörjas när kortinnehavarens mjukvara begär en kopia av portens certifikat. Meddelandet från kortinnehavaren kommer att indikera vilken betalningskortsorganisation som kommer att användas för transaktionen.



Figur 3f: Köpbegäran

När handlaren får önskemålet, så tilldelas en unik transaktionsidentifierare till meddelandet. Det överför sedan handlarens och portens certifikat som motsvarar betalningskortsorganisationen som indikerades av kortinnehavaren, tillsammans med transaktionsidentifieraren till kortinnehavaren. Kortinnehavarens mjukvara verifierar handlarens och portens certifikat genom att följa förtroendekedjan (se figur 3c) till rotnyckeln, och mjukvaran håller sedan dessa certifikat för att använda det sedan under order-processen.

Kortinnehavarens mjukvara skapar OrderInformationen (OI) och BetalningsInstruktioner (BI). Mjukvaran placerar transaktionsidentifieraren tilldelat av handlaren i OI och BI; denna identifierare kommer att användas av betalningsporten för att länka OI och BI tillsammans när handlaren kräver bemyndigande.

Notera att OI innehåller inte orderdata så som beskrivning av varor (vilka varor och kvantiteten på dem) eller ordervillkoret (så som antalet avbetalningar). Denna information utbytes mellan kortinnehavarens och handlarens mjukvara under handlingsfasen innan det första SET-meddelandet. Kortinnehavarens mjukvara genererar en dubbel signatur för OI och BI genom att räkna bägge meddelandesammandragen, länka samman de två sammandragen, och räkna resultatet av meddelandesammandragen och kryptera det genom att använda kortinnehavarens privata signaturnyckel. Meddelandesammandragen av OI och BI skickas tillsammans med den dubbla signaturen. Sedan så genererar mjukvaran en slumpmässig

symmetrisk krypteringsnyckel och använder den till att kryptera BI som är dubbelsignerat. Mjukvaran krypterar sedan kortinnehavarens kontonummer och den slumpmässiga symmetriska nyckeln som används för att kryptera BI in till den digitala plånboken genom att använda betalningsportens nyckel-utväxlingsnyckel. Slutligen, så överför mjukvaran ett meddelande som består av OI och BI till handlaren.

När handlarens mjukvara tar emot ordern, så verifieras kortinnehavarens signaturcertifikat genom att följa förtroendekedjan till rotnyckeln. Sedan, så använder den kortinnehavarens publika signaturnyckel och meddelandesammandraget av BI och OI för att kontrollera den digitala signaturen för att försäkra att ingen fifflat med ordern under transporten och att det var signerat genom att använda kortinnehavarens privata signaturnyckel. Handlarens mjukvara utför ordern inklusive betalningsbemyndigande. Det är inte nödvändigt för handlaren att utföra bemyndigandefasen tidigare än att skicka ett gensvar till kortinnehavaren. Kortinnehavaren kan bestämma senare om bemyndigandet har utförts genom att skicka ett orderförfråganmeddelande.

Efter det att OI har bearbetats, så genererar handlarens mjukvara en digital signatur och signerar denna ett svar på köpförfrågan, som inkluderar handlarens signaturcertifikat och indikerar att kortinnehavarens order har mottagits av handlaren. Gensvaret överförs sedan till kortinnehavaren. Om bemyndigandet indikerar att transaktionen är godkänd, så kommer handlaren att sända varorna eller utföra den service som indikerades i ordern. När kortinnehavarens mjukvara tar emot köpgensvarmeddelandet från handlaren, så verifieras handlarens signaturcertifikat genom att följa förtroendekedjan till rotnyckeln. Det använder handlarens publika signaturnyckel för att kontrollera handlarens digitala signatur. Slutligen, så kan det ske några ändringar i innehållet av gensvar-meddelandet, så som att visa upp ett meddelande för kortinnehavaren eller uppdatera en databas med orderns status. Kortinnehavaren kan bestämma statusen på ordern (ifall den har blivit bemyndigad eller utsatt för betalning) genom att skicka ett orderförfråganmeddelande.

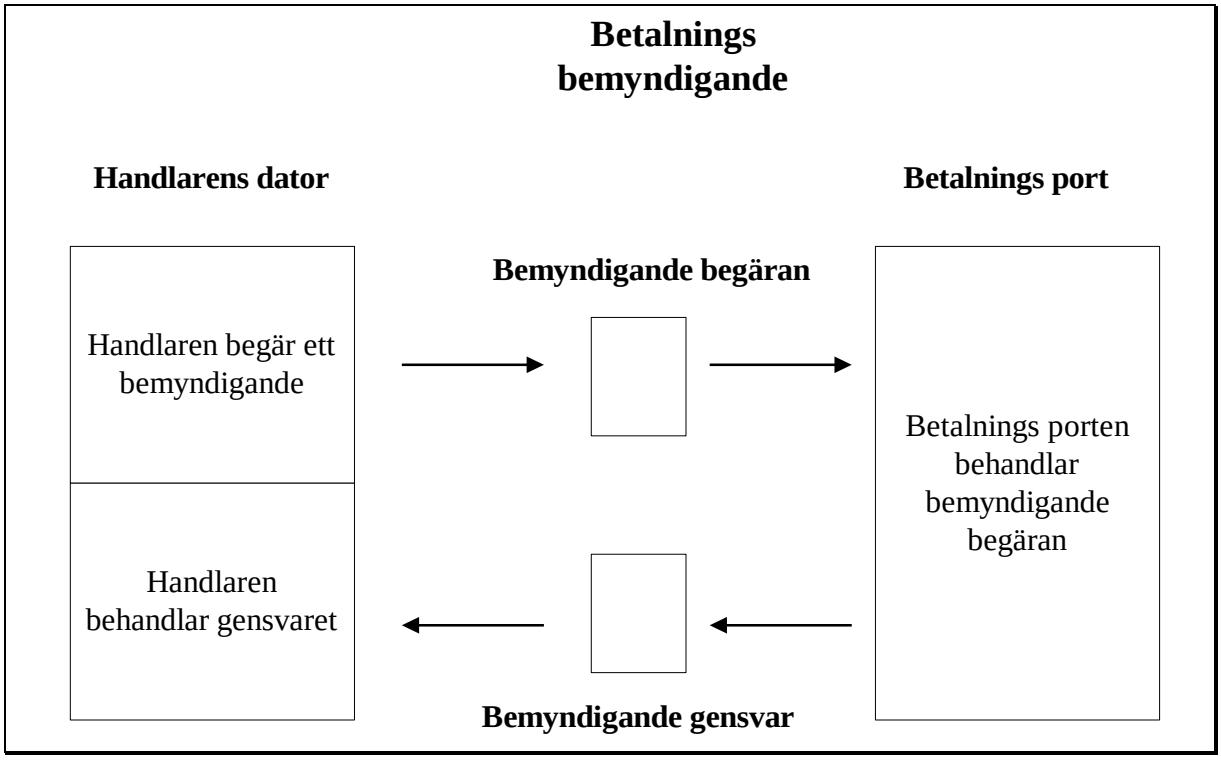
3.6.4 Betalningsbemyndigande

Figur 3g på nästa sida ger en överblick över processen för en handlares betalningsbemyndigande, genom att visa dess tre grundläggande steg. Varje steg beskrivs sedan mer i detalj.

Under en behandling av en order från en kortinnehavare, så kommer handlaren att godkänna transaktionen. Handlarens mjukvara genererar och signerar en berättigande begäran digitalt, som inkluderar transaktions identifieraren från OI, och annan information angående transaktionen. Önskemålet krypteras sedan genom att använda en ny slumpmässig genererad symmetrisk nyckel, som i sin tur krypteras genom att använda den publika nyckel-utväxlings-nyckel av betalningsporten. (Denna nyckeln är densamma som kortinnehavaren använder till att kryptera den digitala plånboken för betalningsinstruktioner). Berättigandebegärandet och kortinnehavarens betalningsinstruktioner överförs sedan till betalningsporten.

SET-protokollet inkluderar också en säljtransaktion som tillåter en handlare att godkänna en transaktion och begära betalning i ett enda meddelande. När betalningsporten får begäran om bemyndigande, så dekrypteras den digitala plånboken för att erhålla den symmetriska krypteringsnyckeln. Mjukvaran använder den symmetriska nyckeln för att dekryptera begärandet. Sedan så verifieras handlarens signaturcertifikat genom att följa förtroendekedjan

till rotnyckeln. Mjukvaran ser också till att verifiera att certifikatet inte har gått ut. Mjukvaran använder handlarens publika signaturnyckel för att försäkra att önskemålet var signerat genom att använda handlarens privata signaturnyckel.



Figur 3g: Betalnings bemyndigande

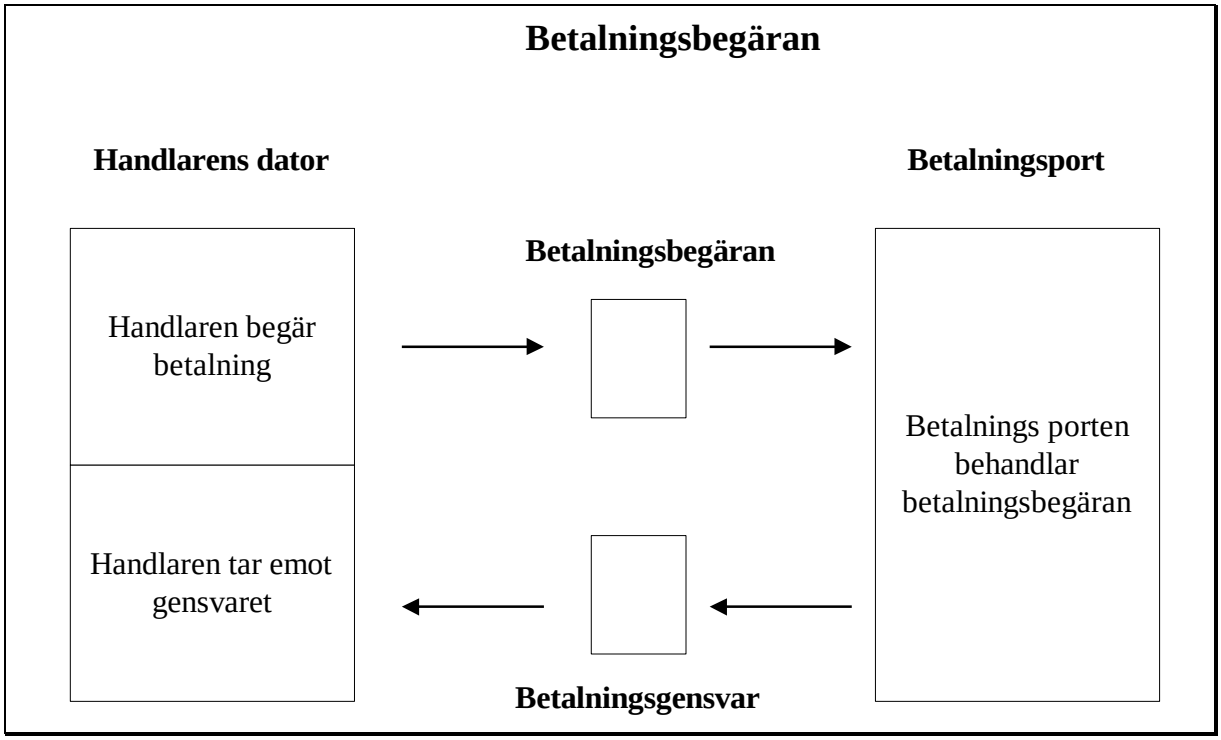
Sedan så dekrypterar betalningsporten digitala plånbokens betalningsinstruktioner för att erhålla den symmetriska krypteringsnyckeln och kontoinformationen. Det använder den symmetriska nyckeln till att dekryptera BI. Sedan så verifieras kortinnehavarens signatur-certifikat genom att följa förtroendekedjan till rotnyckeln. Det verifierar också om datumet har gått ut för certifikatet. Efter detta så används kortinnehavarens publika signaturnyckel och meddelandesammandragen av OI (inkluderad i BI) till att kontrollera den digitala signaturen för att försäkra att BI inte har fifflats mellan överföringen och då den blev signerat genom att använda kortinnehavarens privata signaturnyckel. Sedan, så verifierar betalningsporten att transaktionsidentifieraren som den fick från handlaren stämmer överens med den i kortinnehavarens betalningsinstruktion. Betalningsporten formaterar och skickar en bemyndigandebegäran till utfärdaren via ett betalningssystem. När väl betalningsporten tar emot bemyndigandegensvaret från utfärdaren, så genererar och signerar betalningsporten ett gensvar meddelande som är digitalt, som inkluderar utfärdarens gensvar och en kopia av betalningsportens signaturcertifikat. Gensvaret inkluderar också en valfri bevis emottagande med information som betalningsporten kommer att behöva för att behandla en betalningsönskemål. Bevis emottagandet inkluderas endast om förvärvaren kräver det. Gensvaret krypteras sedan genom att använda en slumpmässig genererad symmetrisk nyckel, som i sin tur är krypterad genom användning av handlarens publika nyckel-utväxlingsnyckel. Därefter så överförs gensvaret till handlaren.

När handlarens mjukvara tar emot svaret på förfrågan om bemyndigande från betalnings-porten, så dekrypteras den digitala plånboken för att erhålla den symmetriska krypterings-

nyckeln. Det använder symmetriska nyckeln till att dekryptera meddelandegensvaret. Det verifierar sedan betalningsportens signaturcertifikat genom att följa förtroendekedjan till rot-nyckeln. Betalningsportens publika signaturnyckel används till att kontrollera betalnings-portens digitala signatur. Handlarens mjukvara sparar undan bemyndigandegensvaret och bevis på emottagandet för att använda de när det begärs en betalning genom en betalningsbegäran. Sedan så avslutar handlaren att behandla kortinnehavarens order genom att transportera varorna eller utför den service som påpekas i ordern.

3.6.5 Betalningsbegäran

Figur 3h visar en överblick över en handlares betalningsbegäran, genom att visa dess tre grundläggande steg. Varje steg som finns i figuren beskrivs mer i detalj här nedan.



Figur 3h: Betalningsbegäran

Efter avslutning av bearbetningen av en order från en kortinnehavare, så kommer handlaren att kräva betalning. Det kommer ofta att bli en signifikant tidsförlopp mellan bemyndigande-begäran och betalningsbegäran. Handlarens mjukvara genererar och signerar en betalnings-begäran digitalt, vilket som inkluderar det slutgiltiga beloppet av transaktionen, transaktions-identifieraren från OI, och annan information angående transaktionen. Önskemålet krypteras sedan genom användning av en ny slumpmässig genererad symmetrisk nyckel, vilket som i sin tur krypteras genom användning av betalningsportens publika nyckel-utväxlingsnyckel. Betalningsbegärandet och frivilliga betalningsbeviset om det var inkluderat i bemyndigande-gensvaret överförs sedan till betalningsporten. Det är viktigt att poängtera att medan flödet som beskrivits här innehåller en enda betalningsbegäran, så har handlarens mjukvara tillåtelse till att ta ett parti multipla begäran in i ett enda meddelande.

När betalningsporten tar emot betalningsbegärandet, så dekrypteras den digitala plånboken av betalningsbegärandet för erhålla den symmetriska krypteringsnyckeln. Det använder den symmetriska nyckeln till dekryptera begärandet. Det använder sedan handlarens publika signaturnyckel för att försäkra att begärandet var signerat genom användning av handlarens privata signaturnyckel. Betalningsporten dekrypterar det mottagna beviset (om den är närvarande) och använder sedan informationen från betalningsbegärandet och beviset till att formatera en klargörande begäran, vilket som det sänder till utfärdaren via ett betalningskorts-system. Betalningsporten genererar och signerar sedan ett betalningsgensvar digitalt, vilket inkluderar en kopia av betalningsportens certifikatsignatur. Gensvaret krypteras sedan genom användning av en ny slumpmässig genererad symmetrisk nyckel, vilket som i sin tur är krypterad genom användning av handlarens publika nyckel-utväxlings-nyckel. Därefter så överförs gensvaret till handlaren.

När handlarens mjukvara tar emot det mottagna gensvar meddelandet från betalningsporten, så dekrypteras den digitala plånboken för att erhålla den symmetriska krypteringsnyckeln. Det använder den symmetriska krypteringsnyckeln till att dekryptera meddelandetgensvaret. Sedan så verifieras betalningsportens certifikatsignatur genom att följa förtroendekedjan till rotnyckeln. Det använder betalningsportens publika signaturnyckel för kontrollera betalnings-portens digitala signatur. Handlarens mjukvara sparar undan det mottagna gensvaret för att sedan använda det i en uppgörelse med betalningsmottagandet från förvärvaren.

4 Intervjuer om SET

För att man skall kunna få en helhetsbild över det hela så har jag gjort intervjuer därför att jag ville se vad de som var inne i branschen tyckte och tänkte. Personerna jobbar med SET dagligen, och jag tog kontakt med de via telefon och intervjuerna gjordes via e-post. Jag hittade de personer som skulle intervjuas på Internet. De personer som har intervjuats har jag ställt dessa nedanstående frågor. Vissa frågor har en lite mer teknisk karaktär medan vissa är lite mer generella. Frågorna representeras per fråga och inte per person, dvs alla frågor som personerna har svarat på har jag slagit ihop under respektive fråga. Det är viktigt att påpeka att personernas namn är påhittade.

Frågor angående SET finns på början av varje delrubrik och därefter så följer svaren. De personer som intervjuades svarade:

1. "Hur är robustheten, kompabiliteten och säkerheten ?" - Bästa tänkbara tillgängliga idag - 1024 bit krypto garanterar god säkerhet i nätet. SET är en standard. Jag upplever att version 1.0 inte är tillräckligt specifik i alla delar för att garantera ”plug and play” interoperabilitet mellan alla leverantörers SET-moduler. Interoperabiliteten måste konstateras genom tester. Sådana pågår. Robustheten är olika för moduler från olika leverantörer. Säkerheten är hög.
2. "Hur är gränssnittet och användarvänligheten, är det lätt att komma igång?" - Min egen bedömning är att det är enkelt och användar vänligt - men det skall vår pilot utvisa då vi kommer att fråga alla kunder vad dom tycker. Gränssnittet är olika beroende på leverantör. De jag har sett har varit lätta att arbeta med.
3. "Hur ser ni på att kunden är anonym när han/hon betalar sina räkningar, är detta en viktig fråga för kunden och för er?" - Total anonymitet är omöjligt då det skall ske betalning från bankkonto - banken måste veta att det är du som beordrar betalningen, och säljaren måste veta att det du köper skall skeppas till dig. Kunden är inte anonym i SET. Både butiken och banken måste ju veta vem det är som handlar. Butiken kan inte se den finansiella informationen och banken kan inte se vad som köpts. Den uppdelningen är bra.
4. "Vilken syn har kunden gentemot denna nya standard?" - Köparens syn utvärderas som sagt i piloten - med den metoden ansluter ju till ett befintligt betalmedel - kontokortet - varför det i sig inte är nytt för kunden - bara betaltekniken är ny. Detta kommer vi att utvärdera under vårt pilotprojekt.
5. "Kommer man i en snar framtid att göra det möjligt till att transaktioner mellan två privatpersoner kan ske?" - Blir svårt eftersom myndigheterna i de flesta länder förutsätter revisionsspår i systemen för att hindra penningtvätt och svarta affärer - men på lång (5år) sikt tror jag att detta ändå kommer. Betalningen sker mellan ett säljföretag som har inlösenavtal med en bank och en kortinnehavare som disponerar ett kort utgivet av en bank. Betalningen kan inte ske mellan två kortinnehavare.
6. "Tror du att SET kommer att ta över betalnignsystemen, om så varför?" - Det finns inga system att för Internetbetalning att ta över ännu - SET är det första och enda hittills för internationell spontanhandel. Andra kommer säkert men det tar tid. SET kommer att bli det dominerande betalningssättet för köp på Internet. Skälet är att det är en global standard som stöds av de ledande kortorganisationerna såsom Visa och MasterCard.
7. "Vad händer ifall min dator skulle krasvha eller att förbindelsen skulle brytas när jag var på väg att utföra en transaktion?" - Om din dator kraschar kan vi rekonstruera den transaktionen som du höll på med och backa den alternativt - fullfölja - systemet tar hänsyn

till avbrott. Eftersom SET genererar kontokortsbetalningar så finns inga ”pengar” ute i luften på Internet och det ända som behöver ske är att rekonstruera och bekräfta till dig att transaktionen inte blev av p.g.a. störning i Internet, din dator m.m. och uppmana dig att fullfölja köpet om du vill det. Antingen blev transaktionen av eller ej. Vilket kan du konstatera när du kommer igång igen. SET-standarden definierar avbrottshanteringen noga.

8. "Hur ser framtiden ut för betalningar över Internet?" - Internet kommer att växa till sig som affärskanal och det kommer att förmedlas ett stort antal köp både internationellt och nationellt. Euro-valutan kommer att föra hela EU till ”inrikes” vilket ytterligare ökar marknaden när valutarisker och växlingskostnader försvinner mellan köpare och säljare inom EU. Vår gissning: Svenska köpare handlar för 5-10 MRD SEK inom fem år. Både konsumenter och företag kommer att handla upp varor/tjänster via Internet och flera olika betalningsmetoder kommer att användas i denna marknad och bankerna kommer att erbjuda dessa metoder. Vi förutsätter en avsevärd tillväxt.
9. "Kostar det något ifall man vill göra transaktioner via SET?" - I piloten tar vi inte betalt av köparna för tillgången till systemet men det kommer vi säkert att göra när SET blir ordinarie tjänst. Antagligen ett inträdespris på 50-100 kr och ett årligt abonnemang på 50-100 kr för certifikatet. Säljande företag betalar sina vanliga priser för transaktionsinlösen till sin bank precis som dom också betar för att kända in dagskassor i bankboxen. Alla sådana priser sätts i konkurrens mellan olika banker så tiden utvisar vilka priser som etablerar sig på denna nya ”marknad”. Kortinnehavaren måste betala en årsavgift för sitt kort. Butiken betalar avgifter enligt sitt inlösenavtal. Vi tar betalt för vårt jobb - att transportera betalinformationen mellan olika banker där pengarna finns, att ge betalgaranti till säljaren, att ge leveransgaranti till köparen, att reda ut fel som kan uppstå mellan säljare och köpare, att växla valutor mellan säljare och köpare att rapportera och statistikbehandla transaktionerna åt säljare och köpare m.m. En betalning är så mycket mer än bara att sända x st bits med information från PC till server hos säljare på en marknad där dessa inte känner varandra och inte kan komma i direkt kontakt…
10. "Vilka är fördelarna med att använda sig av SET jämfört med det traditionella sättet?" - SET är den idag enda metoden som klarar av att i internationell spontanhandel identifiera köpare och säljare samt säkert sända information in i banksystemet. Några ”gamla vanliga” metoder för Internet finns inte utan SET är den första som börjar lanseras. Alla andra förutsätter att köparen på något sätt registrerar sig i förväg (typ postens torg) och sen kan använda den betalmetoden just där. Spontan köp klaras inte av och i allmänget inte heller internationella köp. Metoden att bara knappa in ett kortnummer till säljaren som sedan skall tillverka en korttransaktion och sända in denna i det vanliga kortsystemet - oftast via en vanlig butiksterminal - kommer att döda sig själv. Förlusterna för oärliga köp växer lavinartat och säljarna som ytterst får bära kostnaderna kommer att byte metod snarast. Dessutom - en ”metod” som innebär att jag kan knappa in ditt kortnummer och få loss leveransen - och du får kostnaden - kommer relativt snabbt att döda sig själv då du förstås inte accepterar att regelbundet klaga hos din kortutgivare på alla köp som jag gjort på ditt kort. Säljaren som efter ditt klagomål blir av med sin likvid klarar förstås inte heller av att ta förlusterna. Problemet har hittills varit att det inte finns någon vettig metod som skyddar både köparen och säljaren. SET åstadkommer detta och kan snabbt spridas genom att SET-certifikatet ju kopplas till existerande Visa- eller MasterCard kort. Det finns 900 muljoner sådana kort utgivna i över 200 länder och 28 000 banker förmedlar betalningar i Visa och MasterCard näten. Det svåra är inte att bygga tekniken för betalning - det är på gång och nästan klart visa SET - utan att åstadkomma ett globalt transaktionsnätverk så att köpare och säljare över hela världen kan göra affärer med varandra inklusive regelverk på hur transaktionerna äger rum, vem som står för risken m.m. Visa och MasterCard som ägs

kollektivt av de 28 000 medlemsbankerna har redan det nätverket och regelverket på plats för kontokorten. Därför blir SET ”bara” en front end för att hantera transaktionerna via Internet. Med SET är parterna identifierade och banken kan garantera betalningen till säljföretaget. Det går inte på något annat sätt.

5 Slutsats

De personer som intervjuades har samma synpunkt angående säkerheten, då de anser att den är väldigt hög. Och med tanke på hur långa krypteringsnycklarna kan bli så kan man verkligen hålla med dem. Gränssnittet ser olika ut beroende på leverantör men de gränssnitt som de intervjuade har sett tycker de är enkla att jobba med och användarvänliga. Hur kunderna ser på SET kommer att utvärderas i pilotprojektet, men en viktig punkt är bra att poängtera nämligen att kontokortsbetalningar är inte nytt för kunden utan det är bara betaltekniken som är ny. För närvarande så kan inte transaktioner ske mellan två privatpersoner beroende på att myndigheterna i de flesta länderna förutsätter revisionsspår i systemen för att hindra penningtvätt och svarta affärer men på lång sikt så tror Person A på att det kommer att komma. Person B tror att SET kommer att vara det dominerande betalningssättet för köp på Internet, skälet är att det är en global standard som stöds av de ledande kortorganisationerna såsom Visa och MasterCard. Ifall din dator kraschar och en transaktion avbryts så tar SET hänsyn till detta och när du startar datorn igen så får du meddelandet att transaktionen inte blev av, men är det så att du vill fullfölja transaktionen så frågar systemet det. Avbrottshanteringen hanteras noga. Både Person B och Person A håller med om att Internet kommer att växa till sig som affärskanal. SET är inte en ordinarie tjänst ännu men när det väl blir det så kommer man ta ett inträdes pris på 50-100 kr och ett årligt abonnemang på 50-100 kr för certifikatet, enligt Person A. Medan en butik betalar enligt sitt inlösenavtal.

Den tekniska utvecklingen har öppnat en rad möjligheter för nya produkter och tjänster för försäljning och betalningssätt på Internet. I och med att man sköter betalning och leverans av produkter över Internet så uppstår det stora fördelar, både för kunden i form av enklare betalning och snabbare leverans av produkten, och för säljaren i form av att marknadsföra och sälja produkter på nätet. Utvecklingen av elektronisk handel har än så länge huvudsakligen varit teknikdriven. En av effekterna som man märkbart kan se är en rad av olika lösningar på problemet med säkra betalningar över Internet.

Det nya betalningssystemet SET är en väldigt ny företeelse och för närvarande så testas den av kunder runt omkring i landet. Efter att testet har genomförts så kommer man att se vilken effekt det har haft och vilken effekt det kommer att ha. SETs användning av krypterings-nycklar kan man jämföra med det som används i det militära, bägge använder samma kryptering, 1024-bitars som är det bästa som finns tillgängligt idag.

När det gäller frågorna som ställdes till de personer som jobbar med SET dagligen, ska det avsnittet inte betraktas som huvuddel i uppsatsen, och det har heller inte varit min ambition utan det har varit att få information och tankar från personer som är insatta i SET och inte något som redan var dokumenterat. En gemensam åsikt som de hade var att SET kommer att ta över transaktioner på Internet. Detta håller jag med om därför att en viktig kugge i hjulet är att SET har tagits fram av världsledande IT- och kreditkorts företag.

Efter det att pilottestet har genomförts så kommer man att se vilken effekt SET har haft på testkunderna. Största svårigheten tveksamheten hos kunderna. SET håller en mycket hög säkerhet men det finns ingen garanti på att det fungerar till 100%. För några månader sedan så hade några personer kommit in i USAs säkerhetstjänsts datorer, så att när det handlar om stora system så är det näst intill omöjligt att få 100% säkerhet. Skulle man jämföra SET med att betala med kontokort i en butik, så är SET mycket säkrare. Det räcker ju bara med att se vilken kontokortsnummer en person har och därefter så är det bara att handla.

Fördelarna med SET:

- Kortinnehavare och försäljningsställen kan känna sig säkra på att det är lika säkert som när folk handlar från nätet eller som vid vanliga inköp.
- Eftersom SET är en global standard som de flesta stora företagen står bakom, bl a IBM, Microsoft, Netscape, Visa och MasterCard, så ger det kunderna och försäljningsställena stora möjligheter till att handla varor och produkter över hela världen.
- Man får som konsument, handlare och betalningsförmedlare legitimera och bevisa att man är behöriga att göra affärer över Internet.
- Andra personer kan inte se vad och hur mycket det är som har köpts.
- Det går inte att som utomstående göra några ändringar i köporderna.
- Standarden för inköp är plattforms oberoende, dvs kortinnehavare med SET-anpassad mjukvara kan kommunicera med handlarens SET-mjukvara oberoende på datortypen.
- Systemet är utvecklat på ett sådant sett så att det skall skapa största möjliga säkerhet för alla inblandade parter. I form av att den tredje parten och den avancerade krypteringen används så kan man säga att systemet är lika säkert eller kanske säkrare än vanliga kontokortsbetalningar. Till skillnad från betalning i affärer med kontokort får säljaren inte tillgång till kundens namnunderskrift.

Nackdelarna med SET:

- Det lämpar sig inte för mikrobetalningar därför att administrations kostnaderna är ganska höga.
- Systemet tillåter inte anonymitet för köparen, men möjligen för säljaren.
- Det går inte att utföra transaktioner mellan två privatpersoner då mottagaren måste vara auktoriserad handlare av kortföretaget eller banken.

Eftersom gränssnittet är olika beroende på leverantörerna så kan det vara svårt som användare att sätta sig in i det. Jag tror att det skulle vara bättre ifall man hade någon sorts standard där alla leverantörer hade flera saker gemensamt så att det skulle underlätta för användarna. I och för sig så tyckte de personer som intervjuades att det var ganska lätt att sätta sig in i det, men skall tänka på att det är lättare för en person som håller på med datorer varje dag.

En viktig fråga är hur påverkar det människan att göra t ex sina betalningar via Internet istället för att gå till banken ? Nu för tillfället så finns det ju flera saker som man skulle göra hemma istället för att göra det någon annanstans. Människan blir lat, och man tappar kontakten med människor ifall man skulle göra allt hemifrån. Men mycket av detta beror på hur människan använder sig av den nya tekniken. Tekniken fortsätter raka spåret framåt men det är fortfarande vi som bestämmer till vilken grad man kommer att använda sig av den nya tekniken.

Bilaga 1:Begreppslista

Kortinnehavare	En auktoriserad innehavare av ett betalningskort som har stöd av en utfärdare, och registrerad för att utföra elektronisk handel.
Handlare	En handlare som förser med varor, service, och/eller information som tillåter betalning för de elektroniskt, och kan kanske förse försäljnings service och/eller elektronisk leverans av artiklar för försäljning så som information.
Utfärdare	En finansiell institution som stödjer utgivande av betalningskort produkter till individer.
Förvärvare	En finansiell institution som stödjer handlare genom att förse service för bearbetning av betalningskortstransaktioner.
Betalningsport	Ett system som förser elektronisk handel service till handlare för att stödja förvärvare, och samverkar till förvärvaren för att stödja bemyndigandet och mottagande av transaktioner.
Kortorganisation	En franchiser av betalnings system.
Certifikat Myndighet	En agent av ett eller flera betalningskortorganisationer som förser för skapande och distribuerande av elektroniska certifikat för kortinnehavare, handlare, och betalningsportar.
Mikrobetalning	En mycket liten betalning, t ex 0,05 kr. Mikrobetalningar gör det möjligt att ta betalt för t ex enstaka nyhetsartiklar.
Kryptering	Att göra om en fullt läsbar text till oläsligt. Används till att skydda information. Om obehöriga får tag på informationen så kan de inte läsa det därför att istället för vanlig text så står det en massa konstiga tecken. Strykan i den krypteringsform som SET bygger på räknas i bitar (*bits)*. SETs krypteringen är 1024 bitar stark, vilket är i klass med militär säkerhet.
Dekryptering	För att man skall kunna läsa den information som skickas till sig själv så måste man dekryptera informationen för att kunna läsa den. Med andra ord så används det till avkodning av information.
Nyckel	En serie siffror och tecken som används till att kryptera information. Ju längre nycklarna är så är krypteringen starkare och det blir svårare för obehöriga att komma på informationen.
Digitalt Certifikat	Ett meddelande som är digitalt och som innehåller information om kontokortsinnehavare. Det digitala certifikatet innehåller även nycklar som används vid kryptering och dekryptering. När certifikatet används vid SET-transaktioner så binds kontonumret

	till krypteringsnyckeln.
Digital Signatur	Är en krypterad information där det används till att visa att ett meddelande verkligen kommer från rätt avsändare.
RSA	En asymmetriskt krypteringsmetod som är uppkallad efter dess skapare Rivest, Shamir och Adleman.
Server	En dator som är anslutet till ett nätverk där den erbjuder tjänster till andra datorer på nätverket. Ett exempel är att istället för att installera Word i alla datorer så kan man installera det i servern och där kan alla som är anslutna till nätverket öppna Word utan att programmet är installerade på sin egen dator.
DES	DES är en symmetrisk krypteringsmetod som är skapad av bl a IBM.
Digital plånbok	En digital plånbok är en allmän kryptografisk teknik för att kryptera data och sända krypterings nyckeln tillsammans datan. Generellt, så används en symmetrisk algoritm för att kryptera data, och en asymmetrisk algoritm används till att kryptera krypterings nyckeln.
Hash algoritm	Säker hash algoritm (SHA-1) skall användas för alla hashar i denna version av SET, inklusive hashen som används i signaturen.
Bit	Datorer kommunicerar med ‘0’ och ‘1’. Där en bit är representerad som en ‘1’ eller en ‘0’.

7 Källförteckning

SET - det virtuella kortet
http://www.pagina.se/navigera/1997/Nr6/set.html
1998-02-03 kl. 13.32

Säkra Elektroniska Betalningar
http://mark.sebank.se/sebank/kort/set.htm
1998-04-12 kl. 10.24

Elektroniska Betalningsformer
http://194.251.183.23:81/elekbetal.htm
1998-03-03 kl. 11.33

Så här fungerar SET
http://www.idg.se/mikrodatorn/testcentret/teknik/md9712/set.htm
1998-04-13 kl. 14.24

http://www.knowit.se/Inlagg_v11.html
1998-02-15 kl. 15.23

MasterCard International
http://www-stl.mastercard.com/set/vendorstatus2.htm
1998-03-12 kl. 10.23

Secure Electronic Transaction - FAQ
http://multimedia.snp.com.sg/set2/faq.htm
1998-02-10 kl. 11.23

http://www.cisivlelight.com/mpeg/newswire/sep97/00010422.htm
1998-04-07 kl. 13.30

http://www.1stud.ii.uib.no/¨s768/I191.html
1998-02-20 kl. 11.20

http://as400service.rochester.ibm.com/as400/as400v4rl/97nc/97ncp23.htm
1998-03-22 kl. 14.40

Visa
http://www.visa.com
1998-04-23 kl. 10.20

Pro Gloria Musicae
http://www.pgm.com
1998-02-17 kl. 13.32

RSA Data Security
http://www.rsa.com
1998-04-29 kl.14.44