Innehåll

1 Introduktion

I början av 1996 fick elektronisk betalning över Internet ett genombrott. Olika företag började på allvar intressera sig för Internets möjligheter som marknadsplats och media för affärstransaktioner och så kallade Internet Malls började bli vanliga. Förslag till elektroniska betalsystem hade dock tagits fram flera år tidigare.

De system som kommer att få praktisk användning börjar nu kunna urskiljas. Denna rapport avslutar rapporteringen från det examensarbete om elektronisk betalning som utfördes på SISU under 1996.

Examensarbetet var uppdelat i två moment. Det första utgjordes av en undersökning och strukturering av olika system. Detta resulterade i en delrapport [1]. Det andra momentet utgjordes av design och implementation av en tillämpning för utvärdering av betalsystem och betaltjänster. Utgående från information från det första delmomentet valdes ett betalsystem för användning i tillämpningen.

Denna rapport följer upp arbetet med att beskriva SISU Shop [32], testtillämpningen som togs fram under examensarbetets senare del, och erfarenheter från utvecklingen av denna. En sammanställning av ett urval betalsystem görs enligt samma principer som i förra rapporten [1]. Utvecklingen går dock snabbt, så för en överblick av dagsläget hänvisas till SISU och Tidningsutgivarnas tjänst PayWatch [30]. Rapporten avslutas med en sammanfattning och diskussion av området och de erfarenheter som gjorts.

2 Handel på Internet i korthet

Fördelen och genomslagskraften hos world wide web ligger i möjligheten att genom ett gränssnitt, och ett nätverk, få tillgång till en stor mängd information, och även varor och tjänster. Många av de varor och tjänster som kan distribueras via Internet kräver att de som tillhandahåller tjänsten kan få kompensation för vad de levererar, om så bara för att täcka framställningskostnaderna. Några exempel är:

- Tillgång till upphovsrättsskyddat material via Internet, som till exempel läromedel, musik, statistik, multimedia och programvara.
- Sökningar i databaser.
- Användande av systemresurser eller programvara.
- Försäljning av traditionella varor och tjänster som levereras utanför Internet.

För företag som vill marknadsföra sina varor och tjänster innebär Internet och world wide web ett helt nytt sätt att nå ut till sina kunder. Internet erbjuder fördelar främst för små företag, som med små medel kan nå ut till en marknad de inte skulle haft resurser till annars. Möjligheten för privatpersoner och företag att göra transaktioner över Internet möjliggör också helt nya affärsidéer och verksamheter som är unika för mediet.

Två grupper av produkter kan urskiljas, med olika förutsättningar och krav på betalsystem. Produkter som kan levereras över Internet och produkter som inte kan det. Kraven som ställs på betalningsmetoder för de två typerna av tjänster är olika.

Internet lämpar sig mycket väl för företag som säljer information och tjänster. Dessa produkter kan levereras direkt över Internet. Företagen kan använda mediet för såväl marknadsföring som distribution, vilket innebär att nästan all försäljningsverksamhet kan automatiseras. Ett intressant nytt område är tjänster där tillgång till programvara eller systemresurser kan hyras tillfälligt. Denna typ av tjänster kan behöva stöd för transaktioner med mycket små summor. För informationsförsäljning kan det vara nödvändigt med system som kan ge bekräftelse på transaktioner i realtid, och som möjliggör transaktioner i flera led som involverar mellanled eller mäklare.

För företag som levererar varor och tjänster utanför Internet är inte kraven så stora på de betalsystem som används. Stöd för mycket små betalningar är inte nödvändiga, då dessa produkter oftast befinner sig i en lite högre prisklass och leveransavgifter kommer att läggas till priset. En viss tidsfördröjning i bekräftelsen av köpet är också acceptabel, då leveransen kan uppskjutas tills transaktionen är avslutad.

3 Säkerhet för betalsystem

3.1 Risker

Genom att betalningarna sker över ett öppet nätverk som Internet, är betalsystemen utsatta för vissa problem som de existerande finansiella nätverken, som kommunicerar över slutna nätverk inte har. En stor mängd användare är anslutna till Internet och tillgången till nätverket kan inte begränsas via yttre säkerhetsåtgärder. Detta gör dessa betalningssystem mer sårbara för attacker än de tidigare systemen. En risk är avlyssning och kopiering av den information som sänds. Detta är möjligt eftersom informationen kan fångas upp då den sänds över nätet. Andra risker är förfalskning av meddelanden eller intrång i kunders, handlares eller bankers system i avsikt att förfalska transaktioner eller skaffa information som tillåter detta. Lättheten i att sätta upp en webbplats och svårigheten att kontrollera handlare gör också att det kan bli lönsamt att sätta upp en webbaffär för att någon vecka senare ta ned den och försvinna med pengar eller insamlad information om kunder och kontonummer. Därför krävs tekniker för att kunna garantera att ett meddelande inte kan läsas av utomstående eller ändras och metoder att garantera att kunder och handlare är vad de ger sig ut för att vara.

3.2 Kryptografi

Förutom några få system som använder sig av en extra bekräftelse av köpet via e-post 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) [17]. Det kan här vara på sin plats med en kort förklaring av dessa begrepp.

I symmetrisk kryptografi sker avkodning av ett meddelande med samma nyckel med vilket det kodades. Symmetrisk kryptografi kräver därför att båda parter, till exempel kund och handlare, har tillgång till gemensam kunskap om krypteringsnyckeln. 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. Vissa problem kvarstår dock. Överföring av krypteringsnyckeln till de inblandade måste ske skyddat, och måste ske innan kommunikationen inleds. Alla parter som skall kommunicera med varandra måste också ha tillgång till alla nycklar, eller så måste varje part ha en unik nyckel för varje annan part. På grund av detta går det inte heller att bevisa att det verkligen är en viss person som har sänt ett meddelande, till exempel att det är en viss kund som har gjort en transaktion.

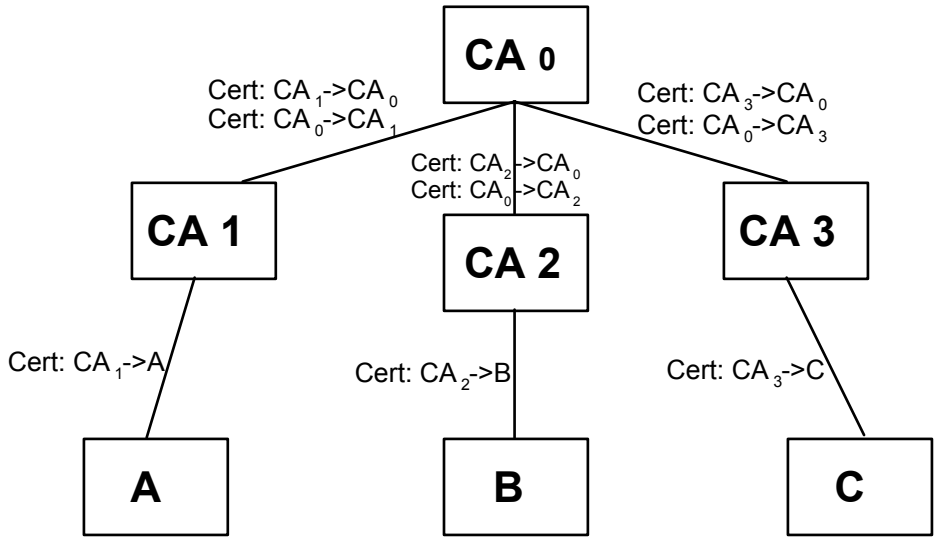
Asymmetrisk kryptografi baserar sig på möjligheten att beräkna en krypteringsnyckel och en dekrypteringsnyckel på sådant sätt att den ena nyckeln inte kan beräknas från den andra, ens med tillgång till algoritmen. Den ena nyckeln hålls hemlig, och den andra publiceras offentligt. När ett krypterat meddelande 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 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. Asymmetrisk kryptografi används också för digitala kuvert, som döljer meddelandets innehåll för de mellanhänder som hanterar det, och för märkning av information för att garantera att den inte blivit ändrad. Digitala kuvert kan används i system för digitala pengar för att hindra banken från att knyta pengarna till en specifik kund. Det i särklass mest kända asymmetriska krypteringssystemet är RSA, döpt efter dess skapare Rivest, Shamir och Adleman.

Symmetrisk kryptografi är dock snabbare är asymmetrisk, som måste utföra operationer med mycket stora tal. Ofta 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.

3.3 Certifikat

Ett certifikat är en datastruktur digitalt signerad av en certifikatutfärdare (eng. certificate authority), som användarna av certifikatet litar på. Detta system kan användas för att distribuera asymmetriska nycklar, genom att inkludera nyckeln i ett signerat certifikat (eng. public-key certificate). På detta sätt kan man binda en nyckel eller signatur till en viss person och verifiera detta genom att kontrollera med utfärdaren av certifikatet. För att slippa samla alla nycklar hos en global utfärdare av certifikat, används oftast en trädstruktur av utfärdare, där varje utfärdare garanterar äktheten hos ett antal andra utfärdare. Så länge som två parter kan nå varandra genom en gemensam nod båda litar på, kan de acceptera varandras certifikat. Detta kan användas till exempel i kreditkortssystem för att garantera att kundens och handlarens identiteter.



Figur A: En enkel certifikathierarki.

I figuren ovan syns en enkel certifikathierarki. Om till exempel A vill kontrollera C:s nyckel, använder A certifikatet CA_1->CA_0 för att kunna acceptera certifikatet CA_0->CA_3, som är utfärdat av CA_0. När sedan A kan lita på certifikatutfärdaren CA_3, använder A certifikatet CA_3->C som garanti för att C:s nyckel är korrekt.

3.4 Tekniker

En hashalgoritm [17] kan används för att skapa ett ”fingeravtryck” av ett dokument eller meddelande. Algoritmen tar ett meddelande av godtycklig längd som indata och returnerar ett 128-bit ”fingeravtryck” eller ”message digest” av meddelandet. Det är praktiskt omöjligt att återskapa meddelandet från resultatet eller att två olika meddelanden skall ha samma resultat. Även en liten ändring i meddelandet leder till ett helt annorlunda fingeravtryck. Denna teknik kan användas för att garantera att ett dokument inte har ändrats eller för att signera meddelanden. MD5 är en sådan algoritm som producerar ett 128-bit fingeravtryck. En annan är SHA (Secure Hash Algorithm), med ett 160-bit resultat.

SSL (Secure Sockets Layer) [8] är ett protokoll utvecklat av Netscape Communications. Protokollet upprättar en skyddad förbindelse som kan användas av protokoll på högre nivå som HTTP, telnet eller FTP. Det hanterar autentisering av server och eventuellt klienten, samt skyddar integritet och innehåll hos det data som sänds. SSL används ofta vid överföring av kreditkortsnummer via HTML-formulär.

S-HTTP (Secure Hypertext Transfer Protocol) [13] är ett protokoll för krypterad kommunikation mellan webbläsare och servrar. Då det är en komplettering av HTTP kan det användas ovanpå säkerhetsprotokoll för lägre kommunikationslager, som SSL. Protokollet använder sig av både asymmetrisk och symmetrisk kryptering. Netscape Commerce Server, som är en vanlig lösning för slutna betaltjänster, använder sig av detta protokoll.

4 Klassificering av betalsystem

Vid den första kontakten med ämnet befanns en viss begreppsförvirring råda, troligen beroende på att området var relativt nytt. Samma termer användes för system som var väsentligt olika och ibland användes olika termer för samma system, beroende på om systemet betraktades ur implementations- eller användningssynpunkt. Arbetet inleddes därför med att göra en strukturering av ämnet och en indelning av systemen i olika kategorier. De termer som används definieras och viktiga begrepp samt egenskaper tas upp i detta kapitel.

4.1 Relevanta egenskaper hos betalsystem

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

4.1.1 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 verkar utan tvekan till fördel för system som redan har stort kundunderlag eller stöds av inflytelserika organisationer eller företag. Andelen personer med teknisk utbildning bland användarna av Internet sjunker stadigt. De flesta presumtiva användare har ingen möjlighet att själva bedöma säkerhet och prestanda hos ett visst system annat än efter hur det beskrivs i media och 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 troligt att ett system som lätt kan integreras med övriga system har lättare att bli accepterat. Lagstiftningen vad beträffar upphovsrätt och giltigheten av digitala signaturer släpar också efter i stora delar av världen.

4.1.2 Anonymitet

Kundens anonymitet vad beträffar transaktioner gentemot säljare, betalningsförmedlare och banker är en fråga som är viktig på längre sikt. Kunden kan ha partiell anonymitet, om identiteten inte röjs, eller total, där transaktionerna är helt ospårbara. Vissa använder termerna anonymitet (eng. anonymit*y*) och ospårbarhet (eng. untraceability). 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 oftast fallet. Man accepterar att vissa transaktioner bokförs av handlare eller kreditkortsföretag. Anonymitet kan är dock önskvärt vid många tillfällen, till exempel köp av politiskt känslig litteratur eller tidskrifter i vissa länder. Möjligheten att bli dränkt i en flod av direktreklam från de företag man handlat hos, eller från ett centralt register över köpbeteendet hos betalsystemets användare, är inte heller så lockande.

4.1.3 Betalningar mellan privatpersoner

Det är av intresse att veta om ett betalsystem tillåter privatpersoner att genomföra transaktioner mellan varandra. Ett betalsystem tillåter betalningar mellan privatpersoner om krav och förberedelser för att ta emot betalningar i systemet inte skiljer sig från de som

gäller för att göra utbetalningar. Detta möjliggör tillämpningar där privatpersoner får betalt av leverantören av en produkt, till exempel för att ta del i marknadsundersökningar eller läsa reklambudskap. Att det blir möjligt att betala skulder och låna ut pengar till vänner och bekanta ökar användningen av systemet, vilket i sin tur kan generera intäkter till utgivaren och ger systemet fler användningsområden. En annan fördel är att det blir lättare att etablera sig som handlare. Ju fler produkter som finns tillgängliga, desto större spridning kan betalsystemet få.

4.1.4 Betalningsstruktur

I betalningsstrukturen ligger aspekter som huruvida systemet hanterar förbetalda värdebärande symboler, så kallad symbolisk valuta, eller betalningsinstrument innehållande instruktioner om och auktorisering av ändringar av nominell valuta. 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.

4.1.5 Kompatibilitet

Betalningssystemets möjligheter att på ett enkelt sätt integreras och samexistera med existerande betalningssystem för banker och kreditkortsinstitut 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 mot de system som endast har tillämpningar för Internet. De har en mycket större potential än endast handel på Internet.

4.1.6 Mikrobetalningar

Begreppet mikrobetalningar syftar på transaktioner med små belopp. Sådana är nödvändiga främst för försäljning av små mängder information, till exempel enstaka tidningsartiklar, java-applets eller dokumentation. Andra tillämpningar av mikrobetalningar är att prissättning av en tjänst baseras på små enheter, till exempel betalning per sökning i en databas eller per tidsenhet i ett konferenssystem. Betalsystem där avgifterna per transaktion är för höga kan inte användas för detta ändamål. Teoretiskt kan en mikrobetalning vara hur liten som helst, så länge värdet av transaktionen är högre än kostnaden för att genomföra den. Kostnader som spelar in är hur mycket datorkraft det tar att processa transaktionen och hur stora risker utfärdaren tar.

De risker som finns för utfärdaren kompenseras oftast med avgifter per transaktion. Bäst är naturligtvis om det samtidigt inte finns någon övre gräns för de transaktioner som kan göras.

Benämning	Storlek
Makrobetalningar	>50 kr
Minibetalningar	5-50 kr

Mikrobetalningar	<5 kr

Eftersom begreppet mikrotransaktioner har fått en positiv laddning definierar många företag det efter sina egna produkter. Det kan därför vara bra att definiera begreppet för denna rapport. Jag använder mig även av ett annat begrepp, minibetalningar. Större belopp än så benämns makrobetalningar.

4.1.7 Robusthet

Systemets tålighet vad beträffar överlastning och oförutsedda fel i kommunikationer och hårdvara är viktig 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.

4.1.8 Skalbarhet

Internetanvändningen ökar fortfarande. 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 offlinesystem en klar fördel. De kräver inte att en tredje part kontaktas under transaktionen och har därmed inte samma benägenhet för ”flaskhalsar” som onlinesystem. Distribuerade system, där ett flertal instanser finns som kan verifiera transaktionen, är en annan lösning på problemet. Kontroll av dubbelspendering görs oftast online 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.

4.1.9 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 de datorer som är anslutna inte har någon form av säkerhet, och intrång lätt kan göras. Dubbelspendering, det vill säga att en exakt kopia av ett redan använt serienummer används som betalning, 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.

4.2 Abstraktionsnivåer hos betalsystem

Det finns många sätt att dela upp olika betalsystem i kategorier. Detta sker efter olika egenskaper hos systemen, vilket gör att en del uppdelningar är disjunkta och andra inte är det. För att tydliggöra de grunder på vilka kategoriseringarna gjorts har jag delat in dem 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 (W3C) [21]. 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 inte är

beroende av varandra. Dock ställer modellen krav på dataflödet, och val av dataflöde begränsar möjliga mekanismer. Modellnivån motsvarar inte helt Policy-nivån i Dr Hallam-Bakers modell, utan vissa av de koncept som ingår i denna tas upp under övriga relevanta egenskaper.

4.3 Modeller

Modellen motsvarar systemets gränssnitt mot användaren, och den form av transaktion systemet utför. Den fungerar som en metafor för betalsystemet, som åskådliggör dess funktion för användaren. De system de flesta är bekanta med är transaktioner med värdebärande valutasymboler, som kontanter, eller betalningsorder utgörande instruktioner om ändringar i registreringar av nominell valuta hos banker och kreditinstitut [3]. Dessa har fått ligga till grund för de modeller som används för elektroniska betalsystem. Den vanligaste uppdelningen av betalsystem är i kontanter, debet/kreditorder eller kreditkorts-betalningar. Detta betyder dock inte att systemen är helt analoga med motsvarigheter i den fysiska världen. Speciellt för kontantmodeller skiljer sig den faktiska funktionen hos systemet från modellen.

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 som gäller för system i den fysiska världen.

4.3.1 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 hänföras [16].

4.3.1.1 Kontanter

Kontanter är symboler som i sig utgör ett värde, precis som ett mynt eller en sedel. De till skillnad från checkar eller kreditkort inte knutna till en viss person, utan samma enhet av betalningsmedlet kan användas av flera personer. Värdet av kontanter måste först debiteras kunden i någon annan form av valuta, som till exempel ändring av saldot på 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 pengarna med sin hemliga nyckel, och dekrypteringsnyckeln finns tillgänglig för alla, så att vem som helst kan kontrollera att pengarna är äkta.

De flesta kontantsystem fungerar dock som fysiska kontanter endast ur användarens synvinkel, det vill säga på modellnivå enligt uppdelningen ovan. Ser man till dataflödet och mekanismerna hos systemen fungerar de ofta mer som kuponger, resecheckar eller polletter gör i den fysiska världen. De är notationella system, där transaktionerna utgör instruktioner om överföringar mellan konton. Pengarna lämnar aldrig banken, utan stannar på ett särskilt konto avsett för betalsystemet tills transaktionen genomförts.

Digitala kontanter kan erbjuda anonymitet eller ospårbarhet, genom att de inte behöver vara knutna till en viss person för att vara giltiga. Kontantsystem är lämpliga för mikrobetalningar. Genom att betala en avgift per uttag, som är den vanligaste modellen, kan användaren sedan själv sprida denna kostnad över ett flertal transaktioner. Begreppet digitala kontanter används ofta som synonymt med system för mikrobetalningar. Mikrobetalningar utgör därför ett bättre och tydligare begrepp.

Att förfalska digitala kontanter utan tillgång till bankens hemliga nyckel är näst intill omöjligt. Dubbelspendering är dock ett problem med digitala pengar. Det är mycket lätt för en förfalskare att helt enkelt göra kopior av äkta digitala pengar, utan att behöva känna till bankens signatur. Sedan kan man betala flera handlare med identiska kopior. Alla kommer att vara giltiga när de kontrolleras med bankens nyckel. 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. Utgivaren kan skydda sig mot detta genom att kontrollera serienumret mot en databas med spenderade pengar. Efter att den första kopian lösts in är de andra ogiltiga. Problemet med detta är att alla transaktioner då måste kontrolleras centralt när de sker. I olika kortbaserade system löses problemet genom att programvara på kortet kontrollerar att pengarna inte används mer än en gång.

Det är också ett problem om den utfärdande bankens signatur skulle röjas, till exempel genom internt spionage. På grund av att det är mycket lätt att på kort tid framställa digitala pengar, skulle en sådan händelse kunna undergräva hela systemet på mycket kort tid. För system med central kontroll av valutan kan dock den förfalskade serien lätt spärras, särskilt om varje nyckel används till endast en kort serie kontanter. Att ha begränsad giltighetstid på pengarna tills de måste lösas in mot nya är en annan lösning. Förfalskning med hjälp av tillgång till den hemliga nyckeln är ett problem som också finns för checkmodeller, men det får mycket mindre omfattning för dessa.

4.3.1.2 Debet/kreditorder eller checkmodeller

Då betalningen sker genom att pengar förs över från kundens konto till handlarens, 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 blir giltig genom utställarens signatur. Samma mekanism med asymmetrisk kryptografi som nämndes ovan för att utfärda digitala kontanter, kan också användas för digitala signaturer på betalningsorder som skickas över nätverk. Skillnaden mellan de system som kallas digitala kontanter och de som kallas digitala checkar är att de förra är förbetalda, det vill säga en summa pengar förs över från kundens konto och reserveras för att sedan kunna föras över till handlaren när ett köp görs. För digitala checkar förs pengarna över direkt från kundens konto till handlarens när köpet görs. Båda typerna är dock i de flesta fall notationella system.

Checksystem är inte lika känsliga för förfalskning som kontantsystem, då det endast är ett konto som kan drabbas. Genom uppsamlingsagenter, som ackumulerar betalningar, kan checksystem göras lämpliga för mikrobetalningar. Checksystemen är oftast mindre komplicerade än kontantsystemen. De är ofta avsedda för att betala till exempel räkningar

och fakturor och föreslås ofta som ett alternativ till girobetalningar för privatpersoner. De kan ses som en konkurrent till de ”bank på Internet”-lösningar som erbjuds idag.

Ett checksystem kan inte erbjuda anonymitet eller ospårbarhet, annat än möjligtvis hos handlaren.

4.3.1.3 Kreditkort

Att överföra kreditkortsinformation dök upp som en av de första lösningarna för elektronisk betalning på Internet. De första varianterna var inte säkra, utan kundens kreditkortsinformation sändes i klartext över Internet via e-post eller HTTP. 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 finns som är kopplade till det vanliga clearingsystemet för kreditkortshandel, så att en handlare på Internet inte nämnvärt skiljer sig från en butik med kortläsare. Ett protokoll presenterat av MasterCard och VISA under 1996, SET (*Secure Electronic Transactions*) [31], har accepteras som defactostandard för kreditkortsbetalningar. Detta utesluter dock inte att olika leverantörer erbjuder egna system och speciella tjänster som följer standarden, men erbjuder utökade tjänster.

Säkert överförd kreditkortsinformation fyller ett stort behov hos kunder intresserade av handel på Internet. Det är ett mycket vanligt betalningssätt vid köp utanför Internet. Tillgängligheten och den spridda användningen kreditkortsbetalningar hos allmänheten gör systemen till självskrivna alternativ för elektronisk betalning.

Kreditkortsbetalningar är lämpliga för överföringar av större belopp. Kreditkorts-innehavaren betalar efter att handlarens konto krediterats. Systemet är väl beprövat och juridiska frågor, som hantering av utebliven betalning, är väl definierade. Detta ger kunden större säkerhet vad gäller falska betalningskrav och liknande, men osäkerheten för kreditkortsfirman, och omkostnader för transaktionen tas ut i form av avgifter per överföring, något som gör systemen olämpliga för mikrobetalningar.

4.3.2 Öppna och slutna system

En distinktion som ofta görs är den mellan 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 en relation dem emellan. Det enda som krävs är att de använder samma betalsystem. En analogi är skillnaden mellan 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 handla. 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 han redan har. Så kallade marknadsplatser använder sig av detta koncept. Dessa underlättar processen genom att flera handlare ansluter sig till samma marknadsplats. Dock måste kunden och handlaren binda sig till marknadsplatsen och dess system.

4.4 Dataflöde

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. Exempel på sådana uppdelningar är online och offlinesystem, öppna och slutna system, och system som erbjuder uppsamling av betalningar eller direkt förbindelse med existerande clearingnätverk.

4.4.1 Online och Offlinesystem

När man på dataflödesnivå talar om transaktioner över nätverk skiljer man på om de sker online eller offline [10]. Om transaktionen sker online, 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 onlinesystem. 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 offlinesystem 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 (Personal Digital Assistant) med läsare för smarta kort. De flesta av dessa system är inte avsedda för Internet, även om möjligheten finns, och faller utanför ramarna för denna rapport. Några kommer dock att tas upp kort, då kännedom om dem är intressant.

4.4.2 Uppsamlingsagenter och förbindelseagenter

En förekommande, men något vag uppdelning är mellan uppsamlingsagenter och förbindelseagenter. Ett system som använder en uppsamlingsagent (eng. collection agent) fungerar genom att kunden och eventuellt också 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, alternativt fakturerar kunden. Detta möjliggör mikrobetalningar, eftersom avgifterna för kort eller checkkonto sprids över många betalningar.

En förbindelseagent (eng. 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 förmedlar endast transaktionen. Denna typ av system har också möjligheten att vara distribuerade, och inte använda sig av en central server, som kan bli överbelastad.

4.5 Mekanismer

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. Det finns även system som inte använder sig av kryptering överhuvud taget, som First Virtual Internet Payment System.

5 Exempel på betalsystem

Nedanstående genomgång använder sig av de uppdelningar och begrepp som nämnts i föregående kapitel. Det finns en stor mängd mer eller mindre seriösa ansatser till betalsystem för Internet. Två löst definierade kriterier har gällt för att ett system skall tas med i sammanställningen.

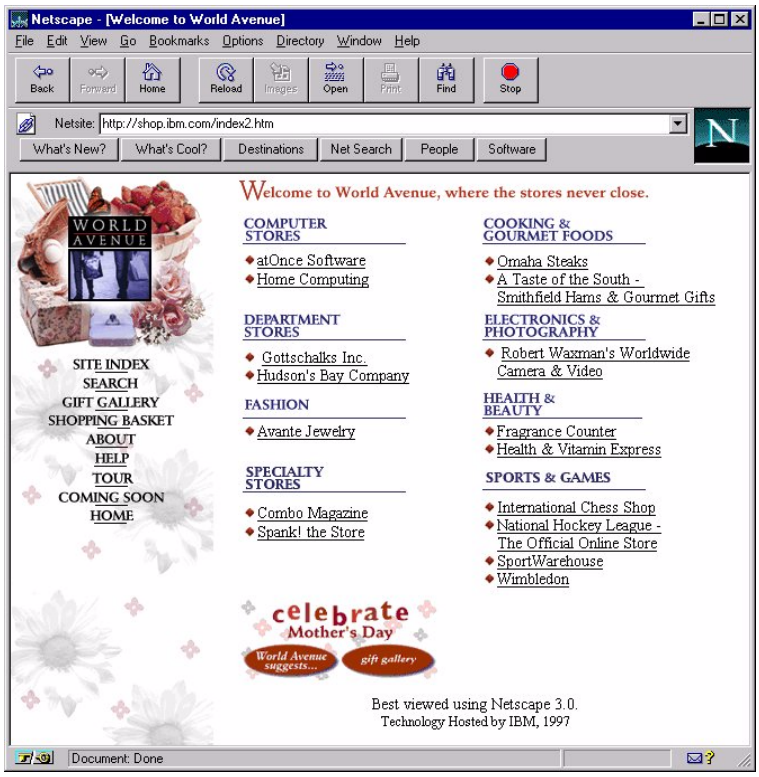
- Systemet skall ha utvecklats som en seriös satsning av forskningsinstitut, universitet eller företag med möjlighet att föra ut systemet i praktisk användning.
- Systemet skall ha möjlighet att vara aktuellt för användning i Sverige av svenska företag inom en period av två år.

Många av de system som har studerats under instuderingsfasen har inte uppfyllt dessa krav. Då kraven inte har varit möjliga att definiera stringent, har urvalet skett generöst. De system som har störst spridning, eller kan förväntas få detta genom stöd från myndigheter eller större företag, får en längre genomgång, medan mindre och lokala system som kan vara av visst intresse att känna till endast ges en kortare beskrivning. System som ännu inte tagits i bruk får också en kortare genomgång. I de fall där användning för Internethandel är trolig, nämns även system som baserar sig på särskild hårdvara. Vissa system som var aktuella under arbetets början och fanns medtagna i examensarbetets första rapport har av olika skäl inte fått den spridning som kunde väntas och är därför inte med här.

5.1 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, till exempel via telefon, 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 säkra protokoll, som S-HTTP. Lösningen är enkel för handlaren, men erbjuder inte några fördelar för kunden.

Det vanligaste är att ett företag administrerar en webbserver på vilken olika företag kan köpa plats. Exempel på dessa IBM World Avenue [35] och Postens Torget [33].



Figur B: IBM World Avenue.

Nackdelar med dessa system är att de inte erbjuder någon anonymitet, och inte heller någon flexibilitet. De är heller inte avsedda för transaktioner mellan privatpersoner. Registreringsproceduren, som måste göras separat för varje sådan handlare, förhindrar spontana inköp, och används endast för en tillämpning åt gången. Framtidens digitala handel kommer troligtvis att omfatta mer än bara www-butiker. Min åsikt är att kunder kommer att vilja använda samma betalsystem för att handla mat, kläder, information, grupparbetsplatser på Internet och andra produkter vi inte sett än. Denna typ av betalning har en nisch, men är för begränsad för att täcka alla behov och möjligheter hos elektronisk handel.

5.2 Öppna system

Öppna system är mer flexibla och utgör enligt min åsikt framtiden för elektronisk handel. De mer framsynta systemen har också potentialen att erbjuda mycket mer är endast Internethandel, och vissa har till och med målsättningen att i framtiden helt ersätta de existerande betalningsmedlen. Det var denna kategori som var intressant att närmare undersöka och implementera i testtillämpningen. Utvecklingen efter arbetets avslutande har visat på att en uppdelning av systemen efter transaktionernas storlek troligtvis är mer relevant än den som gjorts nedan. För att vara konsekvent med den tidigare publicerade rapporten har dock uppdelningen som används där behållits.

5.2.1 Säkert överförd kreditkortsinformation

5.2.1.1 CyberCash

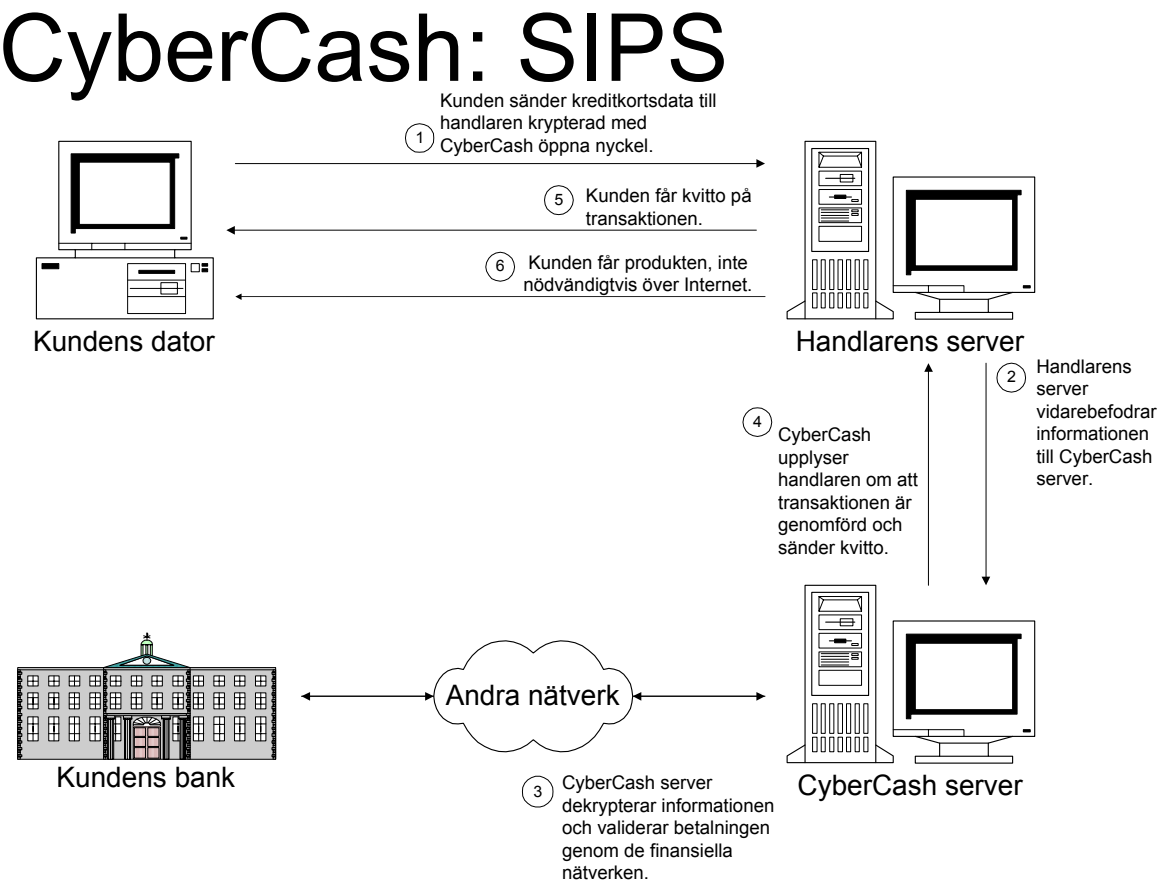
CyberCash marknadsför ett system de kallar SIPS, Secure Internet Payment Service [7][19]. CyberCash system är uppbyggt som en förbindelseagenttjänst, med servrar som länkar till de nätverk som används av banker för elektroniska transaktioner. Kunden har en

klientprogramvara, en så kallad ”elektronisk plånbok”, som distribueras gratis. Denna kommunicerar med handlarens programvara, som sänder betalningsorder vidare till CyberCashs server. Handlarens programvara fungerar som en kortterminal av den typ som används i vanliga butiker.

I kundens plånbok erbjuder CyberCash ett flertal betalningsformer, med check- eller kontantmetafor eller via kreditkort. CyberCash checksystem heter PayNow och kontantsystemet har döpts till CyberCoin. Kunden kan sedan vid betalningstillfället välja den metod som passar bäst. Vid installationen av plånboken genereras privat och publik RSA-nyckel för kunden. I plånboken lagras sedan information om kundens konton, kreditkort och eventuella CyberCoins i krypterad form.

Då kunden funnit något intressant att köpa, klickar han på en länk på någon av handlarens sidor. Han laddar då ned en fil av MIME-typ ”application/cybercash” till sin webbläsare. Köparens plånbok startas då automatiskt från webbläsaren. Köparen väljer betalningsmetod, till exempel kreditkort. Därefter signerar och krypterar kundens CyberCash-klient betalningsordern tillsammans med informationen CyberCash betalningsbrygga behöver och för över den till handlarens server. Handlaren kan inte avläsa kundens kreditkorts- eller kontoinformation. Hos handlaren kontrolleras informationen och handlaren lägger till en debiteringsorder för köparens kort. Denna krypteras och signeras med handlarens privata nyckel. Sedan sänds informationen vidare till en CyberCash-server som är kopplad till det vanliga kreditkortsnätet, på samma sätt som en kortläsare i en affär. CyberCash-servern dekrypterar meddelandet, som kontrolleras för äkthet och sänds vidare till clearingsystemet. Handlaren får en bekräftelse på betalningen om allt gick bra, eller ett felmeddelande om transaktionen inte godkändes. Detta sänds vidare till kunden. Förfarandet är likartat för övriga betalningsmetoder i plånboken.

CyberCash använder sig av både DES- och RSA-kryptografi för att skydda 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. Varken kunden eller handlaren kan heller förneka att de initierat transaktionen, då transaktionsmeddelandet signeras av respektive part.



Figur C: En CyberCash-transaktion.

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 och handlaren har aldrig tillgång till den. Företaget avser att i framtiden följa SET-specifikationen. Företaget har en stark ställning på marknaden för betalsystem, och ett brett utbud av tjänster inkluderade i sin klientprogramvara. CyberCash har ytterligare stärkt sin ställning genom att köpa NetBill. Dock har CyberCash gjort mycket stora investeringar i sina produkter, som är mer avancerade än konkurrerande många konkurrerande system. Företaget måste ha en mycket bred kundbas för att få igen dessa investeringar. Jämför med till exempel First Virtual, som inte har någon särskild programvara för kunden och vars system för handlarna är mycket enkelt uppbyggt.

5.2.1.2 Globe ID

GlobeID är ett uppsamlingssystem efter debet-kreditmodell som är under testning i Frankrike [23][24][25]. Det skall komma att hantera förbetalda checkar, köpta genom GlobeID, på kundens dator för små transaktioner, och kreditkortstransaktioner för större summor. Alla transaktioner hanteras av GlobeID, och kund och handlare måste ha konton på GlobeID 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 kreditkortsmodeller. För kunden innebär detta att samtliga betalningar skall vara tillgängliga i samma programvara, som kallas för kundens ”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 med MD5 och RSA-teknik för identifiering av kunden och kryptering av information.

När en kund har verifierat att han vill köpa produkten, sänder handlarens server en begäran om betalning till GlobeIDs server. Servern hanterar sedan verifiering av betalningen och kontroll av kundens identitet. Därefter förs summan över från kundens konto till handlarens. Handlaren får ett kvitto från GlobeID-servern på att transaktionen är utförd, och levererar produkten.

5.2.1.3 SET

SET [31] är en öppen standard avsedd för betalkortshandel över öppna nätverk som har blivit framtagen på initiativ av Visa och Mastercard. Delvis på grund av dessa företags dominans på betalkortsmarknaden har många andra företag ställt sig bakom förslaget, som blivit accepterat som de-facto standard. SET är en mängd protokoll och rekommendationer som avser att uttömmande specificera alla transaktioner hos korthandel över öppna nätverk. Systemet skall tillhandahålla samma tjänster som finns tillgängliga för kreditkortsterminaler. Ambitionsnivån går därvid utöver den för många alternativa system. Detaljer i implementationen har lämnas dock öppna för att tillåta olikheter hos utfärdarnas bakomliggande system. SET kombinerar digitala signaturer, DES- och RSA-baserad kryptering för skydda konfidentialitet och integritet hos betalnings- och orderinformation och för att verifiera ursprunget hos meddelanden. Kunden, handlaren och parten som hanterar betalningen verifieras genom certifikat. Publika nycklar används för att kryptera de meddelanden som sänds. Kortinformationen passerar krypterad genom handlarens system och denne kan alltså inte avläsa kortnumret eller annan information som endast är nödvändig för banken. På samma sätt kan inte heller banken avläsa vilka varor som handlades.

Särskild mjukvara krävs hos kunden och handlaren samt hos handlarens bank för att behandla transaktionerna.

De transaktioner som SET specificerar är finns sammanfattade nedan. På grund av att tillfredsställande översättningar inte finns tillgängliga används engelska termer.

- Card holder registration (Registering av kortinnehavare.)
- Merchant registration (Registrering av handlare.)
- Purchase request (Begäran om köp från kunden.)
- Payment authorization (Verifikation/kontroll av köp och godkännande från banken.)
- Payment capture (Överföring av tillgångar till handlaren efter avslutat köp.)
- Certificate query (Certifikatförfrågan.)
- Purchase inquiry (Köpeförfrågan.)
- Purchase notification (Meddelande om köp.)
- Sale transaction (Säljtransaktion.)
- Authorization reversal (Indragande av transaktionens godkännande – se ovan.)
- Capture reversal (Indragande av slutlig överföring.)
- Credit (Kredit.)
- Credit reversal (Indragande av kredit.)

SET kan implementeras med eller utan certifiering av kunden, det vill säga ett alternativ där endast handlaren och parten som hanterar betalningen använder certifikat och ett där alla tre parter certifieras. Kunden och handlaren kan också välja att först kontrollera varandras identiteter innan transaktionen initieras. För närvarande är det kanske mest

realistiskt att implementera varianten där kunden inte använder certifikat, eftersom det är tveksamt om certifieringsinstanserna klarar av den belastningen.

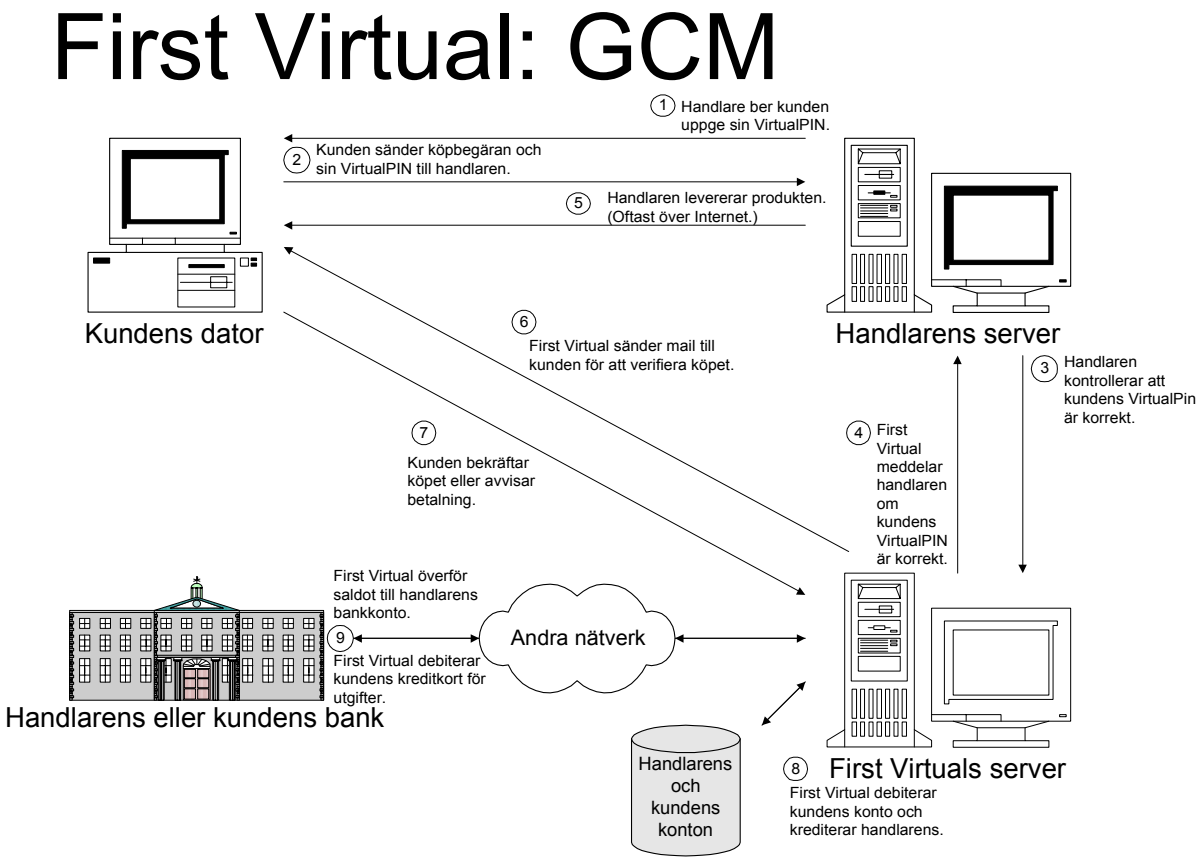
SET är mycket beräkningstungt, på grund av de beräkningar som är nödvändiga för kryptering, signaturer och certifikat. Varje köptransaktion innebär två eller fyra meddelanden mellan kunden och handlaren, och två meddelanden mellan handlaren och servern som utgör bryggan till bankernas nätverk. När två parter skall kommunicera, behöver deras certifikat verifieras. För varje meddelande skall sedan digitala signaturer användas, kommunikationen skall skyddas med DES och meddelanden skall krypteras och dekrypteras med RSA. Varje transaktion kräver också omfattande kommunikation med olika instanser, något som kan bli problematiskt på grund av Internets något opålitliga natur, med borttappade paket och ibland otillräcklig kapacitet. Dessa faktorer kan driva upp priset per transaktion så att systemet inte blir ekonomiskt möjligt att använda för mindre summor. Det påverkar också skalbarheten hos systemet. Den infrastruktur av certifieringsinstanser och bryggor till finansiella nätverk som behövs full att systemet skall kunna användas i full skala kan komma att dröja. Med en mängd aktörer på marknaden och många olika implementationer, är det också en fråga om hur de investeringar som görs i SET skall kunna ge tillräcklig avkastning.

5.2.2 Checkmodeller

5.2.2.1 First Virtual Internet Payment System

First Virtual är ett uppsamlingssystem baserat på ett protokoll för Internetbetalningar kallat Green Commerce Model (GCM) [16][22]. GCM definierar ett flertal tjänster. För närvarande är det dock främst transaktioner mellan konton som hanteras. Systemet är avsett för informationsförsäljning med möjlighet till mikrobetalningar.

De transaktioner som utförs sker mellan konton hos First Virtual, där utgifter från köp och inkomster från försäljning ackumuleras. Det är för tjänster kopplade till detta konto som systemet är avsett. Handel med småsummor är möjlig genom ackumuleringen av dessa på klientens konto. Därför sorterar systemet snarare under debet-kreditorder än kreditkortssystem, trots att utbetalningar i slutändan debiteras kundens kreditkort. På regelbunden basis debiteras kundens kreditkort och inkomna betalningar förs över till handlarens konto. Till detta konto har kunden knutit ett kreditkort vilket debiteras då en viss summa uppnåtts. Kundens kreditkortsinformation förs över till First Virtual endast en gång, när kunden öppnar sitt konto. Detta sker per telefon. Vid olika transaktioner används istället en så kallad VirtualPIN, som används för att identifiera både kunder och handlare. Kunden får sin VPIN via e-post då kreditkortsinformationen är överförd. Då ett köp skall genomföras, sänder kunden sin VPIN till handlaren. Denne sänder en transaktionsbegäran till en Green Commerce-server, med båda parters VPIN inkluderad. Green Commerce-servern sänder ett e-postmeddelande till kunden för att bekräfta transaktionen. Kunden svarar via e-post med ett av tre möjliga alternativ: ”*yes”*, ”*no”* eller ”*fraud”*. Det sista alternativet används då kunden inte initierat transaktionen, det vill säga att någon annan använt kundens VPIN. Ett negativt svar resulterar i att transaktionen inte genomförs, medan ”*fraud”* innebär att kundens konto stängs av tills vidare för att förhindra missbruk. First Virtual rekommenderar de handlare som använder systemet att låta kunden granska varorna innan betalning. Det är alltså möjligt att låta bli att betala för informationen om kunden inte finner den prisvärd. First Virtual avstänger dock kunder som missbrukar denna möjlighet.



Figur D: En Green Commerce-transaktion.

Systemet är främst till för att sälja små bitar information till låg styckkostnad. För de handlare som inte har tillgång till en egen server tillhandahåller First Virtual en marknadsplats, InfoHaus.

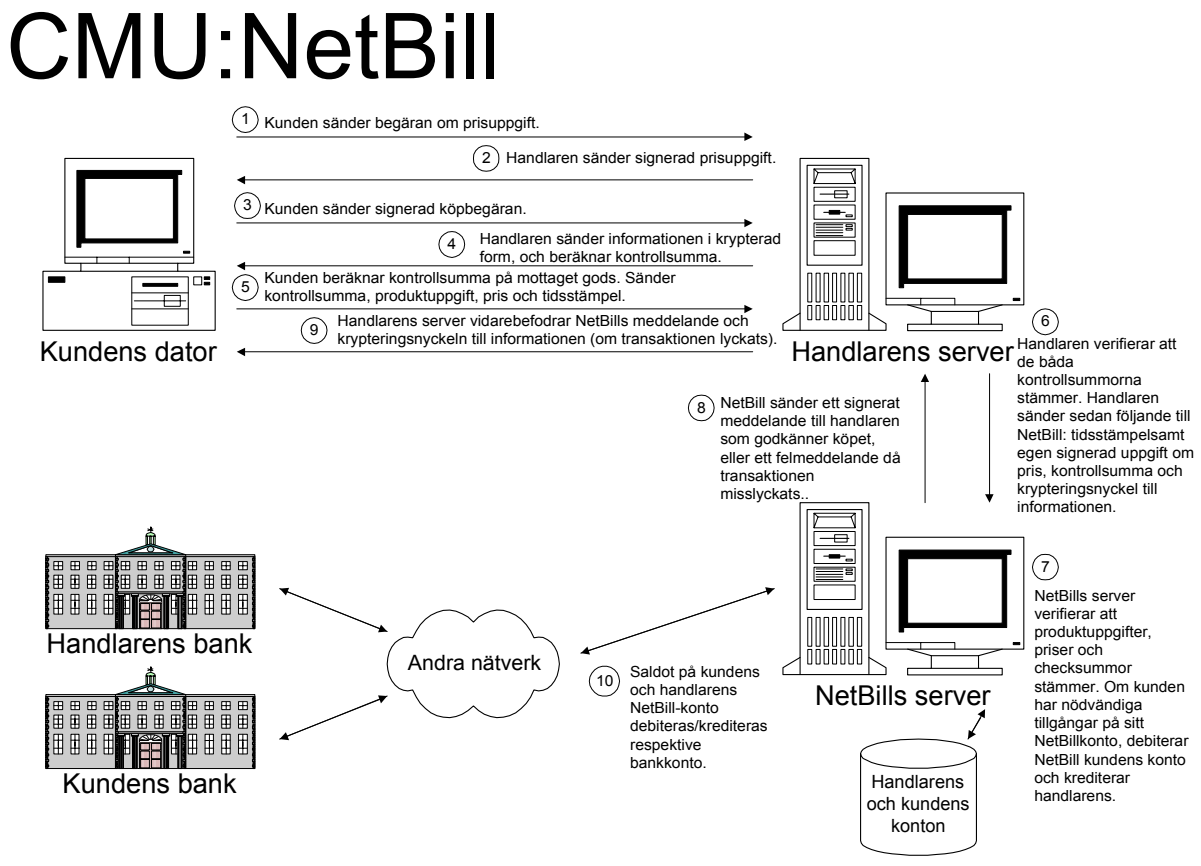
En av de stora fördelarna med systemet gentemot andra uppsamlingsagenter för kreditkort är att det är enkelt att bli First Virtual-handlare. Systemet är lätt att ansluta sig till, och transaktioner kan ske utan särskild programvara. En annan fördel med systemet är att det är uppbyggt kring Internetstandarder och tar hänsyn till de egenheter nätverket har, som långa väntetider och osäker tillgänglighet.

En nackdel med First Virtuals system är att säljaren inte han någon betalningssäkerhet om han inte före leverans kontrollerar att kunden godkänt transaktionen. Överföringar från person till person är inte möjliga om inte mottagaren är handlare. För detta krävs att ett bankkonto knyts till First Virtual-kontot. Kunden har inte heller någon anonymitet gentemot First Virtual. Handlaren behöver dock inte känna till kundens identitet. Det enda han måste få veta är kundens VPIN 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.

5.2.2.2 NetBill

NetBill [14][27] är ett debet-kreditsystem som är avsett för att sälja information över Internet. Carnegie Mellon University, som utvecklat systemet, anser att marknaden för information är den viktigaste på Internet. Man har därför särskilt tagit hänsyn till att möjliggöra ett stort antal mikrotransaktioner till låg kostnad. Systemet handhar inte enbart betalningstransaktioner, utan tar hand om hela transaktionen, inklusive produktleveransen. Detta gör att kunden alltid kan vara säker på att få varan om betalningen har skett. De flesta andra system tar inte hänsyn till detta problem. För att kunna använda NetBill krävs att kunden och handlaren har ett konto hos NetBill, som NetBill administrerar, och att de har för NetBill-handel avsedd programvara installerad.

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 informationen, 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 man ämnar utveckla systemet för att använda asymmetrisk kryptografi.



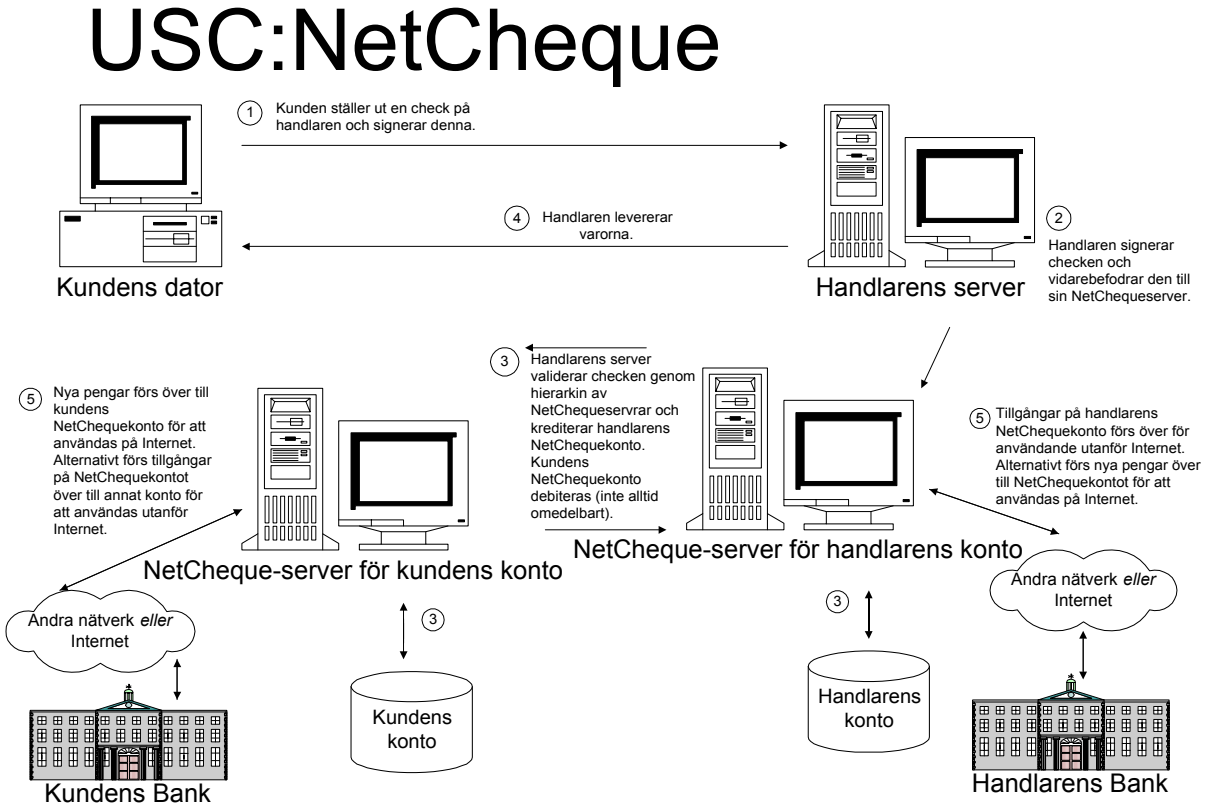
Figur E: En NetBill-transaktion.

Genom att systemet tar hand om alla delar i en transaktion, från order till leverans och betalning får kunden en större trygghet. Detta ramverk saknas i de flesta andra system, som ofta endast hanterar betalningen.

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.

5.2.2.3 NetCheque

NetCheque [12][29] 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. Exportlicens krävs för att använda programvaran utanför USA och Kanada.



Figur F: En NetCheque-transaktion.

5.2.2.4 PayNow

CyberCash har utvecklat en tjänst kallad PayNow [19] för att kunna göra betalningar direkt från kundens bankkonton, som en form av elektroniska checkar. Tjänsten ingår i företagets ”plånbok” med betaltjänster. PayNow är främst avsett för att betala räkningar direkt från webbsidor och kan användas istället för giroinbetalningar. PayNow kan för närvarande inte hantera transaktioner mellan privatpersoner, men CyberCash avser att stödja sådana i framtiden. Kontoinformation lagras i kundens plånbok, samma klientprogramvara som för CyberCash kreditkortssystem och för CyberCoin. Det företag som väljer att ta emot betalningar på detta sätt betalar en avgift per transaktion för tjänsten. Transaktionerna hanteras på samma sätt som för CyberCash kreditkortssystem. Efter att CyberCashs server tagit emot och sänt en bekräftelse på betalningsordern sänds den vidare till tredje part för att genomföra överföringen mellan kundens och handlarens konton.

5.2.3 Kontantsystem

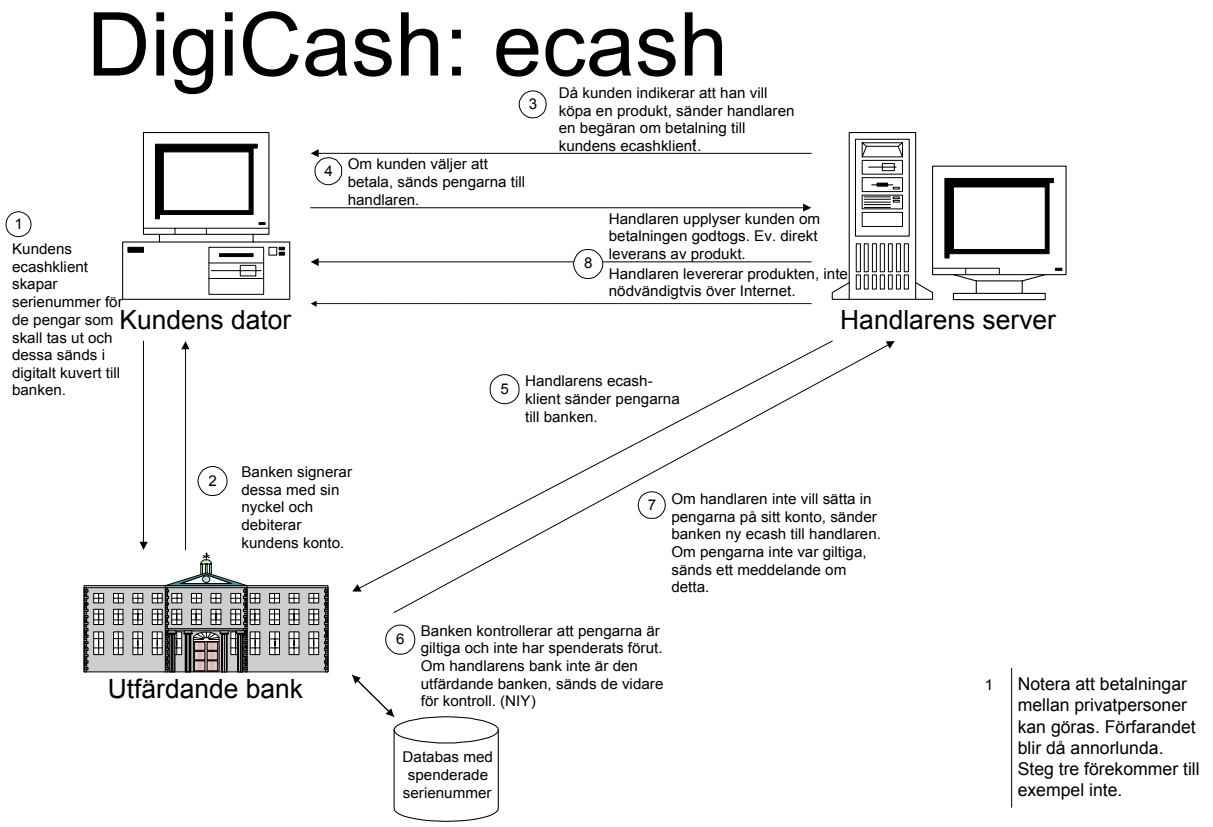
5.2.3.1 CyberCoin

För att även kunna stödja mikrobetalningar, har CyberCash tagit fram CyberCoin [19]. Tjänsten är ett komplement till övriga betalsystem i CyberCash klientprogramvara. Efter att plånboken har kopplats till kundens kreditkort eller bankkonto, kan dessa användas för att köpa CyberCoin. Dessa registreras i kundens plånbok och de faktiska tillgångarna förs över från kundens konto på ett reserverat konto hos kundens bank. Där stannar de tills handlaren löser in de CyberCoins han mottagit som betalning.

Köpförfarandet är detsamma som för CyberCash övriga system fram till det att kunden valt CyberCoin som betalningsmedel. Kundens plånbok drar köpesumman från de CyberCoins kunden har i sin plånbok och sänder dessa till handlaren. Transaktionsmeddelandet tas emot av handlarens programvara, kallad Cash Register, och registreras där. Från handlarens Cash Register förs sedan tillgångarna på handlarens begäran över till dennes konto. CyberCoin kan inte användas för betalningar mellan privatpersoner och systemet är inte anonymt. Att systemet ingår i CyberCash hela svit med betalsystem är en fördel, då det är lätt att köpa och börja använda CyberCoins jämfört med andra system för mikrotransaktioner. Jämför med till exempel Digicash ecash, där ett särskilt konto måste upprättas för de digitala mynten, eller Millicent, där kunden måste upprätta kontakt med de mäklare som säljer den önskade handlarens scrip.

5.2.3.2 Ecash

DigiCash har ett helt öppet system för elektroniska kontanter, ecash [3][6][5][20]. Systemet bygger på kryptografisk teknik utvecklad av David Chaum, som också grundat företaget. Digicash betonar starkt vikten av total anonymitet för kunden.



Figur G: En ecash-transaktion.

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 tillbaka 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.

Dubbelspendering kontrolleras dels genom att när kunden andra gången spenderar pengarna avslöjar han sin identitet, dels genom kontroll med bankens databas över spenderade pengar. Notera att samma pengar aldrig används två gånger. Då en överföring av pengar mellan två personer skett, byter mottagaren de kontanter han mottagit mot nya pengar han själv skapar. Kontrollen mot bankens databas skyddar ju endast banken, och inte den kund som mottagit redan använda betalningsmedel. Om man accepterar en betalning via e-post, är det därför säkrast att så snabbt som möjligt byta denna mot nya pengar. Systemet fungerar via banker och är därför redan integrerat med betalningssystem utanför Internet.

5.2.3.3 Millicent

Millicent [9][26] är ett kontantsystem designat av Digital Equipment. Det är avsett för mikrobetalningar offline, det vill säga att ingen tredje part behöver kontaktas vid transaktionen. Beloppen systemet är avsett för ligger mellan en hundradels dollar till fem dollar. Validering av valutan sker hos handlaren, och därför behövs ingen central kontroll av dubbelspenderade pengar. Detta uppnås genom att varje handlare har sin egen valuta, så kallade scrips. Dessa kan sägas fungera ungefär som ett kuponghäfte. De kan köpas hos utfärdaren, en så kallad *broker*, eller mäklare, för användning hos en särskild handlare. Handlaren licensierar mäklaren att sälja handlarens scrips. En handlare har sedan ett konto hos varje mäklare som säljer handlarens scrips. Den mäklare som sålde handlarens scrip betalar sedan handlaren. Digital tänker sig att mäklarna skall vara till exempel olika internetleverantörer snarare än mer traditionella institutioner, som banker. Huvudsaken är att kunder och handlare har en långsiktig relation till mäklaren.

Hos en eller flera mäklare kan kunden köpa scrips. Kunden måste ha ett konto hos varje mäklare. Vid köp kontrolleras sedan valutan för äkthet lokalt hos handlaren, och den spenderade summan dras av från kundens scrips. Mekanismen använder sig av envägs hashfunktioner, som MD5, för att signera scrips. Dubbelspendering av scrips är inte möjlig, då det är handlaren som löser in sina egna scrips. All kommunikation sker via HTTP, då millicentprotokollet är implementerat som en utvidgning av HTTP. Inga andra förbindelser behövs vid transaktionen.

Fördelar med systemet är att verifiering sker lokalt, vilket kräver mindre av nätverket och gör transaktionerna snabbare. Systemet stödjer också transaktioner med mycket små belopp. Innan ett köp görs måste dock kunden se till att ha rätt summa till hands i form av handlarens scrips. Finns dessa inte hos kundens mäklare måste en ny mäklare först kontaktas. Detta gör att systemet inte är lika flexibelt som de system där valutan kan användas hos samtliga anslutna handlare. Det är möjligt att göra betalningar från handlaren till kunden, men inte mellan privatpersoner. Detta är möjligt hos flera konkurrerande system, som DigiCash ecash och NetCash.

5.2.3.4 Mondex

Mondex är ett system för smarta kort som verkar kunna få stor spridning. Systemet har testats i Storbritannien, Hong Kong, Nya Zealand och Kanada och projektet är mycket längre framskridet än till exempel CAFE (Conditional Access For Europe) och andra konkurrerande system. Speciell hårdvara, som kortläsare, tillverkas av flera olika företag. Det finns ett flertal sådana produkter tillgängliga, från enkla nyckelringar som kan användas för att kontrollera saldot på kortet till plånböcker med infraröd överföring av betalningar. Det finns även telefoner som kan användas för att föra över pengar till Mondexkort och kortläsare till datorer.

Mondex är designat för att kunna genomföra transaktioner över valfri form av förbindelse, under förutsättning att en Mondex-kompatibel kortläsare finns ansluten i varje ände Exempel på möjliga förbindelser är över telefonlinjer, via kommunikation med infrarött ljus, över mobiltelefonnät eller över datornätverk. . Transaktioner över Internet är alltså möjliga, men kräver att en kortläsare ansluts till kundens dator. Mondex Detta ger stor flexibilitet hos systemet. Endast det sändande och det mottagande kortet deltar i transaktionen, ingen verifikation av tredje part behövs.

Digitala signaturer identifierar korten som används och garanterar att de är äkta Mondexkort. Varje transaktion är märkt med sändande och mottagande kort för att ingen skall kunna avlyssna och ta emot betalningen på vägen. Tillverkaren räknar med att

förfalskning inte blir lönsamt, genom att Mondex är baserat på särskild hårdvara som måste kopieras eller omprogrammeras för att kunna förfalska transaktioner. Mondex har även planer på att regelbundet uppgradera korten, så att eventuella lyckade förfalskningar snabbt blir värdelösa. Överföringar mellan privatpersoner är möjliga. Ett Mondexkort identifieras av sin signatur när det används, vilket skulle kunna vara negativt ur anonymitetssynpunkt. Dock är kortet inte bundet till en viss person och transaktionen registreras inte centralt, så detta är ett mindre problem.

Mondex är ett mycket flexibelt system, som dessutom är nästan lika portabelt som kontanter eftersom kontakt med tredje part inte behövs under transaktionen. Detta är en stor fördel mot till exempel VISA Cash, där alla transaktioner måste administreras centralt. Systemet ger tillfredsställande, om inte absolut, anonymitet åt kunden. Som nämnts har också Mondex kommit mycket långt vad gäller spridning och tillverkning av nödvändig utrustning. Aktiemajoriteten i Mondex ägs av Mastercard.

5.2.3.5 NetCash

NetCash [11][28] har utvecklats på University of Southern California, som en del av det betalningssystem som NetCheque utgör. Kunden köper NetCash med hjälp av NetCheque 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 asymmetrisk 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.

5.3 Övrigt

CAFE, eller Conditional Access For Europe, är ett offline kontantsystem för anonym betalning baserat på ett system för smarta kort. Kortet skall kunna användas både för transaktioner och identifiering och stödjer flera valutor. Systemet skall användas för transaktioner i alla sammanhang, även över Internet. Systemet testas under slutet av 1995 och början av 1996. Mondex har dock kommit längre. Andra offlinesystem som använder smarta kort för elektroniska plånböcker är First Card och VISAs Stored Value Cards, Europays Express, Danmont och Proton. I Sverige testar Sparbanken 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.

5.4 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 onlinesystem, 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 offline, något som avlastar nätet avsevärt.

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.

Kreditkort har redan ett enormt kundunderlag jämfört med de andra modellerna, som måste marknadsföra sina system till nya kunder. De är också beprövade system jämfört med andra modeller och kan dra nytta av tidigare kortsystem. 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 som är aktuella. Det bör även finnas möjlighet att ta emot betalningar utan alltför stora omkostnader eller arrangemang. 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 kontantsystem, 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 ett system 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 till hands kan användas, till exempel kreditkort eller elektroniska plånböcker, som Mondex.

6 Att sälja information via WWW – SISU Shop

För att skaffa praktisk erfarenhet av att bygga www-baserade betaltjänster och de olika betalsystem dessa använder sig av ingick i arbetet att implementera en sådan tillämpning för SISU. Det bestämdes att den till att börja med skulle användas för att sälja SISU-rapporter för leverans via Internet i lämpligt filformat. Dessa dokument hade tidigare kunnat beställas för betalning mot faktura och levererades då med post. Rapporterna fanns tillgängliga i lämpligt format för överföring från webbservern och lämpade sig väl som testprodukt. Tillämpningen döptes till SISU Shop.

6.1 Krav på systemet

Med hjälp av denna tillämpning skulle SISU skaffa praktisk erfarenhet av att bygga betaltjänster för Internet, samt utvärdera olika betalsystem avsedda för handel på Internet. Det lämpligaste sättet att göra detta fanns vara att bygga en tillämpning där de olika systemen kunde testas varefter de blev tillgängliga. Tillämpningen skulle utgöras av en grupp webbsidor, där rapporter och annan information kunde säljas genom ett gemensamt gränssnitt. Ett antal krav på systemet togs fram.

Systemet måste vara flexibelt, det vill säga möjligt att utvidga för att acceptera fler än ett betalsystem. Detta måste kunna ske utan stora ingrepp i systemet, och helst utan att betalningsförfarandet i tillämpningen ändrades. De flesta system var under utveckling och i flera fall fanns ännu ingen prototyp, varför inga uppgifter fanns hur de olika systemen skilde sig åt i implementation eller vilken mängd arbete som krävdes för att integrera dem i samma tillämpning.

Systemet måste vara möjligt att utvidga så att det kan användas för att ta betalt för fler tjänster i framtiden, till exempel anmälningar till seminarier, och enligt olika metoder. Detta för att kunna prova betalsystemens användbarhet för olika tillämpningar. Olika prissättningsmodeller diskuterades också, som betalning per sida med fast eller stigande avgift, eller sjunkande pris för varje köpt rapport. Konverteringstjänster mellan olika valutor var också en möjlig framtida tillämpning som diskuterades. Systemet måste därför vara lätt att utvidga för dessa ändamål.

Systemets gränssnitt måste också vara lättanvänt, då användare som vill pröva att använda olika betalsystem inte får skrämmas bort. Det bör dessutom ändras så lite som möjligt mellan de olika betalsystem som används.

6.2 Relaterad teknik

De flesta betaltjänster för Internet som finns idag utgörs av försäljning av varor eller tjänster via webbsidor. Förutom kunskaper om det aktuella betalsystemet krävs även kunskaper om hur detta kan integreras i tillämpningen. För leverans av filer via Internet, till exempel till en webbläsare krävs även viss kunskap om protokoll för detta. Två tekniker som kan behöva förklaras är CGI och MIME.

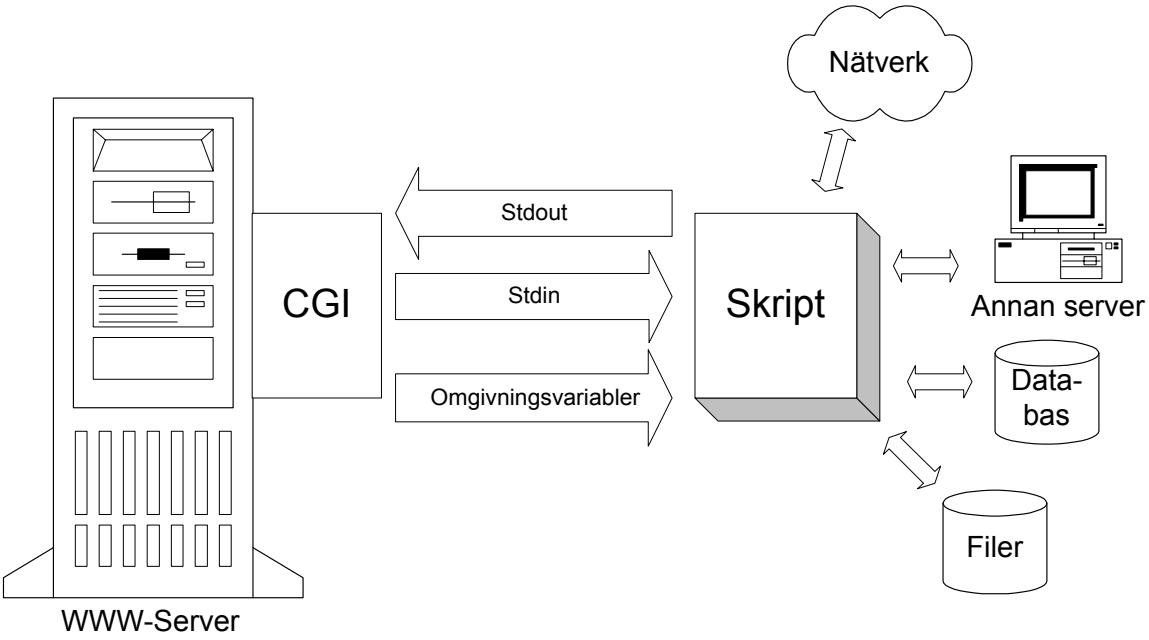
6.2.1 CGI (Common Gateway Interface)

CGI [18] är en standard för att integrera externa tillämpningar med en webbserver. Via CGI kan servern starta program, ofta kallade CGI-skripts, och från dem få utdata till klienter. Klienter sänder en URL till webbservern som refererar till CGI-skriptet. Servern

startar skriptet och överför de data som är nödvändiga via omgivningsvariabler och standard input.

Skriptet kan sedan hämta data från filer, nätverk eller databaser och leverera dessa till servern i lämpligt format. Utdata från skriptets överförs till servern som ett MIME-meddelande från skriptets standard output. Det gör det möjligt att dynamiskt skapa till exempel webbsidor i HTML, istället för att läsa dem statiskt från filer. Möjligheterna att skapa meningsfulla tillämpningar på webben blir därigenom mycket större.

Problem med CGI-skript är att processen startar när servern mottar en URL som refererar till skriptet, och avslutas när resultatet levererats. Detta ger prestandaproblem då många användare samtidigt använder skriptet och en mängd processer på servern arbetar samtidigt. Det ger dessutom mycket begränsade möjligheter att bibehålla ett tillstånd hos klienten. Skriptet startas på nytt varje gång en klient skall interagera med det, och tillståndsinformation får därför lagras hos klienten antingen genom så kallade ”cookies”, vilka klienten kan stänga av hos sin läsare, eller genom att informationen skrivs in i den av skriptet levererade HTML-koden. Detta begränsar interaktionsmöjligheterna hos systemet.



Figur H: Common Gateway Interface.

Efter utvecklingen av SISU Shop har andra alternativ att åstadkomma samma funktionalitet hos en webbserver tagits fram, där olika anrop hanteras av samma process. NSAPI (Netscape API) från Netscape och ISAPI (Internet Server API) från Microsoft är gränssnitt avsedda för specifika kommersiella servrar från de båda företagen. De är effektivare, men svårare att programmera. Den aktuella versionen av CGI är v1.1.

6.2.2 MIME (Multipurpose Internet Mail Extentions)

MIME [2] är en standard för elektronisk post på Internet som gör det möjligt att sända meddelanden med olika teckenuppsättningar, formaterad text och även inkludera bilder, binärfiler och multimedia, som ljud och rörlig bild, i meddelandet. Denna togs fram för att

slippa de begränsningar som Internetstandarden för e-post som beskrivs i RFC 822 hade, som bara tillåter text med radbrytningar i sjubitars ASCII.

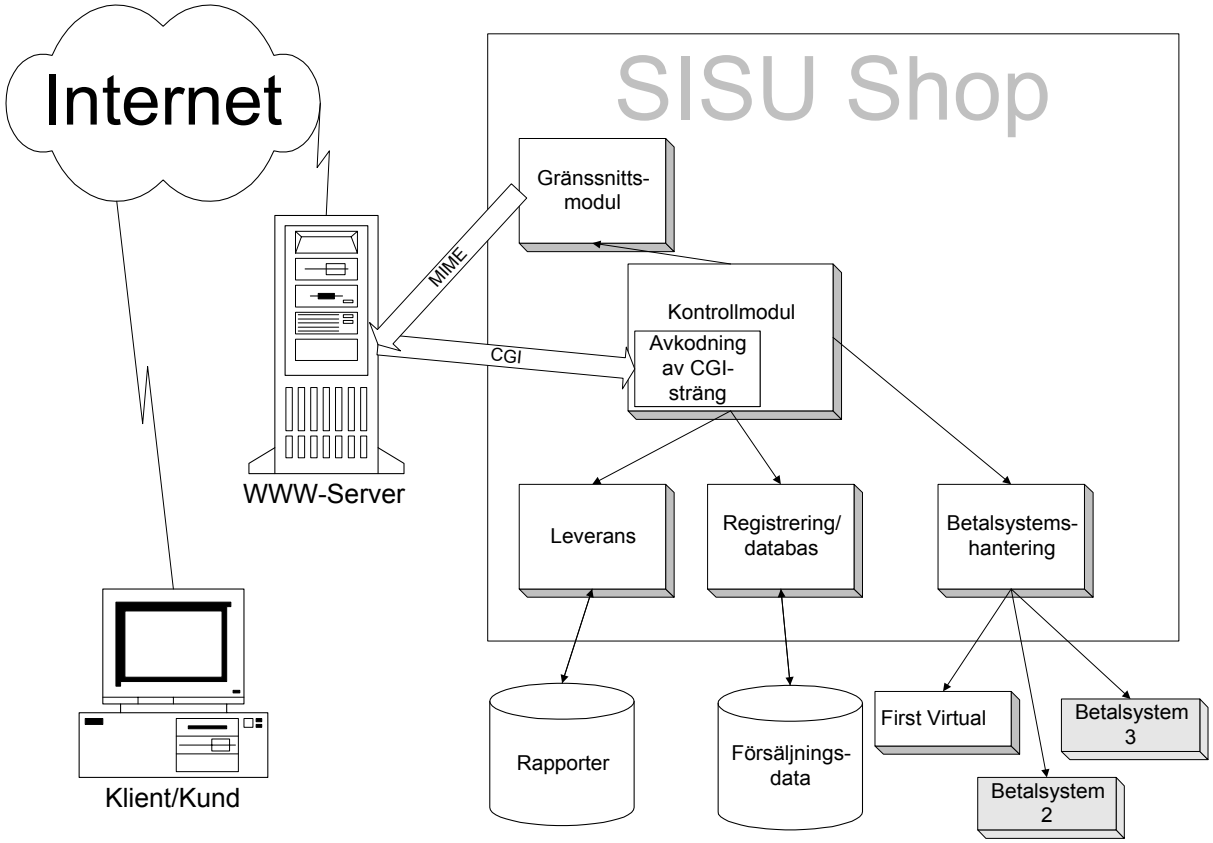
Ett MIME-meddelande består av en ”header” och en ”body”. ”Headern” beskriver bland annat meddelandets innehållstyp eller mediatyp, ”content-type”, och ”content-transfer-encoding” hos kroppen. Informationen i ”content-transfer-encoding” anger hur meddelandet skall transformeras från den sjubitars ASCII-text det sänds som. Mediatypen beskriver hur kroppen hos meddelandet skall tolkas och presenteras för användaren, och kan vara en enkel typ, som text, formaterad text, bild eller ljud, eller vara sammansatt av flera meddelanden. För varje mediatyp kan det finnas flera subtyper, som närmare specificerar meddelandets format. Tillsammans ger mediatypen och subtypen tillräcklig information för att kunna hantera meddelandet korrekt. Nya subtyper tillkommer löpande varefter nya filformat eller tillämpningar uppstår, som till exempel ”application/green-commerce” eller ”application/ cybercash”.

För närvarande finns fem mediatyper definierade [RFC 2046]. Mediatypen ”text” används för olika typer av text. Subtypen ”plain” refererar till ren oformaterad text som kan visas precis som den är. De andra subtyperna till text är avsedda för formaterad text som behöver speciella tillämpningar för att hantera formateringen, men är läsbar utan särskild programvara. Mediatypen ”image” är avsedd för stillbilder som kan visas med lämplig tillämpning. Exempel är ”image/gif” och ”image/jpg”. För ljud finns mediatypen ”audio”, och för rörliga bilder, ofta i kombination med ljud, finns ”video”. Mediatypen ”application” används för data som endast kan tolkas av särskilda tillämpningar, och för överföring av filer via MIME. Subtypen anger sedan vilken tillämpning som kan tolka meddelandet.

Det finns två sammansatta mediatyper: ”message” och ”multipart”. Typen ”message” används för att kapsla in ett annat meddelande eller delar av det. Kroppen hos ett sådant meddelande utgörs av ett helt meddelande, dock inte av MIME-typ. Innehållstypen ”multipart” innebär att kroppen hos meddelandet består av ett eller flera MIME-meddelanden, åtskiljda av en markörsträng som inte får återfinnas i något av meddelandena. Ett ”multipart”-meddelande kan i sin tur bestå av andra ”multipart”-meddelanden. Det finns flera subtyper till ”multipart”-typen, varav två är intressanta för diskussionen av SISU Shop. Subtypen ”mixed” används för ett meddelande innehållande flera andra meddelanden av olika typ och ”alternative” för att representera samma data i flera format och därigenom tillåta den mottagande tillämpningen att välja bästa möjliga sätt att presentera informationen.

6.3 Arkitektur

För att kunna svara mot kraven på flexibilitet hos systemet, fick inte de olika delarna av systemet vara alltför beroende av varandra, eller av en specifik tillämpning av systemet, som till exempel rapportförsäljning. Det var därför nödvändigt att bygga systemet som flera väl avgränsade delsystem. Uppdelningen i delsystem gjordes efter de huvudfunktioner som fanns i systemet, och består av fem moduler.



Figur I: Arkitektur för SISU Shop.

En modul som tar emot indata från servern via CGI, avkodar detta och styr de andra modulerna. Denna modul hanterar betalningsförfarandet på övergripande nivå, och fångar upp eventuella fel som uppstår vid inmatning.

En modul för att dynamiskt generera webbsidor i HTML, det vill säga systemets gränssnitt mot kunden. Denna kan även användas för att sända andra meddelanden i MIME-format till klienten via HTTP.

En modul som generiskt hanterar betalningar för olika system, transparent för det övriga systemet. Denna tar emot den information som lämnas vid en köpförfrågan och delegerar den vidare till valt system. Då betalningsförfarandet mellan olika system kan skilja sig åt på flera punkter, hanterar denna modul hela betalningen tills dess att den antingen är klar eller har misslyckats.

En modul för att registrera köp och hantera beständig information i systemet. Vid användning i större skala blir det troligtvis nödvändigt att koppla denna till en lämplig databas och till andra system inom SISU. För tillfället används dock endast textfiler.

En separat del som hanterar leverans av rapporter och andra filer bedömdes också vara nödvändig. Denna komplicerades senare av att mekanismer måste införas för att hindra utebliven leverans. Detta på grund av att fel hos kundens läsare eller hjälptillämpningar för denna visade sig vara vanliga. Detta system anropas sedan av SISUs webbserver, till vilken levereras webbsidor i HTML eller data som skall överföras till kundens läsare.

6.4 Kontrollmodul

Till skriptet levereras en via CGI en parameterlista som måste avkodas. Denna innehåller information om vilken ny sida som önskas och klientens tillstånd som sparats på webbsidan från förra gången skriptet anropades av denna klient. Då rapporter skall köpas innehåller den också information om vilka rapporter kunden önskar köpa, val av betalsystem och för vissa betalsystem kundens kod. Kontrollmodulen avkodar denna information och aktiverar de övriga modulerna med aktuella parametrar då detta krävs.

6.5 Gränssnitt

Gränssnittet begränsades i viss mån av den begränsade möjligheten till återkoppling hos hypertextmediet. Rapportförsäljningssystemet skulle dessutom smälta in bland övriga webbsidor på SISUs server. Det beslutades att gränssnittet endast skulle stödja de två mest använda läsarna på marknaden våren 1996: Netscape Navigator från och med version 2.0, och Microsoft Explorer från och med version 2.0. Detta för att inte införa alltför många obekanta faktorer på klientsidan av tillämpningen, och för att garantera tillräcklig funktionalitet hos klienten.

Sidorna som utgör ”SISU Shop” genereras dynamiskt av CGI-skriptet. De sidor som har statiskt innehåll läses in från vanliga HTML-filer, men levereras ändå till servern som utdata från CGI-skriptet. På detta sätt fås ett konsekvent gränssnitt för SISU Shop, som är lätt att uppdatera, då eventuella generella ändringar i gränssnitt och layout endast behövs göras en gång. För att bibehålla information om klientens tillstånd, skrivs denna in i HTML-formulär på sidorna.

Strukturen hos gränssnittet är enkel, med en huvudsida som översiktligt förklarar vad systemet gör och hur det används, som har länkar till de olika delarna. De sidor som systemet består av är hierarkiskt uppbyggda, med åtkomst från huvudsidan till de olika huvuddelarna. För att underlätta navigationen i systemet finns en snabbvalsmeny tillgänglig på alla sidor i systemet, så att alla huvuddelar i systemet finns tillgängliga överallt.

6.6 Betalsystem

6.6.1 Val av betalsystem

Avgörande för valet av det betalsystem som skulle bli det första att användas i SISU Shop var att det inte skulle vara i prototypstadiet, utan i praktisk drift och dessutom vara tillgängligt för SISUs kunder och intressenter. Många av de system som var aktuella under våren 1996 fanns ännu inte implementerade, eller tillgängliga för handlare i Sverige.

Tre system utgjorde huvudalternativ till första betalsystem för SISU Shop. DigiCash ecash, First Virtual Internet Payment System och CyberCash kreditkortssystem. DigiCash ecash var det intressantaste och mest innovativa av de tillgängliga alternativen för betalning med digitala kontanter. Systemet var även väl dokumenterat, men bedömdes vara för besvärligt för kunder i Sverige att ansluta sig till. Systemet blir aktuellt att integrera i SISU Shop när Posten, som har ett avtal med Digicash, lanserar ecash i Sverige. First Virtual Internet Payment System var enkelt, väl dokumenterat och lättillgängligt för svenska kunder. CyberCash var mycket lättillgängligt för kunder i Sverige, men saknade möjlighet för handlare utanför USA att etablera sig. Det visade sig också vara svårt att få dokumentation om systemet från leverantören. Detta system har dock under hösten inkluderats i SISU Shop.

Valet gjordes att som första betalsystem för SISU Shop använda First Virtual Internet Payment System, på grund av att det dels var lätt tillgängligt för de tänkta kunderna, dels redan fanns i praktisk drift. Systemet var även väldokumenterat hos leverantören, och bedömdes vara tämligen enkelt att installera. Det fanns färdiga produkter för webbförsäljning att tillgå från First Virtual. Dessa kunde dock inte användas, då den inte kunde integreras med andra betalsystem.

6.6.2 Alternativ implementation

För en handlare som vill använda sig av First Virtuals system, utan att ansluta sig till InfoHaus, finns ett antal alternativ att tillgå. First Virtual har färdiga tillämpningar bestående av CGI-skripts och webbsidor för enklare behov, och ett mer avancerat API för att bygga hela tillämpningar. SISU Shop använder sig dock inte av någon av dessa. Dessa alternativ är användbara för den som snabbt vill börja sälja produkter via www eller FTP, och inte har tid, råd eller kunnande för att konstruera en egen tillämpning. Eftersom dessa utgjorde alternativ till att utveckla en egen tillämpning för teständamål, beskrivs de kort nedan.

Member är ett paket för försäljning av fysiska produkter, tjänster och betalning av medlemskap i föreningar. Det består av ett CGI-skript som skapar ett HTML-formulär där kunden fyller i sin Virtual PIN. Resultatet formateras och sänds till First Virtuals transaktionsserver. Member kräver ingen programmering eller speciell konfigurering. Det är dock inte flexibelt och lämpar sig endast för mindre handlare med en enda eller mycket få produkter. Inget stöd finns för leverans av informationsprodukter.

Websale är ett CGI-skript för att hantera försäljning av information som kan hämtas direkt via en webbläsare. Programmet hanterar både leverans, administration och betalning av informationsprodukter. Transaktionerna sänds som application/green-commerce-formaterade meddelanden via e-post till First Virtual. Skriptet tillåter viss konfigurering av både prissättning och typ av informationsprodukt.

FV API består av ett antal program som tillhandahåller funktionalitet för att konstruera en tillämpning för försäljning av informationsprodukter på Internet. Med FV API kan en mycket mer specialiserad tillämpning konstrueras än vad de tidigare nämnda produkterna erbjuder. Funktioner finns för försäljning via e-post, FTP eller www. För den som skall konstruera sin egen tillämpning utgör FV API en användbar resurs, förutsatt att man är villig att binda sig till First Virtual IPS som betalsystem.

6.6.3 Transaktioner i SISU Shop

Varje transaktion i Green Commerce Model utgörs av ett MIME-meddelande, som kan sändas via e-post eller SGCP (Simple Green Commerce Protocol) [16][22]. SGCP är en specialfall av SMXP (Simple MIME Exchange Protocol), vilket är ett generellt protokoll för utbyte av MIME-meddelanden. Som alla specialfall av SMXP för olika tillämpningsområden definierar SGCP, förutom namnet på det resulterande protokollet, vilken TCP-port servern skall använda (440) och de olika MIME-meddelanden som används. SGCP skall inte närmare beskrivas här, då det inte används i SISU Shop.

Alla transaktioner mellan en Green Commerce-server och en klient till denna har MIME-typen ”application/green-commerce”. Orsaken till att alla meddelanden utgörs av en subtyp till ”application” är att underlätta automatisk hantering av meddelanden med hjälp av särskild programvara. För att de meddelanden som skickas till användare som endast använder sig av helt textbaserade e-postläsare skall vara läsbara, sänds alla dessa både som

text och ”application/green-commerce” i ett meddelande med typen ”multipart/alternative”.

Alla typer av transaktioner har samma MIME-typ, och skiljs åt genom en innehållstypsparameter (eng. Content-type parameter), ”transaction”. De attribut som ingår i en transaktion beror på transaktionstypen. Det finns för närvarande ungefär 40 olika transaktionstyper, rörande betalningar, förfrågningar om dessa och administration av First Virtual-konto, men endast ett fåtal av dessa används i SISU Shop. För en fullständig lista över transaktionstyper hänvisas till First Virtuals dokumentation.

Det meddelande SISU Shop sänder till First Virtuals server för att begära betalning för en produkt är av transaktionstypen ”transfer-request”. När First Virtuals Green Commerce Server mottar meddelandet, sänder den ett ”transfer-query”-meddelande till köparen för att verifiera köpet. På detta svarar köparen med ett ”transfer-response”-meddelande, vilket kan innehålla värdena ”yes”, ”no” eller ”fraud”. När en Green Commerce-server mottagit detta meddelande, sänder den ett ”transfer-result”-meddelande till säljaren, som därmed vet om köparen godkänt transaktionen eller inte.

För varje transaktionstyp finns en mängd attribut definierade. Det är dock inte alla som är absolut nödvändiga att inkludera i en transaktion. För att begära en ”transfer-request”-transaktion, måste minst fem attribut inkluderas i meddelandet. Då denna transaktionstyp är central för First Virtual-betalningar i SISU Shop, ges en närmare beskrivning nedan.

BUYER: Köparens VPIN.
SELLER: Säljarens VPIN.
AMOUNT: Den summa, angiven i aktuell valuta, som köparen skall debiteras.

CURRENCY: Den valuta som skall används vid transaktionen, angiven med förkortning enligt ISO 4217 och i klartext.

DESCRIPTION: En maximalt 40 tecken lång textsträng med en beskrivning av transaktionen.

Förutom dessa finns åtta valfria attribut.

TRANSFER-TYPE: En sträng som anger orsaken till transaktionen. Denna används inte av servern, utan anges som information mellan köpare och säljare. Standard är ”info-sale”.

TRANSFER-ID: En upp till 78 tecken lång sträng innesluten av ”<>” som används i de resulterande ”transfer-query”- och ”transfer-result”-meddelandena.

SECURITY-REQUIREMENTS: En lista av extra säkerhetsåtgärder för transaktionen, åtskilda av semikolon.

DELIVERY-STATUS: En sträng som anger status för leverans av varan. Denna används inte av servern, utan anges som information mellan köpare och säljare. Standard är ”delivered”.

NOTIFICATION-CC: En e-postadress dit en kopia av ”transfer-result”-meddelandet skall skickas.

PAYMENT-EXPECTED: Har ett av värdena ”yes” eller ”no”. Värdet ”no” används då betalning är frivillig eller vid tester för att inte kunden skall få sitt First Virtual-konto avstängt om betalning uteblir. Standard är ”yes”.

DAYS-TO-TIMEOUT: Antal dagar Green Commerce-servern skall vänta på bekräftelse av köpet från kunden innan betalning antas utebli. Standard är 20 dagar.

FULL-NAME: Namnet på säljaren i klartext. 30 tecken långt.

För SISU Shop var det ett krav att kunna använda flera olika betalsystem, och hantera betalningen så fristående från den övriga tillämpningen som möjligt. Betalningen skall dessutom kunna används för ett flertal olika produkter och betalningsformer. Därför utgjorde inget av de färdiga alternativen en bra lösning för systemet. SISU Shop formaterar istället egna transaktionsmeddelanden.

Transaktionerna i SISU Shop hanteras i stort sett likadant som i Websale, det vill säga genom e-postmeddelanden med MIME-typ ”application/green-commerce” som sänds till First Virtuals transaktionsserver. Transaktionerna skulle gå snabbare, men vara något mer arbetskrävande att implementera, om SGCP använts. Nedan syns ett exempel på ett ”transfer-request”-meddelande från SISU Shop till en Green Commerce-server.

```
From: axling@sisu.se
To: transfer@card.com
cc:
Subject: shopsale
Content-type: application/green-commerce;transaction=transfer-request

seller: shop-vpin
buyer: kldu-axling
remote-host: red21.nada.kth.se
transfer-id: <961691415.8203@ernie>
amount: 30.00
currency: USD US Dollars
description: 9604-reports
payment-expected: yes

Thank you for your purchase from
SISU Shop on 960617.
```

Den fördröjning som uppstår då transaktionerna sänds via e-post rör sig om några minuter, mellan två och tio minuter i normalfallet – det beror på antal användare på Internet för stunden och kundens uppkoppling. Detta bedömdes vara fullt acceptabelt, eftersom kunden bekräftar sitt köp via e-post, och därigenom kan fördröja betalningen godtyckligt länge. Eftersom SISU beslutat sig för att följa First Virtuals policy att låta kunden granska materialet innan han betalar är det inte heller intressant att verifiera betalningen innan leverans. Skulle detta ändra sig måste ”transfer-result”-meddelandet från Green Commerce-servern inväntas innan leverans kan ske.

Under hösten 1997 infördes också möjligheten att få en bekräftelse på att köparens kreditkort blivit debiterat för köpet, med digital signatur, vilket gör systemet säkrare för handlaren. Köpförfarandet för informationsprodukter kan dock bli oacceptabelt långsamt om handlaren väntar på en sådan innan leverans.

6.7 Datalagring

Den information systemet behöver lagra består i huvudsak av uppgifter om tillgängliga rapporter, samt försäljningsdata. Denna information lagras i textfiler, då detta bedömdes vara den enklaste lösningen. För närvarande finns inget behov av att analysera informationen och administrationen av rapporterna är ingen betungande uppgift. Skulle detta ändras kan datalagringsdelen av systemet ändras till en koppling mot lämplig databas.

6.8 Leverans av filer

I den första implementationen av leveransmodulen sändes filerna direkt efter avslutad transaktion. De sändes via HTTP-servern i en följd som ett MIME/multipart-meddelande. Från klientens läsare startas sedan en hjälptillämpning, som kan hantera filformatet, eller så kan kunden spara filerna på sin hårddisk. Då det visade sig att hjälptillämpningarna och webbläsaren ofta utgjordes av betaversioner av produkten och inte var särskilt robusta, ändrades detta. Det kunde annars hända att en fil registrerades som levererad, fast kunden inte mottagit den. Istället registreras kundens transaktion och en webbsida överförs, från vilken kunden kan ladda ned sina filer en i taget. På detta sätt kan kunden försöka ladda ned filerna flera gånger om webbläsaren eller någon annan komponent skulle krascha. Leveransmodulen kontrollerar för varje fil som laddas ned att den verkligen köptes av den aktuella kunden från den dator den skall levereras till.

6.9 Erfarenheter

För att bygga en webbtillämpning som använder elektronisk betalning krävs kunskap om allmänna begrepp för att bygga webbtillämpning, såsom HTML, MIME, och hur man skriver CGI-skripts. För ytterligare funktionalitet på klientsidan kan kunskaper i Java vara användbara. Att designa gränssnittet har dock blivit mycket enkelt genom tillkomsten av en mängd HTML-editorer samt program- och klassbibliotek.

Under arbetet med SISU Shop framkom problem med de hjälptillämpningar som läsaren startade för att presentera de köpta dokumenten. Dessa visade sig vara instabila, och systemet låste sig vid flera tillfällen efter det att dokumentet laddats. Köparen fick därvid inget dokument, trots att betalning gjorts. Detta belyste på ett effektivt sätt vikten av mekanismer för att säkerställa leverans av varan efter betalning, samtidigt som handlaren måste vara säker på att få betalt innan varan levereras. Det är inte alla system som stödjer detta i sin transaktionsmodell. I många fall är det också svårt att verifiera betalningens giltighet i realtid på ett tillfredsställande sätt. I till exempel First Virtual Internet Payment System löses detta genom att kunden ges förtroendet att granska varan, det vill säga informationen, innan betalning sker. Att ge kunden ett sådant stort förtroende är dock inte möjligt för alla handlare, och kan i vissa fall inte användas för upphovsrättsskyddat material.

Betalsystemen har tämligen olika uppbyggnad och är olika enkla att använda sig av. De flesta befinner sig dock på utvecklingsstadiet och kräver rätt stor egen arbetsinsats och förståelse för att passa den egna tillämpningen. Osäkerhet om standarder för elektronisk betalning och spridningen av de olika systemen gör att det är svårt att hitta ett lämpligt system att ansluta sig till. Det system man väljer kan komma att kräva mycket resurser att integrera i sin tillämpning, och det krävs att systemet har tillräckligt stor spridning för att det skall vara värt kostnaden.

För kommersiella tillämpningar i full skala torde det också krävas viss integrering med bokförings- och ordersystem, vilket inte gjordes för SISU Shop. Lösningen som gjordes för denna del av systemet är mycket bristfällig.

Paketlösningar för kommersiella webbtillämpningar kommer troligtvis att finnas tillgängliga om intresset visar sig vara tillräckligt stort. Den typ av tillämpningar av betalsystem för Internet som SISU Shop utgör kommer troligtvis inte att byggas från grunden, utan köpas som färdiga produkter. I andra typer av system där det är av intresse att integrera betalsystem, till exempel distribuerade arbetsplatser, distansundervisning, eller andra mer specialiserade tillämpningar, blir dock djupare kunskaper i ämnet

nödvändiga. För vissa tjänster kan det vara nödvändigt att lagra information i mer än en databas, och koppla systemet till andra system inom SISU. Ändringar av denna typ måste kunna genomföras enkelt. På grund av att inget system fanns för rapportförsäljningen, var det dock inte aktuellt att genomföra denna typ av koppling.

7 Diskussion

Det finns en mängd betalsystem utvecklade för Internethandel. De baserar sig på olika modeller och tekniska lösningar. Tre tydliga huvudgrupper är system för mikrobetalningar, debet/kreditsystem och kreditkortshandel. System för mikrobetalningar är avsedda för att sälja små bitar information direkt över Internet, som nyheter, musik, programvara, multimedia eller resultat från databassökningar. Debet/kreditsystem utgör ett alternativ till kreditkortshandel, men är ofta avsedda att användas för att betala räkningar och fakturor. Kreditkort är ett mycket vanligt betalningsmedel och kan användas både på och utanför Internet, något som gör att de har varit lätta att acceptera som betalningsmedel.

Saker att ta hänsyn till vid valet av betalsystem för försäljning av produkter över Internet, är bland annat. betalsystemets spridning, säkerhet, betalningsstruktur och transaktionsstorlek. För informationsförsäljning är tidsfördröjningar vid bekräftelse och validering av transaktionen kritiska, då varan helst bör levereras omedelbart efter köpet. Vid försäljning av fysiska produkter, där leveransen ändå tar några dagar, kan däremot en fördröjning på flera timmar vara acceptabel.

Tillämpningar som SISU Shop kommer inte att behöva byggas från grunden i fortsättningen, utan färdig programvara kommer att finnas tillgänglig. Antagligen kommer det också att gå att välja mellan flera olika alternativ för betalning i samma tillämpning. Resultaten är dock relevanta för system som integrerar betalning med mer avancerade typer av tjänster, som till exempel SISU Virtual Workplace [34].

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 informationsförsäljning 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 har begränsat vissa system, som NetCheque och NetCash, till USA och Kanada. Dock håller detta på att ändras. Det som verkar ha haft en avgörande effekt på utvecklingen är att de stora aktörerna går samman om lösningar.

Nya typer av tjänster, som kan realiseras med hjälp av något av de system som nämnts i rapporten, är ett mycket intressant område. Möjligheter finns att skapa helt nya verksamheter och nischer på den nya marknad som Internet utgör. Möjligheten att enkelt och säkert kunna göra betalningar från slutkonsument till leverantör mellan olika platser i världen, kombinerat med användning av Internet för marknadsföring, gör att många mellanhänder i olika branscher kan komma att försvinna.

8 Tabell

Betalsystem	*Modell*	*Dataflöde*	*Mekanismer*	*Leverantör /utvecklare*	*Status*	*Kommentar*
CyberCash	Betalkort	On-line, förbindelse	RSA, DES	CyberCash Inc.	I drift	I samma "plånbok" ingår även PayNow och CyberCoin.
First Virtual Internet Payment System	Mikrobetal-ningar	On-line, uppsamling	Köp bekräftas via e-post.	First Virtual Holdings Inc.	I drift	Robust men inte vattentätt mot störningar. (Pengarna är dock säkra.)
NetBill	Mikrobetal-ningar	On-line, uppsamling?	DES	Carnegie Mellon, Visa. Köpt av CyberCash.	Testas	Köptes nyligen av CyberCash
CyberCoin	Mikrobetal-ningar	On-line, förbindelse	RSA, DES	CyberCash Inc.	I drift	
PayNow	Check	On-line, förbindelse.	RSA, DES	CyberCash Inc.	Testas	
Ecash	Mikrobetal-ningar	On-line, förbindelse	Patenterat system.	DigiCash bv.	I drift	Anonymt. Har avtal med ett flertal banker.
Millicent	Mikrobetal-ningar	Off-line, uppsamling	RSA, MD5	Digital Equipment Corp.	Testas	
Mondex	Mikrobetal-ningar	Off-line	Hårdvarulös-ning	Mondex Inc.	I drift	God uppslutning från leverantörer av kringutrustning. Mycket lyckade tester.

Litteraturförteckning

Artiklar

[1] Axling, M., Betalsystem för Internet – en överblick, SISU Publikation 96:04, April 1996.

[2] Borenstein, N., Freed, N., MIME Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies, Internet Draft, 1993.

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

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

[5] Digicash: An introduction to ecash, DigiCash bv., 1995.

[6] DigiCash: Ecash Protocol Version 1.2, DigiCash bv., 1996.

[7] Eastlake 3rd, D., Boesch, B. , Crocker, S., Yesil, M., CyberCash Credit Card Protocol Version 0.8, Internet Draft, Februari 1996.

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

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

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

[11]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.

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

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

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

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

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

Böcker

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

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

URL:er

[18]Common Gateway Interface
http://hoohoo.ncsa.uiuc.edu/cgi/overview.html

[19]CyberCash
http://www.cybercash.com/

[20]DigiCash
http://www.digicash.com/

[21]Electronic Payment Schemes
http://www.w3.org/pub/WWW/Payments/roadmap.html

[22]First Virtual
http://www.fv.com/

[23]GCTech
http://www.gctec.com/

[24]GlobeID
http://www.globeid.com/

[25]GlobeOnline
http://www.globeonline.com/

[26]Millicent
http://www.millicent.com/

[27]NetBill
http://www.netbill.com/

[28]NetCash
http://gost.isi.edu/info/netcash/

[29]NetCheque
http://nii-server.isi.edu/info/NetCheque/

[30]PayWatch
http://paywatch.sisu.se/tu/Paywatch_project.htm

[31]Secure Electronic Transactions
http://www.visa.com/cgi-bin/vee/sf/standard.html?2+0

[32]SISU Shop
http://cgi-bin.sisu.se/shop.cgi

[33]Torget
http://www.torget.se/

[34]Virtual Workplace
http://vw.sisu.se/

[35]World Avenue
http://shop.ibm.com/index2.htm