SISU

PUBLIKATION 96:04

DOKUMENT – APRIL 1996

Betalsystem för Internet

– en överblick

Mathias Axling

SVENSKA INSTITUTET FÖR SYSTEMUTVECKLING

SISU

Innehållsförteckning

1 Introduktion

Från att ha varit ett nätverk främst för högskolor och universitet, har Internet bara under de två senaste åren vuxit till ett begrepp alla känner till. Tack vare möjligheten att grafiskt och användarvänligt kunna presentera information, har möjligheten öppnats för alla att kunna använda sig av Internet. Den marknad som Internetanvändarna utgör, började växa sig tillräckligt stor för att verka intressant. Snart började kommersiella tillämpningar av hypertextsidor dyka upp. Först som enkla företagspresentationer på en World Wide Web-sida, senare som försäljning av varor mot att kunden skickade sitt kreditkortsnummer för fakturering. Sådana lösningar är dock opraktiska, och kunden är i viss mån beroende av handlarens goda vilja. Nya lösningar krävdes, och lät inte vänta på sig. För närvarande finns en mängd förslag på olika betalsystem, som bygger på kreditkort, elektroniska checkar som skickas över nätet, och digitalt signerade kontanter. Vissa lämpar sig för speciella tillämpningar, och andra siktar på att bli det dominerande betalningsmedlet för framtiden. Genom att betalningarna sker över ett öppet nätverk som Internet, är betalsystemen utsatta för vissa problem som de existerande finansiella nätverken inte har. Mängden användare anslutna till nätet, vars tillgång till nätet inte kan begränsas via yttre säkerhetsåtgärder, och möjligheten till avlyssning och kopiering av den information som sänds över det, gör dessa betalningssystem är särskilt sårbara för avsiktligt intrång, förfalskning och sabotage.

För närvarande finns ingen standard för elektronisk handel över öppna nätverk, men en mängd förslag finns. Några av dessa har möjlighet att utvecklas till de-facto standard eller accepteras som standard av de organisationer som arbetar för framtagande av sådana.

World Wide Web Consortium, där SISU är medlem, är en organisation som arbetar med framtagande av standarder för World Wide Web och att främja den fortsatta utvecklingen av denna tillämpning. CommerceNet, liksom dess svenska motsvarighet Swebizz, arbetar med att främja kommersiella tillämpningar av Internet, och framtagande av standarder för dessa. CommerceNet och Swebizz, där SISU är medlem, fungerar också som nätverk för utbyte av information om elektronisk handel, och har medlemmar från både teknik- och tillämpningssidan. Genom att samla erfarenheter och sammanföra intressen från olika håll skapas synergieffekter som underlättar och påskyndar utvecklingen mot en öppen elektronisk marknadsplats.

Syftet med denna rapport är att ge en överblick av de olika betaltjänster som finns för Internet. En kort beskrivning av de olika förslagen, med lite längre genomgångar av de just nu viktigaste, kommer att ges. Vidare är det av intresse att beskriva typiska och lämpliga användningsområden och begränsningar hos de olika systemen. Överblicken kommer att använda sig av en strukturering av de olika betalningssystemen jag har funnit generellt användbar, och som i vissa bitar är allmänt vedertagen. I de fall den bygger på andras arbete har så angivits. Överblicken begränsas till att omfatta

betalningssystem avsedda för Internet, med tonvikt på de system som inte använder sig av särskild hårdvara, och är tillgängliga i dagsläget. Även kortare orienteringar om begrepp som omnämns i rapporten, och en kort beskrivning av marknaden kommer att inkluderas.

1.1 Betalsystemens abstraktionsnivåer

Systemen kan med fördel beskrivas i tre abstraktionsnivåer. Dessa har jag valt att kalla modell, dataflöde och mekanismer, fritt efter ett förslag publicerat av Dr Philip M. Hallam-Baker, World Wide Web Consortium.[1] Denna indelning valdes för att den ger ganska tydliga avgränsningar, och de fördelar som ges av att den används av W3C. Det bör noteras att de tre nivåerna är bundna till och begränsar varandra. Modellen ställer krav på dataflödet, och val av dataflöde begränsar möjliga mekanismer. Modellnivån motsvarar inte helt Policynivån i Dr Hallam-Bakers modell, utan vissa av de koncept som ingår i denna tas upp under övriga relevanta egenskaper.

Modellen motsvarar systemets gränssnitt mot användaren, och den form av transaktion systemet utför. Systemen kan hantera transaktioner med värdebärande valutasymboler, som kontanter, eller betalningsorder utgörande instruktioner om ändringar i registreringar av nominell valuta hos banker och kreditinstitut. Kort sagt kan systemet fungera som kontanter eller debet/kreditorder och kredit/debetkortsbetalningar. Dessa typer av system tas upp senare i denna rapport.

Dataflödet är en beskrivning av den datalagring och kommunikation mellan köpare, handlare, bank/kreditinstitut och systemleverantörer som systemet kräver. Inte bara överföring av betalningsmeddelanden, utan också kontosaldon, kunduppgifter och liknande.

Mekanismerna är de protokoll och/eller krypteringsmetoder som används för att uppnå önskad säkerhet och funktion hos systemet. Systemen kan använda sig av generella säkerhetsprotokoll, vilket är vanligt när det gäller överföring av kreditkortsinformation, eller specifika krypteringssystem, vilket är fallet med de flesta system för digitala kontanter.

1.2 Relevanta egenskaper hos betalningssystemen

Vissa egenskaper är speciellt viktiga att beakta just när det gäller betalsystem avsedda för Internet. Några av de jag anser mest relevanta finns listade i bokstavsordning nedan.

Acceptans och tillgänglighet: Ett faktum som ofta glöms bort i den ivriga diskussionen av krypteringsalgoritmer, säkerhetsfrågor och databashantering är att det till slut faktiskt är kunderna som bestämmer. Detta kan verkar utan tvekan till fördel för system som redan har stort kundunderlag, som

[1]Hallam-Baker 1995.

kreditkortslösningar stödda av VISA och MasterCard, och de system som redan är kända. Andelen tekniker bland användarna av Internet, och den tänkta marknaden för elektronisk handel, sjunker stadigt. De flesta presumtiva användare har ingen möjlighet att själva bedöma säkerhet och prestanda hos ett visst system annat än efter vad som sägs om det i media och av hur det beter sig under användning. Detta gör det svårt att bedöma vilket system som kommer att dominera marknaden om några år. Det kanske inte blir den tekniskt bästa lösningen, utan den enklast tillgängliga och mest spridda. Ju fler handlare som accepterar betalsystemet, desto fler kunder kommer att använda det. Denna fråga har också en viss koppling till kompatibiliteten hos systemet. Det är också troligt att ett system som lätt kan integreras med övriga system har lättare att bli accepterat. Ingen vill ju bli sittande på de digitala kontanternas motsvarighet till betamax-video. Lagstiftningen vad beträffar upphovsrätt och giltigheten av digitala signaturer släpar också efter i stora delar av världen.

Anonymitet: Kundens anonymitet vad beträffar transaktioner gentemot säljare, betalningsförmedlare och banker. Kunden kan ha partiell anonymitet, om identiteten inte röjs, eller total, om transaktionerna är helt ospårbara. Vissa använder termerna anonymitet (*anonymity*) och ospårbarhet (*untraceability*).[2] Då mer och mer handel kan komma att ske via elektroniska media, blir frågan om anonymitet och privatliv mer aktuell. Kunder är troligtvis beredda att göra vissa köp utan anonymitet; vid icke-elektronisk handel är detta ofta fallet. Man accepterar att vissa transaktioner bokförs av handlare eller kreditkortsföretag när man köper till exempel bilar, hus eller vissa andra varor. Men hur många skulle vilja att vartenda köp eller transaktion de gjorde skulle registreras? Till exempel köp av politiskt känslig litteratur eller tidskrifter kan i vissa länder vara något man helst inte vill ha registrerat, om inte annat för karriärens skull.

Betalningsstruktur: I betalningsstrukturen ligger aspekter som huruvida systemet hanterar förbetalda, värdebärande symboler, så kallad symbolisk valuta, eller betalningsinstrument eller -order innehållande instruktioner om och auktorisering av ändringar av nominell valuta.[3] Nominell valuta utgörs av registreringar av valutainnehav, till exempel konton hos banker. Systemet kan använda sig av särskilda konton hos en uppsamlingsagent, eller vara direkt kopplat till de existerande finansiella nätverken. Detta medför skillnader i risktagande och kostnad mellan de olika parterna i systemet. Hantering av betalningsinstrument för nominell valuta är ofta kopplat till vissa avgifter, något kan göra systemen olämpliga för hantering av mycket små belopp, så kallade mikrobetalningar. Detta avhjälps i många system genom ackumulation av mikrobetalningar hos en uppsamlingsagent för att sprida administrativa kostnader över flera betalningar.

Kompatibilitet: Betalningssystemets möjligheter att på ett enkelt sätt integreras och samexistera med existerande betalningssystem för banker och kreditkorts-institut är viktiga för dess förmåga att bli accepterat och använt. Ett system som kan användas både i snabbköpet runt hörnet och på WWW har en fördel

---

[2]Janson, Waidner 1995.

[3]Camp, Sirbu, Tygar 1995.

mot de system som endast har tillämpningar för Internet. De har en mycket större potential än endast handel på Internet. Exempel på förslag som syftar till att ta fram betalningsmedel för användning både på och utanför Internet är Mondex, FSTC Electronic Check Project och Digicash olika produkter. Kreditkortssystem som VISA/MasterCards SET-protokoll överför ett existerande betalningssystem till Internet .

Robusthet: Systemets tålighet vad beträffar överlastning och oförutsedda fel i kommunikationer och hårdvara är viktiga för dess prestanda och säkerhet. Överlastning eller tillfälligt fel i en uppsamlings- eller förbindelseagents server kan medföra att transaktioner förblir oavslutade under en längre tid. Det är önskvärt att transaktionerna avslutas inom så kort tid som möjligt, för att undvika problem med oavslutade köp och utebliven leverans. Dessa frågor har implikationer för skalbarheten hos systemet.

Skalbarhet: Internetanvändningen ökar fortfarande med 10 procent i månaden. Ett system som skall ha någon potential för att komma till allmän användning i stor skala, måste kunna hantera den teoretiskt maximala användningen av systemet. Speciellt för digitala kontanter och checkar är detta viktigt, då mängder av mikrotransaktioner måste kunna hanteras utan fördröjningar eller felaktiga transaktioner. Här har off-linesystem en klar fördel, då de inte har samma benägenhet för "flaskhalsar" som on-linesystem. Distribuerade system, som NetCheque, är också en lösning på problemet. Kontroll av dubbelspendering görs oftast on-line mot en databas med använda serienummer. Även om alla pengar har ett utgångsdatum, kan systemet bli överlastat av mängder med småtransaktioner som skall kontrolleras. Mängden serienummer i databasen beror ju inte bara på livslängd hos pengarna, utan även på omsättningshastigheten.

Säkerhet: Det faktum att så många har tillgång till nätverket, och kan få tillgång till informationen som passerar, är ett hot mot säker handel på Internet. Ett annat problem är att många av det datorer som är anslutna inte har någon form av säkerhet, och intrång lätt kan göras. Dubbelspendering är en fråga som är mycket viktig för system som bygger på digitala kontanter. Även möjligheter att få transaktionerna bindande är nödvändiga för att handel skall kunna ske. Eftersom viss säkerhetsteknik är belagd med exportförbud i USA, kan vissa lösningar utvecklade i USA inte exporteras till övriga världen.

2 Strukturering av överblicken

Den vanligaste uppdelningen av betalningssystem görs i tre grupper, med avseende på den betalningsform som den överförda betalningsinformationen utgör. Som nämnts ovan utgörs dessa av värdebärande valutasymboler, som kontanter, eller betalningsorder utgörande instruktioner om ändringar i registreringar av nominell valuta hos banker och kreditinstitut. Gränserna kan ibland vara något otydliga, på grund av att förutsättningarna för elektroniska betalsystem skiljer sig från de för "fysiska" system. Andra viktiga uppdelningar är mellan on-line och off-linesystem, öppna och slutna system, och system som erbjuder uppsamling av betalningar eller direkt förbindelse med existerande clearingnätverk. Den första uppdelningen utgår från modellen, medan de andra utgår från dataflödet. Andra uppdelningar som kan göras är efter mekanismen. Dock förekommer system som använder sig av symmetrisk kryptografi, asymmetrisk kryptografi, protokoll som använder kombinationer av dessa, eller ingen kryptografi alls, vilket gör uppdelningen mindre användbar.

2.1 Kontanter, checkar och kreditkort

De modeller för betalning över Internet som tagits fram bygger oftast på en idé eller modell för valutaöverföring tagen från tidigare system. Kontanter, checkar och kredit/debetkort är tre modeller för betalning till vilka de flesta betalningsmodeller för Internet kan sorteras.[4] [5] Denna indelning är också allmänt vedertagen.

2.1.1 Kontantmodeller

Kontanter är symboler som i sig utgör ett värde, precis som ett mynt eller en sedel. Värdet av kontanter, eller symboliska pengar måste först debiteras kunden i någon annan form av valuta, som ett bankkonto. System baserade på kontantmodeller grundar sig på möjligheten att utfärda valutasymboler vars äkthet kan verifieras oberoende av den utfärdande institutionen.

Med fysiska sedlar sker detta genom sedelnumret, och för att ytterligare skydda sig mot förfalskningar används också speciellt papper, vattenstämplar och text som endast går att läsa i belysning med UV-ljus. Digitala kontanter, däremot, består av ett serienummer och eventuell annan information den utfärdande institutionen lagt till, existerande endast som information lagrat på något elektromagnetiskt medium. Trots detta går det att bortom all tvekan garantera valutans äkthet. Detta är möjligt genom asymmetrisk kryptografi, där krypteringsnyckeln – som hålls hemlig – inte går att härleda från dekrypteringsnyckeln. Banken eller den utfärdande institutionen kan signera

---

[4]Hallam-Baker 1995.

[5]Kalakota, Whinston 1995, s 299 ff.

pengarna med sin hemliga nyckel, och dekrypteringsnyckeln finns tillgänglig för alla, så att vem som helst kan kontrollera att pengarna är äkta.

Digitala kontanter kan erbjuda total anonymitet och mikrobetalningar. Dubbelspendering av pengar är dock ett problem med digitala pengar. En eventuell förfalskare har inga som helst problem att helt enkelt göra kopior av äkta digitala pengar, utan att behöva knäcka bankens signatur. Det måste alltså finnas ett skydd mot att göra hundra kopior av en digital sedel, och bli miljonär på några minuter genom att betala hundra handlare med samma pengar. Detta löses i on-linesystem genom kontroll mot en databas med spenderade pengar. Det är också ett stort problem om den utfärdande bankens signatur skulle röjas, till exempel genom internt spionage. På grund av den mycket större skalan hos brottet vid förfalskning av digitala pengar, skulle en sådan händelse kunna undergräva hela systemet på mycket kort tid. Detta är ett problem som får mycket mindre omfattning för checkmodeller.

2.1.2 Debet/kreditorder eller checkmodeller

Då systemet hanterar order om ändringar av ackumulerande konton hos en mellanhand, eller saldoändringar direkt hos inblandade banker, talar man om debet/kreditsystem, eller digitala checkar. En check utgör en order eller ett kontrakt om debitering av utställarens konto, till förmån för betalningsmottagaren. Checken görs brukbar genom utställarens signatur på checken. Samma mekanism som nämndes ovan för att utfärda digitala kontanter, kan också användas för digitala signaturer på betalningsorder som skickas över nätverk. Den fundamentala skillnaden mot kontanter – och gränserna är inte alls så skarpa när det gäller elektroniska betalningsmedel – är att utställaren av betalningsordern är den som gör betalningen. Det är en fördel ur skalbarhets- och avgiftssynpunkt om checksystem är distribuerade och/eller kopplade direkt till existerande finansiella nätverk. Checksystem är inte lika känsliga för förfalskning som kontantsystem, då det endast är ett konto som drabbas. Genom uppsamlingsagenter kan dock checksystem göras lämpliga för mikrobetalningar.

2.1.3 Säkert överförd kreditkortsinformation

Säkert överförd kredit/debetkortsinformation dök upp som en av de första lösningarna för elektronisk betalning på Internet. De första varianterna var inte ens säkra, utan man hoppades på att ingen skulle avlyssna trafiken när kundens kreditkortsinformation sändes över nätet. Många av de första systemen var också slutna, det vill säga man sände sitt kreditkortsnummer till en viss handlare för att kunna handla där senare. Detta innebär att man måste sända sitt kreditkortsnummer till varje handlare man vill göra affärer med. Handlaren får då tillgång till kreditkortsnumret, och kan om han är oärlig missbruka detta. Senare system är kopplade till det vanliga clearingsystemet för kreditkortshandel, så att en Internethandlare inte nämnvärt skiljer sig från en butik med kortläsare.

Säkert överförd kreditkortsinformation fyller ett stort behov hos kunder intresserade av handel på Internet. Det är ett mycket vanligt betalningssätt vid köp utanför Internet, och bara tillgängligheten och den vida acceptansen av kreditkortsbetalningar hos allmänheten gör systemen till självskrivna alternativ för elektronisk betalning. Kreditkortsbetalningar är lämpliga för överföringar av större belopp. Kreditkortsinnehavaren betalar efter att handlarens konto krediterats. Detta ger kunden större säkerhet vad gäller falska betalningskrav, men osäkerheten för kreditkortsfirman, och omkostnader för transaktionen tas ut i form av avgifter per överföring, något som gör systemen olämpliga för mindre belopp. Ett nyligen presenterat protokoll presenterat av MasterCard och VISA, SET (*Secure Electronic Transactions*), verkar ha goda möjligheter att accepteras som standard.

2.2 Öppna och slutna system

Slutna system är lösningar där kunden måste ha en fast relation med handlaren innan köpet inleds. Det vanligaste är att kunden har ett fast konto hos handlaren, där köpen ackumuleras. Betalningen sker för det mesta sedan utanför Internet, via kreditkort eller med vanlig faktura. I öppna system behöver inte kunden och handlaren ha haft någon tidigare kontakt med varandra, utan köpet kan ske utan upprättande av relation dem emellan. Det enda som krävs är att de använder samma betalningssystem. Motsvarigheter i den fysiska världen är en bokklubb, där du inte kan köpa en bok om du inte först är medlem, och en bokhandel, där du kan gå in när som helst och utan förvarning köpa en bok. De system där kunden måste ha ett särskilt konto hos en uppsamlingsagent utgör ett slags mellanting; det mest önskvärda vore att kunden inte behövde använda några andra konton än de han redan har. Ju enklare och snabbare det är att börja använda ett betalsystem, desto mer sannolikt är det att kunder ansluter sig, och gör impulsköp.

2.3 On-line och Off-linesystem

Transaktioner över nätverk kan ske on-line eller off-line.[6] Om transaktionen sker on-line, behövs kontakt med en tredje parts server för att transaktionens äkthet skall kunna kontrolleras. De flesta av de system som behandlas i denna överblick är on-linesystem. De har generellt den fördelen att ingen specifik hårdvara behövs för kunden eller handlaren. Nackdelen är att de kräver mer kommunikation mellan de inblandade parterna, vilket belastar nätverket och tar längre tid.

I ett off-linesystem behövs inte kontakt med någon tredje part under transaktionen. De kräver oftast någon form av dedicerad hårdvara, som så kallade elektroniska plånböcker. Dessa består av så kallade smarta kort, eller PDA (Personliga Digitala Assistenter, eng. Personal Digital Assistants) med läsare för smarta kort. De flesta av dessa system är inte avsedda för Internet, även om möjligheten finns, och kommer endast att ges en kort genomgång.

---

[6]Janson, Waidner 1995.

2.4 Uppsamlingsagenter och förbindelseagenter

Ett system som använder en uppsamlingsagent (*collection agent*) fungerar genom att kunden och/eller handlaren har ett fast konto hos ytterligare en aktör. Denne administrerar kontot och bokför inkomster och utgifter. Då en betalning görs, tar uppsamlingsagenten emot denna, informerar handlaren om att betalningen är utförd, och flyttar vid senare tillfälle över pengarna till handlarens "vanliga" bankkonto. Vanligt för kunden är att uppsamlingsagenten med jämna mellanrum tar ut spenderad summa plus avgifter från köparens kreditkort eller checkkonto. Detta möjliggör mikrobetalningar via checkkonto eller kreditkort, eftersom avgifterna för kort eller checkkonto sprids över många betalningar.

En förbindelseagent (*connection agent*) tillhandahåller en länk eller "brygga" till banker och/eller kreditkortsinstitut. Då kunden gör ett köp, går transaktionen från handlaren till agenten, som sköter kommunikationen med bank eller kreditkortsinstitut. Skillnaden mot en uppsamlingsagent är att kunden inte behöver ha ett extra konto hos tredje part. Denna typ av system har också möjligheten att vara distribuerade, och inte använda sig av en central server, som kan bli överbelastad.

3 Kort om Kryptografi

Förutom några få system som använder sig av en extra konfirmering av köpet via email eller telefon, baseras de flesta system på någon form av kryptering vid överföring av meddelandet, och signaturer för godkännande av transaktionen. Det finns två huvudtyper av kryptografi: symmetrisk (eng. shared-key), och asymmetrisk (eng. public-key).[7][8]

Symmetrisk kryptografi kräver att båda parter, till exempel kund och handlare, har tillgång till gemensam kunskap om krypteringsnyckeln. Från den ena krypteringsnyckeln kan den andra lätt beräknas. Tidigare var det också så, att om krypteringsalgoritmen blir allmänt bekant, blir det mycket lätt att därifrån beräkna nyckeln. DES (Data Encryption Standard), framtagen 1975 av NSA (National Security Agency), NBS (National Bureau of Standards) och IBM, löste dock detta problem genom att definiera en grupp av krypteringsalgoritmer, med en algoritm definierad för (nästan) alla tal lägre än 256. Detta gör det i princip omöjligt att knäcka systemet. Det har även framkommit nya system, som är snabbare än DES, även om DES är mycket vanligt idag. Dock medför symmetrisk kryptografi vissa problem. Överföring av krypteringsnyckeln till de inblandade måste ske skyddat, och måste ske innan kommunikationen inleds. Båda parter i ett system har också tillgång till alla nycklar. Det går därför inte att bevisa att det verkligen är kunden som har gjort transaktionen. Symmetrisk kryptografi är dock snabbare är asymmetrisk, som måste utföra operationer med mycket stora tal. I till exempel PGP[9] (Pretty Good Privacy), används därför asymmetrisk kryptografi för att sända nyckeln till en symmetrisk krypteringsalgoritm, vilken sedan används för att sända själva meddelandet. Detta för att göra systemet snabbare, med bibehållen hög säkerhet.

Asymmetrisk kryptografi baserar sig på möjligheten att beräkna en krypteringsnyckel och en dekrypteringsnyckel på sådant sätt att den ena nyckeln inte kan beräknas från den andra, ens med tillgång till algoritmen. Den ena nyckeln hålls hemlig, och den andra sprids ut (därav public-key). När ett krypterat meddelande skall skickas till innehavaren av den hemliga nyckeln, krypteras detta med den offentliga nyckeln. Meddelandet kan sedan endast dekrypteras med den hemliga nyckeln. Omvänt kan ett meddelande krypteras med den hemliga nyckeln. Vem som helst kan sedan kontrollera dekryptera meddelandet för att kontrollera att det kommer från innehavaren av den hemliga nyckeln. Detta möjliggör så kallade digitala signaturer, som kan garantera avsändarens identitet, något som används för att garantera äktheten hos digitala pengar i system som NetCash och ecash. Asymmetrisk kryptografi används också för "digitala kuvert", som döljer meddelandets innehåll för de mellanhänder som hanterar det, och för "stämpling" av information för att garantera att den inte blivit ändrad. DigiCash använder digitala kuvert för

---

[7]Solinsky 1995.
[8]Pfleeger 1989, s 88 ff.
[9]Kalakota, Whinston 1996, s 208-210.

att hindra banken från att knyta pengarna till en specifik kund. I CyberCash kreditkortssystem används de för att dölja känslig kreditkortsinformation för handlaren. Den i särklass mest kända asymmetriska krypteringssystemet är RSA, döpt efter dess skapare Rivest, Shamir och Adleman. Även den teknik Digicash använder sig av grundar sig på asymmetrisk kryptografi, utvecklad av företagets grundare, David Chaum.

SSL[10] (Secure Sockets Layer) är ett generellt protokoll för säker kommunikation mellan WWW-läsare och -servrar. Det bygger på RSA-teknik, som tyvärr är belagd med exportförbud i USA. Den nedbantade exportversionen har kunnat knäckas genom "brute force"-metoden, det vill säga testning med alla möjliga dekrypteringsnycklar. Även USA-versionen har kunna knäckas; detta berodde dock på ett fel i implementationen som medförde att de genererade nycklarna inte var helt slumpmässiga, vilket är en förutsättning för teknikens säkerhet.

[10]Freier, Karlton, Kocher 1996.

4 Betalsystem för Internet

Nedanstående genomgång använder sig av de uppdelningar och begrepp som nämnts ovan. Uppräkningen kan tyvärr inte sägas vara helt fullständig, då några mindre betalsystem kan ha förbisetts, och nya ständigt tillkommer. De största och mest lovande systemen får en längre genomgång, medan mindre och lokala system endast ges en kortare beskrivning. System som baserar sig på särskild hårdvara eller ännu inte tagits i bruk får också en kortare genomgång. System för vilka inga litteraturhänvisningar görs har information främst publicerad på WWW.

4.1 Slutna system

Slutna system baseras på att kunden knyts i en fast relation till handlaren, till exempel genom att kunden har ett konto hos handlaren, som debiteras då ett köp görs. En annan variant är att handlaren vid första köptillfället ber om kundens kreditkortsnummer, som levereras via säker kommunikation eller utanför Internet, och sedan debiteras vid återkommande köp. Betalning sker utanför Internet via faktura eller via handlarens ordinarie rutiner för kredit- och betalkortshandel. Generellt kan sägas att dessa system inte ställer andra krav på mekanismer än att kommunikationen sker via generella säkerhetsprotokoll. Lösningen är enkel för handlaren, men erbjuder inte några fördelar för kunden.

Det vanligaste är att ett företag administrerar en WWW-server på vilken olika företag kan köpa plats. Exempel på dessa är BarclaySquare, som drivs av BarclayCard för BarclayCards kunder, vilket har den positiva effekten att det är ointressant att dölja information för mellanhanden. Andra exempel är NetMarket, Downtown Anywhere eller Internet Shopping Network, som använder Netscape Merchant Server.

Nackdelar med dessa system är att de inte erbjuder någon anonymitet, och inte heller någon flexibilitet. Vidare är de oftast inte lämpliga för mikrobetalningar, på grund av de avgifter kreditkortsföretagen och mellanhänderna tar. Framtidens digitala handel kommer att omfatta mer än bara WWW-butiker. Denna typ av betalning har en nisch, men är för begränsad för att täcka alla behov och möjligheter hos elektronisk handel.

4.2 Öppna system

Öppna system är mer flexibla och utgör definitivt framtiden för elektronisk handel. De mest framsynta systemen har också potentialen att erbjuda mycket mer är endast Internethandel, och vissa siktar till och med på att slutligen ersätta de existerande betalningsmedlen.

4.2.1 Kontantsystem

Med NetCash[11] köper kunder kontanter med hjälp av NetCheque, beskrivet nedan, som också utvecklats på University of Southern California, i ett system av kontantutfärdande NetCash-servrar kopplade till kontohanterande NetCheque-servrar. Kontanternas värde stöds genom att kontantservern krediteras de utfärdade pengarna i NetCheque-systemet. NetCash använder också NetCheque för överföringar mellan olika kontantservrar, och för att sätta in pengar på handlares konton. Eftersom kontanterna registreras på kontantserverns konto hos NetCheque-servern, är betalningarna i princip anonyma, men inte ospårbara. Det lämnas åt serveradministratörens godtycke att registrera uttagen eller inte. Då detta är ett extra lager på NetCheque, har systemet i stort samma egenskaper. Betalning från person till person är möjlig, men saknar kontroll av dubbelspenderade pengar. NetCash bygger på public-key-kryptografi för att verifiera pengarnas äkthet. Mekanismer av den typ som beskrivits av David Chaum kan användas för högre grad av anonymitet. I övrigt använder sig systemet av NetCheque som underliggande mekanism. Systemet är ännu inte i drift, och lyder under samma lagar som förbjuder export av NetCheque.

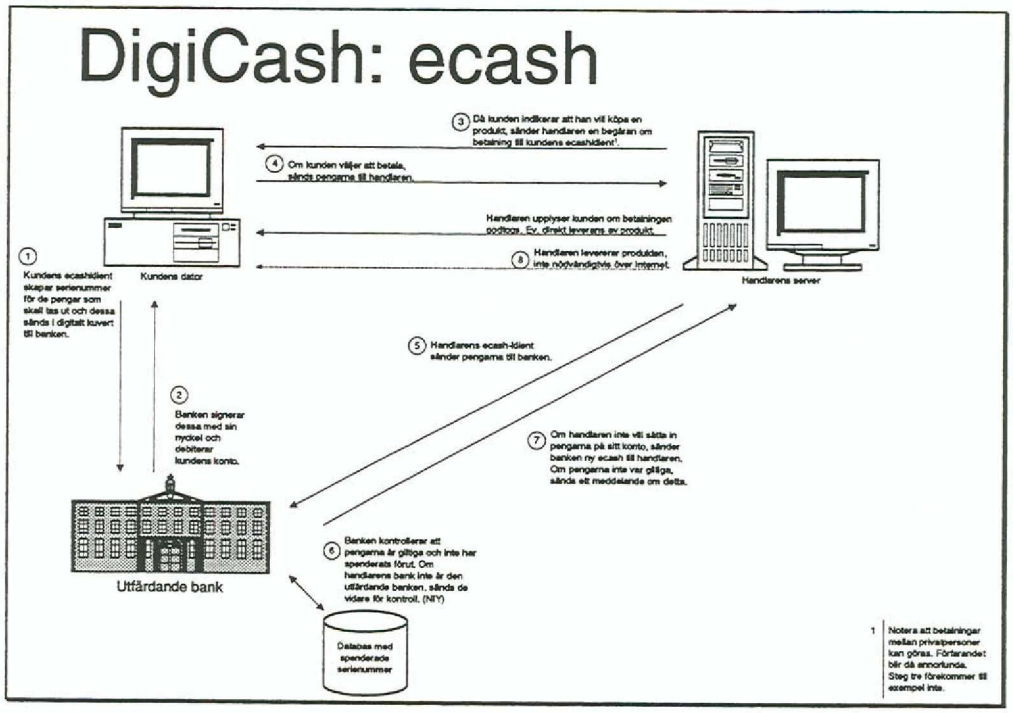
DigiCash har ett helt öppet system för elektroniska kontanter, ecash.[12][13] Systemet bygger på kryptografisk teknik utvecklad av David Chaum, som också grundat företaget.[14] Via uttag från sitt konto hos en bank som stödjer DigiCash ecash får kunden det aktuella beloppet i ecash. Det går i korthet till så att kundens programvara skapar serienummer för det aktuella beloppet, som skickas i ett så kallat digitalt kuvert till kundens bank. Där tas pengarna ut från kundens konto, banken sätter sin signatur på pengarna och skickar dem till kunden. Denne tar bort det digitala kuvertet, och de är färdiga att användas. Banken har aldrig sett serienumret på pengarna, och de kan därför inte spåras till kunden. Denne kan dock alltid bevisa att det är han som gjort en viss betalning. Systemet använder sig av asymmetrisk kryptografi, där ett nyckelpar används för att applicera och ta bort det digitala kuvertet och ett för att sätta bankens signatur på pengarna. Med den andra delen av bankens nyckel kan det sedan avgöras vilken bank som utfärdat dem. Kundens digitala kuvert som används för att göra serienumren oläsbara för banken är kommutativt med bankens signatur.[15]

Dubbelspendering kontrolleras dels genom att när kunden andra gången spenderar pengarna avslöjar sin identitet, dels genom kontroll med bankens databas över spenderade pengar.[16] Notera att samma pengar aldrig används två gånger; då en överföring av pengar mellan två personer sker, får mottagaren nya pengar i samma valör. Systemet fungerar via banker och är därför redan integrerat med betalningssystem utanför Internet. Det finns inga hinder för att via enkla mekanismer växla till och från andra betalningssystem för

---

[11]Medvinsky, Neuman 1993.
[12]Kalakota, Whinston 1996, s 302 ff.
[13]DigiCash 1996.
[14] Chaum 1992.
[15] DigiCash 1995.
[16]Chaum 1988.

Internet. Registreringen av spenderade pengar är dock ett hinder för skalbarheten. Visserligen har alla pengar ett utgångsdatum, men det maximala antalet serienummer som behöver lagras i databasen är ju snarare beroende av omsättningshastighet än giltighetstid.



Figur 1: Betalningsförfarande med ecash.

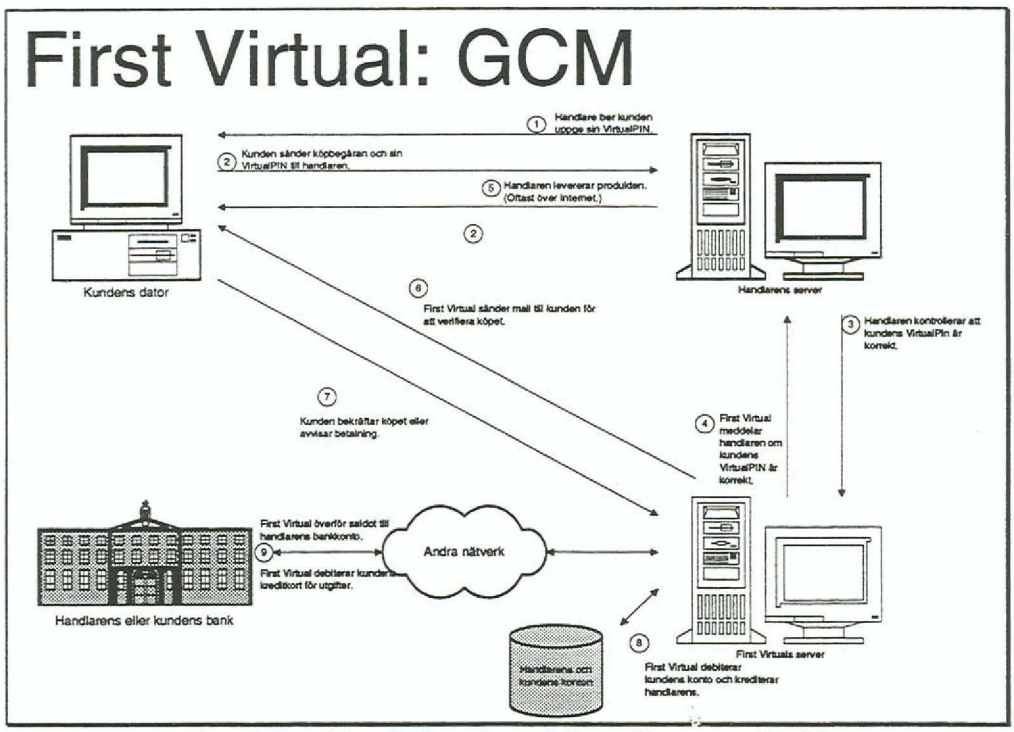
Net Banks Net Cash, ej att förväxla med USCs NetCash, är ett tidigt kontantsystem. Kunden köper kontanter i form av serienummer via en modemuppkoppling eller fax, och summan debiteras kundens telefonräkning. Handlaren tar emot pengarna i form av email och sänder dessa till Net Bank, som krediterar handlarens konto. Systemet erbjuder inget skydd mot avlyssning, men Net Bank rekommenderar att pengarna sänds krypterade med PGP. Kunden har inget sätt att bevisa att en betalning gjorts, eller att pengarna tillhör denne. Serienumren genereras slumpmässigt, utan digitala signaturer. Net Bank tänker sig att förfalskningar skall kunna spåras genom kontroll av upprepade försök med falska pengar.

4.2.2 Debet-kreditorder eller checkmodeller

First Virtual är ett uppsamlingssystem baserat på ett system för betalning kallat Green Commerce Model.[17][18] Klienten har ett konto hos First Virtual, där utgifter från köp och inkomster från försäljning ackumuleras. På

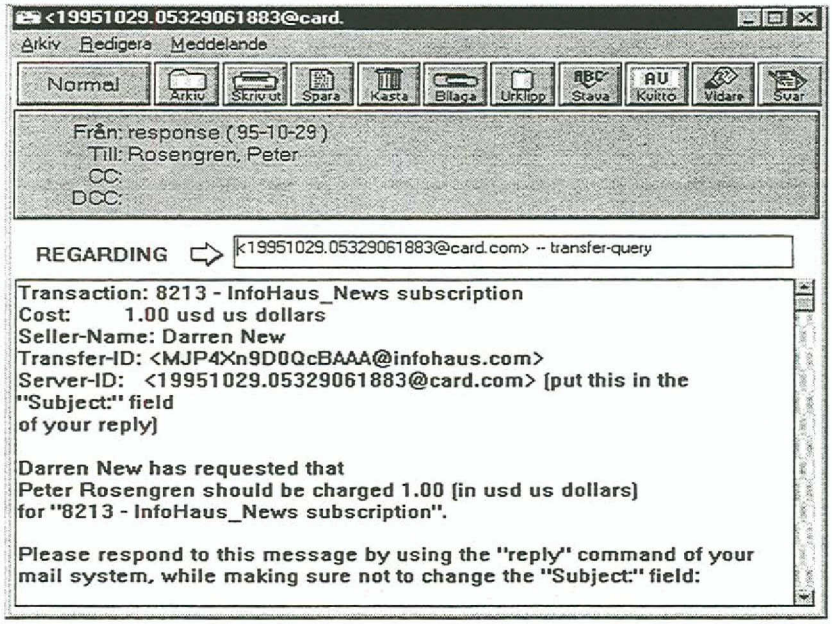
[17]Stein, Stefferud, Borenstein 1995.
[18]Kalakota, Whinston 1996, s 321 ff.

regelbunden basis förs sedan saldot över till klientens kreditkorts- eller checkkonto. Kreditkortsinformationen för denna transaktion förs över till FV endast en gång, utanför Internet. Vid köp används istället en så kallad VirtualPIN, som kunden får av FV. Därför är systemet snarare ett system för debet-kreditorder än ett kreditkortssystem. Systemet är främst till för att sälja små bitar information till låg styckkostnad. Handel med småsummor är möjlig genom att FV ackumulerar dessa på klientens konto tills överföring sker. Systemet använder inte kryptering, utan köpet konfirmeras via email, efter att leverans har skett. Det är alltså möjligt att låta bli att betala för informationen om kunden inte finner den prisvärd. FV avstänger dock kunder som missbrukar denna möjlighet. FV rekommenderar att säljaren överlåter åt köparen att avgöra om han vill betala för produkten, men systemet kan modifieras till att leverera efter att betalning skett.



Figur 2: Betalningsförfarande med Green Commerce Model.

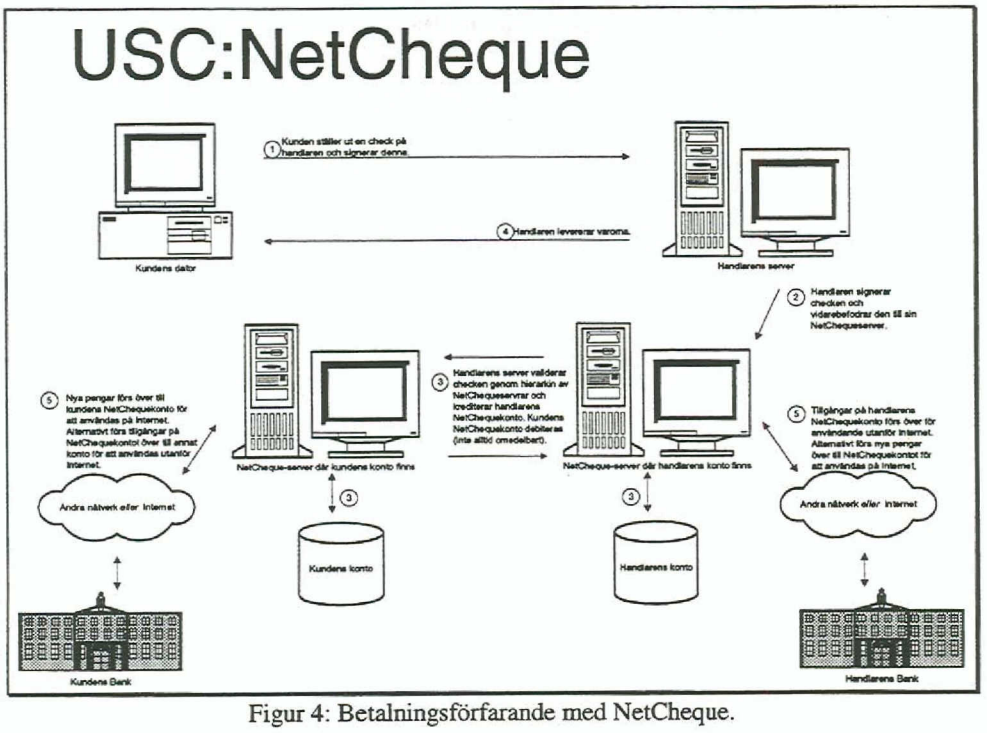
Nackdelar med First Virtuals system är att säljaren inte han någon betalnings-säkerhet, och att överföringar från person till person är inte möjliga om inte minst mottagaren är handlare. Kunden har inte heller någon anonymitet gentemot First Virtual. Handlaren behöver dock inte känna till kundens identitet; det enda han måste få veta är numret på kundens FV-konto och adressen dit informationen skall levereras. Då systemet kräver att FV hanterar all information centralt, kan dess kapacitet komma att bli överskriden vid kraftig belastning. Transaktionerna kan också lämnas öppna länge, vilket ytterligare belastar systemet och handlarnas system. Systemet var ett av de första som togs i bruk, och ett flertal FV-handlare finns.



Figur 3: Bekräftelse av betalning i First Virtuals system.

En av de stora fördelarna med systemet gentemot andra uppsamlingsagenter för kreditkort är att det är mycket enkelt att bli First Virtual handlare. Däremot är det tveksamt om First Virtuals system kan konkurrera med de mer avancerade systemen för kreditkortshandel när dessa börjar utvidga sina tjänster, som till exempel en fullständig CyberCash-"plånbok" för kredit, check och kontanthandel.

NetChex, lanserad av Net1, är en lösning efter checkmodell, gjord för betalningar till anslutna handlare. NetChex fungerar som en uppsamlingsagent, som vidarebefordrar betalningar till handlare via respektive bank. Kunden kopplar sitt vanliga check-, debetkort- eller kreditkortskonto till ett NetChex-konto. På kundens dator finns en NetChex klient, som innehåller kundens checkbok och personliga nycklar. Med denna han kan skriva ut checkar ställda på sitt NetChexkonto. Detta system är även tänkt att kunna användas för att göra andra betalningar än till Internet-handlare, som räkningar, hyra och så vidare. Modellen påminner lite om vissa av de tjänster CheckFree erbjuder. Handlaren behöver alltså inte vara uppkopplad, utan email- eller vanliga kvitton på köpet sänds ut till kund och handlare. Validering av betalningsordern görs med en signatur beräknad på föregående signaturer, belopp, handlare och andra faktorer. Detta för att en utomstående som analyserar skickade meddelanden inte skall kunna generera nästa check. Förutom detta signeras checken med kundens privata signatur.



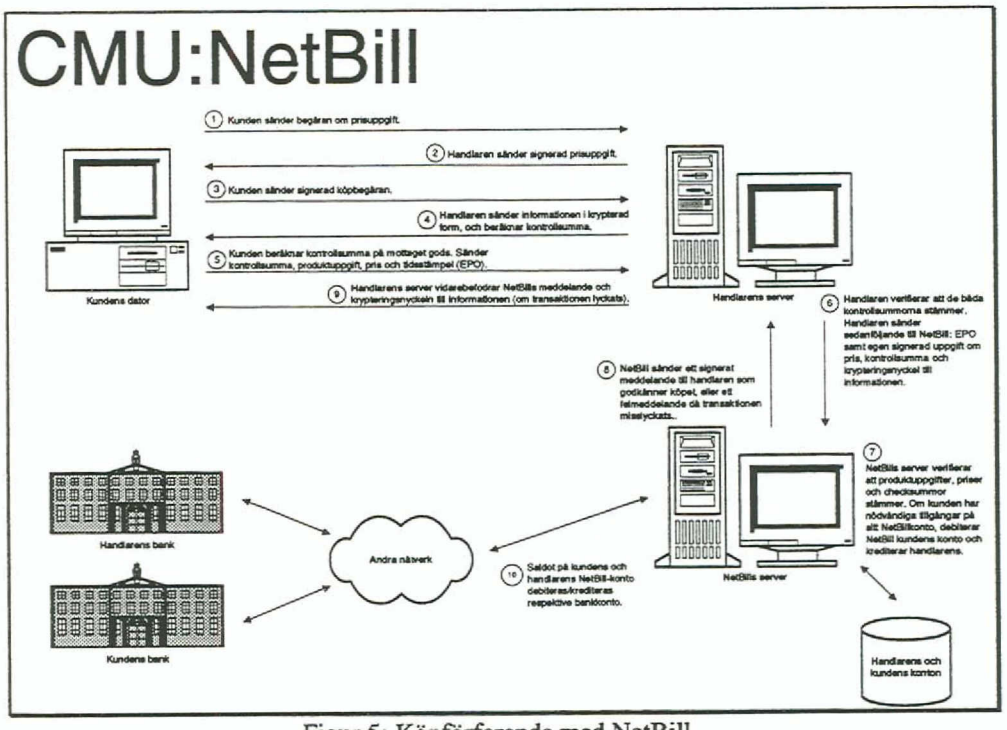
Figur 4: Betalningsförfarande med NetCheque.

NetCheque[19] är ett debet-kreditsystem utvecklat vid University of Southern California, där köparen utfärdar en betalningsorder till handlaren helt analog med en vanlig check. Checken hanteras av multipla NetCheque-servrar, för skalbarhet och robusthet. Klienten har ett konto på någon av dessa. När en check löses in sker detta om så är nödvändigt genom transaktioner över flera servrar, som har konton hos varandra. Banker är uppkopplade till dessa servrar på samma sätt som övriga klienter. På detta sätt knyts systemet till de existerande finansiella nätverken. Mekanismen baserar sig på symmetrisk kryptografi och använder Kerberos för kontroll av digitala signaturer på checkarna.[20] Systemet har nyligen tagits i drift i USA och Kanada. Exportlicens krävs för att använda programvaran utanför dessa länder.

NetBill[21] är ett kredit-debetsystem som främst är avsett för att sälja information. Man har därför särskilt tagit hänsyn till att möjliggöra ett stort antal mikrotransaktioner till låg kostnad. Systemet handhar inte enbart betalningstransaktioner, utan siktar på att styra hela transaktionen, inklusive produktleveransen. Carnegie Mellon University, som utvecklat systemet, anser att marknaden för information är den viktigaste på Internet. För att kunna använda NetBill krävs att kunden och handlaren har ett konto hos

[19]Medvinsky, Neuman 1995.
[20]Neuman 1993.
[21]Sirbu, Tygar 1995.

NetBill, som NetBill administrerar, och att de har för NetBill-handel avsedd programvara installerad.



Figur 5: Köpförfarande med NetBill.

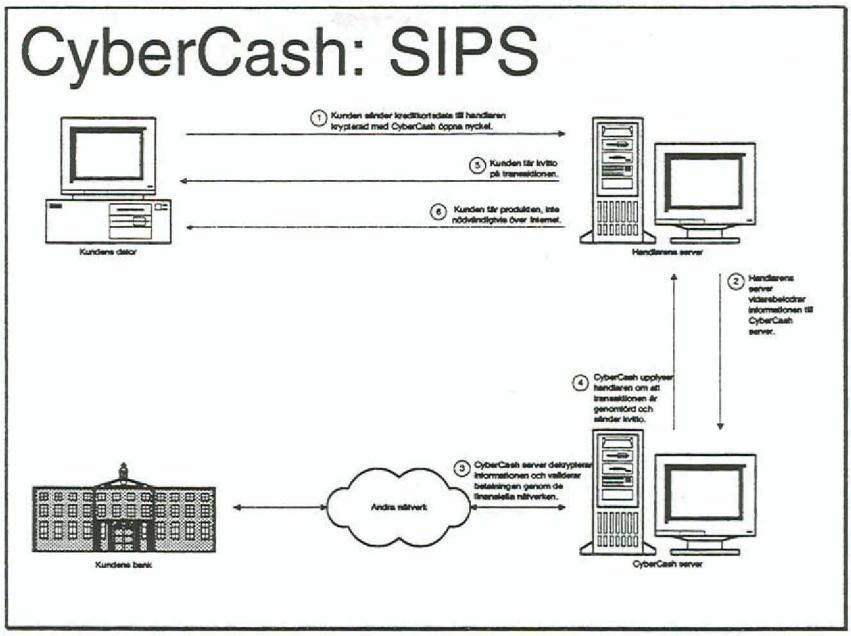
När ett köp skall göras efterfrågar kunden ett pris på produkten, se figur. Detta kan i NetBills system sättas dynamiskt beroende på om kunden har rabatter, är prenumerant eller liknande. När kunden fått offerten, kan denne skicka en köpbegäran. Som svar på denna sänder handlaren över informationen i krypterad form, samt beräknar en checksumma på den. När kunden mottagit detta, sänder denne över en betalningsorder till handlaren, där en av kunden beräknad checksumma ingår. Om de båda checksummorna stämmer, sänder handlaren över betalningsordern plus kontrolluppgifter till NetBills server. Servern kontrollerar att alla uppgifter stämmer, och att pengar finns tillgängliga för överföring. Om allt stämmer, görs överföringen och ett meddelande sänds över till handlaren. Denne sänder då kunden krypteringsnyckeln. Systemet använder sig av symmetrisk kryptografi och av Kerberos för att garantera köparens identitet, men ämnar utveckla systemet för att använda asymmetrisk kryptografi. Det krävs sex överföringar mellan handlaren och kunden för att utföra ett köp, och ytterligare två för kommunikation med NetBills server. Med tanke på den kraftigt ökande användningen av Internet, kan detta ha negativ inverkan på prestanda hos systemet. Kryptering och dekryptering av informationen tar också tid. Utrymme för en kraftig uppskalning av systemet skall möjliggöras genom att minimera antalet kommunikationer med NetBills server. VISA har annonserat att de ämnar samarbeta med NetBill i ett test av systemet.

Financial Services Technology Consortiums (FSTC) checkmodell baserar sig på identifiering med digitala signaturer. Den använder sig av PCMCIA-kort för säker lagring av signaturer, och fungerar via det existerande finansiella clearingssystemen. Kortet innehåller ett checkhäfte, varifrån checkar kan dras. Systemet är främst utvecklat för Internet, men också för att fungera som en förbättring av det existerande checksystemet.

Globe ID är ett uppsamlingssystem efter kredit-debetmodell som är under testning i Frankrike. Det hanterar förbetalda checkar, köpta genom Globe ID, på kundens dator för små transaktioner, och kreditkortstransaktioner för större summor. Alla transaktioner hanteras av Globe ID, och kund och handlare måste ha konton på Globe ID Bank. GC-Tech SA, som står bakom Globe Online, har ett system kallat SEPS (*Secure Electronic Payment System*) som skall integrera mikrotransaktioner, debet/kredit, och kreditkorts-modeller. För kunden innebär detta att samtliga betalningar skall vara tillgängliga i samma programvara, i vanlig ordning kallad "plånbok". En speciell egenskap hos detta system är att all clearing sker mellan kundens dator och betalsystemet, istället för mellan handlaren och utfärdarens server. Handlaren behöver alltså endast kommunicera med kunden, och får kvittens på godkänd betalning via denne. Detta minskar belastningen på handlarens nätanslutning. Systemet använder sig av digitala signaturer för identifiering av kunden och kryptering av information. Ingen anonymitet erbjuds för kontantköp.

4.2.3 Säkert överförd kreditkortsinformation

Förbindelseagenten CyberCash marknadsför ett system de kallar SIPS, Secure Internet Payment Service. Kunden har ett program för betalning, en så kallad CyberCash-klient, eller "plånbok". (Denna metafor är mycket vanlig hos betalsystem.) Denna lagrar kundens kreditkortsinformation i krypterad form. Vid köp krypterar kundens CyberCash-klient kreditkortsinformationen och för över den till handlaren. Denne sänder informationen vidare till en CyberCash-server, som är kopplad till det vanliga kreditkortsnätet, på samma sätt som en kortläsare i en affär. CyberCash har andra delen av nyckelparet och kan dekryptera meddelandet. CyberCash kontrollerar och godkänner köpet, som betalas som vilket kreditkortsköp som helst, och underrättar handlaren. Handlaren kan inte avläsa kundens kreditkortsnummer.

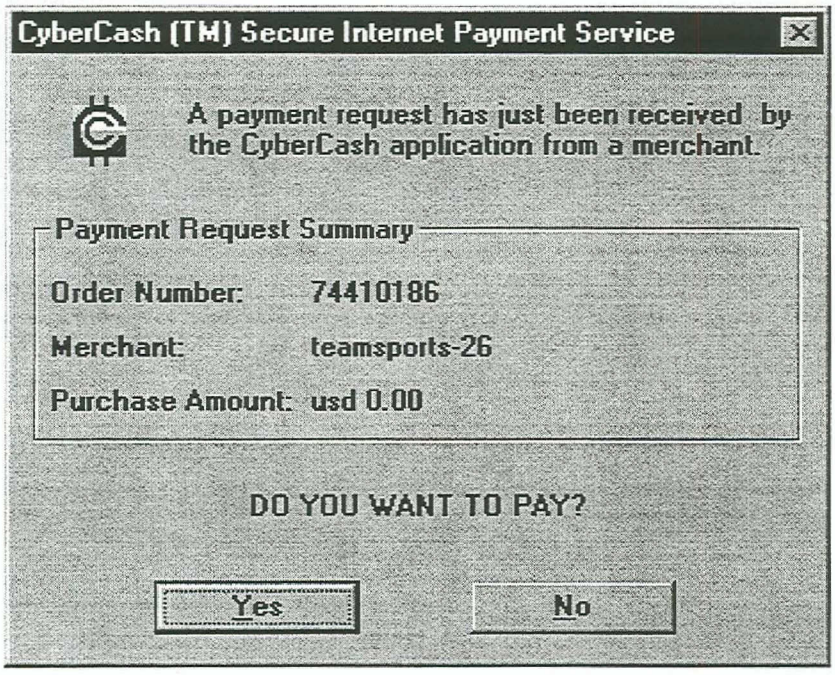


Figur 6: Köpförfarande med Secure Internet Payment Service.

CyberCash använder sig av en kombination av DES- och RSA-kryptografi för kryptering av informationen. Kundens identitet garanteras av att köp endast görs via kundens CyberCash-klient. Kunden har faktiskt bättre skydd mot informationsutlämning än vid ett vanligt kreditkortsköp i en affär.

Systemet är skalbart, då CyberCash bara fungerar som länk till kreditkortssystemet, och en centraliserad server inte behövs. Den känsliga kreditkortsinformationen skrivs in i klartext endast en gång. Då flera kreditkort kan användas, och från kunden sida är mycket lättanvänt, är potentialen stor hos systemet.

Systemet är etablerat och CyberCash planerar även att kunna erbjuda ett kredit-debetsystem och ett kontantsystem till hösten 1996. Inga noggrannare uppgifter om dessa har funnits att tillgå, dock är de tänkta att integreras i den nuvarande CyberCash-klienten. CyberCash samarbetar med CheckFree och Compuserve. CyberCash-, CheckFree- och Compuserve-klientprogramvara, eller "plånböcker", är alltså samma system och helt kompatibla. Företaget har även annonserat att de kommer att stödja VISA och MasterCards SET-protokoll när detta lanseras. Nyligen etablerade sig CyberCash i Sverige, i samarbete med Point Scandinavia.



Figur 7: Bekräftelse av betalning i CyberCash-klienten.

Secure Courier är ett system för säkra transaktioner utvecklat av Netscape, som är marknadsledande inom WWW-servrar och -läsare. Secure Courier baserar sig på SSL, ett generellt protokoll för säker kommunikation byggt på RSA-kryptografi, är utvecklat i samarbete med MasterCard och Intuit. Secure Courier skyddar informationen mot obehöriga under transporten genom digitala kuvert.

IBM har utvecklat ett protokoll kallat iKP[22] (*Internet Keyed Payment Protocols*) avsett för säker överföring av kreditkortsinformation. Asymmetrisk kryptografi används för att skydda kundens kreditkortsnummer och signera köpen. Det finns tre alternativ för överföringen. 1KP är analog med CyberCashs system, där kundens kreditkortsnummer döljs för handlaren, och endast förbindelseagenten har en nyckel. Med 2KP har handlaren möjlighet att signera de köp som görs hos honom, och med 3KP kan kunden signera sina köp för ytterligare säkerhet. SEPP, vars utveckling finansierats av MasterCard, bygger på iKP.

S-HTTP (*Secure Hypertext Transfer Protocol*) är ett protokoll som erbjuder nödvändiga tjänster för säker Internethandel. Då det är en komplettering av HTTP kan det användas ovanpå säkerhetsprotokoll för lägre kommunikationslager, som SSL. Systemet utvecklades först av EIT och CommerceNet, och utvecklas nu kommersiellt av Terisa Systems, ett dotterbolag till RSA

[22]Bellare, Garay, Hauser m.fl. 1995.

Data Security och EIT. Protokollet använder sig av både asymmetrisk och symmetrisk kryptering.

Secure Electronic Payments Protocol (SEPP) är ett protokoll för kreditkortsbetalningar baserat på IBMs iKP-protokoll. Det har utvecklats av MasterCard i samarbete med IBM, Netscape, CyberCash och GTE. MasterCard och VISA kungjorde vid månadsskiftet januari-februari 1996 att SEPP och STT skulle integreras i ett gemensamt system kallat SET (Secure Electronic Transactions). Dokumentation om detta skall finnas tillgänglig i februari 1996.

STT (*Secure Transaction Technology*) är ett protokoll för säker överföring av kreditkortsinformation som utvecklats av VISA i samarbete med Microsoft. MasterCard och VISA kungjorde vid månadsskiftet januari-februari 1996 att SEPP och STT skulle integreras i ett gemensamt system kallat SET (Secure Electronic Transactions). Dokumentation om detta skall finnas tillgänglig i februari 1996.

Ziplock är en förbindelseagent för Internethandel med kreditkort, som är i aktivt bruk. Produkten laddas krypterad (RSA-teknik används) från distributören, och en dekrypteringsnyckel erhålls vid avslutad betalning. Kundens Ziplockklient kommunicerar via direkt modemuppkoppling med en brygga mot ett kreditkortsclearingsystem. Handlaren får sedan ett kvitto på att köpet genomförts.

4.3 Off-linesystem

Millicent[23] är ett kontantsystem designat av Digital Equipment Corporation. Det är avsett för mikrobetalningar off-line. Validering av valutan sker decentraliserat, och ingen central kontroll av dubbelspenderade pengar behövs. Detta uppnås genom att varje handlare har sin egen valuta, så kallade scrips. Dessa fungerar ungefär som ett häfte rikskuponger. De kan köpas hos utfärdaren för användning hos en särskild handlare, valutan kontrolleras sedan för äkthet lokalt hos handlaren vid köp, och den spenderade summan dras av från kundens scrips. Hos en eller flera så kallade brokers som kunden har en långsiktig relation med, som ens bank eller kreditkortsfirma, kan kunden köpa scrips för en speciell handlare. Betalningarna görs sedan mellan den broker som sålde handlarens scrip och handlaren. En handlare har ett konto hos varje broker som säljer handlarens scrips. Mekanismen använder sig av envägs hashfunktioner, som MD5, för att signera scrips.

Mondex är ett kontantsystem baserat på så kallade smarta kort. Överföringar mellan privatpersoner är möjliga, dock erbjuder systemet ingen anonymitet, då kortet signerar transaktionerna. Systemet kan utnyttjas för handel över Internet, men kräver att en läsare för smarta kort kopplas till kundens dator. Systemet har testats i Swindon, Storbritannien och i Ontario Kanada. Flera länder i Sydostasien har också anmält intresse.

---

[23]Glassman, Manasse, Abadi, m.fl. 1995.

DigiCash, som utvecklat ecash, medverkar också i flera europeiska projekt, varav CAFE och SEMPER, som nämns i 4.4, är särskilt intressanta. CAFE, eller Conditional Access For Europe, är ett off-line kontantsystem för anonym betalning baserat på ett system för smarta kort. Kortet skall kunna användas både för transaktioner och identifiering och stödjer flera valutor. För intresserade finns en pedagogisk mjukvarusimulering av systemet tillgänglig på WWW. Systemet skall användas för transaktioner i alla sammanhang, även över Internet. Systemet testas under slutet av 1995 och början av 1996.

Andra off-linesystem som använder smarta kort för elektroniska plånböcker är First och VISAs Stored Value Cards, Europays Express, Danmont och Proton. I Sverige testar Sparbanken i Lund ett liknande system. Teoretiskt sett kan alla dessa system användas för betalning över Internet med en läsare för smarta kort som tillsats till kundens dator.

4.4 Övrigt

Open Market är ett företag som säljer fullständiga lösningar, både för transaktioner, lagerhantering och redovisning. Företagets produkter integrerar existerande betalsystem genom en generisk "payment switch" och kopplar den till övriga redovisningssystem. Detta är en bransch som kan bli mycket lönande, då de flesta betalsystem inte erbjuder några helhetslösningar för de företag som vill etablera sig på Internet.

SEMPER *(Secure Electronic Marketplace for Europe)* är inget betalsystem, men är ändå intressant att nämna. Projektet är tänkt att resultera detaljerade beskrivningar av juridiska, kommersiella, sociala, och tekniska krav och möjligheter för en elektronisk marknadsplats på öppna nätverk, samt ta fram en generell arkitektur för en elektronisk marknadsplats. Projektet skall också stödja framtagandet av standards inom området genom att utnyttja existerande system och stödja integrationen av dessa. Betalsystem för öppna nätverk ingår alltså som en del i projektet.

PPV (Pay Per View) är ett protokoll utvecklat av USC för NetCheque och NetCash, för att hantera leverans och prissättning vid handel. Protokollet går dock att använda för andra betalsystem.

PayWard och MicroMint är två enkla system avsedda för mikrobetalningar, utvecklade av Rivest och Shamir på RSA Data Security Inc. MPTP (Micro Payments Transfer Protocol), under utveckling hos W3C, implementerar en version av PayWard. Stefan Brands, forskare på Centrum vor Wiiskunde en Informatica i Amsterdam, har föreslagit ett system för elektroniska kontanter på Internet, och även system för betalning med smarta kort.

Netscape och Verifone har nyligen startat ett samarbete för att integrera sina system för elektronisk betalning i en helhetslösning, avsedd att integrera Internet med de system för elektronisk handel som redan nu används av handlare. Då Netscape dominerar marknaden för WWW-läsare och WWW-servrar, och Verifone har stor erfarenhet av att hantera elektroniska transaktioner, kan detta samarbete visa sig få stor effekt på marknaden.

4.5 Sammanfattning

De olika formerna av betalning erbjuder olika för- och nackdelar. De flesta system innebär att klienten blir beroende av ytterligare en aktör, förutom sin bank eller sitt kreditkortsinstitut. Särskilt gäller detta för uppsamlingsagenter, som innebär ytterligare en part konsumenten måste kontakta och öppna konto hos innan han kan börja använda systemet. Dessa system riskerar dessutom att inte vara skalbara, genom sin centraliserade uppbyggnad. Skalbarheten är också ett problem för alla on-linesystem, även de distribuerade, då kontakt med utfärdande eller kontoadministrerande institution alltid krävs.

Kontantlösningar erbjuder partiell eller total anonymitet, och är lämpade för mikrobetalningar. Nackdelarna är att de kan ha svårt att få förtroende från konsumenter, och att de oftast kräver omfattande beräkningar och kommunikation för validering av valutan och kontroll av dubbelspendering. Det finns dock flera system med potential att fungera off-line, något som avlastar nätet avsevärt. Valutans värdebas och de svåra följderna av lyckad förfalskning är också problem.

Debet/kreditmodeller har den fördelen att eventuell förfalskning inte kan få lika stor effekt, då endast en kontoinnehavare kan drabbas. De har dock inte samma potential för anonymitet som kontantmodeller.

Kreditkortspresentation har redan ett enormt kundunderlag jämfört med de andra modellerna, som måste marknadsföra sina system till nya kunder. De är också förhållandevis enkla system att förverkliga och utveckla jämfört med andra modeller. Nackdelarna är att de inte erbjuder anonymitet vid köpen, och har ganska höga transaktionskostnader, vilket är ett hinder för mikrobetalningar.

När det gäller informationsförsäljning är det främst de system som möjliggör mikrobetalningar och enkla möjligheter att bli handlare som är aktuella. Dels därför att informationen troligtvis säljs i mindre enheter till små belopp, och dels för att information är en vara som kan tillhandahållas av privatpersoner, forskare och andra som inte gör affärer på regelbunden basis. Olika kontant-system, som DigiCashs ecash, är särskilt lämpade för detta, och även system som NetBill, NetCheque, och First Virtual. För försäljning av produkter till högre kostnad, lämpar sig modeller för kreditkortspresentation och checkmodeller utan uppsamling utmärkt.

Möjligheter att använda systemen även för att köpa produkter utanför Internet kan ge systemet större allmän användning. Personer som endast sällan använder Internet för inköp, kommer troligtvis inte att ansluta sig till ett nytt system bara för att köpa en särskild produkt. Det är då praktiskt om ett betalningsmedel som redan finns tillhands kan användas, till exempel kredit-kort eller elektroniska plånböcker, om dessa slår igenom. Det största hindret för ett genombrott för handel på Internet är dock osäkerheten om vilka som kommer att dominera i framtiden.

5 Kort om marknadens förutsättningar

Intresset för handel på Internet är som sagt stort just nu, både för försäljning via WWW-sidor och användning av Internet som medium för penning-transaktioner med sk "electronic wallets". Det kan ifrågasättas vilka tjänster och produkter som verkligen lämpar sig för försäljning på Internet. Följande text utgör ingen egentlig analys av marknaden för produktförsäljning via Internet, utan består främst av egna reflektioner över ämnet. Utgående från de välkända 4-5P:n (Pris, Plats, Produkt, Promotion och Personal)[24] som brukar ingå i varje översikt av marknadsföringens grunder, kan man dra följande (ytliga) slutsatser.

Vad beträffar pris, lämpar sig mediet mycket väl för små företag och kostnadsledarstrategier, då mediet erbjuder mycket liten kostnad för marknadsföring. Plats, eller tillgängligheten, är mycket god, särskilt för information, då en WWW-sida kan nå kunder över hela världen. Antalet Internetanvändare växer också stadigt. Dock visar undersökningar på en ganska homogen kundgrupp av relativt högavlönade akademiker i åldrarna 20-40 år. Fysiska produkter har dock inte lika hög tillgänglighet som i en vanlig affär, då de kräver leverans utanför Internet. Vad beträffar produkten kan inte så mycket sägas, utom att mediet är utomordentligt väl lämpat för informationsprodukter. Den fjärde posten, promotion, är jämfört med andra medier mycket billig och tillgänglig. Den femte posten, personal, är dock en svaghet. Personlig service är svår att få, och de sociala dimensionen av att handla i en vanlig butik saknas.

För till exempel mjukvaruföretag och informationsleverantörer bör Internet lämpa sig utmärkt, då det finns möjlighet att leverera varan via samma medium där transaktionen sker. Exempel på dessa är speltillverkare som ID Software, Bungie och Elite som ger möjlighet att ladda ner en demoversion av produkten, en utmärkt tillämpning av mediet. Vad beträffar försäljning av produkter utan direkt anknytning till mediet är användbarheten mer tveksam. Undersökningar gjorda i USA pekar på att beställning med traditionella postorderkataloger ses som mer njutbart och mindre krångligt än att beställa över Internet. Handel via WWW-sidor upplevdes som mer uppmärksamhets-krävande och därför mindre socialt än att använda tryckta kataloger. För många i undersökningen var det också viktigt med den sociala gemenskapen och kontakten med andra människor som upplevdes vid handel i köpcenter och affärer. Undersökningen är något gammal, men resultaten visar på en möjlig begränsning hos WWW-handel. [25]

Min egen tolkning är att den stora potentialen troligtvis finns hos de produkter som kan levereras över Internet, utan fördröjning. Vidare anser jag att försäljning främst bör rikta sig till den professionella marknaden, med olika former av informationsprodukter. De flesta har tillgång till Internet på jobbet,

---

[24]Kotler 1991, s 68 ff.
[25] Cordeiro 1994.

vilket gör det lämpligt att rikta marknadsföringen mot de grupper som kan använda Internettjänster i sin yrkesverksamhet. Detta är ett klart identifierbart behov. Beställa heminredning och kläder är något som enligt egen erfarenhet görs i hemmet under långa söndagseftermiddagar, främst under social samvaro. Det viktigaste är att erbjuda kunden mer värde för pengarna än konkurrenternas produkter, och det är tveksamt om Internet som marknadsplats möjliggör detta för alla produkter. Många sidor för försäljning ger intryck av att man utgått från mediet istället från produkten när man skapat tjänsten. Det är troligt att många av de WWW-sidor som nu erbjuder produkter kommer att försvinna när nyhetens behag har gått över.

6 Tabell

Följande tabell sammanfattar några betalsystem för Internet. De system som tagits med är möjliga att använda i Europa, eller är planerade att kunna använda i Europa, och är avsedda för Internethandel. Det finns fler förslag som befinner sig på planeringsstadiet som inte tagits med, då framtiden för dessa är oklar.

Namn	Typ av system	Kommentar	Status
CyberCash	Kreditkort. Kontant- och checksystem utlovat under 1996.	Kreditkortsbetalningar via förbindelse med CC. Kunden har anonymitet gentemot handlaren.	Systemet har använts under en längre tid, i vissa fall med stor kommersiell framgång. Cyber-Cash har nyligen etablerat sig i Skandinavien.
DigiCash	Kontanter.	Helt anonyma digitala kontanter. Betalningar mellan privatpersoner möjliga	Två utgivare av ecash finns för närvarande, Mark Twain Bank i USA, och EUnet via Merita Bank i Finland. Posten i Sverige skall också ge ut ecash senare i år.
First Virtual	Debet/Kredit.	Uppsamlingssystem främst avsett för informationsförsäljning. Skall stödja handlare utanför USA.	Systemet har använts under längre tid, och har ett flertal användare. För närvarande krävs konto på bank i USA för att kunna ta emot betalningar med systemet.
Globe ID	Kontanter/ Kreditkort.	System liknande CyberCash; kontanter kopplade till kreditkort.	Systemet testas för närvarande i ett antal europeiska länder. Främst franska företag medverkar.
Mondex	Kontanter på kort.	Kräver kortläsare för att användas på Internet. Person till person-betalningar är möjliga.[26]	Systemet har testats i Swindon, Storbritannien, och skall testas i Kanada och Hong Kong.
NetBill	Debet/Kredit	Avsett för informations-försäljning.	Systemet testas för närvarande. VISA är med och utvecklar.
SET	Kreditkort	Lanserades under början av 1996 av VISA och MasterCard och ersatte då tidigare förslag, som STT & SEPP.	Systemet anses av många vara en blivande standard för kreditkorts-betalningar över öppna nätverk. Systemet testas under 1996 och kan tas i drift under senare delen av året.

[26] Notera att DigiCash och Mondex är de enda kontantsystemen där överföringar mellan privatpersoner är möjliga. Detta gör det möjligt att ta emot betalningar utan att registrera sig som köpare.

7 Sammanfattning och slutsatser

Det finns en mängd betalsystem utvecklade för Internethandel. De baserar sig på olika modeller och tekniska lösningar. Tre tydliga huvudgrupper av system är kontantsystem, debet/kreditsystem och kreditkortshandel. Kontantsystem och debet/kreditsystem kan möjliggöra handel med små belopp, mikro-betalningar. Kontantsystem kan erbjuda anonym handel, och handel mellan privatpersoner. Kreditkortshandel har en större omedelbar tillgänglighet.

Det finns flera organisationer som arbetar för framtagande av standarder inom området, varav Swebizz i Sverige, CommerceNet, W3C, IETF, och olika EU-projekt, som SEMPER och CAFE, är några. MasterCards och VISAs nya SET-protokoll är också en stark kandidat till de facto standard för kreditkortshandel, och de båda företagen har redan en stor mängd användare. Netscape och Verifones nyligen tillkännagivna samarbete för att integrera sina system för elektronisk betalning i en helhetslösning för handlare är ett stort steg mot ett genombrott för elektronisk betalning. Holländska DigiCash verkar ha möjlighet att få ett starkt grepp om de europeiska marknaden, inte minst genom sin medverkan i olika EU-projekt.

Projekt som siktar mot att använda Internet och öppna nätverk tillsammans med de existerande, slutna finansiella nätverken snarare än endast användas för handel på Internet har troligtvis framtiden för sig. Förutom kreditkort består dessa system främst av olika lösningar som använder sig av smarta kort. Av de mer specialiserade systemen är de som har informations-försäljning som huvudtillämpning lovande. Troligtvis kommer flera olika system för samma användningsområde att samexistera. Detta beroende på geografiska, sociala, kulturella och politiska skillnader. USAs exportförbud för viss kryptografisk teknik är ett exempel på en sådan faktor, som kan komma att begränsa dessa system till USA och Kanada. EUs strävanden efter en europeisk standard för elektronisk handel är en annan politisk faktor som kan komma att styra utvecklingen. Det som verkar gälla just nu är annars att de stora aktörerna går samman om lösningar, vilket troligtvis kommer att ha en avgörande effekt på utvecklingen.

Litteraturreferenser

Bellare, M., Garay, J. A., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Tsudik, G., Waidner, M.: iKP – A Family of Secure Electronic Payment Protocols, IBM Research, 1995.

Benaloh, J.,Lampson, B., m. fl.: Microsoft Corporation's Private Communication Technology Protocol, Microsoft Corporation, 1995.

Camp, L. J., Sirbu, M., Tygar, J. D.: Token and Notational Money in Electronic Commerce, Usenix Workshop on Electronic Commerce, 1995.

Chaum, D.: Achieving Electronic Privacy, Scientific American, 1992, 96-101.

Cordeiro, D.: Executive Summary of RITIM Report: To Shop or not to Shop, The Interactive Way, The Research Institute for Telecommunications and Information Marketing, 1994.

Digicash: An introduction to ecash, DigiCash bv., 1995.

DigiCash: Ecash Protocol Version 1.2, DigiCash bv., 1996.

Freier, A. O., Karlton, P., Kocher, P. C.: The SSL Protocol Version 3.0, Internet Draft, Mars 1996.

Glassman, S., Manasse, M., Abadi, M., Gauthier, P., Sobalvarro, P.: The Millicent Protocol fo Inexpensive Electronic Commerce, Systems Research Center, Digital Equipment Corporation, 1995.

Janson, P., Waidner, M.:Electronic Payment over Open Networks, IBM 1995.

Kalakota, R., Whinston, A. B.:Frontiers of Electronic Commerce, Addison-Wesley 1996.

Kotler, P.: Marketing Management, Prentice-Hall 1991.

Medvinsky, G., Neuman, B. C.: NetCash: A design for practical electronic currency on the Internet, Proceedings of the First ACM Conference on Computer and Communications Security, November 1993.

Medvinsky, G., Neuman, B. C.: Requirements for Network Payment: The NetCheque Perspective, Proceedings of IEEE Compcon Mars 1995

Neuman, B. C.: Proxy-based Authorization and Accounting for Distributed Systems: Proceedings of the 13th International Conference on Distributed Computing Systems, 1993.

Pfleeger, C. P.: Security in Computing, Prentice-Hall 1989.

Rescorla, E., Schiffman, A.: The Secure Hypertext Transfer Protocol, Internet Draft, 1996.

Sirbu, M., Tygar, J. D. : NetBill: An electronic commerce system optimized for network delivered information and services. Proceedings of IEEE Compcon, 1995.

Solinsky, J.:An Introduction to Electronic Commerce, Massachusetts Institute of Technology Press, 1995.

Stein, L. H., Stefferud, E. A., Borenstein, N., Rose, M. T.: The Green Commerce Model, First Virtual Holdings Incorporated, 1995.