INFOBET
State of the art innen betalingssystemer for salg av elektroniske informasjonstjenester på globale nett

Rapport nr. 891

Katarina de Brisis
Beate Jacobsen
Anders Kluge
Jon Ølnes

31.03.1995

Tittel/Title:
INFOBET
State of the art inne betalingssystemer for salg av elektroniske informasjonstjenester på globale nett

Dato/Date: 31. mars
År/Year: 1995
ISBN: 82-539-0387-1
Publikasjonsnr: 891
Publication no:

Forfatter/Author:
Katarina de Brisis
Beate Jacobsen
Anders Kluge
Jon Ølnes

Sammendrag/Abstract:
Rapporten beskriver situasjonen innen utvikling av betalingsinfrastrukturer og -systemer for handel med elektronisk informasjon over globale datanett. Tradisjonelle løsninger for slik salg beskrives, disse forutsetter som regel abonnementsforhold. Modeller for systemer som skal støtte løssalg av elektronisk informasjon skisseres og vurderes. Kortselskapenes strategier omtales. Rapporten inneholder også en vurdering av de juridiske sider ved betaling for elektronisk informasjon på nettet. Sikkerhetskravene til betalingsssytemer er også beskrevet. De ulike modeller for betalingssystemer blir vurdert med hensyn på anvendelighet til løssalg av elektronisk informasjon over nett, på kort og lengre sikt.
Vedlegget til rapporten beskriver en rekke eksisterende løsninger og løsninger under utvikling, som anvendes for salg av elektronisk informasjon over globale nett (Internett).

Dokumentet er tilgjengelig elektronisk: http://www.nr.no/publications/infobet-soa.ps.gz

Emneord: elektroniske informasjonstjenester, betalingssystemer, Internett
Indexing terms:

Målgruppe/Target group:

Tilgjengelighet/Availability: Åpen

Prosjektdata/Project data: Prosjekt INFOBET

Prosjektnr/Project no: 046001

Antall sider/No of pages: 43+vedlegg

1. Innledning

1.1 Bakgrunn

Den eksplosive fremveksten av Internet-bruken i de siste årene bringer med seg en rekke problemstillinger knyttet til utnyttelse av informasjonen som ligger på nettet. Det er nå klart at stadig flere tjenester som er tilgjengelig på Internettet vil etterhvert bli belagt med en avgift. Dette er en naturlig utvikling, tatt i betraktning kostnader knyttet til utvikling og vedlikehold av seriøse informasjonstjenester.

Det finnes ulike modeller for hvordan betalingssystemer kan fungere i forbindelse med online-tjenester. De to vanligste modeller er kiosk-betaling og abonnementsbasert betaling. Begge disse finnes i mange ulike varianter.

Den første modellen karakteriseres ved at brukeren av tjenestene ikke behøver å identifisere seg overfor en tjenesteleverandør - han/hun skal kun være identifiserbar overfor eieren av nettet som tjenestene formidles på. Betaling for bruk av tjenestene foregår i form av "tellerskritt" og det skjer videre avregning mellom netteier og tjenesteleverandørene. (jfr. Teletorg-konseptet). I enkelte varianter av denne modellen kan selve faktureringsfunksjonen bli "outsourcet" til en underleverandør.

Den andre modellen krever at brukeren inngår en forpliktende avtale med tjenesteleverandøren og betaler ihht. til avtalte abonnementsvilkår direkte til denne, eventuelt går betalingen via en formidler, f.eks. eier av et elektronisk torg - One-Stop-Shop. Da vil brukeren inngå avtale med torgeieren.

Ved bruk av tjenester i globale nett som Internet, er ingen av disse to modellene særlig egnet - kiosk fordi det ikke finnes én eier av nettet, og abonnement fordi det er etterhvert blitt så mange tjenester som mange bruker kun sporadisk. Tegning av et abonnement blir en altfor tung prosedyre og det blir for kostbart for tjenesteleverandørene å vedlikeholde brukeroppfølgingssystemer.

En mulig løsning på disse problemene er et system der brukeren identifiserer seg ved bruk av tjenesten og betaler kun for det han/hun har brukt. Dette praktiseres i dag, særlig i USA og Frankrike, og det brukes kredittkort og/eller direkte debiteringskort som betalingsmiddel. Brukeren av en elektronisk tjeneste trenger kun å oppgi sitt kortnummer og så sendes regningen til kortselskapet eller banken. I prinsippet behøver ikke tjenesteleverandøren vite hvem brukeren er, bare regningen blir sendt til riktig sted. Tjenesteleverandøren trenger derimot en bekreftelse på at det er dekning for regningen.

Bruk av kort fører med seg en rekke problemer, så som fare for misbruk, samt elektroniske spor (kortselskapet vil få oversikt over hva kunden handler av elektronisk informasjon).

Betaling med et kort, gjerne kombinert med en sikkerhetskode ("elektronisk signatur") er én mulig måte å løse betalingsspørsmålet på. Elektronisk autentisering av brukere fører riktignok med seg en rekke nye problemstillinger, så som Tiltrodd Tredje Part (TTP) og ulike teknologier for autentisering. Andre modeller opererer med "petty cash"

kort (så kalte småpengesystemer) eller med en clearingshouse-modell der det opprettes en virtuell "bank" på nettet.

En enkel og sikker betalingsmåte, som ikke krever mye anstrengelser fra brukerens side og omfattende avtaler og avregningssystemer hos leverandøren, er en viktig del av en informasjonsinfrastruktur. Enkle betalingsløsninger vil fremme bruken av elektroniske informasjonstjenester og elektronisk handel generelt. De er også en forutsetning for å få seriøse informasjonsforhandlere til å satse på Internet som formidlingskanal og for å tiltrekke "kjøpesterke" brukere, dvs. brukere som utnytter informasjonen på nettet til profesjonelle formål, og ikke bare til underholdning. Også andre typer verdensomspennende nettverk der informasjon omsettes vil profittere på enkle, sikre og rimelige elektroniske betalingssystemer.

1.2 Prosjektgjennomføring

Prosjekt INFOBET s overordnede mål var å bidra til bedre tilgjengelighet og større utbredelse av elektroniske tjenester tilgjengelig på globale nett. Prosjektets operative mål var å finne frem til anvendelige løsninger for betaling av bruken av de elektroniske tjenestene.

Hoveddelmål for prosjektet var å:

- få oversikt over state-of-the-art innen elektroniske betalingssystemer egnet for elektroniske informasjonstjenester i globale nett
- definere krav og forutsetninger for en pilotløsning av et betalingssystem som kan implementeres innen 1995 på testbasis; testen skulle kunne utføres hos Uninett AS og Telenor AS.

Prosjektet var et samarbeid mellom Telenor Forskning, Uninett AS, Norsk Impact og Norges Forskningsråd v/IT-planen for næringslivet. Hver av partene bidro med kr. 100.000 til prosjektet, som hadde et totalbudsjett på kr. 400.000. Representanter fra hver av de samarbeidende partene utgjorde styringsgruppen for prosjektet. Styringsgruppen besto av: Harald T. Alvestrand, Uninett AS, Halvor Nafstad, Telenor Forskning, Terje Olsen, Norges Forskningsråd og Tor Evensen, Norsk Impact.

Prosjektet ble gjennomført av Norsk Regnesentral. Prosjektleder har vært Katarina de Brisis, IMEDIA. Deltagere i prosjektgruppen har vært Anders Kluge, Gisle Aas, begge IMEDIA, Beate Jacobsen, Institutt for Rettsinformatikk/IMEDIA og Jon Ølnes, DTEK. Even Aaby Larsen, ITIP, har også bidratt med sine kunnskaper om betalingsløsninger.

Prosjektet startet opp 21.november 1994 og ble avsluttet i mars 1995. I løpet av prosjektet har NR hatt møter med BBS (kontaktperson Tom Pedersen), Norges Bank (kontaktperson Eline Vedel), VISA Norge (kontaktperson Jesper Holme) og deltatt i et seminar, arrangert av BBS, om fremtidens bank-grensesnitt mot brukeren.

Prosjektet har hatt direkte kontakt med Einar Stefferud og Darren New hos First Virtual Inc., David Petersen hos Open Market og Peter Paradiso og Dan Schutzer hos

CitiCorp., alle U.S.A. Prosjektet har også hatt kontakt med Stig Frode Mjølsnes, SINTEF om CAFE-prosjektet.

Styringsgruppen for prosjektet har hatt 3 møter (inklusive oppstartmøte) i løpet av prosjektet, prosjektgruppen har hatt 7 møter.

Prosjektets resultater er denne rapporten (SOA-rapport) og et notat med spesifikasjon av en kortsiktig løsning for elektronisk betaling for tjenester/varer tilgjengelig på nett, med tilhørende implementasjonsplan.

1.3 Oppsummering av denne rapporten

Det finnes en mengde leverandører av informasjonstjenester i USA og Europa, den såkalte databaseindustrien. Kunden kjøper slike tjenester ved direkte avtale med databaseverten (tjenesteleverandøren). En databasevert har gjerne en rekke informasjonsleverandører. Utviklingen teknologisk har gått fra at kundene har hatt oppringt samband inn til databasene, til pakkesvitsjet samband, og til at flere og flere bruker Internett til kommunikasjon inn mot databasene. Prisingsstrukturen er gjerne en kombinasjon av fast pris og trafikkavgift etter hvor mye tjenesten brukes. Det er imidlertid en utvikling mot at det er informasjonsenheten som blir priset og ikke den tiden brukeren er oppkoblet mot basen.

For å få til løssalg av informasjonstjenester over nett, er det behov for nye løsninger når det gjelder kunde-leverandørforhold, prisingsmetoder og betalingsformidling. Vi presenterer tre grunnmodeller for å håndtere løssalg av elektroniske informasjonstjenester over nett, i tillegg til den tradisjonelle abonnementsmodellen.

Én modell er basert på at kjøper og selger har et kontohold i en avregningssentral, som tar imot elektroniske betalingsanvisninger over nettet, krediterer og debiterer kontoer, samt sender regninger etter nærmere avtaler.

Kortselskaps-modellen er basert på at kjøper og selger har et forhold til samme kortselskap, selgeren som brukersted og kjøperen som kortholder. Her vil kortnummeret bli brukt som identifikasjon, og kjøperens kort vil bli belastet ved en handel.

Den siste modellen er basert på elektroniske penger, noe som har størst potensiale til å utnyttes til handel på nett. Her vil kjøper og selger sende penger over nettet, i prinsippet på samme måte som kontanter flyter i økonomien i dag.

Alle de tre store kortselskapene er involvert i samarbeid som har til hensikt å skaffe seg markedsandeler av kommersiell virksomhet på nettet. VISA har inngått et samarbeid med Microsoft, men det er lite informasjon om hva dette samarbeidet skal gå ut på, bortsett fra at det vil bli en del av Windows95-lanseringen. Marstercard samarbeider med Netscape Communications som leverer den mest brukte leseren på nettet per i dag. American Express har inngått samarbeid med den store databaseverten America Online.

Løssalg av informasjonstjenester over nett gir en rekke nye juridiske problemstilliger, i forhold til forbrukerrett, personvern og banklovgivning. I forhold til en

avregningssentral som har kontohold for kjøper og selger blir grenseoppgangen mot banklovgivningen viktig. Avregningssentralen kan også komme i berøring med lov om personregistre.

Sikkerhet karakteriseres gjerne av tilgjengelighet, integritet og konfidensialitet. Ved elektronisk betaling vil det også være relevant å vurdere sporbarhet. For å få til et sikkert teknisk system må man ta utgangspunkt i noe en velger å stole på i systemet, gjerne såkalte tiltrodde tredjeparter. Tilliten kan være på to plan, i forhold til kundens betalingsvillighet og -evne og i forhold til mulighet for misbruk. Det bør være signerte og krypterte meldinger mellom aktørene, løsningene bør være basert på offentlig nøkkel kryptografi, og det bør være muligheter for logging av meldinger.

De sentrale elementer ved vurdering av en implementasjon av et betalingssystem for løssalg av informasjonstjenester over nett er sikkerhet, pålitelighet, skalerbarhet, aksept, effektivitet og bruksterskel. Ut fra en vurdering av de fire hovedmodellene som er presentert, anser vi modellen med avregningssentral som den mest formålstjenelige. Den kan realisere løssalg av informasjon over nett med et akseptabelt kostnadsnivå per transaksjon for småkjøp. Det kan også modellen med elektroniske penger, men vi vurderer det slik at elektroniske penger ikke vil få aksept i finansverdenen på kort sikt.

I vedlegg har vi beskrivelser av en rekke løsninger for salg av informasjonstjenester over nett. Løsningene ble forsøkt beskrevet i forhold til autentisering, ordrebehandling, kontering, fakturering og betalingsformidling. Det gis også en vurdering av hver løsning.

2. Elektroniske informasjonstjenester på globale nett - tradisjonelle betalingsløsninger

2.1 Online databaseverter, Europa og U.S.A.

Databaseindustrien har eksistert siden 1960 årene og har egentlig den lengste erfaring med salg av elektroniske tjenester over datanettet. Tradisjonelle databasetjenester aksesseres via direkte telefonlinjer (oppringte samband), pakkesvitsjede offentlige (og private) nett, linjesvitsjede nett (meget sjelden) og Internet (telnet). Bruk av slike tjenester baserer seg utelukkende på en direkte avtale mellom brukere og databaseverten. Databaseverten (tjenesteleverandøren) opptrer ofte på vegne av en rekke databaseprodusenter (informasjonsleverandører). De største vertene som Dialog Information Services (Knight-Ridder) tilbyr over 600 ulike databaser i sin porteføljе.

Databaseindustrien er preget av konsentrasjonstendenser og oppkjøp, slik at stadig flere tjenester (databaser) konsentreres hos en og samme eier. Denne konsentrasjonskoeffisienten har steget i de siste årene, dog mest i U.S.A., og ikke i samme grad i Europa.

Tjenesteleverandørene har i stadig økende grad benyttet seg av nettverksleverandører (distributører) for tilgang til sine tjenester. På 80-tallet har direkte oppringt aksess således veket for pakkesvitsjet aksess via offentlige (Televerk-eide) datanett og private nett som Tymnet i U.S.A. På begynnelsen av 90-tallet har fremveksten av Internet ført

til at stadig flere verter satser på Internet (telnet)-tilknytning, i tillegg til den pakkesvitsjede. Brukererfaringer tilsier at den pakkesvitsjede aksessmetoden fungerer mest tilfredstillende m.h.p. effektivitet. Prisingsstrukturen for slik kommunikasjon er også tilpasset bruken av informasjonstjenester ("burst"- trafikk, med forholdsvis små datamengder). Prising av Internet-basert kommunikasjon er foreløpig et uklart område, da det foregår en veldig vekst i antall selskaper som vil tilby slik aksess og samtrafikk-problematikken ikke er avklart i tilstrekkelig grad (jfr. ComputerWorld-oppslag om Oslonett og TelePost). Fra brukerens side oppleves ofte telnet-basert aksess som treg og upålitelig (begrenset antall samtidige telnet-brukere hos flere databaseverter).

Adgang til tjenesteleverandørers tjenester (databaser) baserer seg, som sagt, på direkte avtaler med brukere. Enkelte store verter (f.eks. ESA-IRS) baserer seg på lokale agenter i regioner/land, som opptrer på vegne av dem, inklusive innkreving av betaling. Dette har innvirkning på betalingsformidlingsmetoden som benyttes.

Brukerne inngår en abonnementsavtale med tjenesteleverandøren. En avtale kan omfatte flere brukeridentiteter og/eller passord, slik at en institusjon kan være én abonnent med flere underliggende brukere.

Brukernes identitet blir verifisert gjennom en egen brukeridentifikator (et tall i f.eks. Dialog) og et passord. I enkelte tilfeller, f.eks. ESA-IRS, blir kun passord benyttet. Ingen av disse kan velges av brukerne - de blir tildelt autoritativt av tjenesteleverandørene eller deres agenter.

Vertene benytter seg av sterkt varierende prisingsskjema. Generelt observerer man en trend der vertene beveget seg fra ren tidsprising (betaling pr. minutt tid online mot en bestemt base) til en differensiert pris for informasjonen som hentes ut i en online sesjon. De varierende prisingsskjemaene forårsaker at tidspunktet for "når ordre om kjøp blir gitt" varierer kraftig fra vert til vert og fra database til database.

Dette kan illustreres med eksemplene ESA-IRS, Dialog Information Services, BLAISE (British Library Online Information Service) og Dow-Jones News/Retrieval.

ESA-IRS var tidlig ute med deres PFI (Pay For Information) skjema der man kombinerer ulike prisingsstrategier. Verten tar ikke betalt for opprettelse av et abonnement (noe som ofte forekommer hos mindre verter, jfr. Lovdata i Norge). Det opereres heller ikke med årlig fast avgift, men det finnes et minimumsbeløp som skal kunne faktureres pr. år. Verten opererer med en fast betalingsenhet - AU - Accounting Unit (tilsvarende ca 1 ECU). Det benyttes også faste vekslingsrater, uttrykt i AU, mellom de mest kjente valuta (de fleste europeiske valuta pluss dollar, kanadisk dollar, australsk dollar og yen).

Online aksess til alle tjenester hos ESA har en grunnpris - en flat rate på 10 AU pr. time oppkoblingstid. Videre prises databasene som ESA-IRS er selv vert for ved å anvende en flat sesjonsavgift (session rate) som gir brukeren rett til å søke i vedkommende database (eller gruppe av databaser) i ubestemt lang tid. Sesjonsavgiften varierer for de ulike basene (gruppene). I tillegg kommer prisen for informasjonen som hentes ut. Denne prisen settes per informasjonsenhet som hentes ut v.h.a. visningskommandoer, og også avhengig av formatet informasjonen vises i. Det finnes

separat pris for nedlasting av informasjonen til brukerens utstyr. I den senere tid har ESA-IRS gått bort fra sesjonsavgifter på en del databaser og innført "5 gratis kommandoer" i de basene der sesjonsavgiften fremdeles finnes. Dette gir brukeren mulighet å gi 5 kommandoer til databasen før "taksameteret" begynner å løpe.

Andre databaser, som ESA-IRS formidler adgang til, men ikke huser selv, prises med en tidsavgift pr. time oppkoblet tid pluss avgifter for informasjonsenheter som hentes ut.

Abonnenten får periodisk (f.eks. månedlig) faktura fra den lokale agenten (i Norge: NTUB) vedlagt detaljert spesifikasjon av tjenestebruk fra ESA-IRS. Spesifikasjonen omfatter tidsavgifter, sesjonsavgifter og online uthenting av informasjonsenheter. Ved bruk av agenter ser det ut som at minimumsbeløp-bestemmelsen ikke gjelder for individuelle brukere. Faktura betales manuelt via vanlig betalingsformidlingssystem - bankgiro.

Dialog Information Services benytter også en sammensatt prisingsstruktur, med stadig større vekt på prising pr. informasjonsenhet og ikke online tid. Ifølge den gjeldende prisingsstrategi tar Dialog inn tidsavgifter pr. time tilkoblet tid, definert etter skalaen 0, 15, 30, 60, 90 og 120 US dollar. I tillegg kommer avgifter pr. uthentet informasjonsenhet og en egen "view" avgift på 1 dollar. Dialog tilbyr en rekke tilleggstjenester, som f.eks. utsendelse av resultater til brukeren via elektronisk post (istedenfor å se på de online). I den forbindelse kreves det inn en ekstra avgift pr. informasjonsenhet, som også gjøres avhengig av størrelsen (pris pr. block = 1024 tegn). Verten har ingen avgifter knyttet til etablering av abonnementet, men de krever inn en fast årlig avgift pr. passord hos en abonnent. Avgiften er for tiden $75 i U.S.A., $50 i Japan og $45 i resten av verden.

Abonnenten får en spesifisert faktura, f.eks. månedlig. Spesifikasjonen omfatter, i tillegg til ovenfor nevnte avgifter, en spesifikasjon av telekommunikasjonskostnader på Tymnet.

Faktura sendes abonnenten direkte fra Dialog. Brukerne i Norge er nødt å benytte manuelle betalingsmetoder av typen Postsjekk der pengene krediteres vertens konto i en amerikansk bank.

Dialog har også en rekke discount-skjema, der abonnenten tilbys fast-avgift-ubegrenset-bruk løsninger (bulksalg).

Ingen av disse vertene tilbyr i dag en direkte betalingstjeneste i tilknytning til deres informasjonstjenester. Dette er heller ikke nødvendig, da forholdet mellom tjenesteleverandøren og brukeren baserer seg på et abonnement.

BLAISE opererer også med avregningsenheter (Billing Account Units). Disse enheter kan ha ulik pris i ulike valutasorter. Dette gjør det mulig å differensiere prisen melleom britiske, europeiske og ikke-europeiske brukere.

Tjenesten akesseres via pakkesvitjede nett og/eller Internet (telnet). Brukere identifiseres ved passord. Prisingsstrukturen er forholdsvis enkel: det kreves årlig

abonnementsavgift (GBP 85 i Storbritannia og GBP 100 for andre land), det finnes en online tilkoblingstid-avgift (GBP 12 pr. time) og en avgift pr. uthentet informasjonsenhet (GBP 0.45).

Dow-Jones nyhetstjeneste har nokså lik prisingsstruktur, med GBP 0,45 pr. minutt tilkoblet tid og GBP 0,45 for hver informasjonsenhet skrevet ut. Informasjonsenhet defineres dog forskjellig hos BLAISE og hos Dow-Jones: de er en post (referanse) og 1000 tegn respektivt.

En interessant konklusjon som kan trekkes fra ovenstående beskrivelse er at det eksisterer en signifikant forskjell mellom online salg av informasjon og online salg av varer. Forskjellen gir seg særlig utslag i behovet for, og kompleksiteten i, "konteringsmekanismer" hos tjenesteleverandøren. Salg av varer innebærer at brukeren blir debitert en online avgift (f.eks. for tilkoblet tid) pluss prisen for den solgte varen og evt. ekspedisjonskostnader. Salg av informasjon, særlig fra strukturerte databaser, innebærer en nøye overvåking av brukernes forbruk etter en rekke ulike kriteria. Dersom man ser på salg av informasjon via f.eks. World Wide Web, kan pris pr. side være én mulighet, men dette kan vise seg altfor rigid og uhensiktsmessig strategi ("side"-begrepet i WWW er meget løselig definert, dette kan være alt fra noen få linjer til omfattende, samensatte multimedia-dokumenter). Pris pr. en nærmere definert informasjonsenhet synes å være en bedre tilnærming. Slike prisingsstrategier vil være avgjørende i forhold til krav som må stilles til konteringssystemer som tjenesteleverandørene på Internettet, eller andre globale nett, må implementere. Eksempler på informasjonsprisingsstrategier på Internettet finnes i bl.a. beskrivelsen av First Virtual og deres Infohaus.

Prisingsstrategier (og tilhørende konteringssystemer) bør ta hensyn til mangfoldet av informasjonstjenester som kan være tilgjengelig på f.eks. Internettet. WWW (dokument-delen) er én type tjeneste, det finnes også tjenester som Gopher, FTP, WAIS, Veronica osv. Database-grensesnitt i WWW vil gi tilgang til "tradisjonelle" databaser som beskrevet ovenfor. Konteringssystemer hos disse vertene vil måtte tilpasses bruken av tjenestene av "anonyme" brukere, der faktura-grunnlaget må produseres på stedet og oppgjøret vil skje ummiddelbart.

2.2 Amerikanske leverandører av online informasjonstjenester

Det finnes en mengde leverandører av informasjonstjenester i USA. Leverandørene tilbyr gjerne databasetjenester kombinert med forskjellige typer nyheter. Det kan være værmeldinger, sport, vanlige nyheter, elektroniske versjoner av aviser og magasiner, tilgang på elektroniske oppslagsverk, tilbud om forskjellige produkter eller tjenester mm. I tillegg gis det gjerne muligheter for brukerne til å sende meldinger til hverandre. I løpet av 1994 er også flere leverandører begynt å gi tilgang for også å kommunisere med Internett-brukere.

Det er Prodigy, America Online og CompuServe som dominerer det amerikanske markedet. Disse tre er forholdsvis like både når det gjelder antall brukere, hvilken type informasjon de tilbyr og når det gjelder prisingsstruktur.

De tre store leverandørene har omkring 2 millioner brukere hver i USA. CompuServe er størst internasjonalt med omkring 800.000 brukere utenfor USA. Prisingsmodellen er slik at det tilbys en gruppe basistjenester for en månedlig abonnementspris på omkring $10. Basistjenestene kan brukes ubegrenset eller begrenset til et visst antall timer per måned uten avgift så lenge abonnementet er betalt. Så har hver leverandør en mengde andre tjenester som det betales for etter hvor mye brukeren benytter seg av tjenesten (såkalt trafikkavgift). Den kan typisk være på $4-10 per time.

Leverandørene utarbeider informasjon selv eller kjøper tilgang til andre, også av sine konkurrenter. Mens leverandørene av informasjonstjenester tidligere har sett på Internettet som for useriøst og ustrukturert for dem, har "de tre store" nå snudd og alle har i løpet av 1994 gitt sine brukere anledning til å sende og motta epost-meldinger gjennom porter som leverandørene har etablert inn til Internett. Full aksess til Internett er det imidlertid bare Prodigy som har etablert gjennom sitt AstraNet, og det skjedde i januar 1995. De har utviklet sin egen Web-leser som 250.000 Prodigy-kunder lastet ned den første måneden den var tilgjenelig. America Online og CompuServe planlegger å tilby full tilgang til Internett i løpet av mars-april 1995.

I online informasjonstjeneste-bransjen inngåes det nå en mengde allianser og det foregår ulike typer samarbeid. Utviklingen går mot at leverandørene av online tjenester allierer seg med virksomheter som kan levere innholdet i deres online tjeneste. Således samarbeider America Online med Time, Prodigy med Newsweek og CompuServe med People Magazine. Alle disse gir tilgang til en full versjon av disse magasinene før de er tilgjengelig i kioskene og butikkene. Det finnes også mange dagsaviser i elektronisk form hos online-leverandørene. Her er det America Online som har markert seg sterkest. Nylig (i slutten av februar 1995) inngikk America Online også en avtale med Bertelsmann AG, et stort tysk mediekonglomerat som omfatter platebransjen, film og publisering. Dette samarbeidet er høyst sannsynlig en del av America Onlines satsing for å få innpass på det europeiske markedet.

America Online har også inngått samarbeid med American Express om informasjonstjenester fra kortselskapet. Det er ikke lagt opp til noen direkte betalingsmekanismer gjennom nettet, men man kan sjekke sin kontosituasjon hos AmEx og skaffe seg en del reiseinformasjon (se også kap. 4.3). Prodigy har noe liknende samarbeid med Visa.

2.3 Teletel

Teletel er betegnelsen for France Telecoms mest vellykte tjeneste - et torg for mange elektroniske tjenester, tilgjengelig via Videotex-teknologi for både bedrifter og private husholdninger. Tilgangen til tjenestene baserer seg i stor utstrekning på Minitel - et videotex-basert nett (Minitelnet) med dedikerte terminaler (som betraktes ofte som synonyme med Minitel). France Telecom har foretatt en storstilet utplassering av slike terminaler i franske bedrifter og privathusholdninger i løpet av 80-årene. Utbudet av tjenester hos Teletel har vokst stadig de siste årene og teller nå hundrevis av databaser og andre typer informasjonstjenester. Minitel aksesseres via en rekke oppringte aksesspunkter (PAVI). Det eneste kunden trenger for å få adgang til Minitel er et telefonabonnement og en Minitel-terminal (det finnes flere ulike varianter av disse).

Teletel-tjenester prises etter ulike prinsipper, de ulike prisingsskjemaene (takstgruppene) betegnes med bokstavene t0, t1, t7 osv. Bak disse kodene skjuler det seg ulike prisings- og ikke minst avregningsstrategier, der kunden, tjenesteleverandøren og France Telecom (nettleverandøren) er involvert.

Grunnlegende takstgruppe er t0, som tilsvarer "grønn linje" i Norge. Tjenesteleverandører som ønsker å tilby sin informasjon via t0 må betale til France Telecom alle kostnader knyttet til nettbruken. Kunden får tjenesten gratis.

Takstgruppe t1 benyttes til bedriftsinterne tjenester og databasetjenester basert på brukerabonnement. Brukeren og tjenesteleverandøren deler på nettkostnadene, dvs. tjenesteleverandøren betaler delvis France Telecom for bruk av nettet, slik at nettaksess til tjenesten ikke skulle falle for dyrt for brukeren. Tjenesteleverandøren henter så sine penger i form av bruksavgifter fra brukeren. Takstgruppe t3 benyttes til publikumsorienterte "profesjonelle" tjenester som er fullstendig brukerfinansiert, dvs. nettbruken påligger brukeren å betale til France Telecom. Tjenesteleverandøren kan i tillegg kreve inn bruksavgifter fra brukeren. "Kommersielle" databasetjenester benytter seg ofte av denne takstgruppen.

Takstgruppene t3 - t7 utgjør så kalte "kiosk"- tilbud hos Teletel. Dette tilbudet fungerer slik at France Telecom fakturerer brukeren bruken av de ulike tjenestene og siden avregner mot tjenesteleverandørene deres andel av inntekten. Denne andelen stiger i takt med stigningen i taksten mot brukeren (selv om den ikke er direkte proporsjonell). Gruppe t3 har således 3 ulike takster å velge imellom (valget er for tjenesteleverandørene) for publikumsrettede tjenester og 2 takster for "profesjonelle" tjenester. Gruppene t4, t6 og t7 har én takst hver, der t7 er den høyeste.

Eksempelvis var takstene (i 1993) for t1 0,13 FF/ min, for t2 0,37 FF/min, for t36 1,25 FF/min, t4 2,19 FF/min, t6 5,48 FF/min og t7 9,06 FF/min.

Eksempler på prising av databaser tilgjengelig via Teletel er gitt nedenfor:

BIL (juridiske data om franske selskaper) koster 450 FF/time + moms samt takst t2. Databasen kan også aksesseres via kiosk, takstgruppe t4.

BILANS Service (finansiell informasjon om store selskaper) er tilgjengelig på t1 og koster i tillegg 890 FF/time + moms.

CALLISTEL (energi-informasjon) er tilgjengelig på t2 og koster i tillegg 5000 FF + moms for 20 timers bruk.

BODACC (tinglysingsdatabase) er tilgjengelig på t1 og koster i tillegg 2500 FF + moms for 2500 user connect units (u.c.). Bruken avregnes så slik: minutt pålogget: 5 u.c., vise dokument: 2 u.c. og bestille dokument: 3 u.c.

Eksemplene skulle illustrere en variert prisingspolicy i Teletel. Brukerne av Teletel må i mange tilfelle fremdeles forholde seg til både France Telecom og til

tjenesteleverandørene, unntatt kiosktjenestene. Ulike tjenester kan være tilgjengelig både via kiosk og via abonnement.

Så til France Telecoms arbeid med betalingssystemer i tilknytning til Minitel/Teletel. På slutten av 80-årene har France Telecom og ulike andre organisasjoner formet ADTP - Association de Développement du Télépaiement. ADTP har blant annet utviklet tekniske spesifikasjoner for kommunikasjon mellom banker og tjenesteleverandører og ergonomiske spesifikasjoner for et brukervennlig betalingsgrensesnitt mot sluttbrukerne. De tekniske spesifikasjoner ble så standardisert av CFONB (de franske bankenes standardiseringsorganisasjon). Brukerspesifikasjonene ble publisert i en Guide to Electronic Billing.

Resultatet av arbeider til ADTP ble etablering av Sodetel (Société de Développement du Télépaiement) i slutten av 1992. Selskapet ble etablert i fellesskap av France Telecom, BNP, Crédit du Nord, EDF (Electricite de France) og SNCF (franske jernbaner). Sodetel tilbød to betalingstjenester: Telefact og Facitel. Telefact og Facitel ble organisert som uavhengige aksjeselskaper med henholdsvis 23,5 og 3,5 mill FF kapital. Aksjeeiere i Telefact er BNP, Credit Mutuel, Credit du Nord og France Telecom. Facitel eies av Air Inter, BNP, France Telecom og SNCF.

Telefact er et home-banking system som gjør det mulig for brukeren å betale regninger online. Helt spesifikt dreier det seg om store betalingsmottakere som France Telecom (telefonregninger), EDF (strømregninger) og vannverkene (vannregninger). Videre ble systemet utvidet til å omfatte forsikringsselskaper og offentlige myndigheter (forfalt skatt). Brukeren må være registrert for å benytte seg av Telefact. Dersom brukeren allerede benytter et home-banking system fra en av de franske bankene vil han/hun bli automatisk viderekoblet til Telefact fra dette system. Telefact hadde en prøveperiode i 1991-1992 og ble utvidet til full dekning i 1993. Betalingsmottakere bak Telefact trodde at ca 10% av "vanlige" regningsbetalere vil gå over til dette system etterhvert.

Telefact kan aksesseres både via Minitel og via vanlig telefon. Bankene er direktekoblet systemet. Tilleggstjenester i Telefact gjør det mulig for bankene å avregne tilgodehavender seg i mellom og for kundene å se og kontrollere sine regninger som ligger til betaling.

Tjenesten ligner på den norske Postex-tjeneste drevet av Postbanken/Postgiro, bortsett fra at den tillater kun å betale regninger til de tjenesteleverandører som er tilkoblet Telefact.

Facitel er en tjeneste som gjør det mulig å betale direkte for varer/tjenester som er tilgjengelig via Minitel. Tjenesten ble satt ut i prøvedrift i 1993 med en gruppe på 20.000 brukere (husholdninger og bedrifter). Tjenesteleverandører må bli medlemmer av "Minitel Shopping Club" for å kunne benytte seg av Facitel i salg av sine tjenester. Betalingssystemet baserer seg på bruk av vanlige (bank)smartkort med tilhørende PIN-kode. Brukere må ha en smartkort-leser, enten integrert i Minitel-terminalen (Minitel Magis) eller som en frittstående enhet (Lecam Facitel) som kobles mot den vanlige Minitel-terminalen. Facitel forutsettes å bli tatt i bruk av min. 30% av Minitels brukere.

Eksempelvis skal leie av Minitel Magis koste 29,5 FF i måneden og leie av Lecam Facitel 25 FF i måneden.

På det nåværende tidspunkt er følgende tjensteleverandører tilgjengelig via Facitel:
Air Inter (salg av flybilletter)
France Telecom (betaling av telefonregninger)
Interflora (salg av blomster og gaver)
MC France (salg av billetter til idrettsarrangementer)
Reflex (salg av bilforsikring)
SNCF (salg av togbilletter).

Tjenesten fungerer slik at brukeren først gjennomfører selve valget av varen/tjenesten for så å effekturere kjøpet ved å sette inn sitt smartkort i leseren og taste inn PIN-koden. Minitelnet redirigerer da trafikken fra kjøperen til bankenes nett. PIN-koden verifiseres av bankens system og kontoen belastes umiddelbart, slik tilfelle er med POS-terminaler. Bruken av smartkortet mot Facitel styres av det samme regelverket som styrer bruken av bankkort.

I den nærmeste tiden skal flere tjenester bli tilgjengelig gjennom Facitel: hotellbestillinger (Groupe ACCOR), konsertbilletter (Rock MC), bøker og CD-plater (A la Page), plater og videokassetter (Novalis). På lengre sikt skal servicespekteret utvides med flere tjenester fra fritids- , reiseliv- og transportsektorene.

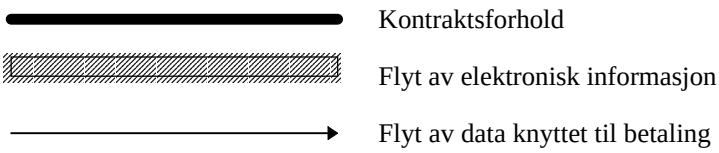
3. Modeller for betalingssystemer for salg av elektroniske tjenester i globale nett

Elektronisk handel på datanett har til i dag stortsett foregått ved at det eksisterte på forhånd etablerte kontrakter mellom selger og kjøper, med en mellompart eller uten. Utbredelse av, og større tilgjengelighet til globale nett introduserer muligheten for "løssalg" av informasjon, uten at det eksisterer et på forhånd avtalt abonnementsforhold mellom tjenesteleverandøren og brukeren. En slik situasjon fordrer at betalingen vil måtte sje umiddelbart, når handelen effektueres. Kjøperen vil være i kontakt med selgeren kun i salgsøyeblikket, slik det foregår i vanlige butikker.

Ulike typer løsninger har tvunget seg frem for å understøtte muligheten for global handel på datanett. Noen av dem forutsetter kundeforhold (kontrakter) og noen gjør ikke det. Vi har prøvd å ordne modellen inn i typiske grupper. Fire hovedgrupper peker seg ut:

1. Abonnement
2. Avregningssentral (kreditt-debet)
3. Elektroniske penger ("digital cash")
4. Direkte belastning av kreditt- og debetkort

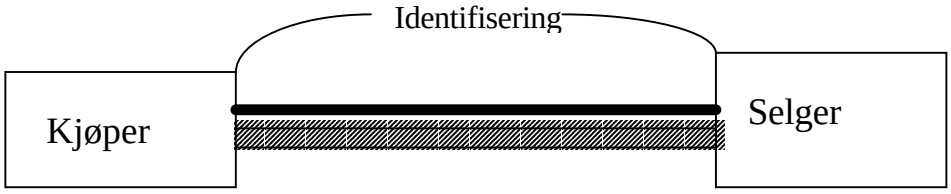
Nedenfor omtaler vi hver av disse modellene mer i detalj. I den grafiske fremstillingen av modellene har vi brukt følgende symboler:



3.1 Abonnement

I denne modellen har kjøperen tilgang på en informajonstjeneste som en selger har lagt ut på et nett. Det kan være en database, en nyhetstjeneste eller liknenede, eller flere tjenester samlet. Det vil vanligvis ikke være betaling over nett, men modellen er likevel tatt med her for helhetens skyld. Modellen forutsetter at kjøperen og informasjonsleverandøren har et kontraktsforhold.
En variant av denne modellen er når flere selgere opptrer sammen hos en databasevert eller på en lokasjon på nettet, gjerne med felles markedsføring, organisering og prisingsstruktur. Da kalles det gjerne markedsplass eller informasjonstorg. Her må kjøperen identifisere seg for at selger / markedsplass skal vite om vedkommende har abonnement, eventuelt for å identifisere hvor faktura skal sendes. Prisingsstruktur vil gjerne være en kombinasjon av betaling for å få tilgang til markedsplassen / selgeren, og for informasjonstjenester som brukes.

Modell 1: Abonnement



3.2 Avregningssentral

En enkel løsning for elektronisk handel ville være å benytte kredittkort direkte mot tjenesteleverandørene. Dette er imidlertid vanskelig av to hovedgrunner:

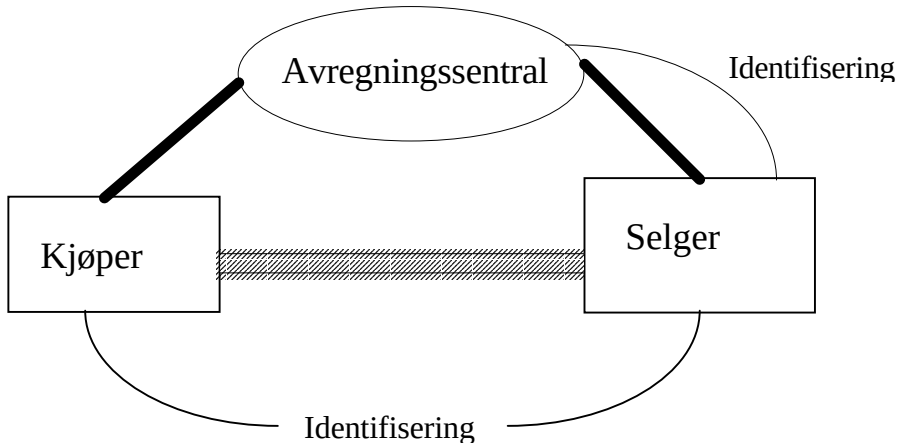
- få av informasjonsselgerne på Internettet er i stand til å oppnå kredittkort-mottager status
- sikkerhetsmekanismer som er nødvendig for å beskytte kortbrukeren mot svindel er kostbare å implementere og vedlikeholde
- transaksjonskostnader er for høye i forhold til kjøpstransaksjoner som ofte er små.

Ovennevnte forhold har gitt støtet til etablering av "meglere" mellom finansverdenen og handelsaktører på nettet. En avregningssentral er en slags elektronisk kontoholder og et clearingshouse for mellomværender mellom kjøpere og selgere på nettet. Begge etablerer kundeforhold og "konti" hos avregningssentralen. Selgeren vil ved forespørsel

om kjøp verifisere om kjøperen har en konto hos en avregningssentral som selgeren har tillit til.

Sentralen sjekker om kjøperen har et kontraktsforhold og kjøpet belastes kundens konto i avregningssentralen. Kjøperen kan faktureres etter avtale (f.eks. periodisk eller etter at saldoen har nådd et vist nivå). Alternativt kan belastninger overføres til kjøperens kredittkort i passende store bolker. Sentralen vil godskrive selgerens konto og overføre hans tilgodehavender periodevis til vedkommendes bank. Både kjøper og selger må ha et kontraktsforhold til en avregningssentral. I noen tilfeller vil det være den samme betalingssentralen, i andre vil selger og kjøper kunne ha konti i ulike avregningssentraler. Da vil det eksistere avregningssentraler for clearing av betalinger mellom "vanlige" avregningssentraler, der selgere og kjøpere har sine konti.
I praksis er avregningssentralene på nettet et bindeledd mellom det virkelige banksystemet og nettet. De leverer også programvare for autentisering, kryptering og bokholderi for kjøpere og selgere. De kan ha opplegg for forhåndsbetaling eller kreditt for sine kunder.

Modell 2: Avregningssentral



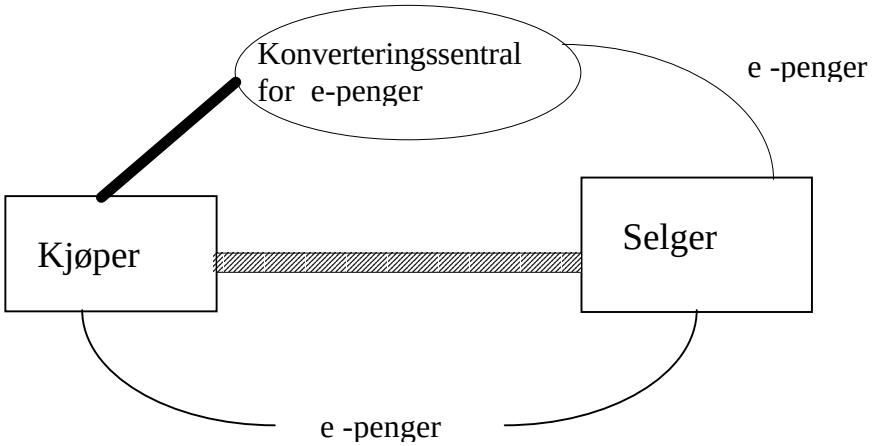
3.3 Elektroniske penger

Elektroniske penger er digitale koder som representerer en verdi. Ved hjelp av kryptografiske metoder kan kodene representere en banks garanti for at dette er et gyldig betalingsmiddel.
Denne modellen er avhengig av at det finnes en institusjon som står som garantist for de elektroniske pengene. Institusjonen må kunne konvertere mellom elektroniske og vanlige penger på en enkel måte. Den må altså være som en "nasjonalbank" for elektroniske penger.

Kjøperen må ha elektroniske penger lokalt, enten ved en form for autoriserte elektroniske penger på en fil, eller ved at et smartkort ladet med penger, koblet opp til kjøperens maskin. Ved kjøp av informasjon, vil riktig beløp trekkes fra filen / smartkortet og bli overført elektronisk til selgeren. Da er det "penger" som går over nettet, ikke ordre om belastning, slik det er i de andre modellene. Selgeren må ha et

mottagerapparat for pengene, en fil eller et smartkort som kan ta dem imot. Når pengene er mottatt må de kunne realiseres ved kreditering av selgerens konto, tas ut ved en minibankliknende automat eller brukes videre ved elektronisk overføring.

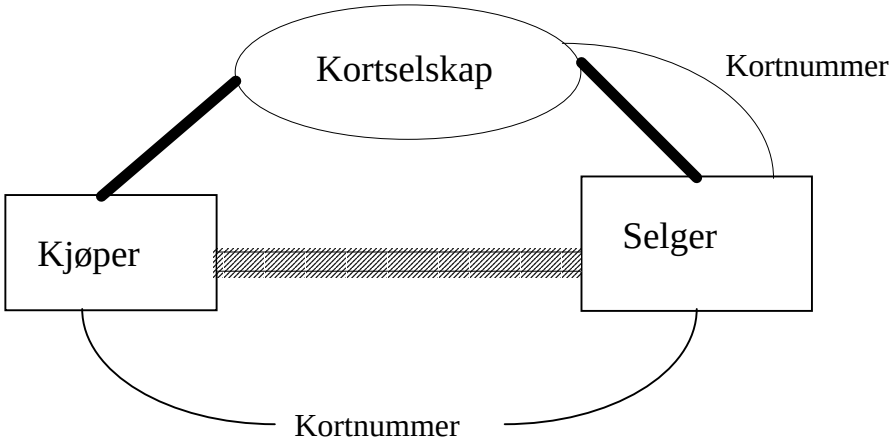
Modell 3: Elektroniske penger



3.4 Belastning av kreditt- og debetkort

Denne modellen er i prinsippet den samme som modellen med avregningssentralen, men med den viktige forskjellen at hvert kjøp belastes direkte kjøperens kort. Dermed er pengeformidlingen håndtert ved etablerte rutiner i kortselskapene. Handel er avhengig av at kjøper og selger har samme kortselskap. Denne modellen forutsetter også at kjøperen vil kunne oppgi sitt kredittkortnummer til selgeren på en sikker måte. Selgeren vil også måtte være tilknyttet kortselskapenes infrastruktur for validering av kort.

Modell 4: Belastning av kort



4. Kortselskapenes strategier

På samme måte som det er en rekke initiativer for tekniske løsninger for formidling av betalingstjenester på nettet, er det mange felles initiativer fra aktører innenfor betalingsformidling og teknologi. Det er verd å merke seg disse initiativene, fordi de representerer en bredde i kompetanse, erfaring og markedskunnskap, som de tekniske initiativene vi ellers har studert ofte mangler. Imidlertid bringer den overveiende del av initiativene de tradisjonelle strukturer videre, som kanskje ikke utnytter det genuint nye ved globale informasjonsnett.

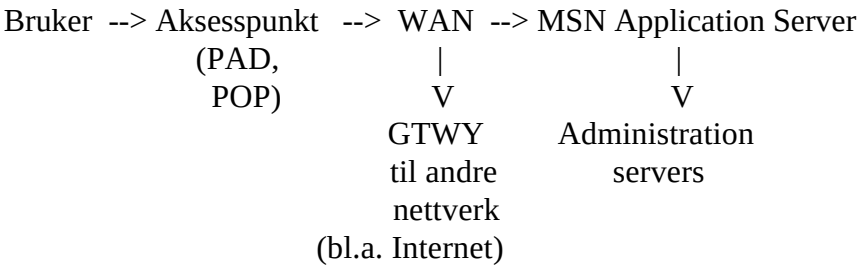
4.1 VISA og Microsoft Network

VISA er ett av de kortselskapene som har markert seg i forbindelse med fremveksten av elektronisk handel. Den mest publiserte begivenhet i denne sammenheng har vært annonseringen av en allianse mellom Microsoft og VISA, der foranledningen var Microsofts lansering av Microsoft Network - et konsept for et VAN med aksess fullstendig intergrert i Microsofts nye operativsystem/brukermiljø Windows 95.

Alliansen befinner seg i skrivende stund på intensjonsavtale-nivå og veldig lite er kjent hverken om arkitekturen og løsningene i Microsoft Network eller VISAs involvering i dette konsept.

Foreliggende informasjon om Microsoft Network kan oppsummeres i det følgende.

Nettverkets arkitektur skal være som skissert nedenfor:



Nettverket skal kunne aksesseres i Norge gjennom Telenor som skal tilby aksess via BT i England. Man ser for seg en 800-nummer tjeneste for adgang til MS Network.

MS Network skal ha et sett med basistjenester som omfatter elektronisk post, BBS, Internet aksess, programvarenedlasting og "chat"-tjeneste. Videre forutsettes det et stort utvalg av "content"-tjenester, levert av ulike , selvstendige tjenesteleverandører som vil ha avtale med MS Network. Microsoft skal selv sørge for leveranse av basis tjenester. Innholdstjenestene vil på kort sikt kun finnes på de "store" språk, som engelsk, fransk, tysk osv.

Microsoft vil basere adgangen til nettets tjenester på en "Exchange Client", en felles klient for e-post, Internet, CompuServe mm. Denne skal være et standard komponent i

Windows 95. Tjenesteleverandører vil implementere server-programvare for MS Network.
Flere satellitter skal sørge for tilgjengeligheten av nettet, som skal være tilgjengelig i 35 land (de land der Windows oversettes til det nasjonale språket). Microsoft har også innledet samarbeidet med Compaq, Sharp og AST for å utvikle en "Wallet PC" som skal kunne aksessere MS Network trådløst. På lengre sikt er også aksess via kabel-TV planlagt.

Nettverket skal støtte den samme betalingsmetode for alle tjenesteleverandører, alle typer varer og tjenester. Nettverket skal ha et grensesnitt mot bankenes systemer og det skal samkjøres med VISAs nettverk. Sikkerhetsmekanismene i nettet vil tilby autentisering, beskyttelse av sensistiv informasjon og signerte kvitteringer.

Det er foreløpig ukjent hvordan VISAs betalingsformidlingsnettverk vil integreres i Microsoft Network. VISA-nettverket heter VisaNet og tilbyr i hovedsak to tjenester: autentiserig / validering (BASE 1) og betalingsformidling (BASE 2). Nettverket aksesseres via VAP (VisaNet Access Points). Meldinger som sendes på nettet er i et proprietært VISA-format. Aktørene i nettverket er banker tilsluttet VISA-systemet, VISA International sine sentra i U.S.A og Storbritannia, der det befinner seg maskiner kalt MIP (Member Interface Processor), selskaper som samler opp POS-transaksjoner (som 3C i Norge) samt POS-automater hos VISA-kjøpmenn og ATM (minibanker).

BASE 1 tjeneste gjør det mulig å online validere om et kort er ikke sperret eller utløpt og om det er dekning på konto som kortet er knyttet til (VISA er primært et debet-kort). En kan merke seg at det ikke foretas sjekk på adresse eller andre data om kortinnehaveren. Dette gjør at bruk av kortnummer alene for betaling av bl.a. elektroniske tjenester kan være en nokså svindel-utsatt betalingsmetode. Ved bruk i POS-automater og minibanker sikrer PIN-koden mot misbruk, dette er imidlertid ikke mulig ved f.eks. teleshopping eller kjøp på Internettet.

BASE 2 tjeneste som er en ren clearing-funksjon foregår i batch, 1 gang i døgnet. I Norge sendes transaksjonene via Fellesdata, PAYEX, NOVIT og Telebank.

VisaNet har idag ingen forbindelse til Internettet. I fremtiden kan en tenkt scenario være at man vil etablere en eller flere Internett-adresser, som vil være "innfallsporter" mot VisaNet, for å kunne sende valideringstransaksjoner fra andre Internett-servere.

En slik scenario ville gjøre det mulig å foreta en validering av kortnummeret i sanntid, når det oppgis ved f.eks. kjøp av en elektronisk tjeneste. Man måtte i tillegg ha egne autentiseringsrutiner som vil sikre at det er kortinnehaveren som bruker det. Dette kan gjøres f.eks. vha kortleser tilknyttet PC-en eller elektronisk signatur (som vel forutsetter offentlig nøkkel og TTP). Det har ikke vært mulig i skrivende stund å finne ut hvilken type løsning Microsoft og VISA vil bestemme seg for. Det ligger også i kortene at VISA vil ikke være den eneste samarbeidspartneren til Microsoft på lengre sikt.

4.2 Netscapes samarbeid med Mastercard og Bank of America

Netscape Communications Corporation leverer en såkalt "leser", en applikasjon som gjør det mulig å aksessere Internettet og World Wide Web på en brukervennlig måte. De utvikler også `servere' for Web, dvs. applikasjoner som gjør det mulig for brukere med tilgang til Internettet å aksessere den informasjonen som en virksomhet velger å legge ut til offentligheten.

Netscape Communications Corporation er en viktig aktør på Internettet fordi de leverer meget populær programvare for å søke seg fram til informasjon på nettet. Netscape har vært aktive i å få til samarbeid med sentrale aktører i pengefornmidling. De har inngått avtale med blant andre Bank of America (USAs største forretningsbank) for å få til sanntids (umiddelbar) godkjenning på belastning av en rekke kreditt- og debetkort (Visa, Mastercard, American Express med flere), ved hjelp av sikker kommunikasjon med mellom kortholder, brukersted og bank. Tjenesten skulle være operativ januar 1995, men er i skrivede stund (medio februar), ennå ikke operativ.

Mastercard og Netscape har også annonsert et samarbeid. Det er uklart hvordan dette initiativet skiller seg fra samarbeidet Netscape har med Bank of America. Det legges opp til den samme formen for sikker overføring av kortnummer over nettet, og sanntids godkjenning av kjøp. Signalene fra Netscape tyder på at man i samarbeidet med Mastercard skal legge vekt på å lage en egen applikasjon med stor brukervennlighet som skal kunne aksessere Mastercards eget nett via Internett. Applikasjon skal være klar i midten av 1995.

4.3 Amex og America Online

Ifølge Wall Street Journal har også Amex etablert en strategisk allianse med sikte på å tilby online elektroniske betalingstjenester. Den nye tjenesten hos America Online vil gjøre det mulig for brukere å se på reiselivsinformasjon og bestille reiser online. Videre vil brukerne kunne betale sine regninger online og motta betalingsoversikter som vil kunne importeres direkte i lokale hjemmeregnskapsverktøy.

5. Juridiske aspekter ved kjøp og salg av informasjonstjenester over nett

5.1 Innledning

I dette kapittel skal vi vurdere systemer for salg av informasjonstjenester i globale nettverk ut fra en juridisk synsvinkel. I denne sammenheng kan det dreie seg om transaksjoner som tenkes gjort mellom flere aktører i ulike land. Det vil først og fremst være en selger og en kjøper av informasjonstjenesten. I tillegg vil det også være andre parter involvert i transaksjonen, som f. eks. en avregningssentral, alternativt et kredittkortselskap, i tillegg til vanlige banker. Antallet impliserte parter vil variere med den løsningen som blir valgt.

Det som blir omsatt er informasjon. Dette kan være ulike former for informasjonstjenester som kan overføres via et datanettverk, f. eks. programvare, lyd, tekst eller bilder.

Det kan være ulike måter å nærme seg problemstillingene på. Man kan diskutere de ulike typene juridiske regler som kommer til anvendelse, men vi tror at det for oversiktens skyld er mer hensiktsmessig å diskutere reglene ut fra de ulike hovedaktørenes ståsted. Disse vil være selger, kjøper (kunden), og avregningssentralen samt debet- eller kredittkortselskapet. I tillegg til disse kommer den virkelige banken inn i bildet når kjøper med endelig og frigjørende virkning får gjort opp sitt mellomværende med selger.

Men innledningsvis er det nyttig å se nærmere på enkelte begreper hvor det kan være uklare oppfatninger. Betalingsformidling innebærer at en selger(kreditor) via en tredjemann får betaling for tjenesten eller varen fra kjøper(debitor).

Betalingsformidling kan sies å bestå av tre hovedelementer. For det første dreier det seg om at et fordringsforhold mellom selger og kjøper blir oppgjort. Oppgjøret består i at kreditor får realisert sine fordringer dvs. får midlene til sin disposisjon. Dette igjen betyr at midlene blir godskrevet selgers konto i egen bank, dvs. at selgeren får økt sin fordring på egen bank. Tilsvarende gjør kjøperen opp sin skyld ved å redusere sin fordring til egen bank ved at det overføres penger fra kjøpers konto til selgers konto. Det som skjer er at det blir transportert et innskudd fra kjøpers bank til selgers bank.

Disse innskuddene transporteres imidlertid ikke direkte fra en bank til en annen. Det som i realiteten skjer, er at det gjennom betalingsformidlingen hvor fordringen transporteres vil bli generert endringer i fordringsforholdet mellom bankene. Selgers bank vil få en fordring på banken til kjøper. Utregning av den posisjon de ulike bankene vil være i på bakgrunn av de ulike betalingsformidlingsoppdragene kalles avregning. Tilslutt vil den enkelte bank enten skylde penger eller banken vil ha penger til gode i andre banker.

For å få gjort opp sin fordring på andre banker dvs. det beløpet banken har til gode etter en avregning må bankene gå til sin bank igjen som er Norges Bank. Bankene gjør opp seg imellom ved å transportere sine fordringer på Norges Bank.

Dette betyr at det kun er banker som kan være tilbydere av betalingstjenester som skal ivareta oppgjørsfunksjonen mellom selger og kjøper. Dette fordi oppgjør mellom selger og kjøper består av transport av innskudd, og det er bare banker som kan tilby dette til kunder. Betalingsformidling er noe annet enn en ordinær informasjonsformidling. Det dreier seg om transaksjonsutveksling som har stor betydning for og påvirker den enkeltes banks likviditet Det er derfor viktig at informasjonen (de elektroniske meldingene) som utveksles i betalingsformidlingsøyemed er korrekt.

Et betalingssystem gjør det som kjent mulig å overføre informasjon om at betalingsmidler, dvs. midler som kan konverteres til sedler, mynt eller fordringer, skal flyttes fra kjøpers eventuelle konto og til selgers eventuelle konto. Men her må man huske på at et kontoforhold ikke er nødvendig for at systemer skal fungere, det kan jo også f.eks være kontant innbetaling fra kjøper til selgers konto.

Før vi går over til å peke på enkelte rettslige problemstillinger som må vurderes i forbindelse med de enkelte aktørenes rettslige posisjoner, vil vi legge til grunn noen forutsetninger. Før en informasjonstjeneste kan tilbys til salg gjennom et globalt nettverk, vil det være sluttet en rekke avtaler mellom aktører både nasjonalt og internasjonalt. Dette vil bl.a. være avtaler angående det materialet som tenkes solgt gjennom informasjonstjenesten, og at det må være klarert med den originære opphavsmann, slik at selger eller informasjonsleverandør har skaffet seg rett til å selge materialet til tredjepart. Dette dreier seg for det første om retten til eksemplarfremstilling (f. eks. ved å la kjøper kunne ta utskrift), og for det andre rett til å formidle eksemplarer til almenheten.

Vi forutsetter også at det er inngått gyldige distribusjonsavtaler mellom tjenesteleverandøren, d.v.s. den som utformer selve tjenesten, og distributør, den som formidler materialet til kjøper. Distributør ivaretar tekniske funkjoner som å vedlikeholde og operere datamaskinanlegget som transporterer informasjonstjenestene. Enkelte ganger kan tjenesteleverandørfunksjonen og distributørfunksjonen tenkes å være ivaretatt av en og samme aktør.

I tillegg vil vi forutsette at informasjonstjenestens innhold ikke strider mot gjeldende nasjonale lover og forskrifter. En slik forutsetning må legges inn fordi det er en stor diskusjon hvilket ansvar en selger kan pådra seg av strafferettslig karakter, f.eks. ærekrenkelser og pornografi. I tillegg kan selger pådra seg ansvar for innholdet i informasjonstjenesten, hvis den informasjonen som selges inneholder opplysninger som ikke er korrekte og kjøper bygger en avgjørelse på denne, og som en følge av dette kommer til å lide et dokumentert økonomisk tap.

5.2 Selgers juridiske situasjon

Vi har lagt til grunn at tjenesteleverandør er i en slik posisjon at det ikke ligger noen rettslige hindringer i veien for at han kan tilby informasjonstjenesten på markedet. Selgers situasjon er først og fremst at han, i motsetning til hva som skjer ved tradisjonell handel, ikke får direkte oppgjør for varen eller tjenesten idet egen ytelse leveres. Selger kan dermed ansees for å yde kreditt til kjøper.

På grunn av dette må selger inngå kontrakt med noen eller noe, dvs. muligens et selskap, som kan holde oversikt med hvilke tjenester eller ytelser selger har levert og til hvem disse er levert. Det viktigste for selger er selvfølgelig hvem som skal betale for hans ytelser. Selger vil da igjen kunne ha inngått kontrakt med en avregningssentral

eller et kreditt- eller debetkortselskap som kjøper vil motta regning fra, og som kjøper betaler til. Betalingsformidlingen vil dermed til sist foregå gjennom det ordinære banksystemet. Men det som er spesielt i denne situasjonen er at informasjon om hvem som skal betale hva blir registrert i avregningssentralen, som så sender ut regning til de ulike kjøperne. Hvis det alternativt tenkes et konsept som inkluderer kreditt/debetselskapet, så tenker en seg en modell hvor faktureringsdata blir overført fra avregningssentralen til kortselskapene som så igjen står for inndrivelsen av pengene.

Som et utgangspunkt er det kontraktsfrihet mellom partene, dvs. selger og avregningssentralen kan inngå avtalen og seg imellom bli enige om hvilke vilkår som skal gjelde. Dette gjelder dog ikke uten visse begrensninger, slike avtalevilkår kan "butte" mot visse lover som vil legge den ytre rammen for hva som kan avtales. Det som vil avtales i dette tilfelle er at avregningssentralen yder selger en tjeneste ved at det holdes en løpende oversikt over kjøpere og kjøp. I tillegg fakturerer avregningssentralen på vegne av selger. I kontrakten må denne tjenesten beskrives nærmere og vederlagsmekanismene må avklares. Et eventuelt ansvar må avklares hvis f.eks. kjøper ikke gjør opp for seg. Og for å forenkle saken juridisk anbefales det at kredittrisikoen tilligger selger.

Selger inngår jo også en rekke “enkeltavtaler” med de ulike kjøperne av informasjonen, idet hvert enkelt kjøp isolert sett innebærer rettigheter og plikter for partene. Selgeren forplikter seg til å overdra informasjon til kjøperen mot å få et vederlag i penger.

Her kan det nevnes at norsk rett gir et utstrakt vern til forbrukere hva angår kjøp til personlig bruk, dvs. forbrukerkjøp. Det oppstår problemer og en uoversiktlig juridisk situasjon ved kjøp mellom parter i ulike land, og dette bringer inn spørsmål om interlegal rett. Dette er de reglene som ligger i de ulike lands nasjonale rett som avgjør hvilket lands regler som skal komme til anvendelse ved ulike rettspørsmål som har tilknytning til avtaleinngåelsen. I dette tilfellet vil det være snakk om internasjonal privatrett. Dette er et såpass omfattende område at det ikke er mulig å gå nærmere inn på disse problemstillingene her.

5.3 Kjøperens juridiske situasjon

Kjøperen vil være en person eller en juridisk person, dvs. et rettsubjekt som f. eks. stat eller kommune, som utad opptrer som en enhet og som erverver rettigheter og plikter. Det viktige her er at rettsubjektet har rettslig handleevne og gjennom denne kan binde seg juridisk.

I forhold til kjøper yder avregningssentralen en tjeneste ved å gi kjøper adgang til informasjonsmarkedet. En potensiell kjøper må opprette en konto i avregningssentralen (den elektroniske “banken”) for å kunne handle informasjon på nettet. Dette gjøres ved at det sluttes en avtale mellom potensiell kjøper og avregningssentralen.. Denne må

regulere forholdet mellom partene gjennom ulike vilkår. Disse vil inneholde angivelser om rettigheter og plikter som følger av den enkelte kontrakten. I avtalen vil det inngå elementer hvor tjenestene beskrives og vederlagsmekanismene avklares. I tillegg vil avtalen beskrive hvilke konsekvenser et eventuelt mislighold mellom kjøper og avregningssentalen skal få, og hvordan en eventuell tvist mellom partene skal løses. En løpetid for avtalen vil også naturlig finnes i en slik avtale. I de tilfellene hvor avregningssentralen sender ut en faktura som kjøper betaler gjennom bank- eller postsystemet, vil det være naturlig at det avtales hvordan og hvor hyppig oppgjøret skal finne sted.

Hvis man hadde brukt kortselskapkonseptet, som vi har diskutert tidligere og som kan tenkes som et alternativ, ville kjøper i tillegg måtte inngå en avtale med et kortselskap som vil sende ut faktura til kjøper etter et nærmere avtalt system. Dette ville da vært en følge av kontrakten mellom kjøper og avregningssentralen og være en forutsetning for at betaling i virkelige penger skal kunne finne sted.

Det må vurderes hvorvidt lov om personregistre m.m. av 9 juni 1978 nr. 48 (heretter prl.) kommer til anvendelse ved utformingen av de mulige betalingskonseptene.

Generelt kan det sies at det kan bli registrert personopplysninger på flere nivåer. Med personopplysninger menes det i prl. «opplysninger og vurderinger som direkte eller indirekte kan knyttes til identifiserbare enkeltpersoner, sammenslutninger eller stiftelser». For det første, må kjøper avgi en rekke opplysninger ved etableringen av kundeforholdet enten til avregningssentralen, kortselskapet eller begge to. Opplysningene kan bl.a. definere hvem som skal faktureres for bruken av tjenesten eller hvilke definerte tjenester kjøper skal få tilgang til. Disse opplysningene må nødvendigvis ligge lagret i et kundesystem hos tjenestetilbyder.

Utgangspunktet er at det etter prl. kreves konsesjon fra Datatilsynet for å opprette et elektronisk personregister jfr. prl. § 9. I den grad de opplysningene som registreres er saklig begrunnet, og relevante i forhold til den tjenesten som tilbys, vil slik konsesjon kunne bli gitt. Slik registrering kunne også være unntatt fra konsesjonsplikten jfr. prl. § 9, annet ledd, jfr. personregisterforskriftene § 2-3. Denne bestemmelsen inneholder et generelt unntak for enkelte kunderegister som inneholder *visse typer* av personopplysninger. Da må det forutsettes at registeret ikke vil inneholde andre opplysninger enn de som er regnet opp i bestemmelsen og at regler om formål, utlevering og sikring m.m. i forskriftene § 2-1 overholdes. Her ville reglene om forbud mot utlevering utløse konsesjonsplikt hvis avregningssentralen skulle videreformidlet personopplysningene til tredjemann i et alternativt konsept f. eks. et kredittkortselskap, med mindre kjøper og selger hadde gitt tillatelse til slik utlevering.

I forskriftene § 2 - 4 er det gitt særskilt unntak for personregistre i banker, her er det gitt hjemmel for at slike personregistre kan inneholde en rekke opplysninger deriblant kundens fødselsnummer.

Det blir generet data også ved bruken av tjenesten. Et sted i systemet må det registreres hva slags informasjon kjøper har hatt tilgang til, hvor lenge han har hatt tilgangen og hva bruken har kostet. På det nåværende tidspunkt vet man ikke hvor detaljert en slik registrering trenger å bli, slik at dette må vurderes nærmere underveis. Et slik register vil være konsesjonspliktig, og det må derfor søkes om konsesjon fra Datatilsynet.

Problematikken rundt dette er velkjent og har mye til felles med den problematikken en kjenner fra diskusjonen rundt elektroniske spor. Elektroniske spor er som kjent betegnelsen på opplysninger som personer etterlater seg ved bruk av ulike elektroniske systemer. Tidligere har man hovedsakelig diskutert de sporene som har avslørt informasjon om personers bruk av forskjellige elektroniske kort, som f. eks. adgangskontrollkort, elektroniske klippekort eller elektroniske betalingskort. I forbindelse med bruk av elektroniske betalingskort har man hatt en registrering av hvilke varer som har blitt kjøpt i de enkelte tilfellene.

I vårt tilfelle dreier det seg om en type elektroniske spor som vil fortelle noe om hvilken informasjon personer har kjøpt. Spørsmålet videre vil da bli om registrering av slik informasjon vil være mere sensitiv enn f. eks. registrering av hvor du har kjøpt mat eller fylt bensin.
Et problem i forbindelse med registrering av elektroniske spor er at det er mulig å bruke slik informasjon til å skape såkalte profiler av kjøper. Ved å registrere det som blir kjøpt av informasjon kan en tenke seg at enkelte selgere skulle ville ønske å rette individuelle tilbud til kjøpere som har vist seg særlig interessert i spesielle emner.

Det som må avklares og diskuteres nærmere er hvorvidt slike elektroniske spor vil bli lagret i betalingssystemet eller ikke, det er selvfølgelig viktig at informasjon slettes med en gang når den ikke er lenger nødvendig. Det vil si, at når kjøperen har gjort opp for seg må avregningssentralen slette all informasjon om hvor informasjonen er kjøpt, og ikke minst hva som har blitt kjøpt. I etterkant av dette kan en også få interessante diskusjoner, som i hvilken grad samtykke fra kjøper kan oppheve restriksjoner på bruken av informasjonen rundt den enkelte kjøpers forhold. Hvis kjøper f. eks. ønsker å få tilbud fra alle som selger informasjon om et spesielt enme. Eller at kjøper gir sin tillatelse til at informasjon om sitt kjøpemønster «selges» fra avregningssentralen til ulike selgere mot f. eks. en rabatt eller et engangsfradrag på kontoen.

Et annet spørsmål som også knytter seg til personregisterloven er hvorvidt reglene som gjelder databehandlingsforetak i prl. § 22 vil kunne komme til anvendelse. I bestemmelsens første ledd er databehandlingsforetak definert som «Virksomhet som består i å bearbeide personopplysninger for andre ved elektroniske hjelpemidler». Hvis avregningssentralen bearbeider personopplysninger for andre som så blir overført til f. eks. et kredittkortselskap vil dette utløse konsesjonsplikt, med mindre avregningssentralen og kortselskapet er innenfor samme konsern. Slik konseptet nå er

kan det selvfølgelig diskuteres hvorvidt avregningssentralen kan sies å bearbeide personopplysninger for andre, dvs. selgerne, og at dette dermed utløste konsesjonsplikt. Imidlertidig er det slått fast at avregningssentralen er en selvstendig enhet som yter en faktureringstjeneste ovenfor både kjøpere og selgere. Det sentrale her vil derfor være spørsmålet om hvem som «eier» de personopplysningene som bearbeides. Avregningssentralen kan muligens sies å «eie» personopplysningene og dermed selv ha råderetten over disse, likedan kan det hevdes at selve bearbeidelsen gjøres for egen del. Likevel, sett ut fra bakgrunnen for regelen om at slike regler er gitt for å forhindre manipulering og kobling av personopplysninger, antar vi at avregningssentralen derfor trenger konsesjon som databehandlingsforetak fra Datatilsynet.

Kjøper må gi seg tilkjenne på riktig måte ovenfor systemet ved å autentisere seg, enten ved hjelp av et elektronisk kort som kan presenteres for systemet eller ved hjelp av at kjøper benytter en spesiell kode. Et spørsmål kan være hvordan dette kan gjøres på en sikrest mulig måte, og hvorvidt det kreves eller vi mener det bør være en spesiell grad av sikkerhet for å etablere et betalingssystem.

I tillegg vil kjøper, avhengig av sin stilling som enten næringsdivende eller forbruker, kunne påberope seg rettigheter. Det er viktig å sondre mellom disse tilfellene. Handlefriheten eller kontraktsfriheten er større mellom to næringsdrivende enn det er mellom næringsdrivende og forbruker. Begrunnelsen ligger i at to profesjonelle parter i utgangspunktet er to jevnbyrdige parter. Forholdet mellom næringsdrivende og forbruker er et forhold som i utgangspunktet er skjevt, idet det på den ene siden dreier seg om en profesjonell og på den annen siden en amatør. Denne skjevheten er det forbrukerlovgivningen som søker å bøte på, bl.a. ved å sette begrensninger i hva partene har rett til å avtale seg i mellom.

Siden et betalingssystem for betaling av informasjonstjenester både skal kunne brukes av private og av profesjonelle, så bør det derfor fremkomme av registreringen i avregningssentralen hvilken gruppe kjøperen er i. Dette vil også få betydning i forbindelse med ansvar, hvis informasjonen som selges viser seg å være feil. Feil informasjon brukt i profesjonell sammenheng vil kunne få store økonomiske konsekvenser for den som er ansvarlig. Det er mindre muligheter for å fraskrive seg ansvar for feil ved varens tilsiktede egenskaper i de tilfellene det er snakk om forbrukerkjøp.

Når enkeltindivider har rollen som forbrukere knytter det seg først og fremst, men ikke bare, en økonomisk interesse til denne rollen. Stikkord som pris, kvalitet, tilgjengelighet, sikkerhet og service kan på en dekkende måte angi en ideal plattform som beskriver en best mulig situasjon for en forbruker som er i den posisjon at han skal velge og kjøpe varer eller tjenester fra en selger.

Prissettingen på informasjonstjenesten er viktig. Den skal være rimelig og riktig. Her kan man skille mellom innholdet man kjøper og informasjonsbærertjenesten. Det beste

for forbrukeren er å kunne forutberegne hva prisen for ytelsen blir med alle eventuelle gebyrer etc. inkludert i prisen. Det skal ikke ligge noen økonomiske overraskelser på lur som kommer med regningen til slutt, og som kunden ikke er klar over.

Kvaliteten på tjenesten må være som forespeilet. Selgeren må ikke markedsføre sin informasjonstjeneste på en villedende måte. Forbrukeren skal på forhånd kunne gjøre seg opp en mening om hva tjenesten inneholder for så å kunne ta stilling til om den er relevant for ham. En villedende markedsføring eller angivelse vil kunne føre til at forbrukeren kjøper en tjeneste han streng tatt ikke ville ha kjøpt hvis han var blitt orientert om innholdet på en objektiv måte. Han fratas dermed muligheten for å foreta et selvstendig valg på et fritt grunnlag. Kvalitetsaspektet gjør seg også gjeldende ved at man kan forvente at oppkoplingen mot systemet og at selve gjennomføringen av informasjonskjøpet skal kunne foregå raskt og uten unødvendig venting for forbrukeren.

Tilgjengelighet omfatter først og fremst fysisk tilgjengelighet. Det må være mulig for den som ønsker det (så sant vedkommende er kredittverdig der hvor det er et vilkår) å kunne få en «konto» i avregningssentralen. Det må være vanskelig, og med god grunn at enkelte forbrukere skulle kunne utelukkes. Tilgjengelighet kan også omfatte psykisk tilgjengelighet i den forstand at det bør legges opp til enkle brukergrensesnitt slik at dette ikke blir en arena bare for de med teknologikompetanse.

Sikkerhetsaspektet omfatter først og fremst at de data som blir registrert ved bruken ikke kommer på avveie og blir brukt i andre sammenhenger eller f.eks. til reklameformål uten forbrukerens eventuelle samtykke. Det omfatter også at forbrukerens fakturagrunnlag skal være beskyttet mot at utenforstående enten kan endre dette, eller at utenforstående kan bruke tjenester som så blir belastet feil person. Her vil mulige sikkerhetsrutiner være sentrale. Hvis kunden blir svindlet, må vedkommende raskt kunne få rettet opp eventuelle feil slik at kunden ikke blir skadelidende.

I tillegg er det også viktig for forbrukeren at en eventuell kontrakt mellom seg og avregningssentral og/eller kreditt/debetkortselskap, inneholder kontraktsvilkår som er balanserte. Likeledes er det viktig at en eventuell reklamasjonssak blir saksbehandlet på best mulig måte, og at adgangen til å få medhold i en klagesak er reell.

5.4 Avregningssentralens juridiske situasjon

Det må avklares hvilken rolle avregningssentralen skal spille i forhold til kortselskapet eller en vanlig bank. En mulig løsning er den hvor avregningssentralen sender ut regning til kjøper med bestemte intervaller, og kjøper betaler denne gjennom bank eller post på vanlig måte. Avregningssentralen sender et endelig oppgjør ut til de ulike selgerne tilslutt.

Man kan stille spørsmål ved om avregningssentralen skal betraktes som en tjenesteyter. Tjenesten består vel i så fall av to ulike tjenester. Den ene går ut på å koble kjøpere og selgere sammen, og eventuelt autentisere kjøper ovenfor selger. Den andre delen går ut på at avregningssentralen holder orden på regnskapet og så sender ut regninger på bakgrunn av dette.

(Alternativet med kortkonseptet ville ført til at avregningssentralen formidlet fakturainformasjon til kortselskapet. Kredittkortselskapet ville mottatt «regnskapstall» fra avregningssentralen og så sendt ut regning til kjøper som måtte gjort opp ved å betale gjennom postgiro eller bank.
Kortselskapet og avregningssentralen ville måtte inngå en avtale som regulerer rettigheter, plikter og ikke minst ansvar hvis noe skulle gå galt, f. eks. hvis kjøper ikke har kredittverdigheten man antok eller hvis avregningssentralen ikke får overført fakturainformasjonen til kortselskapet.)

I forbindelse med hvordan oppgjøret skal finne sted kan en tenke seg to ulike løsninger. Den ene innebærer at kjøper på forhånd har innbetalt en bestemt sum til en egen konto i avregningssentralen, som denne senere kan anvise penger fra til selger. Problemet med denne «forskuddsinnbetalingen» er at den kan føre til at virksomheten kommer inn under banklovgivningen og dermed må følge de regler som gjelder på området.

Bankene har en enerett til å motta innskudd fra allmenheten. I følge lov om forretningsbanker av 24 mai 1961 nr. 2 (fbl.) § 1 annet ledd kommer forretningsbankloven til anvendelse på «alle foretak som skaffer seg midler til sin virksomhet ved å ta mot innskudd fra en ubestemt krets av innskytere». Loven definerer ikke hva som menes med innskudd, men det er antatt at innskudd er lån til banken fra innskyter. Dette betyr at banken kan låne ut de pengene som har blitt satt inn i banken, og reglene er strenge på grunn av den risikoen som løper for et eventuelt tap av penger.

Et forhold som kan føre til at man kommer utenom disse reglene kan være at kjøper setter inn et beløp i avregningssentralen som ikke skal lånes ut men brukes til fortløpende betalinger for det som blir kjøpt. En viss analogi har en i forhåndsbetalte kort. Et eksempel er telekortene hvor man forhåndsbetaler et bestemt antall tellerskritt, eller andre konsept hvor en tenker seg at det skal være mulig å betale for ulike tjenester ved hjelp av samme kortet. I motsetning til et avregningssentral-konsept, vil «innskyter» ved forhåndskjøp av slike kort få et fysisk bevis på sitt «innskudd». Dette spiller etter vår mening mindre rolle, poenget er at det til en viss grad er mulig å forhåndsinnbetale for tjenester eller varer man ikke har kjøpt. Et slik synspunkt kan ha en viss vekt, men om en slik forhåndsinnbetaling vil falle utenfor eller innenfor gjeldende banklovgivning er fortsatt usikkert. Det er vanskelig å trekke denne grensen men hvis det dreier seg om forhåndsinnbetaling av et forholdsvis beskjedent beløp i størrelsesorden inntil 1000 NOK så antar vi at det vil kunne falle utenfor banklovgivningen.

Det man også må se nærmere på er hvorvidt avregningssentralen vil kunne komme inn under gjeldende lov om finansieringsvirksomhet og finansinstitusjoner av 10 juni 1988 nr. 40. Finansieringsvirksomhet er i loven definert som det å «yte, formidle eller stille garanti for kreditt eller på annen måte medvirke med finansiering av annet enn egen virksomhet». Det som i første omgang vil være avgjørende er om det ytes kreditt eller ikke, og dernest hvem som yter kreditten, selgeren eller avregningssentralen. Det er i juridisk teori antatt at kreditt for det første omfatter å stille en ytelse først til rådighet i et kontraktsforhold, og det å ta den økonomiske risikoen for at motytelse ikke erlegges. Kredittbegrepet er i teorien analysert (M. Goode) og inndelt i to hovedgrupper, lån og salgskreditt. Uten å gå nærmere inn på dette, vil vi fastslå at det her dreier seg om en kreditt i lovens forstand. I dette tilfellet vil det ikke være avregningssentralen men selger som yter kreditten, dvs. at avregningssentralen ikke betaler til selgeren før kjøper har betalt for tjenesten. Likevel vil avregningssentralen kunne sies å «medvirke med finansiering av annet enn egen virksomhet».

Dette betyr med andre ord at uavhengig av om det er selger som yter kreditten eller ikke, vil det være finansieringsvirksomhet som finner sted i lovens forstand. Derav følger at lovgivningen vil komme til anvendelse, og vi kan ikke se at det finnes mulighet for unntak i loven.

Kortselskapene American Express, Visa, Eurocard og DinersClub hevdet tidligere at de ikke drev finansieringsvirksomhet. Finansdepartementet har akseptert at Visa som debetkortselskap ikke er å anse for å være finansieringsvirksomhet. Hva angikk kortselskapene ble spørsmålet avgjort i Oslo Byrett, hvor staten ble gitt medhold i sin påstand om at selskapene drev finansieringsvirksomhet. Avgjørelsen ble ikke anket slik at denne står fast. I dommen, som har begrenset verdi fordi det er en underettsavgjørelse, blir det lagt en viss vekt på tidsaspektet ved kreditthenstanden og at det i saken var snakk om kreditthenstand av ikke helt kort varighet. Med andre ord vil en løsning hvor man sender ut fakturaer med jevne mellomrom, f. eks hver uke eller hver annen uke, og hvor kjøper får kort frist på seg til å betale, kunne dempe kreditthenstandsargumentet. Også sett i forhold til de sansynligvis lave beløpene det tross alt her vil være tale om, så vil vi, selv om lovens ordlyd vil kunne regulere forholdet, tvile på at det er noe stort problem. Hvis konseptet implementeres i stor skala og på et forretningsmessig grunnlag er det grunn til å revurdere spørsmålet i lys av dette. Det kan nevnes at den virksomheten som Telenor driver i forbindelse med Teletorg også strengt tatt kommer inn under lov om finansieringsvirksomhet.

Hvis man ønsker en løsning med etterbetaling av tjenester i stor skala kan det for å unngå finansieringslovgivningen være grunn til å vurdere å knytte betalingen opp mot slike selskaper. Kortselskapene har etablerte rutiner som er etablert innenfor de nødvendige juridiske rammer. Et tilleggsmoment er at kortselskapene har etablert seg globalt.

Hvis man ønsker å unngå å få inn en ekstra aktør som et kortselskap fordi ikke alle innehar slike kort, synes det som om løsningen bør være et system med etterhåndsinnbetaling, hvis det dreier seg om mindre summer, og at henstandstiden med betalingen er kort.

6. Sikkerhet, kryptering og TTP

6.1 Innledning

Sikkerhet karakteriseres gjerne ved tre parametre: Tilgjengelighet, integritet og konfidensialitet. Når det gjelder betalingsformidling, er det hensiktsmessig å ta med enda en parameter, nemlig sporbarhet, slik at:

- Tilgjengelighet er den egenskapen at tjenester / informasjon er tilgjengelig for autoriserte brukere.
- Integritet betyr at informasjon ikke skal kunne endres (inkludert forfalskes eller ødelegges) av uautoriserte aktører. Det at komponenter i et system virker som forutsatt (jfr. virus etc.), er også en del av integritetsbegrepet.
- Konfidensialitet betyr at informasjon ikke skal være tilgjengelig for andre enn de den er ment for. Dette kan også gjelde informasjon om aktiviteter i systemet, f.eks. hvem som handler med hvem.
- Sporbarhet er muligheten for å tilbakeføre en handling / begivenhet til den ansvarlige, i ettertid.

Tilgjengelighet skal vi ikke gå nærmere inn på her. Det er likevel verdt å kommentere at enkelte typer betalingstjenester er kritisk avhengig av at bestemte komponenter er tilgjengelige. Dette er i hovedsak et pålitelighetsspørsmål, og løses ved å bruke stabile datamaskiner og gode nok kommunikasjonslinjer, eventuelt med reservealternativer. Såkalte "nektelse av tjeneste" angrep må en likevel ta med i betraktningen - bevisste angrep for å sabotere eller redusere ytelsen til et system.

Det er en rekke aktører involvert ved betalingstransaksjoner for informasjonstjenester. Disse vil til dels ha helt forskjellige krav til sikkerheten i systemet.

Krav til sikkerhet vil kunne variere med typen informasjon / handlinger. For eksempel vil integritet og konfidensialitet være svært viktig for enkelte typer informasjon, men mindre viktig i andre tilfeller. Krav til styrken av de sikkerhetsløsningene som velges, er avhengig av de generelle sikkerhetskravene, men også av omgivelsene (hvilke trusler en er utsatt for), og av tilliten mellom aktørene.

6.2 Om tillit

Sikkerheten i et system må utvikles med utgangspunkt i hva en velger å stole på i systemet. Det er teoretisk umulig å konstruere et sikkert system uten minst ett punkt som er definert som ubetinget sikkert.

Som et eksempel: Dersom jeg går i banken for å ta ut penger, kan personen i skranken stole på meg, eller han kan kreve legitimasjon. Vanligvis vil han stole på legitimasjonen, men vi kan tenke oss at han vil kreve bevis for at legitimasjonen er korrekt. En slik beviskjede er nødt til å stoppe et sted, med en "legitimasjon" som er "garantert troverdig".

Tillit i et betalingssystem går på to plan:

- Tillit til kjøperes betalingsdyktighet og villighet til å betale, seriøsitet av selgere osv. - eller det vi kan kalle tillit mellom aktørene i systemet på et organisasjonsmessig plan.
- Tillit til aktørene at de er den de gir seg ut for å være, og at de ikke misbruker systemet - dette vil ligge mer på et teknisk plan for elektroniske betalingstjenester.

Tillitsforhold kan være ensidige, bilaterale, eller involvere en tredjepart (TTP i sikkerhetsterminologi), som beskrevet i det følgende.

6.2.1 Tillit mellom aktører og krav til sporbarhet

Innen konvensjonell handel finnes det forskjellige eksempler på grad av tillit mellom kjøper og selger - ensidig, bilateralt og med tredjepart:

- En selger vil ofte sende varer og legge ved regning, i tillit til at regningen faktisk blir betalt. I andre tilfeller krever selgeren forskudd, og kjøperen stoler da på at varene vil bli levert.
- Ved mindre grad av tillit kan en sende varer i oppkrav, slik at varene først utleveres mot betaling. Her har en en bilateral tillit til at bestillingen er reell, altså at selger vil sende varene, og at de vil bli hentet, samtidig som selgeren må stole på den som utleverer varene.
- Ved store handelstransaksjoner er det vanlig å bruke en megler, som da opptrer som en TTP, som begge parter har tillit til.

Et viktig poeng er at aktørenes krav til sporbarhet er omvendt proporsjonalt med tilliten mellom dem. Dersom jeg handler med noen jeg kjenner, tar jeg det ikke så nøye med skriftlig dokumentasjon, men i andre tilfeller er sporbarhet svært viktig. Ved bruk av megler er ofte det viktigste ikke å sørge for betalingsformidlingen, men å garantere at det finnes tilstrekkelig dokumentasjon, med en tredjepart som vitne, på hvordan handelen har foregått.

Sporbarheten er aktørenes sikkerhet ved brudd på tilliten. Det finnes lover og regelverk, til og med internasjonale, som kan brukes, forutsatt at tilstrekkelig dokumentasjon kan legges fram. Kjøper vil ha en kvittering for at han har betalt for en gitt vare, dersom han skal klage på at han ikke har fått det han har betalt for. Selger må dokumentere at han har mottatt en bestilling på en gitt vare, og på at varen er levert til kjøperen.

Det er verdt å merke seg at sporbarheten i en del former for handel er svært dårlig. Ett eksempel kan være bestilling av varer over telefon, der en lett havner i en påstand mot påstand situasjon dersom det oppstår uoverensstemmelser.

Slike betraktninger om tillit og krav til sporbarhet kan overføres direkte til elektronisk handel med informasjon. En del former for handel, som oppkrav, blir uaktuelle, men kravene er fortsatt at kjøper må ha tillit til at han får det han betaler for, og selgeren må ha tillit til at det blir betalt for varen, Dersom tilliten ikke er høy nok, må det kreves dokumentasjon for sporbarhet.

Kanskje det viktigste problemet innen elektronisk handel er mangelen på skikkelige mekanismer og konvensjoner for å oppnå sporbarhet. Krav til dokumentasjon er heller ikke nedfelt i lover og regelverk, og det er ikke innarbeidet noen praksis (innen rettsvesenet eller andre steder) for hva som kreves av elektronisk dokumentasjon for f.eks. å underbygge en klage.

Meglerrollen er ikke utviklet for denne typen handel, slik at vi i det følgende ikke kommer til å diskutere det å involvere en tredjepart for å oppnå tilstrekkelig dokumentasjon. Det kan tenkes at resultater av arbeidet innen elektronisk handel basert på EDI kan brukes.

6.2.2 Tillit / sikring mot misbruk og svindel

Innen tradisjonell handel finnes det ett tilfelle der risikoen for svindel er minimal - der kunden møter opp personlig og får se og kanskje prøve varen, og så betaler i kontanter i det varen mottas.

Ved andre former for handel, f.eks. ved bruk av kredittkort, må selger ha tillit til at han handler med korrekt person (eieren av kredittkortet), og kjøper må også ha tillit til selgerens identitet. Igjen kan tillit være enveis, bilateral eller basert på bruk av TTP. Som eksempler:

- En del selgere (lite av dette i Norge foreløbig) godtar bestilling over telefon der bestilleren kun oppgir sitt kredittkortnummer og en enkel sjekk (f.eks. utløpsdato for kortet). Her kan en godt si at selgeren har full tillit til at kjøperen er den han gir seg ut for å være (ensidig). I andre tilfeller vil selgeren kreve skikkelig legitimasjon - da kan en si at utstederen av legitimasjonen fungerer som en TTP.
- En kjøper har tillit til at selgeren ikke vil misbruke informasjon, f.eks. kredittkortnummer og utløpsdato for dette, når kjøperen oppgir denne typen informasjon (jfr. forrige punkt). Kjøperen må også ha tillit til at uvedkommende holdes unna denne informasjonen.
- En selger kan velge å godta betaling med et kort i tillit til at kjøperen har dekning for transaksjonen, eller han kan velge å sjekke med kjøperens bank om det er dekning, før varen kan utleveres. Banken fungerer i dette tilfellet som en TTP.

Også disse betraktningene rundt tillit kan overføres direkte til elektronisk handel med informasjon. Handel med (elektroniske) kontanter er mulig, men i de fleste tilfeller er bruk av betalingsformidling (som f.eks. kredittkort) mer aktuelt, og de samme krav eksisterer til sikring mot misbruk.

De tekniske løsningene for å oppnå f.eks. en "legitimasjon" for elektroniske meldinger, eller for å holde informasjon skjult for uvedkommende, er forholdsvis velkjente, men

gode løsninger er likevel i liten grad tatt i bruk. Et problem her er en mangel på infrastruktur (f.eks. for utstedelse av "legitimasjon"). Tekniske løsninger vil på sikt temmelig sikkert være basert på bruk av TTPer, siden dette nærmest er en forutsetning for å få til et system i virkelig stor (global) skala.

Det er verdt å merke seg at det finnes tre forskjellige slags TTPer (engelske navn her):

- In-line - der alle meldinger mellom selger og kjøper går gjennom TTPen. En megler kan sies å operere på denne måten, og vi kan tenke oss elektroniske meglere i framtida. Dette alternativet vil likevel ikke bli diskutert nærmere.
- On-line - der protokollen for en handel mellom kjøper og selger involverer en separat sekvens av meldinger i sann tid mot TTPen. Dekningskontroll mot en bank er ett eksempel på dette. Flere systemer for autentisering av brukere, f.eks. Kerberos, er også basert på on-line TTPer.
- Off-line - der TTPen forhåndsutsteder informasjon som seinere kan brukes som bevis. En instans som utsteder legitimasjonskort, er et eksempel fra dagliglivet. Innen elektronisk handel vil en utsteder av offentlig-nøkkel sertifikater operere på denne måten.

6. 3 Krav til sikkerhet

6.3.1 Tilgjengelighet

Hvis vi forutsetter at kjøper og selger kan kommunisere, reduseres dette til tilgjengelighet av andre komponenter i systemet, som betalingsformidler eller TTPer. En systemarkitektur som tillater skalering, f.eks. gjennom redundans, er en forutsetning dersom det genereres mye trafikk mot sentrale komponenter.

Det er en fordel dersom betalingssystemet kan fungere (om enn kanskje ikke med full servicegrad) selv om sentrale komponenter ikke er tilgjengelig.

6.3.2 Integritet

Den viktigste egenskapen til et betalingssystem må være at det er sikret mot svindel og manipulering, og at tilfeldige feil ikke kan få konsekvenser i samme retning. Systemet må sikre mot svindel fra utenforstående, og i størst mulig grad også mot misbruk fra noen av aktørene i en handel.

- Det må være "umulig" å forfalske meldinger (inkluderer avspilling av gamle meldinger) på en slik måte at betaling går til eller fra feil konti, eller at systemet "lures" til å tro at en betalingstransaksjon har funnet sted, eller at feil beløp overføres, eller at dekningskontroll godkjennes uten at det er faktisk dekning på konto.
- Det må være "umulig" å utgi seg for å være en annen person/instans.
- Informasjon lagret for sporbarhet, må ikke kunne endres i ettertid uten at det oppdages, spesielt dersom sporbarheten er basert på lagring hos bare en av aktørene.

6.3.3 Konfidensialitet

Når det gjelder krav innen dette området, kan en bli presentert for synspunkter som spenner fra at "dette er ikke så viktig - gjør ikke noe om andre får vite hva jeg handler" til "fullstendig anonymitet for alle parter, og i hvert fall kjøper". Det er derfor vanskelig å skissere absolutte krav til konfidensialitet. Merk også at digitale spor ikke er ønskelig av konfidensialitetshensyn, mens de kan være svært nyttige for å sikre sporbarhet / klagemuligheter.

Elektroniske kontanter (f.eks. DigiCash) kan gjøres "fullstendig" anonyme, men det ansees ikke at slike systemer vil være de mest aktuelle ved kjøp og salg av elektronisk informasjon. Hvis vi i steden ser på betalingsformidlingssystemer, er "need-to-know prinsippet" et godt utgangspunkt: Identifiser den informasjonen de enkelte aktørene trenger adgang til, og legg i størst mulig grad opp til at de ikke får adgang til noe mer enn dette.

- Utenforstående, som ikke på noen måte er part i handelen, skal ikke ha adgang til noe informasjon. Det er selvfølgelig umulig å gardere seg 100% mot at selger eller betalingsformidler lekker opplysninger til utenforstående, men betalingssystemet selv bør beskytte informasjonen mot innsyn.
- Selger må vite hvilken informasjon som er bestilt, og trenger en bekreftelse på at informasjonen er / vil bli betalt. Sikring av integritet må innebære en identifikasjon / autentisering av kjøperen, men ikke nødvendigvis i form av navn eller annen personinformasjon. Selger vil ofte ha adgang til informasjon om hvor "varene" er levert, f.eks. en e-post adresse eller en nettadresse.
- Kjøper må normalt vite selgerens identitet, evt. også kontonummer for betaling.
- Betalingsformidler må vite beløp og kontonummer for kjøper og selger, og vil kjenne tidspunktet for overføringen. Gjennom kontonummeret vil betalingsformidleren normalt kjenne identiteten til kjøperen, kanskje også til selgeren. Betalingsformidleren har ikke behov for å vite hva som ble kjøpt.

Trafikkanalyse, dvs. studier av trafikkmønster mhp. hvem som kommuniserer, volum, lengde på meldinger etc., er det urealistisk å beskytte seg mot i et betalingssystem. En angriper vil kunne trekke begrenset informasjon ut av dette, men det faktum at det har vært kontakt mellom to maskiner kan i helt spesielle tilfeller være sensitivt.

6.3.4 Sporbarhet

Sporbarhet krever logging av meldinger eller hendelser hos en eller flere av aktørene i en betalingstransaksjon, eller hos tredjepart. Følgende krav kan settes opp:

- Manipulering av en logg må kunne oppdages. Dersom samme opplysninger logges flere steder (f.eks. både hos kjøper og selger), kan en sjekke for samsvar. Dersom noe logges ett sted, bør det være hos en informasjonen (kan lagre signert for å beskytte mot endringer, men ikke mot sletting).
- Bruk av tredjepart for logging (såkalt notartjeneste) eller bruk av elektroniske meglertjenester ansees som uaktuelt foreløbig.

6.4 Tekniske løsninger

6.4.1 Tilgjengelighet

For å unngå flaskehalser i systemet er det en fordel å tillate off-line løsninger overfor betalingsformidlere og sikkerhets-TTPer.

Med hensyn på betalingsformidling vanskeliggjør dette dekningskontroll, men en kan evt. tenke seg at en aksepterer off-line transaksjoner under et gitt beløp (eller opp til et akkumulert beløp), mens en krever on-line kontroll ved større overføringer. Et annet alternativ er at systemet normalt fungerer on-line, men med mulighet for off-line operasjon (igjen helst bare inntil et gitt beløp) i tilfelle betalingsformidleren ikke er tilgjengelig.

For TTP-løsninger peker krav til tilgjengelighet i retning av off-line sertifisering av aktører, heller enn on-line autentiseringstjenere av typen Kerberos.

6.4.2 Integritet

Krav til autentisering av kjøperen (og selgeren), til sikring mot modifisering av meldinger, og spesielt det at informasjon skal logges med integritetsbeskyttelse for sporbarhet, indikerer at digitale signaturer basert på offentlig-nøkkel kryptografi er løsningen.

Det er også klart at det ikke er tilstrekkelig å sikre kommunikasjonslinjene. Signaturer mm. må beregnes over veldefinerte meldinger som utveksles mellom partene, der integriteten av hver melding kan verifiseres for seg. Utveksling av denne typen meldinger støttes f.eks. av PEM (Privacy Enhanced Mail, RFC 1421-1424) eller PGP (Pretty Good Privacy), men en må se på om det er nødvendig med noen modifikasjoner.

6.4.3 Konfidensialitet

Beskyttelse mot innsyn fra utenforstående bør være tilstrekkelig ivaretatt dersom kommunikasjonen mellom aktørene foregår kryptert. Dette gjøres enklest ved at meldingene krypteres (støttes av f.eks. PEM og PGP), men en kan også basere seg på at kommunikasjonslinjene krypteres. Andre angrepspunkter, som avlytting av skjermstråling eller inntrengning i maskinene til en aktør (snoking i logger mm.), ligger klart utenfor det et system for betalingsformidling kan beskytte mot.

Når det gjelder å skjule informasjon for aktører i betalingsformidlingen ("need-to-know" prinsippet), kan dette gjøres enklest ved at informasjonen ikke i det hele tatt overføres til aktører som ikke trenger den. Dersom en slik overføring er nødvendig, kan "ekstra" informasjon beskyttes slik at det bare er de som har behov for å se den, som får adgang, f.eks. gjennom bruk av offentlig-nøkkel kryptografi. Slik beskyttelse må ligge i meldingene.

6.4.4 Sporbarhet

Lagring av meldinger med digital signatur gir en meget høy grad av sikkerhet for at innholdet i meldingene er autentisk. Det vesentlige problemet blir da å sørge for at meldingene som lagres, inneholder all den informasjonen som er nødvendig for sporbarhet, men heller ikke noe mer. Den aktøren som foretar loggføringen, skal ha adgang til informasjon etter "need-to-know" prinsippet. Dersom meldinger inneholder informasjon som denne aktøren ikke skal ha adgang til, bør denne informasjonen beskyttes ved en kryptering som en annen aktør må "låse opp".

6.4.5 Nøkkeladministrasjon og infrastruktur

Konklusjonene fra avsnittene over kan oppsummeres slik:

- Det utveksles veldefinerte, digitalt signerte og krypterte meldinger mellom aktørene. Det må være definert protokoller for hvilke meldinger som skal sendes, og i hvilken sekvens.
- Sikkerhetsløsningene bør være basert på offentlig-nøkkel kryptografi.
- Mottatte / avsendte meldinger kan logges for å sikre sporbarhet.

Skikkelige løsninger basert på offentlig-nøkkel kryptografi krever en infrastruktur for sertifisering av nøkler, slik at en sikkert kan verifisere at en offentlig nøkkel faktisk tilhører en gitt identitet.

Hensynet til kjøperens anonymitet tilsier at "identitet" i denne sammenhengen ikke bør være navnet eller annen personinformasjon. En opplagt løsning er å knytte en offentlig nøkkel til et kontonummer gjennom et sertfikat, som da bekrefter at innehaveren av den tilsvarende private nøkkelen har rett til å benytte denne kontoen. Slike sertifikater kan da utstedes av banker, kredittkortselskaper eller andre som administrerer brukerkonti for betalingsformål.

Det viktigste poenget er at sertifikater må utstedes av TTPer som kan gjenkjennes av alle aktører. Dette krever et formelt sertifiseringshierarki, med kryss-sertifisering der det er nødvendig (f.eks. mellom banker), slik at det alltid er mulig å finne en sertifiseringssti mellom selger og kjøper (og betalingsformidler dersom dette er en annen enn sertifikatutstederen).

Det mest brukte programmet for signering og kryptering i dag, PGP, støtter ikke et slikt hierarki. Dette er basert på ad hoc løsninger der brukere sertifiserer hverandre. Bruk av PGP vil derfor ikke kunne være noen langsiktig løsning, men på kort sikt kan PGP gi et bidrag til økt sikkerhet.

Det må defineres et format for offentlig-nøkkel sertifikater for å understøtte andre identifikatorer enn navn.

6.5 Løsninger i dagens systemer

Neuman og Medvinsky (Proceedings of IEEE Compcon'95) deler betalingsmetoder inn i tre alternativer, der alle foreslåtte og implementerte løsninger kan sies å være varianter av en av disse:

- Elektroniske kontanter.
- Elektroniske sjekker (med forhåndsbetaling eller regning i ettertid).
- Sikre transaksjoner med kredittkort.

Den viktigste egenskapen til elektroniske kontanter er anonymitet / konfidensialitet. Løsningen tilbyr imidlertid i utgangspunktet ikke sporbarhet. I de fleste tilfeller vil antagelig kjøpere foretrekke en viss grad av sporbarhet (og dermed klagerett) framfor fullstendig anonymitet. En annen ulempe er at sikring mot misbruk, spesielt bruk av de samme kontantene mer enn en gang, krever mye logging av (anonyme) transaksjoner. En del brukere vil insistere på strenge krav til anonymitet, og det kan tenkes en del typer informasjon - ikke nødvendigvis ulovlig eller suspekt på noen måte - der kjøpere bør være garantert fullstendig anonymitet. Elektroniske kontanter vil derfor, pga. garantert anonymitet, bli en aktuell løsning, men neppe som hovedalternativ for elektronisk betaling.

Elektroniske sjekker er signerte meldinger som godkjenner en utbetaling fra en kjøper til en selger. Slike løsninger gir god sporbarhet, god sikring mot svindel (i hvert fall dersom sjekken heves umiddelbart), og en rimelig grad av anonymitet av kjøper overfor selger. Tilgjengeligheten kan også bli svært god, siden sjekker ikke nødvendigvis må heves umiddelbart. Ulempen er at betalingsformidleren vil sitte med svært mye informasjon om bruken av konti, på samme måte som ved dagens bruk av bankkort. Likevel peker denne løsningen seg ut som den sikkerhetsmessig beste totalt sett, selv om elektroniske kontanter, som nevnt, nok vil bli brukt som et parallelt alternativ.

Sikre transaksjoner med kredittkort kan gjøres sikkerhetsmessig omtrent som elektroniske sjekker, med de samme fordeler og ulemper. Ifølge Neuman og Medvinsky kan det virke som om kredittkortselskapene legger opp til løsninger med noe svakere sikkerhet, særlig når det gjelder autentisering av kortbrukeren overfor selgeren. Fordelene ved denne løsningen ligger først og fremst i antallet selgere som allerede aksepterer kort, noe som ikke minst har betydning ved internasjonal handel. En ulempe er at transaksjonskostnadene er høye (gebyrer etc.) slik at det er en lite hensiktsmessig løsning for små transaksjoner. Det kan være rimelig å anta at elektronisk handel med informasjon, som til dels er et nytt område med nye selgere, vil bli foretatt med elektroniske sjekker, ikke minst av sikkerhetsgrunner. Kredittkort vil heller bli brukt ve elektronisk handel med fysiske varer, spesielt der det er større beløp involvert.

7. Vurdering av løsningene

Vi har gruppert løsningene i fire hovedmodeller, men det finnes flere varianter av hver modell. I det nedenstående ser vi primært på modeller, men vil også trekke inn spesielle egenskaper ved de konkrete løsningene som er beskrevet under hver modellgruppe, der det er hensiktsmessig og belysende.

7.1 Abonnementsmodellen

En fordel ved abonnementsmodellen er at det ikke finnes noe fordyrende ledd mellom selger / markedsplass og kjøperen, men løsningen er uegnet for løssalg av informasjonstjenester, fordi den forutsetter et fast abonnementsforhold mellom kjøper og selger / markedsplass. For å kunne handle tjenester på et globalt nett vil kjøperen måtte ha et utall av avtaler, enten direkte med tjenesteleverandører og/eller med ulike markedsplasser. I forhold til betalingssystemer vil denne løsningen kunne benytte enhver av de andre modellene i tillegg til den tradisjonelle betalingsformidlingen (faktura betalt gjennom bank- eller postgiro).

7.2 Avregningssentral (kreditt-debet)

Fordeler med avregningsssentralmodellen er en god kobling mot bankvesenet. Dette legger til rette for en stor bredde i mulige kjøpere og selgere. En avregningssentral basert på elektronisk akkumulering av krediteringer og debiteringer vil kunne oppnå en lav transasjonskostnad.

Avregningssentraler som støtter elektronisk sjekk-konseptet ser ut til å være den beste løsningen for løshandel på globale nett. Krypterte "sjekker" gir høy grad av sikkerhet, de kan også gi god grad av anonymitet, dersom dette er ønskelig. Sjekkene gir også god sporbarhet i tilfelle tvist mellom selger og kjøper. Offline-prosessering av sjekkene belaster ikke sentralen på samme måte som online-prosessering ville gjøre. Flaskehalser i systemet kan dermed unngåes.

Avregningssentral-modellen ligger til rette for fleksible løsninger mot finansverdenen: forhåndsbetaling, kreditt og fakturering, kreditt og belastning av kredittkort kan implementeres etter behov og vurdering av brukergruppen.

Måten avregningssentraler implementeres på gjør det enkelt å koble virksomheten til finansverdenen uten at store modifikasjoner kreves i måten finansinstitusjoner opererer på (noe som vil måtte skje ved introduksjonen av elektroniske penger).

Problemene er i første rekke knyttet til at modellen innebærer en ny institusjon som skal håndtere betalingsformidling og være et bindeledd mellom kjøper, selger og bankvesen. Den juridiske status av en slik institusjon er i øyeblikket uklar. Avregningssentralen kan f.eks. drives av aksessleverandører. Det må finnes en TTP som skal sertifisere brukere av systemet og forvalte deres kryptonøkler.

En annen problemstilling som reiser seg i forbindelse med denne modellen er monopol vs. konkurranse. En og samme avregningsentral for alle kjøpere og selgere ville gjøre netthandelen virkelig global. På den annen side ville den også kunne bli en gedigen

flaskehals i hele systemet. Mange konkurrerende avregningssentraler ville avhjelpe det siste, men da må særlig selgere ha tilknytning til alle slike sentraler for å være sikker på å nå en størst mulig brukergruppe. Et system med distribuerte avregningssentraler med tilhørende clearingssentraler, slik det forutsettes i NetCheque-konseptet, kunne bli en god løsning, men det fordrer et organisatorisk rammeverk som på kort sikt synes vanskelig å få til.

7.3 Elektroniske penger

Elektroniske penger kan være en modell som er godt egnet for løssalg av elektronisk informasjon, men den forutsetter at de elektroniske pengene er akseptert av mange selgere, og at de er konvertible på en enkel måte til vanlig valuta. Elektroniske penger er gunstige på den måten at de kan realisere en elektronisk økonomi på nettet der pengene kan flyte omtrent som kontanter i den normale økonomien, og gjenbrukes av den som mottar dem. Modellen gir god personvern for kjøperen, da kjøpene kan gjøres helt anonyme, ikke bare i forhold til selgeren, men også i forhold til banken (dette er vanskeligere i de andre modellene, selv om en viss grad av anonymitet kan sikres).

Kritikere av denne modellen påpeker at måten elektroniske penger er realisert på krever en sentral database for kontroll av at pengene ikke misbrukes, dvs forsøkes brukt flere ganger. Dette kan gi ytelsesproblemer når "pengetrafikken" blir virkelig stor.

Det er også andre typer sikkerhetsproblemer med en løsning med rene elektroniske penger, nemlig det at ved tekniske problemer som disk-krasj eller uønsket fjerning av filer, kan pengene gå tapt. Dette kan avhjelpes ved bruk av dedisert, sikker maskinvare (elektronisk lommebok), men da må hele betalingsinfrastrukturen tilpasses dette. Ecash baserer seg på en annen infrastruktur, tilpasset online betaling.

Det er også store institusjonelle hindre å overstige for å innføre denne typen ny valuta i økonomien. Man kan skille mellom to typer elektroniske betalingsmidler; de som er knyttet til den eksisterende økonomi og bare er kontanter på et nytt medium, og de som i realiteten er en ny valuta som ikke har konvertering mot eksisterende økonomi (f.eks. ecash-løsningen til Digicash). I det siste tilfelle er det nye institusjoner utenfor bankverdenen som driver denne virksomheten, og det er en virksomhet som er utenfor kontroll av nasjonalbankene og dermed penge- og valutapolitikken, men den gjenstår å se hvilken betydning og omfang de «nye pengene» vil få. Elektroniske penger knyttet eksisterende øknonomi og valuta vil derimot kreve en institusjon innenfor eksisterende finansverden for å konvertere mellom elektroniske penger og konvensjonelle penger. Det vil i seg selv være en radikal ny måte å oppbevare, håndtere og formidle penger på både for banker og brukere. En overgang til den type betalingsløsninger kan ikke ansees som en realistisk alternativ på kort sikt.

7.4 Direkte belastning av kreditt- og debetkort

Fordelen ved direkte belastning av kredittkort er at løsningen baserer seg på eksisterende institusjoner som har erfaring og kunnskap om betalingsformidling. Problemet er imidlertid at noen av dem (f.eks. debetkort fra VISA) opererer med

transaksjonskostnader ved betalingsformidling som gjør det umulig å drive med småsalg av informasjon som enkelttransaksjoner.

Nødvendigheten av sikkerhetsmekanismer for oversendelse av kredittkortnummer og koblingen til kortselskapenes systemer for validering av kort kan gjøre denne løsningen unødig dyr. Sikkerhetsmekanismene må egentlig kunne forhindre at handelen gjøres med et kort som tilhører en annen person enn kjøperen (noe som er svært enkelt å prøve seg på ved elektronisk handel). Tilkoblingen til kortselskapenes nettverk vil ofte ikke kunne forhindre dette, da de som regel kun sjekker gyldigheten til kortet, og ikke identiteten til brukeren.

Denne betalingsmetoden utelukker også en gruppe brukere av nettet, nemlig de som ikke har kreditt- eller debetkort (som f.eks. studenter). Det samme kan man si om selgere - mange av potensielle småselgere av elektronisk informasjon vil ha problemer med godkjennelsen fra kortselskapene som kortmottager. (eller det ville ikke lønne seg for dem å være det).

Totalt sett er denne løsningen lite egnet for betaling av informasjonstjenester, både på grunn av størrelsen og hyppigheten av transaksjonene og på grunn av manglende sikkerhet for misbruk av kort. Selv om kortnummeret ikke kan plukkes opp av uvedkommende på nettet, så kan det komme på avveie på andre måter - og da kan misbruket ikke forhindres.

8. Konklusjon

Vi har i denne rapporten forsøkt å gi et bilde av utviklingen innen online elektroniske løsninger for handel med informasjonstjenester på globale nett, Internett i særdeleshet.

Dette har vært en givende, om enn vanskelig oppgave, da feltet formelig "eksploderte" i slutten av 1994, da vi tok fatt på prosjektet. Den store veksten i interessen for Internett-tilgang og Internett-tjenester har fremskyndet krav om pålitelige løsninger for elektronisk handel, inklusive betalingsløsninger. Nesten "alle" er nå involvert i utviklingen eller utprøvingen av slike konsepter.

De ulike konseptene vi har vurdert er i hovedsak oppstått i U.S.A., der Internett-utbredelse er størst. Vi har også sett på hvordan både europeisk og amerikansk tradisjonell online-industri løser betalingsspørsmålene og hva gjør de store kredittkortselskaper (i den grad det var mulig å få tak i informasjon) på dette feltet.

Vi har også sett på noen europeiske FoU-tiltak på området, og så vidt berørt pågående europeiske forsøk innen elektroniske småpengesystemer.

De ulike konseptene vi har beskrevet og vurdert, spenner fra generelle "markedsplass"-konsepter for one-stop-shopping basert tilgang til flere tjenester, med tilhørende betalingsopplegg, til forskningspregede tekniske løsninger for formidling av betalinger over nett. Det har derfor vært noe vanskelig å systematisere løsningene og sammenligne dem med hverandre.

Vi har kunnet finne fellestrekk hos de enkelte løsningene som gjorde det mulig å skissere fire hovedmodeller for betalingsløsninger for elektronisk handel over nett. Konkrete forekomster av modellene er beskrevet i vedlegg, mens vi i de foregående kapitler har prøvd å vurdere de ulike modellenes generelle fordeler og ulemper.

For å kunne gi en totalvurdering og anbefaling av en type modell, må man først definere hvilke egenskaper ved modellene det er ønskelig å sammenligne og vurdere, og videre må man også skille mellom hva som er mulig på kort og lang sikt.

De mest vitale egenskaper ved betalingsløsninger er:

- sikkerhet (inkl. anonymitet)
- pålitelighet/stabilitet
- skalerbarhet
- aksept
- effektivitet (inkl. kostnader)
- bruksterskel, både for kjøpere og for selgere

Dersom man vurderer de ulike modellers sikkerhet, må man også være klar over at det ligger iboende motsetninger i sikkerhetsbegrepet, ved at konfidensialiet kan stå i direkte motstrid til sporbarhet. I vår sammenheng vil vi måtte anse systemer som gir en viss grad av konfidensialitet mot god sporbarhet som sikre. Det primære ved en kjøpstransaksjon er at kjøperen får det hun har betalt for og at selgeren får sine penger. Da vil sporbarhet være av mer overordnet betydning enn konfidensialitet. Ved en slik fortolkning av sikkerhet, og tatt i betraktning de andre aspektene, så som integritet, vil abonnementsmodellen være en ganske sikker modell, etterfulgt av avregningssentral helst med distribuert arkitektur, elektroniske penger (også med distribuert arkitektur) og belastning av kredittkort.

Ved vurdering av pålitelighet og stabilitet er det vanskelig å fremheve noen av modellenes fortreffelighet over andre, da dette er veldig implementasjonsavhengig og beror i stor grad på den arkitekturen man har basert realiseringen av systemet på. Videre vil dette også være spørsmål om ressurser, dvs. i hvilken grad man er villig til å investere i f.eks. speilingsteknologi for å holde høy grad av stabilitet i systemet. Vi sitter med det inntrykket at systemer som involverer online elektroniske penger kan være mest utsatt i denne sammenhengen.

Skalerbarheten i modellene innebærer muligheten å dekke stadig økende antall kjøpere og selgere uten signifikante modifikasjoner i en betalingsløsning. Dette igjen er en del arkitektur- og implementasjonsavhengig, men avregningssentralmodellen, med distribuert arkitektur, synes å peke seg ut som en god skalerbar løsning.

Aksept er en meget viktig egenskap i betalingsløninger, i hvertfall med kortsiktig perspektiv. Aksept innebærer muligheten å implementere systemet i “reelle” omgivelser, og at et tilstrekkelig antall kjøpere og selgere vil ha tillit til det som betalingsinstrument. Det viktigste er dog kanskje at den tradisjonelle finansindustrien må kunne akseptere systemet som en del av seg selv eller i hvertfall som en samarbeidspartner. Sett i lys av dette, er abonnementsmodellen helt uproblematisk, kortbelastning er også rimelig greitt. Avregningssentraler vil kunne fungere bra dersom

grenseoppganger til andre finansinstitusjoner defineres klart. Vanskeligst i så måte er elektroniske penger, som krever forholdsvis dype institusjonelle endringer i finansverdenen og risikerer dermed å ikke bli akseptert på kort sikt.

Effektiviteten i betalingsløsningene kan innebære muligheten til å håndtere mange småtransaksjoner til en lavest mulig kostnad - og - på den annen side - den innebærer også at systemet skal ha såpass god ytelse at det kan behandle store mengder transaksjoner uten nevnverdig nedgang i ytelse til hverken selgere eller kjøpere.

Dersom man vurderer selve transaksjonskostnader, så er abonnementsmodellen grei, idet transaksjoner samles opp før betaling. Det samme gjelder avregningssentralen. Best faller elektroniske penger ut, i det kontanttransaksjoner har praktisk talt ingen kostnad. Kortbelastning vil bli dyrest. Dersom man i tillegg vurderer ytelse i systemet, vil abonnementsmodellen være lite relevant, da betaling skjer fullstendig "offline". Avregningssentraler basert på betalingsanvisning vil kunne fungere bra, mens online belastning av kort og særlig elektroniske penger vil kunne få problemer med stor trafikk og sentraliserte løsninger.

Bruksterskelen, dvs. hvor lett det er å ta systemet i bruk, både for selgere og kjøpere, er forsåvidt et aspekt av aksept, men det er såpass viktig at vi har valgt å fremheve den som en egen egenskap. Betalingssystemets mulighet til lett å kunne integreres i en tjenesteleverandørs programvare vil være avgjørende for systemets utbredelse og aksept. Denne egenskapen er igjen i stor grad implementasjonsavhengig, slik at ingen av modellene vil her kunne peke seg ut. Når det gjelder kjøpere, så står man overfor det paradokset at "lett å bruke" betyr egentlig at det ikke skal være for lett å bruke systemet - dvs. brukeren må aldri kunne foreta en betaling uten å ha full kontroll over hva som skjer og uten å ha sikret seg sporbarhet (dvs. kvitteringer for mottatt betaling). I denne sammenheng er elektroniske penger kanskje den mest risikable varianten, likeledes kortbelastning. Abonnementsmodellen er direkte "skummel" da brukeren kan gjøre en hel masse ting uten å ha følelsen av hva dette koster, da regningen kommer i ettertid. Avregningssentral basert på betalingsanvisninger vil kunne gi kjøperen en mulighet til å "tenke seg om" to ganger før endelig betaling foretas - og den kan støtte ulike former for kvitteringer ved kjøp (dette er selvsagt også avhengig av selgerens policy).

Som denne gjennomgangen av ulike egenskaper ved betalingssystemene viser, er det ikke mulig å entydig peke ut en modell som oppfyller alle av egenskapene like bra. Det finnes fordeler og ulemper ved alle av modellene. Den største ulempen ved abonnementsmodellen er at den ikke kan støtte "løssalg" av informasjon over nett - som vil jo være selve kravet ved globalisering av online-markedet. Den største ulempen (på kort sikt) med elektroniske penger er manglende aksept i finansverdenen. Den største ulempen med kortbelastning er kostnadene og uhensiktsmessigheten ved mange små transaksjoner, som betegner løssalg av informasjon. Bare avregningssentralen, selv om den også har en del problemer knyttet til seg, fremstår uten virkelig diskvalifiserende ulemper.

Det er derfor denne modellen vi vil fremheve som en god, kortsiktig løsning for løssalg av informasjon over nett. En slik modell vil kunne fungere godt i avgrensede segmenter av globale nett. For å møte globaliseringen, må avregningsentralene kunne samarbeide

etter etablerte prosedyrer. Dette kan by på mange utfordringer, tekniske så vel som regulatoriske.

På lang sikt kan en derfor tenke seg elektroniske penger som en interessant løsning. Men da må finansinstitusjonene komme på banen og støtte konseptet i en annen grad en hittil. Flere europeiske banker har fattet interesse for, og til og med prøver ut i praksis, elektroniske småpengesystemer. Men disse forsøkene retter seg mot vare- og tjenestesalg "over disk", med dedisert maskinvare som viktige komponenter. Betydelig innsats vil måtte gjøres for å overføre denne tankegangen til elektronisk handel. Og utviklingen tyder jo på at datanett kan i stor grad bli den "disken" der ikke bare informasjonstjenester, men mange forbruksvarer og -tjenester vil kjøpes i årene som kommer.

Ordliste

Avregningssentral - en organsiasjon som vedlikeholder konti for kjøpere og selgere på den elektroniske markedsplassen. AVS formidler også betaling fra kjøpere til selgere.
Betalingsformidling - en ordning der en kreditor (selger) får betaling av sine fordringer fra en debitor (kjøper) gjennom en tredjemann.
Betalingskort - et betalingsmiddel der brukeren får en betalingsutsettelse, dvs. beløpet trukket på kortet må i sin helhet betales innen en viss tid etter at regning er mottatt.
CA (Certification Authority) - en organisasjon som kan utstede offentlig nøkkel sertifikater.
Debetkort - et betalingsmiddel der transakjsoner går direkte inn på konto til kortbrukeren, dvs. det kreves dekning på konto for å gjennomføre transaksjonen.
Elektronisk markedsplass - en type online tjeneste der mange tjenesteleverandører er tilgjengelig "under samme hatt" . Markedsplassen kan også tilby tilleggstjenester, f.eks. et betalingssystem.
Elektronisk signatur - en kryptografisk sjekksum av en melding, kryptert med meldingsavsenderens private nøkkel
Elektroniske informasjonstjenester - produkter som kan fåes tilgang til/overføres via et datanetteverk (f.eks. databaser, beregningskraft, programvare osv.)
Elektronisk lommebok - en elektronisk innretning som gjør det mulig å ta imot, lagre og gi ut elektroniske penger . (kan f.eks. være et smartkort)
Elektroniske penger - digital representasjon av kontanter (sedler, mynter). En elektronisk mynt kan f.eks. bestå av et serienummer og elektronisk signatur til banken som har gitt ut mynten.
FTP (File Transfer protocol) - en tjeneste på Internettet som gjør det mulig å få adgang til datafiler på maskiner tilkoblet nettet og overføre dem mellom de ulike maskinene.
HTTP (HyperText Transfer Protocol) - en høynivå kommunikasjonsprotokoll som benyttes på Internettet til å aksessere og overføre hypertekst-dokumenter (WWW-dokumenter).
Internett - et verdensomspennende nett som er en sammenkobling av flere ulike nett som benytter det samme sett av protokoller for kommunikasjon (som f.eks.TCP/IP, Telnet, SMTP, FTP, HTTP)
Kortselskap - en organisasjon som etablerer og driver en infrastruktur for betalingsformidling basert på bruk av kort (debet, kreditt- og betalingskort).
Kredittkort - et betalingsmiddel der kortbrukeren ydes en kreditt ved kjøp eller kontantuttak. Kreditten må tilbakebetales i avdrag. Det beregnes og betales renter.
Kryptering - transformasjon av en klartekst til en siffertekst ved hjelp av en krypteringsalgoritme og en tilhørende krypteringsnøkkel.
Offentlig nøkkel-kryptering - krypteringsalgoritmer som har den egenskapen at tekst kryptert med privatnøkkel kun kan dekrypteres med den tilsvarende offentlige nøkkelen og omvendt (f.eks. RSA-algoritmen)
Offentlig nøkkel - sertifikat - en kobling mellom en identitet og en offentlig nøkkel, signert av en CA.
Online tjenester - tjenester som man kan få tilgang til ved direkte oppkobling (via telefonlinjer og/eller datanett) til en fjerndatamaskin som huser tjenestene. Tjenestene krever interaktiv, sanntidskommunikasjon med brukeren.

Småpengesystem - en ordning der brukere ved hjelp av spesielle betalingsmidler (kort, elektroniske lommebøker) kan betale for varer og tjenester som koster småbeløp. Slike systemer krever som regel forhåndsinnbetaling av pengene som skal brukes.
Smartkort - en type standardisert plastkort som har påmontert en mikroprosessor som kan lagre og/eller bearbeide data. (ISO-standarder 7816 og 10536)
Symmetrisk kryptering - krypteringsalgoritmer der samme nøkkel brukes både for kryptering og dekryptering (f.eks. DES-algoritmen)
TTP (Tiltrodd Tredje Part) - en organisasjon som to samhandlende parter kan benytte for å etablere gjensidig tillit.
Usenet News - en tjeneste på Internettet som tilbyr store mengder såkalte diskusjonsgrupper, dvs. fora for meningsutveksling. Innlegg i disse fora leveres vha elektronisk post. Andres innlegg kan leses vha ulike lesere.
WWW (World Wide Web) - en Internett-tjeneste som gir tilgang til dokumenter (som kan være tekst, bilder, lyd, video eller kombinasjoner) som er lenket sammen på tvers av maskiner, nett og landegrenser. Alle dokumenter er strukturert i henhold til en standard kalt HTML (HyperText Markup Language).Dokumentene ligger på WWW-servere - datamaskiner med WWW-programvare, som er kontinuerlig tilgjengelig på nettet. For å kunne lese dokumentene må brukeren disponere en WWW-leser.
WWW-leser - en programvare som gjør det mulig å hente inn, vise/avspille, skrive ut og lagre WWW-dokumenter. Lesere benytter HTTP for å hente dokumentene.

VEDLEGG - EKSEMPLER PÅ LØSNINGER FOR ELEKTRONISK HANDEL PÅ NETT

1. Abonnementsmodellen

1.1 Britannica Online

Britannica online er en informasjonstjeneste basert på abonnementsmodellen. Som bruker betaler man et fast beløp periodisk for å få tilgang på denne informasjonstjenesten. Det er ingen avgift på bruk av tjenesten, når det er betalt abonnement har man ubegrenset tilgang.

Britannica online leveres over Internett på WWW. Tjenesten består i fritekstsøk på ord, som gir tilgang på de artiklene som inneholder dette ordet. Dette betyr altså en utvidet opplagsfunksjon i forhold til det man er vant til med papirbaserte leksika. Brukeren kan også søke i form av spørsmål og bruk av naturlig språk.

1.1.1 Autentisering

Det er maskinadressen som bestemmer tilgangen på Britannia Online. Det er altså maskinen som i teknisk forstand har abonnementet. Det betyr at brukeren ikke trenger å identifisere seg ved oppslag i Britannica online, maskinadressen vil fungere som identifikasjon. Det betyr også at alle som har tilgang på en maskin som abonnerer på Britannica online, også vil ha tilgang på tjenesten.

1.1.2 Fakturering og betalingsformidling

Betaling for Brintannica Online foregår som ved et annet tradisjonelt abonnement. Kunden blir krevet for et beløp med jevne mellomrom, og tjenesten blir avstengt hvis regningen ikke betales. Det er ingen form for betaling over nettet.

1.1.3 Samlet vurdering

Britannica Online er en ny type tjeneste, ved at oppslag skjer over WWW. Tjenesten utnytter også mulighetene i elektroniske medier ved at oppslaget kan gjøres i fritekstsøk, slik at det blir en form for flerdimensjonalt oppslag som kan gi bred informasjon. Muligheten for å gjøre bruk av naturlig språk i søk, øker også bruksområdet for tjenesten.

Men når det gjelder utvikling av betalingsmuligheter over nett har ikke Britannica Online bidratt med noen løsninger.

2. Avregningssentral (kreditt-debet)

2.1 First Virtual Inc.

First Virtual Holdings Inc. er et lite firma basert i Ohio, U.S.A. Bak etableringen av firma ligger et konsept for “grønn” handel på elektroniske nettverk satt frem av Internet-veteranene Marshall T. Rose, Einar A. Stefferud, Lee H. Stein og Nathaniel S. Borenstein.

Konseptet har siden blitt utviklet og implementert som FV Internet Payment System. Systemet har blitt satt ut i prøvedrift i oktober 1994.

Hovedtrekkene i konseptet går ut på avregning mot kreditt/debetkort og bruk av elektronisk post til kommunikasjon mellom partene. Konseptets "fedre" fremhever som et stort fortrinn ved det at det ikke benytter krypteringsteknologi.

Bak FV-konseptet ligger det en "demokratisk" visjon, som går ut på å gjøre alle som bruker Internettet til både brukere og selgere av informasjon, dersom de ønsker det. M.a.o., man behøver ikke være stor databasevert for å kunne selge informasjon på nettet.

FV kan benyttes av alle brukere som har et gyldig VISA- eller MasterCard-kort, kreditt- eller debettype. Når det gjelder selgere av informasjon, er forutsetningen at deres bankforbindelse kan ta imot tilgodehavende i amerikanske dollar, direkte fra den amerikanske "BBS" kalt ACH (Federal Reserve Automated Clearing House). Dette kan skape problemer for selgere utenfor U.S.A. og Canada. FV sier at de arbeider med problemet og håper å tilby akseptable løsninger til ikke-amerikanske selgere i nærmeste fremtid (uspesifisert).

FV skal gå ut med en stor, kommersiell annonsering av sin tjeneste i februar 1995.

Prosedyren for å få en "konto" hos FV er følgende:

- kunden fyller ut en "application form", på WWW med form-submit eller som formattert email (skjema sendes og mottas av en mailserver); FV krever fullt navn, adresse, telefon, samt faktureringsadresse for kortselskapet; kunden skal også oppgi en egenkomponert karakterstreng som skal danne stammen i kundens unike kontoidentifikator hos FV
- kort tid etter at skjema er sendt, mottar brukeren en automatisk email melding der søknaden bekreftes og der det oppgis to ting: telefonnummer i U.S.A. der en automatisert tjeneste kan motta og registrere kortnummeret samt et unikt søknadsnummer, som skal sikre at brukeren er den han/hun utgir seg for på det tidspunktet kortnummer oppgis; potensielle selgere av informasjon får også oppgitt en adresse i U.S.A. der de kan sende en sjekk pålydende $10, som skal dekke kontoetableringskostnader; kontoetableringskostnaden for brukere er $2 og debiteres brukerens kort
- etter oppringing, der kunden oppgir sitt kortnummer og søknadsnummer, kommer det en automatisk melding via email med beskjed om at kontoen er nå klar til bruk og med den unike kontoidentifikatoren til kunden (som består av den kundegenererte stammen og et random-generert tillegg); NB: dette går i åpne meldinger over nettet

Vilkår for kjøp- og salgstransaksjoner gjennom FV er definert i et eget dokument (TaC-dokument), datert 14.10.94, men under revisjon nå. Dokumentet fåes fra en mailserver hos FV. En kan abonnere på alle forandringer i dokumentet ved å sende subscribe til denne serveren.

Potensielle selgere av informasjon via FV kan gjøre dette praktisk på to måter:

1) lease plass på FVs egen server ved navnet “Infohaus”
2) bruke egen server, men innstallere FV-kompatibel programvare for salg av informasjon og verifisering av kundene

Foreløbig er det kun selgere som leaser plass hos Infohaus som er tilgjengelig for FV-kunder.

2.1.1 Autentisering

Ved valg av en informasjonsenhet blir brukeren av en FV-kompatibel informasjonstjeneste bedt om å oppgi sin FV-kontoidentifikator. Brukeren får i forveien kun en kort informasjon om hva informasjonsenheten inneholder.
Enheten vises i sin helhet når kunden har oppgitt sin identifikator (i et søkefelt). Selgeren kan verifisere, om ønskelig, kundens identifikator mot FVs server (FVs green commerce protokoll tillater dette) før informasjonen vises til kunden.

2.1.2 Ordrebehandling

Ordren om kjøp av informasjon er “i prinsippet” gitt når kunden har oppgitt sin kontoidentifikator og sendt denne til tjenesteleverandøren. Det ligger imidlertid en liten “hake” her, idet brukeren har, ifølge FV, en rett til å nekte å betale for mottatt informasjon, dersom han/hun ikke er fornøyd med “varen”. Se fakturering.
Eksempler på prising slik det foregår ved salg av informasjon via Infohaus er pr. artikkel (fra en tidsskrift), pr. bilde (JPEG), pr. rapport (fulltekst), pr. programvare “snutt” osv. Prisene som settes bærer preg av at man “føler seg frem”: f. eks. kreves det $6,25 for en (kort) artikkel og $1,25 pr. JPEG-bilde.

2.1.3 Kontering

Selgerens server sender en email melding til FV, med følgende innhold: kjøpers navn og kontoidentifikator, selgers navn og kontoidentifikator, varens navn/beskrivelse og pris. Selgeren er, ifølge TaC-dokumentet, forpliktet å lagre slike salgsdata forsvarlig, og oppbevare dem i minst 3 år.

2.1.4 Fakturering

FV sender en automatisk email melding til kunden som kjøpte informasjonen, med spesifikasjon av transaksjonen. Kunden skal så umiddelbart sende en svarmelding tilbake til FV, med ett av tre mulige svar: yes (ja), no(nei), fraud (svindel). Kunden kan altså bekrefte transaksjonen og derved gi FV klarsignal til å belaste sin konto hos FV (og sitt kort), negere transaksjonen på grunn av manglende verdi i den kjøpte vare (FV forutsetter da at kunden fjerner den elektroniske versjonen av varen fra sitt utstyr) eller varsle FV om at dette er et forsøk på svindel, dvs. kunden kjenner ikke transaksjonen igjen. I det siste tilfellet vil FV øyeblikkelig sperre kundens konto. Kunden vil da måtte gå gjennom kontoetableringsprosedyren på nytt.

Ved normalt salg vil selgeren få sin FV-konto godskrevet med salgets verdi minus FV sine avgifter (ft. $0,29 pr. transaksjon pluss 2% av transaksjonens verdi).

2.1.5 Betalingsformidling

FV vil akkumulere kundens kjøpetransaksjoner til de utgjør et beløp som er stort nok for å kunne belastes kundens kort. FV oppgir ft. ikke størrelsen på dette beløpet, heller ikke når de kan foreta en avregning mot kortselskapet (periodisk, etter bestemt antall transaksjoner el.l.). Kunden vil få FVs belastning spesifisert på sin vanlige faktura fra kortselskapet og betaler på vanlig måte.

Selgeren vil få sitt tilgodehavende overført til den konto som ble spesifisert ved etablering av FV konto. Ifølge TaC-dokumentet kan FV holde selgerens tilgodehavende i inntil 91 dager, før godskriving av selgerens konto. Dette, sier FV, har sammenheng med amerikanske bestemmeler om kortkundenes klagemuligheter og derved regressmuligheter mot FV. Selgeren er dermed foreløpig "den tapende part" i dette betalingsopplegget.

2.1.6 Samlet vurdering

Fordelen ved FV-løsningen er dens enkelhet og at den virker i praksis (dette er testet av oss). Systemet har et greitt definert grensesnitt mot den vanlige finansverden, i hvertfall sett fra kjøperens side. Dersom man vil bli selger gjennom FV er situasjonen imidlertid noe mer uklar, da FV benytter den amerikanske nasjonalbankens clearingssystem for å godskrive selgernes konti i deres banker. Dette kan være en omstendelig og kostbar prosedyre for norske selgere, kanskje ikke lønnsom i det hele tatt, transaksjonenes størrelse tatt i betraktning. Et annet problem med FV er muligheten for at kjøperen vil nekte betaling for mottatt informasjon / tjeneste. Dette blir nokså "stramt" praktisert av FV, men kan være med på å skremme potensielle selgere fra å tilslutte seg konseptet. Det er de som vil måtte bære tap ved tvist med kjøpere, iht. gjeldende vilkår for salg via FV. FVs konsept gir heller ikke noe særlig personvern (selgere får se kjøpernes navn og FV oppbevarer koblinger mellom kjøper/vare/selger), men den gir derimot god sporbarhet i tilfelle tvist.
Til sist, sikkerheten i systemet er ikke god nok. Man baserer seg veldig mye på tillit, ved at man forutsetter at kundens elektroniske postkasse brukes av kunden og ham alene. Uhederlige systemsjefer o.l. vil lett kunne plukke opp de åpne e-post meldinger som går i nettet og benytte opplegget for egne innkjøp, som belaster andres kort.

2.2 Open Market Inc. (OMI)

Open Market er en aktør som har som mål å legge til rette for elektronisk handel på Internettet og tilbyr et sett med verktøy som skal gjøre slik handel mulig. Tilbudet retter seg både mot potensielle selgere og potensielle kjøpere på nettet. Betalingstjenester utgjør en del av dette tilbudet. Bak opprettelsen av selskapet står tre kjente personstørrelser: Shikhar Ghosh, adm. dir., er kjent for å ha bygget opp betalings- og avregningssystemer for mobiltelefonindustrien, David Gifford (Chief Scientific Officer) er professor ved MIT og leder Programming Systems Research Group der og Lawrence C. Stewart (Chief Technology Officer) er kjent for å ha vært med på design av Alpha-prosessor hos D.E.C. Selskapet er basert i Cambridge, Massachussets, U.S.A.

Open Markets forretningsidé er å etablere et avansert rammeverk for elektronisk handel soom gjør det mulig for alle personer / organisasjoner, uavhengig av geografisk plassering, å tilby varer og tjenester elektronisk til en global markedsplass. Konseptet baserer seg på to sammenkoblede komponeneter: en "Merchant Server" og en "Payment Server". Primært vil OMI lease plass på sin Merchant Server til potensielle selgere, men selgere med egne servere utelukkes ikke. Open Market tilbyr følgende tjenester til selgere :

- "StoreBuilder" - programvare verktøy for bygging av butikkfasader på Internettet, med multimedia-kapabiliteter og avanserte indekseringsmekanismer som tilrettelegger for fleksibel søking i informasjonen som legges ut på nettet
- betalingstjenester med mekanismer som tillater ulike prisingspolicy (betal pr. side, avsnitt, kapittel osv.), bl.a. det skal være mulig å selge online tid til en bruker (en type adhoc abonnement)
- konteringsmekanismer med ulike typer rapporter basert på konteringsdata
- "document fingerprinting" for unik merking av solgt informasjon (som middel mot uautorisert spredning av åndsverk)
- feedback-mekanisme fra kjøpere til selgere.

Priseksempler for StoreBuilder verktøykasse og leie av plass hos OMI er US $500 for opprettelse av "butikken" (maks. 5 mbyte) og $75 per måned i leie. Dette inkluderer integrasjon mot betalingssystemet.

For kjøpere av informasjon, varer og tjenester på Internettet tilbyr Open Market et sett med verktøy som inkluderer:

- autentisering (passord- og kryptobasert)
- søkemuligheter i tjenesteutbudet
- filtre som kan skreddersy en kjøpers interesseprofil
- kvitteringsmekanismer som gjør det mulig å overvåke egne innkjøp.

OMI benytter seg av lisensiert programvare fra MIT for sine søke- og filtermekanismer.

Ved opprettelsen av en handlekonto hos OMI kan kredittkort-nummer oppgis på tre ulike måter:

1. Via en automatisk telefontjeneste (oppgir kortnummer og utløpsdato)
2. Via fax (krever kortnummer, utløpsdato og signatur)
3. Ved å sende en PGP-kryptert email eller ved å oppgi nummeret direkte via WWW, men kryptert med PGP.

Det har ikke vært mulig å finne noe slags dokument som skulle beskrive vilkår for en avtale mellom en kjøper og OMI i forbindelse med opprettelsen av en konto. Det har heller ikke vært mulig å finne en lignenede avtale for kjøpere.

Betalingssystemet baserer seg på å benytte URL til koding av betalingstransaksjoner. De skiller mellom en betalingsURL og en aksessURL. BetalingsURL inkluderer hva som skal selges og pris - denne URL vil bringe brukeren til OMI sin betalingsserver som behandler selve betalingstransaksjonen (dette skjer "bak kulissene"), for deretter å redirigere brukeren vha en aksessURL til en server der selve varen befinner seg og kan

hentes (for “harde” varer vil dette være en ordrebekreftelse). Denne URL-en vil inneholde detaljer om hva som var kjøpt og for hvor mye.

Open Market har i slutten av 1994 annonsert en rekke “strategiske allianser”, bl.a. med Digital Equipment Corporation (som skal visst selge OMI-løsninger til finansinstitusjoner). OMI påstår også at de snart skal støtte en rekke andre finansielle instrumenter, så som forhåndsbetalte konti, debetkort, fakturabasert betaling osv.

2.2.1 Autentisering og ordrebehandling

Når en bruker velger en betalingsURL, vil hans leser bli dirigert til OMI betalingsserver. Denne serveren verifiserer validiteten av URLen og autentiserer brukeren. Dette kan gjøres på tre ulike måter: 1) brukernavn og passord via vanlig HTTP-funksjon. 2) “Challenge”-basert verifisering, f.eks. spørsmål om tilleggsdata om brukeren. 3) “Challenge-response”- baserte passordkort som brukeren har lokalt (dette er ikke realisert ennå). Dersom brukeren er OK (dvs. finnes i OMI sitt kunderegister) og har kjøpekraft (dvs. gyldig konto) vil transaksjonen bli prosessert og brukerens leser redirigert (via en standard funksjon i HTTP) til en adgangsURL som “henter” varen.

2.2.2 Kontering

AksessURL kan oppfattes som et fakturagrunnlag for selgeren. Den er en “target” URL for betalingsURL-en og inneholder, i tillegg til informasjon om varen og prisen, felter som gir detaljer om brukerens adgang til varen: utløpstid (ved salg av tidsbegrenset aksess) og brukerens adresse i nettet, for å sikre seg mot misbruk (dvs. at andre enn brukeren henter varen).
WWW-serveren til selgeren vil måtte ha modifisert programvare for å behandle slike aksessURL-er. Alternativt kan CGI-skript brukes for dette.

2.2.3 Fakturering

OMI betalingssystem understøtter kun kredittkort-basert betaling (VISA og MasterCard). De påstår å ha tilgang til kortselskapenes nettverk for klarering av transaksjoner. De påstår at småtransaksjoner kan akkumuleres hos dem og sendes til kortselskapene i en bolk. Så vidt det var mulig å validere, skjer belastningen av kortet umiddelbart ved kjøp og det er ingen angremuligheter. Kjøperen får se en side (så kalt “SmartStatement”) som gir detaljer om sist utførte innkjøp og kostnader involvert. All handel skjer i US dollars. Det gis en “klagemulighet”, ved at det er mulig å sende en melding/forespørsel via WWW til selgeren, dersom brukeren oppdager noen uregelmessigheter i sin “faktura”. Det eksisterer lenker fra denne fakturasiden til selve varen - dvs. man kan hente den igjen dersom dette er informasjon. Tidsbegrenset online-aksess må betales omigjen. For harde varer vil denne lenken føre til en side som forteller om status i bestillingen.

2.2.4 Betalingsformidling

Betaling skjer ved at kunden mottar en vanlig regning fra kortselskapet. I fremtiden vil man støtte belastning av konto i banken ved bruk av debet kort, forhåndsbetalte konti hos OMI, debet konto med fakturering til kunden osv.

2.2.5 Samlet vurdering

OMI fremstår som en forholdsvis lignende konsept som First Virtual. Forskjellen ligger i måten betalingstransaksjonene gjøres på og at OMI selger tilleggstjenester som StoreBuilder.

Betalingssystemet benytter seg av standardfunksjoner i HTTP, med noen tillegg/modifikasjoner. Alle transaksjoner skjer via WWW, elektronisk post benyttes ikke, slik FV gjør. OMI påstår at deres system er sikker, men det vi har sett indikerer noe annet - nemlig at trafikken går via vanlig, ukryptert HTTP, som er lett å "avlytte". Selv om OMI har noen tilleggsfunksjoner for sikkerhet (challenge, f.eks.), går også dette over ukryptert HTTP. De påstår at ved å bruke Mosaic-versjonen som støtter PGP kan dette avhjelpes, men vi har ikke hatt tilgang til denne programvaren og kan ikke verifisere dette.

OMI påstår at de i fremtiden vil støtte SHTTP, Shen osv. , men foreløpig ligger dette på planstadiet.

OMI tilbyr fasiliteter som grenser for totalt kjøp på nettet og øvre grense for hver transaksjon. Dette gir brukeren mulighet for å kontrollere sitt pengeforbruk og skal gi en tilleggssikkerhet for kunden, men dette er illusorisk så lenge verifiseringen baserer seg på challenge-response som sendes via vanlig form-submit i HTTP, som kan avlyttes.

Systemet virker forvirrende for brukeren, med mange nivåer, sider og lenker. Fremgangsmåten ved kjøp er noe komplisert, bl.a. ved at man introduserte "shopping-cart" begrepet (brukeren skal kunne"reservere" varer for kjøp). Dette er en gimmick som ikke gjør systemet mer (for)brukervennlig.

En fordel ved OMI er at alt foregår via en WWW-leser, og brukeren ikke behøver å forholde seg til en e-post leser i tillegg.

Selv om betalingsfunksjonen virker raskt og forholdsvis oversiktlig (selv om vi ikke kunne få innsikt i de interne detaljer), så er sikkerheten ved systemet for dårlig, slik det fremstår i dag, for at det skal være noe alternativ. Dessuten er opplegget skreddersydd for en WWW-basert handel, og kan vanskelig overføres til andre typer tjenester, som ikke støttes av WWW.

2.3 NetCheque

NetCheque er et konsept for elektronisk betaling på Internettet utviklet av Information Sciences Institute (ISI) ved University of Southern California, U.S.A. med finansiell støtte fra ARPA (Advanced Projects Research Agency).

Konseptet er en variant av kreditt-debet-modellen, men det baserer seg på bruk av offline, sikre mekanismer ("sjekker") for betalingsformidling. Mennene bak konseptet er Clifford B. Neuman (som var hovedpersonen i utviklingen av Kerberos-systemet) og

Gennady Medvinsky. Konseptet er nå på forskningsprosjektstadiet og man skal snart begynne å teste det i praksis (med "testpenger").

Konseptet skiller seg fra løsninger av typen FV eller Open Market ved at det introduserer et distribuert betalingsformidlingssystem, der flere avregningsservere (betalingsservere) kommuniserer med hverandre. Brukere kan ha konti på en av slike servere. Brukeren og selgeren behøver ikke å ha konti på samme server.

Systemet var opprinnelig designet for å håndtere ressursbruk-avregning i et distribuert systemmiljø og er, ifølge Neuman og Medvinsky, godt egnet for håndtering av små transaksjoner. Sikkerhetsfunksjoner baserer seg på konvensjonell kryptografi, bl.a. for å sikre høy ytelse ved stor belastning. Mer konkret er systemet basert på bruk av Kerberos' egne funksjoner for elektronisk signatur, de såkalte proxy tickets, med symmetrisk kryptografi (som kan erstattes med offentlig nøkkel kryptografi).

Systemet har en hierarkisk arkitektur, der ulike avregningsservere har ulik grad av autoritet ("trust") i det å klarere betalinger. En "vanlig" avregningsserver vil inneholde konti til f.eks. brukere eller selgere og i tillegg ha en "corresponding account" til nærmeste (i hierarkiet) betalingsklareringsserver. En slik server vil inneholde konti til "vanlige" avregningsservere og vil ha som oppgave å avregne betalinger dem imellom.

NetCheque er et rendyrket betalingssystem og det er foreløpig uklart hvordan det skal integreres med selve tjenestene som skal benytte det. Et slags felles API forespeiles uten at dette er omtalt mer detaljert.

Programvaren betalingssystemet baserer seg på vil, ifølge Neuman og Medvinsky, bli gjort fritt tilgjengelig for ikke-kommersiell bruk (?) og den vil være tilgjengelig på en ikke-eksklusiv lisens for kommersiell bruk.

2.3.1 Autentisering og ordrebehandling

Ved betaling av en vare vil brukeren fylle ut en elektronisk sjekk med følgende opplysninger : beløp, valutaenhet, gyldighetsdato, kontonummer, navnet/identifikasjon av betalingsmottaker. Denne informasjonen skal være leselig for utstederen av sjekken. Noe av den vil bli fylt ut automatisk av systemet. I tillegg vil sjekken utstyres med en elektronisk signatur av utstederen. Sjekken vil også bli "påført" elektroniske signaturer til de avregningsservere som har behandlet den underveis til mottakeren. Disse signaturer skal alltid kunne valideres av serveren som inneholder kontoen som skal belastes.

2.3.2 Kontering

Når sjekken har blitt utfylt og påført elektronisk signatur (som inkluderer en sjekksum generert av sjekkens innhold) vil sjekken bli kryptert med en 64bits nøkkel og sendt til betalingsmottakeren via elektronisk post eller direkte online. Mottakeren vi opprette en kryptert forbindelse til sin avregningsserver. Sjekken, signert av mottakeren, vil bli deponert på serveren.

2.3.3 Betalingsformidling

Dersom kjøperen og selgeren benytter den samme avregningsserveren, vil avregningen skje umiddelbart, og selgeren vil få tilbakemelding om at kontoen hans er godskrevet sjekkens verdi. Dersom dette ikke er tilfelle, vil sjekken bli sendt gjennom serverhierarkiet for å bli "hevet". Mens dette skjer, vil beløpet som sjekken er utstedt på bli "holdt" på mottakerens konto, dvs. han får ikke tilgang til disse pengene før man får bekreftet at sjekken var god og at pengene kan overføres fra kjøperens konto. Dersom sjekken viser seg å ikke ha dekning, vil den bli returnert til mottakeren som da må kontakte utstederen.
Klarering av sjekker skjer vanligvis offline, men mottakeren av en sjekk kan kreve at denne klareres online, dvs. umiddelbart. Dette vil trolig medføre an avgift, for å unngå overbelastning av systemet.

2.3.4 Samlet vurdering

NetCheque er et rendyrket betalingskonsept, derfor er det vanskelig å direkte sammenligne det med konsepter som FV og Open Market, der betalingssystem er integrert med et tjenestesalg-system.

Fordelen ved NetCheque synes å være dens distribuerte arkitektur, der man introduserer flere avrgeningssentraler og derved unngår en "flaskehals". I prinsippet vil hver enkel organisasjon ha sin egen "elektroniske bank" ved å etablere en intern NetCheque-server. I testfasen som skal starte med det første vil dog kun én avregningsserver (hos ISI) være tilgjengelig for brukere av systemet.

Sikkerheten ved systemet er god, selv om bruk av symmetrisk kryptografi baserer seg i stor grad på tillit. Designere av systemet påstår at offentlig nøkkel kryptografi kan introduseres i systemet, men da vil ytelsen lide.

En ulempe ved systemet er at det baserer seg på Kerberos-programvaren, som er en "forbudt" eksportartikkel fra U.S.A. pga at den inneholder kryptoteknologi. Dette gjør systemet lite aktuelt utenom U.S.A.

Et usikkerhetspunkt er strukturen i den foreslåtte API for tjenesteleverandører - det er uklart hvor egnet den er for enkel integrasjon med ulike informasjonstjenester.

2.4 NetBill

NetBill er et konsept fra Carnegie Mellon Universitetet i Pittsburg, USA. Det er ikke noen operativ tjeneste i dag, men de har kommet så langt at det eksisterer prototyper på programvaren som skal brukes i NetBill. Dette konseptet har spesielt prøvd å håndtere to problemer i forhold til løssalg av informasjon over Internett. For det første, hvordan kan man komme ned i transaksjonskostnader for overføring av penger i nettet som gjør det rasjonelt å selge informasjonstjenester som kan ha priser på ned mot 10 cent? Og for det andre, hvordan kan man få til kommunikasjon mellom kjøper, selger og NetBill som sikrer at kjøperen får den informasjon hun har betalt for, og at selgeren får betalt for den informasjon hun gir fra seg?

2.4.1 Autentisering

NetBill har ikke noe eget system for autentisering, men tenker seg å integrere eksisterende løsninger i sitt brukergresesnitt.

2.4.2 Ordrebehandling, fakturering og betalingsformidling

I NetBill-løsningen er det arbeidet med de spesielle problemer løssalg av elektronisk informasjon over nett skaper i forhold til når og hvordan betaling skal foretas, og hvordan kommunikasjon av informasjon og betaling kan foregå når man er avhengig av ustabile nett og maskiner. Problemet er i korthet dette at kjøperen nødig vil betale for informasjonen før hun kan se den og selgeren vil ikke gjøre informasjonen tilgjengelig før hun har en sikkerhet for at den er betalt. Løsningen på dette problemet er skissert i NetBill ved kryptering av informasjon og betaling, samt bruk av sjekksummer. NetBill har også lagt opp hvordan prosedyrene skal være for de forskjellige maskinene ved maskinstans og kommunikasjonsproblemer.

Konseptet til NetBill inneholder egne mekanismer for prisingsforespørsler. De tenker seg at det vil være behov for fleksibel prising, slik at kjøperens ved forespørsel om pris, starter opp en applikasjon hos selgeren som kan beregne pris for nettopp denne kjøperen. Når kjøperen da aksepterer prisen, er det en forpliktene avtale. Kjøperen mottar så informasjonen i kryptert form, uten nøkkel. Kjøperen sender så betalingen sammen med en sjekksum. Denne går til NetBill som kontrollerer at sjekksummen er riktig (det er en garanti for at kjøperen har mottatt riktig informasjon). Da sendes en kvittering til selgeren om at hun har fått pengene for sin informasjon, og selgeren sender over nøkkelen for at kjøperen skal kunne dekryptere informasjonen.

2.4.3 Kontering

Som tildligere nevnt må både kjøper og selger ha konto hos NetBill. Disse opprettes ved at NetBill sender over nødvendig programvare, digitalt signert. Programvaren vil være tilpasset brukerens Web-leser. Programvaren vil være et hjelpemiddel for å holde oversikt over kontoen for brukerne, og fungere som kommunikasjonsenhet mellom NetBill og brukeren. Brukeren må oppgi sitt kortnummer eller sin bankkonto for kreditering og debitering av kjøp og salg.
Modellen de har valgt for NetBill likner på kontomodellen som CyberCash har planer om å utvikle. NetBill tenker seg en tjeneste der brukerne, både kjøpere og selgere, må ha konto hos NetBill. Kontoen akkumulerer opp de små beløpene som skal overføres ved løssalg av informasjonstjenester på Internett. De ansvarlige for NetBill mener at prisen på en pengetransaksjon innenfor NetBill, dvs som kun innvolverer kjøper, selger og NetBill, vil ha størrelsesorden på én cent (dvs. omkring 7 øre). NetBill-koseptet baserer seg på at overføringene mellom det regulære bankvesenet (dvs. betalingssentraler og kortselskaper), og NetBill skjer i relativt større overføringer. Disse overføringene må skje relativt sjeldent, fordi det er belagt med kostnader som er store i forhold til prisene på informasjonstjenestene i nettet. Overføringene kan skje periodisk, i forhold til beløp som er innestående på kontoen i NetBill, eller ved behov. Kontoene hos NetBill kan i prinsippet stå med både positive og negative saldo, avhengig av den enkeltes avtale med NetBill.

2.4.4 Samlet vurdering

Her står vi igjen overfor en rekke planer, og ingen operativ tjeneste. Det er heller ikke lansert noen dato for når tjenesten skal startes, og hvem som skal være selgere i NetBill-systemet. De er imidlertid opptatt av at det skal være en lav terskel både økonomisk og teknisk for å kunne bli leverandør av informasjon på nettet, og mener det må kunne være mulig å gjøre forretning på nettet for det de kaller “micromerchants". De trekker fram Teletel (med minitel-terminalene) i Frankrike som et forbilde i så måte. På samme måte er de opptatt av at det må kunne foregå "micropayments" og mener at det med deres løsning er mulig å komme ned i én cent i transasjonskonstnader i en operativ tjeneste etter deres modell, og at det da vil være mulig å ha enkelttjenester som er priset til 10 cent. Dette er en formidabel ambisjon, og det er vanskelig å vurdere om dette er mulig så lenge konseptet ikke er kommet lenger i realisering. I alle fall er det klart at en så lav transaksjonskostnad vil være avhengig av gunstige avtaler med bankinstitusjoner, et meget stort volum av transaksjoner og fullstendig automatisering av behandlingen av transasjonene.

Det virker som om det er solid kompetanse bak den tekniske løsningen til NetBill. Det er gjort mye arbeid i den konkrete utformingen av en løsning som håndterer formidling av informasjon og betaling i en sammenheng. Løsningen virker noe komplisert, men brukeren vil ikke trenge å forholde seg til all den kommunikasjonen som foregår mellom maskinene i systemet. Problemet med når betaling skal foregå i sammenheng med når brukeren skal ha tilgang på informasjonen er sentral ved salg av informasjon over nett. Her er vi ved en fundamental forskjell mellom tradisjonell handel der man har mer håndfaste produkter å forholde seg til, og handel i elektronisk form. Det gjenstår å se om NetBills løsning vil fungere i praksis. Modellen indikerer at all informasjon mellom kjøperen og NettBill skjer gjennom selgeren, og da vil det ikke gi den nødvendige sikkerhet for at kjøperen betaler for noe hun ikke får, slik materiale fra NetBill påstår. Konseptet med at NetBill som en nøytral tredjepart har kontroll med både kreditering av selgerens konto, og nøkkelen til at kjøperen kan lese informasjonen som er kjøpt, virker imidlertid meget lovende. Da kan betaling og tilgjengeliggjøring av informasjon i praksis skje samtidig.

2.5 Downtown Anywhere

Downtown Anywhere er en markedsplass-konsept for handel over WWW. Bak konseptet står en amerikansk firma ved navnet AnyWare Associates, basert i Boston. Den samme firma markedsfører også epost-fax portnertjeneste ved navnet FAXiNET. Downtown Anywhere-konseptet er i enkelte aspekter nokså lik FV, ved at man baserer seg på belastning av kredittkort. Kjøperen må registrere seg på forhånd som kunde, oppgi sitt kredittkortnummer og e-post adresse der kvitteringer for foretatte innkjøp kan sendes. Ulikt FV, gis det også mulighet for forhåndsbetaling av penger inn på en “Internet-konto” hos DA. Kunden vil bli utstyrt med en “personal payment password” - en kode som identifiserer vedkommende som kontohaver hos DA. I tillegg må kunden kjenne til sitt kontonummer (8-sifret). Passordet og kontonummeret brukes for å overføre penger til sin konto hos DA og til å gjøre innkjøp. Penger som overføres til “Internet konto” hos DA vil siden bli innkrevd via kredittkort.

AnyWare Associates er også inngått en allianse med firmaet SoftLock Inc. basert i Malvern, Maryland i U.S.A. SoftLock-teknologien brukes også til å effektuere kjøp/salg over nettet. Et eksempel på hvordan dette virker er selve innmeldingsprosedyren for å få konto hos DA. Kjøperen får gjennom en WWW-leser form et såkalt SoftLock ID (et unikt nummer generert for henne). I tillegg må kjøperen kjenne produktnummeret til den varen/tjenesten hun vil kjøpe. For medlemskap hos DA er produktnummeret 001. Kjøperen kan så ringe en automatisk telefontjeneste i U.S.A. og, etter å ha oppgitt sine personalia, betalingsmåte (kortnummer og utløpsdato), produktnummer og SoftLock ID, få utlevert en SoftLock passord som kan brukes for å få tilgang til den ønskede varen/tjenesten - i dette tilfelle får man tilgang til sin egen innførsel i kunderegisteret og vil få tildelt kontonummer og PPP (Personal Payment Password).

Det er vanskelig å beskrive hvordan selve kjøpstransaksjonen forløper når man bruker sin DA-konto og PPP. Det virker som konseptet ikke er ferdig implementert og ikke støtter dette ennå. Ifølge firmaet bak konseptet, vil man, ved kjøp av en vare/tjeneste måtte oppgi kontonummer og PPP. Beløpet vil bli debitert ens DA-konto og siden innkrevd via kredittkort.

Selgere av informasjonsprodukter kan i tillegg benytte seg av SoftLock-teknologi for å beskytte seg mot uønsket spredning og også for direkte salg. Deler eller hele produktet skal kunne "låses" med SoftLock (som benytter en type checksum-baserte algoritmer kombinert med kryptering). Kjøperen må kjøpe en SoftLock-passord for å "låse" opp produktet. Kjøpet kan foretas via den automatiske telefontjenesten eller online(?). Vi har ikke kunnet finne eksempel på hvordan denne (online) prosedyren skulle foregå.

2.5.1 Samlet vurdering

Konseptet virker uferdig og bærer preg av at det er noen "typiske" Internett-travere som har gått hen og etablert en så kalt kommersiell tjeneste. Betalingsformidlingsopplegget virker uklart og uferdig. Informasjonen som er tilgjengelig gir ikke noe klart bilde om forpliktelser og rettigheter deltagelse i DA-sitt marked skulle innebære. Det ser heller ikke ut til at DA har mange registrerte kunder foreløpig. Vi anseer dette heller som et slags forsøk som befinner seg i en oppbygningsfase og der det trenges adskillig mer faste forretningsrammer rundt for at det brede publikum som handler på nettet skal kunne ha tillit til det.

2.6 CommerceNet/FSTC

CommerceNet er et konsortium av organisasjoner hvis formål er å etablere en elektronisk markedsplass på Internettet, der handelspartnere vil kunne gjøre forretninger over nettet . Organisasjonen skal arbeide for utvikling av en elektronisk infrastruktur som skal bidra til senkning av kostnader hos bedriftene ved at handel og delvis også leveranse av produkter skjer over datanett. Deltagende selskaper er primært SiliconValley høyteknologi firma samt utdannings- og forskningsinstitusjoner, i tillegg til banker og andre finansorganisasjoner. CommerceNet er 50% finansiert av offentlige bevilgninger (det såkalte Technology Reinvestment Project) og 50% av deltagere selv. Det totale budsjettet for tiltaket er 12 mill. US dollars.

CommerceNet har organisert sine aktiviteter i ulike arbeidsgrupper. Det ble dannet arbeidsgrupper for konnektivitet, verdiøkende nettverkstjenester (sikkerhet, betaling, TTP), kataloger, EDI (over Internett) og CIM / JIT-støtte.

Arbeidsgruppene skal diskutere problemstillinger innenfor de nevnte områder, fastsette prioriteter samt foreslå og gjennomføre pilot-uttestinger av de ulike tjenestene. Det skal også utarbeides defacto-standarder og så kalte best-business-practice veiledninger.

I tillegg skal CommerceNet tilby opplæring og bredt anlagte informasjonsaktiviteter rettet særlig mot Silicon Valley-bedriftene.

Selv om den grunnleggende gruppen av medlemmer i CommerceNet er organisasjoner fra Northern California / Silicon Valley, så kan enhver organisasjon bli medlem, forutsatt at man vil bidra finansielt og på andre måter. Organisasjoner utenfor U.S.A. kan kun delta som associate member eller subscriber (bruker av tjenester).

CommerceNet sine arbeider rettet mot betalingstjenester, sikkerhet og TTP konsentrerer seg i første omgang om SHTTP (Secure HTTP). Dette forutsetter bruk av "Secure Mosaic" klientprogramvare. CommerceNet vil etablere en Certification Authority (CA) for å administrere kryptonøkler for sine medlemmer. Medlemmene selv vil også kunne operere som CA-er.

Når det gjelder betaling, er CommerceNets første løsning sikker oversendelse av kredittkort-nummer, vha RSA, PKCS, 3DES og andre krypteringsalgoritmer.

Videre samarbeider CommerceNet med finansinstitusjoner for å tilby "ekte" banktjenester på nettet. En slik samarbeidspartner er FSTC (Financial Services Technology Consortium).

FSTC ledes av Citibank og inkluderer forøvrig American Express, AMS, Bank of America, Bank of Boston, BancOne, Bank of Montreal, Barnett Bank, Cardinal BancShares, Chase Manhattan Bank, Chemical Bank, CoreStates, Cybercash, Huntington Bancshares, MasterCard, Motorola, New York Clearinghouse, Okidata, NationsBank, Towers Group, VISA, Wells Fargo, NYCHA, U. S. Post Office, Lawrence Livermore, Los Alamos, Oak Ridge and Sandia National Laboratories, Bellcore, Columbia University, Polytechnic University, Stanford, University of California at Berkeley, AT&T, IBM, Unisys og Heuristics.

Formålet med konsortiet er å tilby elektroniske betalingssystemer, bl.a. på Internettet. FSTC er en ideell organisasjon, som skal støtte felles forskning og utvikling av betalingsfomidlingsinfrastrukturer for hele finansindustrien. FSTC er involvert i prosjekter under NII og HPCCI-initiativer fra amerikanske myndigheter.

FSTC arbeider for tiden med fire forskningsprosjekter:

1. Sjekk-imaging (scannede sjekker lenket med elektronisk informasjon om deres innhold) - oversendelse over nettet (for klarering bankene imellom)
2. Elektronisk handel understøttelse - utvikling av en "interbank" innkrevings- og betalingssystem for bl.a. Internett.

3. Elektroniske sjekker - ny form for elektronisk betaling
4. Svindelbekjempelse - forskning innen kryptoteknikker, biometri osv. for å sikre seg mot svindel
5. FSTCnet: tilgjengelighet på WWW.

2.6.1 Autentisering, betalingsformidling

Elektronisk sjekk-prosjektet er et samarbeid med CommerceNet og skal gjennomføres som pilot der. Konseptet baseres seg på offentlig nøkkel kryptografi for autentisering og digitale signaturer. De benytter også sjekksum for dataintergritetsbeskyttelse og i tillegg smartkort-teknologi på brukernes lokale PC-er (PCMCIA-kort og smartkort). eCheck-prosjektet til CommerceNet skal også ha grensenitt mot CyberCash og NetCheck. FSTC har også til hensikt å bygge direkte online forbindelser til eksisterende finansnettverk.

Brukeren vil ha sitt "sjekkhefte" på et smartkort som vil settes inn i en PC / smart-telefon for å kunne skrive ut en sjekk. Sjekken vil være en ASCII-tekst, signert av "sjekkheftet". Sjekken vil sendes online eller via elektronisk post til mottageren.

"Sjekkhefte-programvare" skal være kompatibel med e-post lesere, tekstbehandlere og spesialiserte finanspakker som Quicken (fra Intuit).

Det er noe uklart hvilket status prosjektet befinner seg i nå, men indikasjoner peker i retning en nær-forestående test av dette systemet på CommerceNet.

2.6.2 Samlet vurdering

Det er vanskelig å vurdere dette konseptet ut fra de få opplysninger som foreligger, men det bekrefter trenden mot "elektronisk-sjekk", som her støttes av tunge amerikanske finansverden-representanter. Dette vil åpenbart ha betydning for realisering av elektroniske betalingssystemer i stor skala.

3. Elektroniske penger

3.1 Ecash

Ecash er et forsøk med elektroniske penger i regi av DigiCash bv. i Amsterdam. Det er ingen virkelige penger involvert. Hvem som helst som har tilgang på Internettet kan skrive til DigiCash og få tilsendt "penger". Hver bruker får tildelt 100 enheter (såkalte "cyberbucks"). Denne lukkede økonomien er begrenset til 1.000.000 enheter totalt. Pr. 22/12/94 er det drygt 3.000 prøvebrukere, det vil altså si at over 300.000 enheter hittil er blitt distribuert. Det er foreløpig ikke satt noen grense for hvor lenge forsøket skal pågå.

Fremgangsmåte for å bli deltager i forsøket som bruker:

For å få penger må man skrive en elektronisk melding til DigiCash med en del opplysninger, hovedsakelig av systemteknisk karakter. I retur får man en e-post brev som inneholder passordet som skal brukes i kontakt med DigiCash. Dette passordet

gjør at man kan laste ned programvaren som trengs for å bruke de elektroniske pengene. I denne programvaren ligger det blant annet krypteringsnøkler og algoritmer. Ved forespørsel til DigiCash vil man da, ved hjelp av passord, få tilsendt standardbeløpet på 100 enheter.

Enhetene som man disponerer, ligger på en konto hos DigiCash. Hvis man vil bruke penger, må de først "tas ut" og legges i den virtuelle lommeboken ("cyberwallet"). Den vil ligge lokalt hos den enkelte bruker. Når man som bruker slår opp på en side som krever "betaling" i ecash, vil man få opp summen, og må eksplisitt godkjenne overføringen av enheter til mottagerens konto, før man får tilgang til informasjonen eller dataene.

Fremgangsmåte for å selge informasjon:

Når man har blitt registrert som bruker slik det er beskrevet over, har man i prinsippet det som trengs for å starte en "informasjonsbutikk". DigiCash har imidlertid programvare som kan hentes som gjør det forholdsvis enkelt å sette opp en slik butikk. Ved å sende en epost melding til DigiCash vil de inkludere butikken i sin web-side over butikker.

Hovedideen med ecash er at brukeren ("betaleren") er anonym. Ved hjelp av kryptering når data overføres og når de ligger lokalt hos brukeren og i "butikken", skal det ikke være mulig å spore opp hvem som "handler" i din butikk, og det skal ikke være mulig å snappe opp meldinger og "penger". Krypteringen er basert på offentlig nøkkel kryptering ("public-key encryption") (ref kommer).

Informasjonen man "kjøper" går over World Wide Web, men selve "pengehåndteringen" går utenfor Web med en egen kommunikasjonsprotokoll utviklet av DigiCash.

3.1.1 Autentisering

Brukerens ("kjøperens") identitet blir ikke sporbar i DigiCash. Det er det jo i prinsippet heller ikke behov for, idet beløpet krediteres "selgeren" umiddelbart. Slik sett er det sammenlignbart med kontanter. Det er imidlertid lagt inn en mekanisme som avslører brukerens identitet hvis hun forsøker å bruke de "samme" elektroniske pengene en gang til.

3.1.2 Ordrebehandling og fakturering

Brukeren av en informasjonstjeneste vil velge seg ut noe som hun vil kjøpe og klikke på linken til informasjonsenheten. Da vil det bli startet et script som ber brukeren godkjenne overføring av et beløp som er betalingen for informasjonen, eller alternativt avvise forespørselen om betaling og dermed ikke få informasjonen. "Betaling" skjer altså på forhånd.

3.1.3 Kontering

De fiktive pengene blir plassert på selgerens konto som ligger sentralt hos DigiCash. Ecash penger som kommer inn vil gå direkte inn på mottagerens konto, mens betaling alltid må skje via brukerens virtuelle lommebok. Denne lommeboken må brukeren fylle ved å overføre penger fra sin egen konto.

3.1.4 Betalingsformidling

Det er altså ikke reelle penger involvert. Man mottar 100 enheter som deltager og disse er lagret hos DigiCash. For å kunne bruke pengene må de tas ut av kontoen. Teknisk skjer dette ved at enhetene overføres (i kryptert form) til brukeren og lagres lokalt. Når brukeren skal betale for noe, vil enhetene overføres til mottagers konto sentralt hos DigiCash.

3.1.5 Samlet vurdering

Ecash løsningen fra Digicash illustrerer de mulighetene som ligger i kommersiell virksomhet i globale nett. «Penger» sendes som elektroniske meldinger i nettet. Som kjøper har man anonymitet overfor selger, og pengene kan gjenbrukes uten kostnader for brukeren på samme måte som kontanter. Det er heller ikke noe mellomledd mellom kjøper og selger i en transaksjon som ofte vil fordyre prosessen. Transaksjonskostnader vil eventuelt kun ligge i konverteringer mellom ecash og det tradisjonelle pengesystemet.

Elektroniske penger er den løsningen som i sterkest grad realiserer de nye muligheter som elektroniske nett gir når det gjelder pengetransaksjoner. Imidlertid er det knyttet problemer til hvordan man skal få aksept til å utstede elektroniske penger og til hvordan man kan sikre at elektroniske penger går tapt ved f.eks. tekniske problemer.

Når det gjelder selve forsøket med ecash er det en svakhet at det foregår uten reelle penger. Det er befengt med usikkerhet om man kan overføre erfaringene med brukernes oppførsel når det er «lekepenger» som er innvolvert, til en tjeneste som håndterer reelle penger.

Programvaren til ecash er ikke stabil. Programmet har ukontrollerte termineringer og det foregår ting som er utenfor brukerens kontroll. Systemet har ikke en modenhet i sin nåværende versjon som gjør at det i sin nåværende form kan brukes til virkelige pengetransaksjoner. Imidlertid har løsningen med elektroniske penger et betydelig potensiale, men det gjenstår en rekke juridiske og sikkerhetsmessige spørsmål som må avklares. I tillegg er det psykologiske sperrer ved å ha reelle penger elektronisk lagret som må overvinnes.

3.2 CyberCash

Det er vanskelig å si noe konkret om Cybercash systemet, fordi de ikke ennå har utviklet noen reelle tjenester. Cybercash ble etablert i 1994. De presenterer foreløpig bare planer for hvordan de vil ha betalingstjenester i Internettet. Cybercash Inc. tenker

seg to typer tjenester; ét system for kjøp av informasjon og varer over nett der selgerene er autoriserte for å ta imot kredittkort ("Authorized Merchant Services", som nedenfor er kalt Handel basert på kort) og ét system for mer åpen handel der alle i prinsippet som kan være både kjøpere og selgere av tjenester uten å være avhengige av kredittkort ("Peer-to-peer services", det som nedenfor er kalt "Handel vha. konto hos CyberCash").

Handel basert på (kreditt eller debet) kort
Cybercash tenker seg sitt første operative system baseret på bruk av debet eller kredittkort. De som vil være brukere av denne tjenesten, (enten det er som kjøper eller selger av informasjon eller tjenester), må for det første ha aksess til Internettet. I tillegg må kjøperen ha et kreditt- eller debet-kort, og det må være et kort som selgeren hun henvender seg til er autorisert til å ta imot og belaste.

Hvis overnevnte forutsetninger er på plass, skal kjøpere og selgere kunne henvende seg til CyberCash, og få lastet ned nødvendig programvare. Det er programvare som skal gjøre kjøpere og selgere istand til å kommunisere seg imellom og med CyberCash. Slik løsningen er tenkt implementert, skal CyberCash fungere som en organisasjon og leverandør av tekniske løsninger mellom kortselskap / banker på den ene siden, og kjøper / selger på den andre, men de skal også fungere som en tiltrodd tredjepart og en økonomisk og garantist mellom kjøper og selger.

Handel vha. konto hos CyberCash
Denne tjenesten er tenkt å skulle komme etter at tjenesten basert på kort har vært operativ i en tid.

Handel vha. konto hos CyberCash er basert på en annen modell for betalingstjenester i nettet enn modellen basert på kort. Kundene vil opprette en ikke-rentebærende, virtuell konto hos CyberCash. Kontoen fylles ved at brukeren belaster kontoen i sin bank. CyberCash tenker seg at pengene da fremdeles står i kundens bank, men at de er allokert til bruk som elektroniske penger for kjøp på nettet. Det virker som CyberCash først skal belastes kontoen i banken i forbindelse med at kontoholderen betaler for en tjeneste. Her har heller ikke CyberCash beskrevet noen konkrete løsninger, men de hevder at en fremtidig løsning ikke krever at mottageren av overførselen fra CyberCash-kontoen nødvendigvis selv må ha en slik konto.

CyberCash ser løsningen med handel vha. konto hos dem som en løsning for å handle for små beløp, beløp som er for små til å bli belastet kreditt- eller debet-kort på en konstnadssvarende måte. De tenker seg altså at handel ved hjelp av konto vil fungere som en utvidelse av handelen ved hjelp av kort, slik at CyberCash-kontoen vil i en fremtidig løsning bli brukt til små transasjoner, mens kort vil bli belastet og kreditert i forbindelse med større transaksjoner.

3.2.1 Autentisering

De har ikke noe konkret om autentisering i sitt materiale. Fra CyberCash hevder de imidlertid at brukeren ikke trenger å gjøre noen manuelle operasjoner for å identifisere seg. Det hele skal foregå automatisk, ved hjelp av den programvaren som en bruker skal kunne få gratis lastet ned til sin lokale maskin.

3.2.2 Fakturering og betalingsformidling

Når kjøper har bestemt seg, og prisen er klar, sender selgeren en elektronisk faktura til kjøperen, som hun fyller ut med kortopplysninger, og sender tilbake til selgeren. Selgeren vil imidlertid ikke kunne se kortopplysningene, men vil godkjenne handelen og sende fakturaen videre til CyberCash. CyberCash dekrypterer, sender melding til kortselskap om kreditering og debitering av kjøper og selger hvis det er etter kort-løsningen, alternativt krediterer og debiterer kontoer hos CyberCash hvis den løsningen er brukt. Det kommer en bekreftelse fra CyberCash til selgeren om at den økonomiske transaksjonen har funnet sted. Selgeren kan her velge selv på hvilket punkt hun vil oversende informasjonen som det betales for, det kan være når kjøperen har bestemt seg, når selgeren mottar den krypterte meldingen fra kjøperen, eller når selgeren mottar en bekreftelse på at den økonomiske transasjonen har funnet sted fra CyberCash.

3.2.3 Kontering

I kortløsningen til CyberCash er det kortselskapene som tar seg av konteringen i forbindelse med kjøp og salg. Når det gjelder handel med konto hos CyberCash er det naturlig nok CyberCash som selv vil håndtere kontering. Innskudd på kontoen blir gjort ved å belaste et kort eller en konto i en vanlig bank, og overføre pengene til CyberCash. CyberCash-kontoen vil ikke være rentebærende.

3.2.4 Samlet vurdering

Cybercash tenker seg at de skal få bankene til å betale for det meste av det transasksjonene skal koste. Men også kjøpere og selgere må betale noe. De sies lite om prising av betalingstjenesten i materialet fra CyberCash, bortsett fra at prisene på transasjonene vil bli konkurransedyktige og sammeliknbare med systemer for tradisjonell overføring av penger. De sies også at prisen på transasksjoner vha. CyberCash-konto beskrevet over, vil være sammenliknbart med porto på et vanlig brev.

Cybercash Inc. har lite konkret å vise til, de har planer om å ha sin første tjeneste operativ tidlig i 1995. Når firmaet likevel er trukket fram i mange sammenhenger når det gjelder kommersialisering av nettet generelt, er det nok fordi sentrale aktører innen bankvirksomhet (spesielt belastning av kreditt / debet-kort på salgsstedet), Internettet og elektroniske sikkerhetssystemer er blant stifterne av selskapet.

CyberCash har valgt en forholdsvis rett fram modell for å få til betaling i nett; de utvikler programvare for at kjøpere og selgere kan kommunisere på en sikker måte i nettet, og opptrer selv som et bindeledd mellom bankvesenet / kortselskaper og nettet. Det mest interessante ved deres konsept er ideen om å sende kryptert kontoinformasjon og identifikasjon fra kjøperen gjennom selgeren og til CyberCash. Det gir mulighet for at selgeren kan se at det kommer betaling for informasjon, samtidig som personvern blir opprettholdt i forholdet mellom kjøper og selger. Det gjenstår imidlertid å se om løsningen vil være god nok til at persovern blir ivaretatt, og tillittsskapende nok til at selgere vil føle seg sikre på at betaling er foretatt uten å se det i klartekst.

3.3 NetCash

NetCash er en utvidelse av NetCheque-konseptet beskrevet i kap. 6.3. I motsetning til NetCheque-konseptet, som ikke sikrer kjøperens anonymitet, skal NetCash gjøre dette, dog ikke i samme grad som den absolutte anonymitet som D. Chaums e-cash gir støtte for.

NetCash-konseptet baserer seg på bruk av sertifiserte valutatjenere, som skal kunne gi ut elektroniske penger. En valutatjeners funksjoner skal i tillegg omfatte verifisering av penger (for å avsløre forsøk på dobbelbruk), utveksling av penger for å oppnå ikke-sporbarhet samt veksling av penger i elektroniske sjekker og omvendt.

En valutatjener kan være implementert som en gruppe datamaskiner knyttet til nettverket med ett felles navn (domain name). Hver slik datamaskin (tjener) vil utgi et antall elektroniske penger med ulike valører. En elektronisk "mynt" vil bestå av valutatjeners navn og nettverksadresse, utløpsdato, et serienummer og valør, alt kryptert med valutatjeners private nøkkel. Mottakeren av "mynten" må ha valutatjeners sertifikat for å få tak i dens offentlige nøkkel, slik at mynten kan dekrypteres. Ved å dekryptere en mynt vil man kunne verifisere dens gyldighet, men for å sikre seg mot dobbelbruk må valutatjeneren kontaktes. Tjeneren vedlikeholder en liste over alle mynter som er i omløp. Dersom mynten skal kunne brukes legalt, må dens serienummer være på listen. Nummeret blir fjernet ved utløpet av gyldighetsdato og/eller når mynten "utveksles" mot en ny mynt (med nytt serienummer) for å kunne bruke den videre til nye kjøpstransaksjoner.

Dersom en mynteier prøver å verifisere en mynt mot en tjener som selv ikke har utgitt mynten, vil denne tjeneren kontakte den relevante tjeneren for å konvertere mynten. Til dette brukes den avregningsinfrastrukturen som NetCheque-konseptet baserer seg på, dvs. man utveksler mynt for elektronisk sjekk med tilsvarende verdi.

Forfattere av NetCash-konseptet hevder at det skiller seg fra ecash-konseptet ved at det introduserer en distribuert, global avregningsinfrastruktur (jfr. NetCheque), mens ecash baserer seg på én "sentralbank" som håndterer alle ecash-transaksjoner.

NetCash baserer seg på egenutviklede protokoller som involverer både offentlig nøkkel kryptografi og noe symmetrisk kryptografi. Det hevdes at disse protokoller kan erstattes med Chaums ecash protokoller dersom det er ønskelig, uten å måtte modifisere det øvrige rammeverket for konseptet.

3.3.1 Betalingsformidling

Når en kjøper vil betale en selger med NetCash må hun enten kjenne den offentlige nøkkelen til selgeren eller utveksle medlinger med selgeren får å få tak i en adhoc generert nøkkel til selgeren. Videre vil selve betalingstransaksjonen bestå i at kjøperen oversender til selgeren mynter sammen med identifikator for ønsket vare/tjeneste og en sesjonsnøkkel. Samtidig kan hun sende sertifikatet til valutatjeneren. Sesjonsnøkkel brukes for å sikre at den rette kjøper for varen/tjenesten. Selgeren sender tilbake til

kjøperen en "kvittering" betående av betalt beløp, tidsstempel og og en unik identifikator, som sammen med sesjonsnøkkelen kan brukes for å få varen/tjenesten.

En slik utveksling vil dog ikke garantere selgeren mot svindel (forsøk med betaling med allerede brukte mynter) og kjøperen mot å ikke besitte en gyldig kvittering.

For å oppnå slik sikkerhet, må betalingsprotokollen utvides. NetCash gjør dette ved å introdusere et nytt mynt-begrep, nemlig at en mynt skal kunne "spesialutgis" for en bestemt bruker som skal kunne bruke denne mynten innen en viss bestemt tid.

NetCash foreslår også løsninger for å unngå online validering av mynter. Denne protokollen innebærer imidlertid at betaleren må på forhånd vite hvilken selger hun vil kjøpe fra.

3.3.2 Samlet vurdering

NetCash-konseptet bærer preg av at det ennå ikke er ferdigutviklet som et selvstendig alternativ for realisering av elektroniske penger. Den grunnleggende protokollen kan sikre parters anonymitet, men den kan ikke sikre mot svindel dersom valutatjenere ikke kontaktes for utveksling av mynter hver gang en betaling er mottatt.

Som en fordel ved dette konseptet kan oppfattes dens distribuerte natur, og en mer realistisk kobling mot finansverdenen gjennom utnyttelse av avregningsinfrastrukturen som NetCheque representerer. Denne koblingen forårsaker imidlertid tap av anonymitet for brukeren, slik at NetCash gir svakere beskyttelse enn ecash.

Systemet forutsetter online validering av penger for å unngå svindel. Ved stor trafikk kan valutatjenere som gjør slik validering bli til flaskehalser. Nødvendigheten av kryss-validering mellom ulike valutaservere gjør ikke dette problem mindre.

3.4 CAFE

CAFE er et prosjekt gjennomført under ESPRIT III-programmet under det 3. rammeprogrammet for FoU i den Europeiske Union. Prosjektet ble påbegynt i 1991 og skal avsluttes i 1995. Målet for prosjektet var å utvikle systemer for elektroniske kontanter, så kalte elektroniske småpengesystemer. Vi nevner prosjektet her for kompletthets skyld, selv om det har aldri beskjeftiget seg med elektronisk handel over nett. Løsningene utviklet i CAFE skal kunne brukes til betaling av ulike typer tjenester som parkering, transport, kantinebruk osv. Sammenlignbare kommersielle systemer som nå er i prøvebruk er det engelske MONDEX-systemet og det danske Danmønt.

CAFE har utviklet ulike prototyper av elektronisk lommebok, basert på smartkort-teknologi og spesielt utviklet maskinvare fra bl.a. Siemens. Det grunnleggende konseptet for representasjon av penger er lik konseptet til DigiCash. David Chaum står også bak CAFE-prosjektet.

CAFE-lommeboken fylles med elektroniske penger som trekkes ut fra en bankkonto, slik man gjør med vanlige kontanter. Sånn sett representerer CAFE et forhåndsbetalt

småpengesystem. Lommeboken støtter også omregning mellom ulike valutasorter (etter en kurs som er gitt ved uttaket ev pengene).

Den mest avanserte lommeboken skal kunne kommunisere med mottaker-utstyret (f.eks. type POS-automater) via en infrarød forbindelse. Betaling skjer ved at elektroniske penger overføres (etter kjøpers godkjennelse) til mottakerens utstyr og derfra til mottakerens bank. Uttaket av penegene fra brukerens egen konto skal f.eks. kunne skje i spesielle "minibanker".

Fordelen med CAFE-løsningen er at den sikrer kjøpers anonymitet, da den tilsvarer kontanter, og at den gir høy sikkerhet, både for banken, kjøperen og selgeren. Sikkerheten ivaretas gjennom de spesielle krypteringsalgoritmer som brukes for å danne "pengene" og gjennom det at "pengene" er lagret i dedisert maskinvare som skal være vanskelig å "fikle" med.

Den enkleste varianten av CAFE-lommeboken er et smartkort. Konseptet skal i løpet av 1995 prøves ut i praksis i et begrenset forsøk i EU-kommisjonen i Bryssel, der lommeboken skal kunne brukes til betaling av kantinetjenester o.l.

Representant for prosjektet uttalte at de ikke har beskjeftiget seg med den spesifikke problematikken som elektronisk handel på nettet skaper (betaling vs. utlevering av varen), men at CAFE-konseptet kunne i prinsippet tillempes netthandel ved at man bygget inn lommeboken inn i PC-en, eller brukte smartkort-basert lommebok mot mottakerutstyr i PC-en, basert på PCMCIA-grensesnittet. Infrastrukturen på selgersiden er dog en helt annen problemstilling i denne sammenheng.

Det foreligger planer om videreføring av CAFE i et nytt prosjekt under det kommende ACTS-programmet under det 4. rammeprogram for FoU i EU.

4. Belastning av kreditt- og debetkort (sikkert kort)

4.1 Sikre kommunikasjonsprotokoller

Det er stor aktivitet rundt utarbeidelse av protokoller som tar hånd om en sikker kommunikasjon mellom to parter. Slike protokoller vil man kunne bruke for å overføre et kortnummer fra kjøper til selger på en betryggende måte. I vår sammenheng betyr det en sikker kommunikasjon mellom en selger og en kjøper slik at de kan være sikre på at informasjon ikke blir endret underveis (integritet) og at informasjonsutvekslingen er konfidensiell.

I forhold til World Wide Web betyr dette sikker kommunikasjon mellom en klient-maskin og en tjener-maskin. Det er i dag flere initiativer som tar sike på å bli internasjonale standarder på dette området. De viktigste er Secure HTTP som blant andre EIT (Enterprise Integration Technologies) og CommerceNet er med på å utvikle, og Secure Sockets Layer (SSL) som er integrert i Netscapes WWW-leser.

Disse to standardene håndterer sikkerhet på forskjellig nivå av kommunikasjonen og kan brukes sammen uten å komme i konflikt med hverandre. SSL befinner seg som en tjeneste i selve nettet, mens SHTTP er en sikker protokoll for såkalt ende til ende kommunikasjon for WWW.

Brukere av SHTTP-protokollen må sende noe informasjon "ubeskyttet" over nettet for å etablere en sikker forbindelse (den såkalte forhandlingsfasen), mens dette ikke er nødvendig ved SSL. SSL er integrert med Netscape, som for tiden er den mest populære WWW-leseren. En amerikansk undersøkelse viser at omkring 75% av brukerne på WWW anvender denne. Slik SSL er implementert i Netscape i dag, kan brukeren velge sikker kommunikasjon, men er da avhengig av at tjenermaskinen også forstår SSL, og det vil si har Netscapes tjener-programvare med SSL (Netscape Communications markedsfører denne som Secure Commerce Server).

SHTTP er er utvidelse av HTTP og er selvfølgelig avhengig av det er den protokollen som brukes i kommunikasjonen. Ellers er SHTTP bygget opp fleksibelt ved at man som bruker kan velge hvilke deler av protokollen som skal tas i bruk: de som støtter hhv. integritet, autentisering og kryptering. Dette avgjøres i en forhandlingsfase mellom klient og tjenermaskin.

4.1.1 Samlet vurdering

I tillegg til de ovenfor omtalte forslagene til SHTTP og SSL, foreligger det et forslag fra CERN kalt Shen, som også fremmer utvidelser til HTTP for å gjøre den sikker. IETF (Internet Engineering Task Force) har i desember 1994 etablert en egen arbeidsgruppe for utvikling av krav og spesifikasjoner som skal gjøre HTTP til en sikker protokoll. Denne gruppen er altså nylig etablert og det er åpenbart at flere, tildels konkurrerende løsninger ligger på bordet. Dette gjør at betalingssystemer som skal basere seg på sikker HTTP ligger noe fremover i tid, i det en må først bli enig om hvilken standard som skal legges til grunn. En mulig utvikling er at en av de foreslåtte løsningene vil vinne frem som de facto standard, f.eks. ved at CommerceNet kjører storskala test av SHTTP, men dette er det vanskelig å spå om. Netscape sine løsninger forutsetter foreløpig at deres server-programvare kjører i selger-enden - og dette kan jo være en for hard begrensning (deres Commerce Server selges for USD 5000). Uansett hvilke av forslagene som vinner frem, vil sikker kommunikasjon over WWW, som all annen sikker kommunikasjon, avhenge av etablering av tilhørende infrastruktur for administrasjon av offentlige nøkler mv. (se kap. 6).

4.2 WaveNet

WaveNet leveres av Wave Systems Corp. i New York. Ideen med WaveNet er å registrere bruk av informasjonstjenester. Dette er realisert ved å installere en brikke ("chip"), kalt WaveMeter, i hver maskin som knyttes opp til nettet. WaveMeteret vil også være i stand til å registrere bruk av applikasjoner derved gi et grunnlag for å belaste en kunde ut fra faktisk bruk av programvare. Nedenfor vil vi omtale det som har med salg av informasjon å gjøre.

De som vil tilby informasjon over dette nettet må tilrettelegge og kryptere informasjonen med hjelpemidler og krypteringsnøkler fra Wave. Leveringen av data

skjer over en proprietær kommunikasjonsprotokoll. De har løsninger både over satelitt (såkalt InfoWave, da må brukeren ha en parabolantenne) og via telenettet (AT&T og MCI).

WaveNet er en infrastruktur, og de har blant andre advokatkontorer som kunder.

Bruk av WaveMeteret vil gjøre at en mengde opplysninger blir registrert om hva kunden bruker av informasjon, samt når og hvordan bruken foregår.

WaveNet er også rettet mot å utvikle en sikker tjeneste som er vanskelig å tappe og å misbruke på andre måter. De understreker at de har en proprietær kommunikasjonsprotokoll, noe som gir mindre sjanse for misbruk og "innbrudd" i dataanleggene hos den enkelte bruker eller informasjonsleverandør.

4.2.1 Autentisering

Autentisering er sikret ved at hvert WaveMeter som leveres av Wave har en identifikasjon som knytter brikken til en bruker. Slik vil alt brukeren anvender av informasjon registreres på denne identifikasjonen.

4.2.2 Ordrebehandling

Hvis man mottar satelittnettet WaveNet, vil brukeren ha et såkalt interesse-filter som utformes etter brukerens interesseprofil. Da vil informasjonen enten bli avvist, akseptert eller satt på venteliste som mulig interessant informasjon, alt etter hvordan det blir mottatt av det automatiske filteret. Det gjør at brukeren ikke trenger å ta stilling til informasjonen når det sendes over satelittnettet.
Over telenettet vil brukeren foreta databaseoppslag hos den enkelte informasjonsleverandør, via WaveNet

4.2.3 Kontering

WaveMeteret vil registrere all bruk av informasjon og holde rede på hvor mye brukeren skal belastes med. Fra WaveNet blir priser og avgifter hentet ned til WaveMeteret.

4.2.4 Fakturering

På periodisk basis blir opplysninger om hva som er brukt av informasjon på maskinen overført til WaveNet sentralt.

4.2.5 Betalingsformidling

Wavenet har et system for direkte belasting av kredittkort. Betalingen kan også skje på tradisjonell måte uten elektronisk kommunikasjon.

4.2.6 Samlet vurdering

WaveNet er en proprietær, maskinvarebunden løsning som gjør den vanskelig anvendelig for elektronisk handel på åpne, globale nett. Anvendt til lukkede nett kan den tilby høy grad av sikkerhet, men vil allikevel være utsatt med hensyn på fysisk manipulering og ødeleggelse. Betalingsformidlingen foregår i hovedsak på en tradisjonell måte, så WaveMeter er egentlig primært et konterings- og avregningssystem.

Referanser/Litteratur

1. The Meter Is Running (WaveNet) - fra Information Week + produktbeskrivelse av WaveNet (1994)
2. Program for IOLIM-konferansen, sesjon om betalingssystemer (des. 1994)
3. Betalingsadministrasjon i elektroniske markedsplasser, Halvor Nafstad, TF, 1.12.94
4. Elektronisk markedsplass - informasjon og handel i telenettet, Olai B. Erdal, TF, 17.6.94
5.Marketing Mosaic. The War has Begun. Internet World, oktober 1994
6. E-Money. That's What I Want. Wired, desember 1994
7. Electronic Banking Faces Numerous Hurdles, BYTE, desember 1994
8. How the Internet Will Change the Way You Do Business, Business Week, 14. november 1994
9. Achieving Electronic Privacy, David Chaum, Scientific American, 1992
10. Electronic Money. So Much for the Cashless Society, The Economist, 26.11.94
11. CyberCredit - New Deals To Verify Transactions over the Net (WWW-GNN)
12. First Virtual - Terms and Conditions for applying for an account with First Virtual. Hentet fra FV email-server 28.10.94.
13. Kredittkort på Internet. Nye WWW-protokoller åpner for Internet-shopping. Computer World Norge, 9.12.94.
14. Debitering av bruk av WWW-tjenester, Even Åby Larsen og Karlheinz Kautz, NR-notat, 1.12.94
15. An Introduction to Electronic Commerce, Jason Solinsky, MIT (hentet fra WWW/GNN)
16. Electronic Commerce on the World Wide Web. A Case Study., Blake Ives og Sirkka Jarvenpaa, (hentet fra WWW?)
17. Straight Talk on Electronic Commerce, Christopher Locke, Information Week, august 1994
18. Marketing on the Internet, Ogilvy & Mather Direct, Interactive Marketing Group (hentet fra WWW)
19. First Virtual General Frequently Asked Questions (fra FV email server 28.10.94)
20. Microsoft and Visa to Provide Secure Transaction Technology for Electronic Commerce (pressemelding, 8.11.94)
21. First Virtual Theory List of Frequently Asked Questions (17.8.94)
22. The ESPRIT Project CAFE - High Security Digital Payment Systems (foredrag på EXORCIS 94, Brighton, November 1994).
23. Installing and Using the First Virtual API Utilities (hentet fra FV ftp-server)
24. The Green Commerce Model, notat av Marshall T. Rose, Lee H. Stein, Einar A. Stefferud og Nathaniel S. Borenstein, 10.10.94 (hentet fra FV ftp-server)
25. Netscape Communiactions ships release 1.0 of Netscape Navigator and Netsite servers; 15.12.94, pressemelding (hentet fra WWW)
26. Bank of America to provide secure payment system over Internet using Netscape Communications Software; 5.12.94 pressemelding (hentet fra WWW)
27. MCI selects Netscape Communication's Secure software for new internetMCI service; 21.11.94, pressemelding (hentet fra WWW)
28. First Data brings secure payment processing to the Internet with Netscape Communications software; 11.11.94, pressemelding (hentet fra WWW).
29. The future is VISA - What's in store! Annonsering på VISAs WWW-sider

30. Selling information with First Virtual (TM); hentet fra WWW
31. Buying information with First Virtual (TM); hentet fra WWW.
32. SED - Secure Encryption Device, brosjyre fra Ised corporation
33. EFT heads down a new payments path, Bank Network News, v13, n9, september 1994
34. Technology: Card Payments Head into the Cyber Space, Credit Card News, oktober 1994
35. AT&T plans electronic directory service - Web partnerships, Corporate Billing Services Under Consideration (hentet fra AT&T WWW-server)
36. British Library Customer Update, august 1994
37. Nytt om databaser og databaseverter, DianeNytt, siste kvartal 1994
38. Internetworking Monitor av Scott Bradner: Has it turned into soup yet?, Network World, 3. oktober 1994
39. NetBank Info - generell informasjon fra NetBank Information Server
40. Doctor Bob's Internet Business Guide, Bob Rankin, desember 1994
41. OMI Customer Support Product Backgrounder, fra Open Market information server
42. Electronic Cash, Tokens and Payments in the National Information Infrastructure, XIWT rapport, CNRI, Reston, Va, U.S.A.
43. Off-line Electronic Cash Based on Secret-Key Certificates; Stefan Brands, CWI; Proceedings of the Second International Symposium of Latin American Theoretical Informatics, Valparaiso '95, 3-7 April 1995.
44. Electronic Cash on the Internet; Stefan Brands, CWI; Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security, San Diego, 16-17 Februar 1995.
45. UNINETT Kryptotjeneste, Odd Egil Orøy, Jon Ølnes, NR; foiler fra internt seminar, 27. januar 1995.
46. Anonymous Credit Cards; Steven H. Low and Sanjoy Paul, Bell Labs; Proceedings of the 2nd ACM Conference on Computer and Communication Security, Fairfax, Virginia, U.S.A., 2-4. november 1994.
47. NetCash: A design for practical electronic currency on the Internet; Gennady Medvinsky og B. Clifford Neumann; Proceedings of the First ACM Conference on Computer and Communications Security, november 1993.
48. Requirements for Network Payment: The NetCheque Perspective; B. Clifford Neuman og Gennady Medvinsky; Proceedings of IEEE Compcon '95, San Francisco, mars 1995.
49. Endorsements, Licensing and Insurance for Distributed System Services; Charlie Lai, Gennady Medvinsky, B. Clifford Neuman; Proceedings of the Second ACM Conference on Computer and Communications Security, november 1994.

Relaterte rapporter:

- Debitering i standardisert formidlingskanal. Nasjonal Infrastruktur for EDB, Prosjekt 5, Statskonsult, november 1991

- Sikkerhetsvurderinger for publikumstjenester. Nasjonal Infrastruktur, Prosjekt 6, Statskonsult, oktober 1991

- Kravspesifikasjon og vurdering av programpakker for UNINETT Kryptotjeneste. NR notat av Odd Egil Orøy og Jon Ølnes, juli 1994.

- Meldingssikkerhet. tiltrodde trdejeparter og digitale signaturer. Sluttrapport. Norsk EDIPRO, 7.12.94.

- Betalingsformidling. Rapport 1993. Norges Bank, mai 1994.

- NOU 1994:19 Finansavtaler og finansoppdrag.

- Norges Bank: Finansstatistikk. Utviklingstrekk i betalingsformidlingen første halvår 1994

- Et generelt pengekortsystem i Norge. Anbefalinger fra en arbeidsgruppe. Norges Bank, oktober 1993.

- ELBET Norge. Rapport fra en offentlig nedsatt arbeidsgruppe vedrørende elektronisk betalingsformidling., august 1992.

- The Internet and the European Information Industry, IMO Rapport, Europakommisjonen, IMPACT-programmet, septemeber 1994

- The Main Events and Developments in the Information Market. Draft Annual Report 1993. IMO Rapport, Europakommisjonen, IMPACT-programmet, septemeber 1994.