



Elektroniska pengar och elektroniska betalningar

Gabriela Guibourg

Innehåll

Förord	3
Bakgrund	5
Indelningsgrunder	7
Accessprodukter – kontobaserade system	8
Kontantbaserade system	9
Centralbanksaspekter	13
Penningpolitiska aspekter och seigniorage	13
Stabilitetsaspekter	15
Säkerhet	18
Några olika system	27
Kontobaserade system	27
Kontantbaserade system	32
Nätverksbaserade system	32
Kortbaserade system	34
Klassificering av systemen	42
Sammanfattning och slutsatser	44
Referenser	47
Företagsinformation	48
Ordlista	49

Förord

I denna rapport redogörs för utvecklingen och utvecklingstendenserna inom området elektroniska pengar. I rapporten diskuteras också aspekter på denna utveckling med särskild relevans för centralbanker.

Syftet är att belysa och stimulera diskussionen kring dessa frågor, och kan ses som en del av Riksbankens löpande bevakning av detta nya område. Rapporten har utarbetats av Gabriela Guibourg vid Riksbankens betalningssystemavdelning.

Bakgrund

Elektroniska pengar är föremål för stor uppmärksamhet från media, från allmänheten, och även från myndighetssidan. Många anser att vad vi ser idag är ytterligare ett steg mot högre effektivitet i betalningshanteringen, snarare än någon mer fundamental förändring. Andra menar att detta handlar om en mer djupgående omvälvning av betalningsväsendet och att vad vi bevittnar är en begynnande privatiseringsprocess av pengar.

Målet här är inte att besvara dessa djuplodande frågor utan snarare att beskriva den utveckling vi ser idag: vad det är för produkter som har kommit ut på marknaden, på vilket sätt dessa skiljer sig från redan existerande betalningsinstrument, vad de har för konsekvenser för betalningsväsendet samt vilken utveckling vi kan förvänta oss i den närmaste framtiden ?

Beträffande den framtida utvecklingen finns det vissa faktorer som talar för en relativt snabb spridning för dessa nya betalningsformer. De nya produkterna karaktäriseras av s.k. positiva nätverksexternaliteter, dvs. värdet för den enskilda individen av att ansluta sig till ett visst betalningssystem ökar med antalet redan anslutna användare. Av den anledningen anser många att utvecklingen kommer att bli exponentiell; växa långsamt till att börja med tills ett visst antal användare anslutits - upp till den s.k. kritiska massan - för att sedan växa mycket snabbt. Andra produkter som kännetecknats av positiva nätverksexternaliteter, som t.ex. Internet, telefon och fax, har följt det mönstret.

Utgivarna har också starka ekonomiska incitament att påskynda acceptansen och spridningen. Elektroniska betalningsmedel har stora kostnadsfördelar jämfört med pappersbaserade. De möjliggör dessutom en omfördelning av ränteintäkter från centralbankerna (minskat seigniorage) till bankerna (ökade floatintäkter). Det finns också stordriftsfördelar i de nya betalningssystemen: höga fasta investeringskostnader samt låga rörliga kostnader talar för större lönsamhet ju större volymen är. Bankernas prisättning kommer att styra användarna mot de nya produkterna.

Rapporten består av två delar. Den ena är inriktad på lämpliga klassificeringsgrunder, relevanta aspekter för klassificeringen eller sådana som kan tänkas vara av speciellt intresse för centralbanker. Utgångspunkten är att det finns en relevant klassificering utifrån två viktiga dimensioner: dels huruvida det är fråga om kontantbaserade eller kontobaserade system och dels huruvida de är kortbaserade (smarta kort) eller nätverksbaserade (digitala pengar). Den andra delen är inriktad på att ge fakta och information om de system som faktiskt är i bruk. Ambitionen är att ta fram information om sy-

stemens karaktäristik, spridningsgrad i olika länder och vilka aktörer som står bakom.

Indelningsgrunder

Först ett varningens ord beträffande klassificeringen. Den låter sig inte göras enkelt eftersom de olika systemen inte tillhör en kategori helt och hållet i enlighet med alla relevanta karaktäristika. Det kan också inträffa att ett system tillhör flera kategorier samtidigt. För att möjliggöra analysen ges först en beskrivning av de renodlade indelningsgrunderna. Avsikten är att fokusera på viktiga skillnader mellan olika system för att sedan ta upp nyanser eller undantag

Beträffande kontantbaserade system finns också ambitionen att differentiera systemen - inom en kategori eller över indelningsgränserna - i vilka avseenden de liknar respektive skiljer sig från fysiska kontanter, eller om de bättre låter sig definieras som inlåning. En sådan differentiering kan vara intressant mot bakgrund av diskussionen främst inom EU om huruvida värden inom kortbaserade system är att betrakta som inlåning eller ej.

Som en startpunkt för diskussion kan det vara lämpligt att se på några kännetecken för transaktioner med sedlar och mynt:

- de sker anonymt
- transaktionerna är inte spårbara
- omedelbar avveckling
- direkta transaktioner mellan säljaren och konsumenten sker utan inblandning av tredje part, dvs. transaktionerna sker off-line
- pengarna kan transfereras fritt mellan individerna
- lämpar sig bra för små transaktionsbelopp
- betalningar sker "face-to-face"

De uppenbara nackdelarna med sedlar och mynt är att de lämpar sig väl för brottslig verksamhet (anonymitet och icke-spårbarhet) och dåligt för distansbetalningar och för stora transaktioner. Vanliga inlåningsmedel övervinner dessa begränsningar men på bekostnad av högre transaktionskostnader eftersom de kräver inblandning av en tredje part. Dessutom uppstår finansiella risker, eftersom initieringen och avvecklingen av betalningarna inte sker samtidigt.

En första indelning av elektroniska betalningssystem kan göras med hänsyn till huruvida man syftar på att betalninguppdrag initieras och överförs på elektroniskt vis eller om man syftar på att värdet lagras elektroniskt och fristående från ett inlåningskonto. I den första kategorin ryms exempelvis Internet-anpassade kontokortsbetalningar.

Accessprodukter – kontobaserade system

Med accessprodukter avses konventionella banktjänster och -produkter som kredit- och betalkort, checkar mm. De nya elektroniska accessmetoderna fungerar med samma underliggande betalningsmedel, nämligen medel på ett traditionellt bankkonto. Enda skillnaden är att användarna kommer åt betalningsmedlen med hjälp av en PC och lämplig mjukvara. Betalningar och överföringar av pengar kan ske antingen över ett öppet nätverk som Internet eller över privata nätverk. Denna kategori rymmer även det som kallas för Internetbank. Elektroniska Internet-betalningar och Internetbank ses idag som två separata företeelser, men det är möjligt att de så småningom kommer att växa samman¹ - det finns ingen anledning att tro att konsumenterna skulle vilja ha skilda system, ett för tillgång till bankkonton och ett för elektroniska betalningar. För tydlighetens skull kommer dock frågan om Internet-bank att behandlas separat.

När det gäller elektroniska kontokortsbetalningar finns två olika skolor. Den ena bygger på tanken att Internet är ett osäkert överföringsmedium i den meningen att det är ett öppet nätverk och att kommunikationen lätt kan avlyssnas. System som bygger på den principen undviker överföring av kundernas kreditkortnummer över nätet. Denna information lagras istället på en betrodd tredjepartsserver (ofta en bank, men inte nödvändigtvis) som styrker kundens identitet och att denne har täckning för transaktionen. Exempel på sådana system är *First Virtual* och *Open Market*. Den andra skolan förlitar sig på existerande säkerhetsteknologi - asymmetrisk kryptering med publika/privata nycklar samt digitala certifikat/signaturer - och sköter all dataöverföring över nätet. Även om överföringen kan avlyssnas, kan inte den tydas av obehöriga utan tillgång till krypteringsnycklarna. Hit hör till exempel *CyberCash* och *SET*.

Den gemensamma faktorn för alla elektroniska kontokortssystem är att transaktionerna sker **on-line**, vilket betyder att varje transaktion måste auktoriseras efter kontokontroll av en tredje part (en server oftast hos utgivaren/inlösaren). Detta höjer transaktionskostnaderna dels pga det ställer större krav på kommunikationsflöden men också pga kommissionen till kortföretagen. Kontokortstransaktioner är därmed mindre lämpliga för små transaktionsbelopp och ännu mindre för s.k. mikrobetalningar². Kontokortsbetalningar är för närvarande det dominerande instrumentet för In-

¹ E-Commerce: A survey of existing e-commerce solutions.

URL: <http://www.internet-banking.com/>

² Mikrobetalningar är ett nytt begrepp som uppstått i Internet sammanhang. Det verkar vara svårt att operationalisera begreppet, men det handlar om mycket små belopp. Det finns olika bud av hur små betalningar måste vara för att kvalificera sig, det kan röra sig om bråkdelar av en cent.

ternet betalningar³. De antas accepteras lättare av konsumenterna, eftersom de redan är vana vid dem.

Jämfört med sedlar och mynt kan man säga att accessprodukter skiljer sig från fysiska kontanter i alla de viktiga drag som nämndes ovan. Transaktionerna är inte anonyma, de sker on-line och är fullständigt spårbara. Värdet är inte fritt transfererbart mellan individerna men distansbetalningar är möjliga. De lämpar sig mindre bra för små transaktioner.

Kontantbaserade system

Kontantbaserade system utgörs av de nya produkter som brukar betecknas som **elektroniska pengar**. De är förbetalda instrument där värdet representeras av lagrade elektroniska enheter. Där ligger också likheten med kontanter: instrumentet i sig representerar värdet till skillnad från kontobaserade medel där instrumentet - ett kort eller en blankett - inte innehåller något värde. Till den kontantbaserade kategorin hör både nätverksbaserade och kortbaserade system. Den viktiga distinktionen mellan dessa är, enligt BIS-rapporten "Security of Electronic Money", var lagringen av de elektroniska värdeenheter sker. I kortbaserade system lagras de i en integrerad krets inbakad i själva kortet. I nätverksbaserade system lagras värden direkt i en PC's hårddisk.

Nätverksbaserade system är utvecklade med siktet inställt på nätverksbetalningar, dvs digital handel, även om det också går att köpa fysiska varor på nätet, dvs. sådana varor som kan beställas och betalas över Internet men som kräver icke-digitala distributionskanaler. Kortbaserade system var från början tänkta att användas ute i detaljhandeln. Den distinktionen håller på att suddas ut genom utvecklingen av kortläsare kopplade till eller inbyggda i datorer. Den utvecklingen syftar till att göra även smarta kort lämpliga för Internet betalningar. Även om skillnaden mellan dessa system försvinner med tiden, är det i dagsläget viktigt att göra en distinktion mellan nätverksbaserade och kortbaserade system. Den lätthet med vilka de förstnämnda kan överföras över landgränserna gör också behovet av global harmonisering av regelverk ofrånkomligt.

En jämförelse med fysiska kontanter visar att både nätverksbaserade och kortbaserade system lämpar sig väl för små transaktioner. Några av dem (främst de nätverksbaserade) anses lämpa sig väl även för mikrobetalningar. I Internet-sammanhang är betalningsinstrument som kan stödja mikrobetalningar ett hett diskussionsämne eftersom det kommer att vara

³ E-Commerce; A survey of existing e-commerce solutions.
URL: <http://www.internet-banking.com/>

vanligt förekommande med väldigt små transaktionsbelopp inom handeln med informationsvaror. Dessa varor är speciella eftersom de består av digitala strömmar som kan mätas och prissättas i princip på samma sätt som vatten eller elektricitet. Det finns några system som specialiserar sig på den typen av transaktioner men de är inte särskilt utbredda.

Nätverksbaserade system befinner sig närmare fysiska kontanter än vad kortbaserade system gör i den meningen att de uppfyller flera av de uppställda kriterierna. Dock finns även på den punkten undantag.

Nätverksbaserade system: Här är paradexemplet e-cash (från företaget Digi-Cash). De erbjuder en hög grad av anonymitet. Konsumenten identifieras varken när denne lagrar de elektroniska värdeenheter i sin PC eller när han utför en transaktion. Värdeenheter är fritt transfererbara mellan individer. Transaktionerna är inte spårbara. Transaktioner med nätverksbaserade system sker alltid on-line. Utgivande bank/institut måste kontrollera varje transaktion för att förhindra att värdeenheter kopieras och används flera gånger, men banken har ingen möjlighet att ta reda på vilken individ som utförde transaktionen.

Kortbaserade system: det förbetalda värdet bokförs direkt inne i kortet och det finns inte nödvändigtvis en motsvarande länk till kundens bankkonto. Det finns en del skillnader mellan de olika föreslagna systemen. Generellt kan man säga att de inte erbjuder samma grad av anonymitet som nätverksbaserade. Användaren identifierar sig för utgivande bank när kortet inskaffas, men inte för säljaren vid inköpstillfället. Eftersom transaktionerna är spårbara till kortet och kortet till individen är korttransaktioner inte jämförbara med transaktioner med fysiska kontanter i anonymitetshänseende.

Transferabiliteten är också - med undantag för Mondex systemet - starkt begränsad eller obefintlig. De elektroniska värdeenheter kan bara överföras från konsumenten till säljaren en gång, sedan måste de lösas in av inlösande bank. Däremot skiljer sig dessa system från nätverksbaserade i det att transaktionerna sker **off-line**, dvs. betalningar sker direkt från kunden till säljaren utan att en tredje part blir inblandad för auktorisation. Den minskade säkerheten som off-line karaktäristiken innebär kompenseras med s.k. "tamper resistant" hårdvara inbyggd i kortet eller börsen. Huvudsyftet är att förebygga användarbedrägeri genom att förhindra manipuleringar med de elektroniska värdeenheter. Den typen av bedrägeri som annars skulle vara det största problemet vore att användarna kopierade och använde samma värdeenheter flera gånger. Den mest omtalade fördelen med smarta kort över andra kortbaserade betalningar är den överlägsna säkerhet som den i kortet inbyggda kretsen erbjuder. I själva verket var drivkraften bakom dess utveckling just att stävja de stora kostnader som uppkommer med korthantering på grund av bedrägeri och förfalskning.

Kretskortet är också överlägset magnetkortet i det att det kan lagra 10-100 gånger mer information⁴.

Bortsett från säkerhetsaspekten är skillnaden mellan transaktioner som sker on-line eller off-line intressant i den mån det har effekter på transaktionskostnaderna. Att anpassa kortbaserade system till on-line system skulle höja transaktionskostnaderna avsevärt och göra dem mindre lämpliga för små beloppstransaktioner - det skulle inte längre finnas någon fördel med dessa system jämfört med traditionella kortbetalningar. Vad beträffar transaktionskostnader är inte skillnaden mellan off-line transaktioner med smarta kort och on-line transaktioner med nätverksbaserade pengar särskilt relevant, beroende på att kommunikationkostnaderna i nätverksammanhang är mycket små.

Ytterligare en distinktion kan göras inom kategorin av kontantbaserade system. Oavsett var de elektroniska värdeenheter lagras kan dessa representeras på olika sätt. Antingen i traditionell bokföringsform där värdet krediteras eller debiteras beroende på transaktionstyp eller i form av elektroniska symboler/mynt av ett specifikt värde. Det första alternativet tillåter en hög grad av spårbarhet av transaktionerna medan i det andra sker transaktionerna anonymt.

Om kontantbaserade system kan man sammanfattningsvis säga att en jämförelse mellan dessa och fysiska kontanter inte är lika okomplicerad som fallet var för konventionella, elektroniskt accessbara kontomedel. Några system liknar fysiska kontanter mer, andra mindre.

Dessa indelningsgrunder kan utnyttjas för en preliminär klassificering av de faktiska systemen enligt följande:

1. **Spårbara och on-line:** alla kredit- och betalkort system.
2. **Spårbara och off-line:** elektroniska checksystem⁵ där användaren identifieras men ingen kontokontroll görs.
3. **Anonyma och on-line:** köparens identitet är skyddad men en kontroll görs vid transaktionen mot någon centraliserad databas.
4. **Anonyma och off-line:** i och med att de uppfyller just de två egenskaperna, står dessa system fysiska kontanter närmast.

⁴ Carol Fancher, IEEE SPECTRUM, "Electronic Payments". Också direkt information från Per Lindström från Europay Sweden.

⁵ Det finns i USA elektroniska betalningssystem som är checkbaserade, t.ex. CheckFree och NetCheque. Dessa tas inte upp eftersom de anses ha föga möjligheter att bli särskilt utbredda i Sverige.

Distinktionen görs mellan "spårbara" och "anonyma" och inte mellan "anonyma" och "icke-anonyma" eftersom system som är spårbara tillåter användaranonymitet, dvs en viss grad av anonymitet. Ofta kan man spåra transaktionen till ett kort och kortet till en individ. Anonyma system är sådana där transaktionerna inte kan spåras till en individ.

Generellt gäller att valet av karaktäristik innebär en avvägning mellan motsatta intressen. On-line transaktioner höjer säkerheten men höjer samtidigt kostnaderna. Konsumenterna har behov av att skydda transaktionernas anonymitet - exempelvis av integritetsskäl - men det kravet måste ställas mot kravet om ökad säkerhet som spårbara transaktioner innebär för både säljare och utgivare. Ett fullständigt revisionsspår är också viktigt från myndighetsperspektiv eftersom det minskar risken för kriminell användning i form av skatteflykt och penningtvätt. De elektroniska pengarna skulle visserligen vara mer användbara för konsumenterna om de vore fritt transfererbara, men också detta måste ställas mot säkerhetskraven.

Beträffande transferabiliteten finns det de som tror att det är bara en fråga om utvecklingsstadium. De första telefon- eller transportkortet som dök upp på marknaden innebar ingen intermediär verksamhet. Smarta kort av "closed loop" typen - sådana som bara tillåter betalningar från kund till säljaren - skulle enligt denna tolkning vara nästa steg i en utveckling som förväntas kulminera med enbart "open loop"system - de som också tillåter person-till-person betalningar - i omlopp⁶. Även om detta kan vara en tänkbar utvecklingsväg finns det, som påpekats, faktorer som talar emot, framförallt de större säkerhetsproblem som fri transferabilitet innebär.

⁶ Mike ter Maat, American Bankers Association, "The Economics of e-cash".

Centralbanksaspekter

Elektroniska pengar i olika former innefattar flera aspekter av intresse för en centralbank. Vissa av dessa aspekter kan vara gemensamma för alla kategorier av elektroniska pengar, andra kan vara mer system- eller kategorispecifika. Ambitionen här är att försöka belysa både de relevanta frågeställningarna och frågan om vilka systemkategorier som ger upphov till dessa. Av centralbanksintresse finns det framförallt aspekter att bevaka inom tre huvudområden: penningpolitik, seigniorage och säkerhet/stabilitet.

Penningpolitiska aspekter och seigniorage

Ett av resultaten från den genomgång som gjordes av centralbankerna i G-10 under 1996, och som publicerades i en särskild rapport⁷, är att det inte finns anledning till oro vare sig vad avser effekter på centralbankernas seigniorage - dvs. de vinster som tillfaller centralbankerna tack vare deras sedelutgivningsmonopol och som uppstår till följd av att sedlarnas nominella värde vida överstiger deras produktionskostnad - eller för penningpolitiken, åtminstone inte på kort- eller medellång sikt. Enbart effekterna av kontantbaserade system beaktades i det här sammanhanget, eftersom accessprodukter sågs som en ny elektronisk version av traditionella banktjänster. Ett problem som skulle kunna uppstå med en mer utbredd användning av elektroniska pengar är att penningmängdsaggregatet blir mindre användbart som intermediärt mål eller indikator. Detta skulle inte medföra några större svårigheter för Sverige eftersom det för Riksbanken är inflationstakten som är den direkta målvariabeln för penningpolitiken och inte utvecklingen av penningmängden⁸.

Om andra än banker eller institut som övervakas av centralbankerna är utgivare av elektroniska pengar kan penningmängdsaggregatets informationsinnehåll urholkas. En omfattande spridning av elektroniska pengar skulle kunna leda till underskattningar av mängden pengar i omlopp. En möjlig lösning - om än svår genomförbar - vore att alla utgivare oavsett status underkastades rapporteringskrav. Pengarnas omloppshastighet kan också påverkas om effektivare betalningsinstrument används i större skala. Fram till dess det har stabiliserat sig på en ny jämviktsnivå, vilket kan ta lång tid,

⁷ BIS, Implications for Central Banks of the Development of Electronic Money, 1996

⁸ Även om penningmängdsdefinitionerna varierar, omfattas alltid sedlar och mynt i omlopp.

medför detta att valet av en strategi baserad på penningmängden som intermediärt mål för penningpolitiken blir mindre lämpligt⁹.

"Elektronifieringen" av betalningsmarknaden och den tilltagande innovationshastigheten på den finansiella marknaden i form av Internet banking, aktiehandel över Internet m.m. leder också till att fler finansiella tillgångar blir tillräckligt likvida för att kvalificera sig som betalningsmedel. Tillgångar vars innehav tidigare grundades på spar- eller spekulationsbeteende, börjar i allt större utsträckning mobiliseras som betalningsmedel. Även denna utvecklingen urholkar penningmängdens informationsinnehåll. I USA, t.ex. har den tidigare huvudindikatoren visat sig underskatta inflationen. Federal Reserve har därför gått över till penningmängdsaggregat som inkluderar andelar i obligationsfonder. Visserligen kan alltfler tillgångar inkluderas i penningmängdsstatistiken, men eftersom det är svårt att avgöra hur stor andel av innehavet som används som pengar respektive finansiell förmögenhet, försämras dess informationsvärde.

En omfattande substitution mellan fysiska kontanter och elektroniska pengar leder till förlorade seigniorage-intäkter. Detta problem anses dock inte vara en anledning till omedelbar oro, eftersom spridningen förväntas bli begränsad under den närmaste tiden.

Enligt vissa bedömningar kan dock slutsatserna som dragits i G-10-rapporten innebära en underskattning av effekterna. Framför allt pekar man på att analysen inte beaktar vissa viktiga faktorer som påverkar hastigheten med vilken de nya elektroniska pengarna kan komma att sprida sig när den s.k. kritiska massan uppnås.

Med beaktande av dessa faktorer kan, menar man, effekten på centralbankernas inkomster och balansräkningar bli större och inträffa tidigare än vad som bedöms som sannolikt i BIS-rapporten. Dessutom anses elektroniska pengar ha en snabbare omloppshastighet. Följden av det är att för varje utgiven mängd elektroniska pengar, trängs en större mängd sedlar undan. För utvecklade länderna är dock seignioraget inte särskilt viktigt från statens perspektiv. Väl utvecklade ekonomier har mycket effektiva sätt att dra in skatteintäkter - centralbankernas seigniorageintäkter har därför en marginell betydelse i sammanhanget. Om förlusten av seignioraget är så stor att centralbanken inte längre kan självfinansiera sin verksamhet och måste istället förlita sig på statliga medel, kan detta dock ha en negativ inverkan på centralbankens självständighet.

⁹ Enligt kvantitetsteorin är $Y \times P = V \times M$, där V är omloppshastigheten, M penningmängden, Y är real output och P är prisnivån. Om statistiken för både M och V är mindre tillförlitlig minskar även tillförlitligheten av inflationsprognoser baserade på M .

Det kan också tilläggas att i BIS-rapporten har kontomedel som hanteras elektroniskt, dvs. access-produkter, utslutits från analysen. Utifrån ett seigniorageperspektiv, är det den sammantagna effekten på allmänhetens behov av sedelhållning som är relevant, varför det finns anledning att beakta den kombinerade effekten av bägge dessa faktorer.

Argument har framförts om att den minskning i centralbankens balansräkningar som en minskad sedelhållningskvot leder till, skulle kunna försvåra centralbankernas möjligheter att föra penningpolitik. Detta argument är inte välgrundat; centralbanker kan utföra öppna marknadsoperationer även med en starkt reducerad balansräkning t.ex. via terminsmarknaden. Dessutom kan centralbanken motverka minskningen av balansräkningen genom att ge ut centralbankscertifikat. Visserligen går centralbankerna under ett sådant scenario från räntefri till räntebärande finansiering av tillgångssidan vilket minskar deras ränteintäkter i motsvarande grad. Det finns emellertid sätt att motverka seigniorageförlusten, som till exempel införande av kassakrav på utgivning av elektroniska pengar eller på bankerna i allmänhet. Detta reducerar å andra sidan utgivarnas ekonomiska incitament vilket kan hämma utvecklingen. Dessutom skulle det vara nödvändigt att införa samma krav på utgivare som inte är kreditinstitut och harmonisera kraven internationellt - åtminstone för gränsöverskridande system - för att undvika konkurrenssnedvridande effekter.

Det bör påpekas att varken minskande seigniorageintäkter eller krympande balansräkningar är nya fenomen som uppstår i samband med elektroniska pengar. Det är snarare en fortsättning på en process som pågått i flera decennier i takt med att nya betalningsinstrument ersatt kontanter i allt större utsträckning. Centralbankerna har dock medel till förfogande för att hantera dessa effekter.

Stabilitetsaspekter

Centralbankernas roll beträffande övervakning och tillsyn är att främja betalningssystemets stabilitet och effektivitet, framförallt genom att identifiera och minimera uppkomsten av systemrisk. Elektroniska pengar är för närvarande medel som riktar sig till hushållssektorns transaktionsbehov. Många av de nu existerande systemen är accessprodukter som inte väcker nya frågor från ett övervakningsperspektiv. Det finns däremot säkerhetsaspekter som är nya för alla inblandade kategorier och som måste bevakas. Säkerheten i systemens utformning och administration är utan tvivel en mycket viktig fråga. Den behandlas i ett separat avsnitt.

Från tillsynsperspektivet debatteras intensivt frågan om vilka slag av institut som ska kunna få utgivarstatus, vilka minimikrav som bör ställas på dem,

samt i vilken grad det existerande regelverket täcker de nya produkterna. En relaterad fråga som också är aktuell är skapandet av ett s.k. "level playing field". Det gäller att anpassa regelverket så att vissa sektorer inte drabbas av omotiverade konkurrensnackdelar. Detta skulle till exempel kunna bli fallet om både banker och icke-banker skulle kunna vara utgivare samtidigt som enbart banker regleras med kapitaltäckningskrav, kassakrav, informations- och rapporteringskrav mm.

Interoperabilitet mellan olika system är en viktig faktor i samband med skapandet av rimliga konkurrensvillkor och främjandet av en utveckling som kan medföra stora effektivitetsvinster för betalningssystemet. Om inte interoperabilitetsbehovet tillgodoses är två scenarier möjliga. Å ena sidan kan många mindre omfattande system komma ut på marknaden vilket starkt skulle reducera konsumenternas acceptans av de nya produkterna och göra det svårt för något av dem att nå den kritiska massan. Konsumenterna kommer inte att vilja ha ett antal olika kort som endast kan användas på ett begränsat antal säljställen. Utan interoperabilitet är det andra alternativet att de stora marknadsaktörerna vars produkter redan nått en viss omfattning får en i princip skyddad marknadställning.

Allmänt gäller att den amerikanska inställningen är mer marknadsliberal och mindre regleringsbenägen än den kontinentaleuropeiska. Sverige liksom bl.a. Storbritannien och Japan har intagit en mellanställning. EMI slog fast i en rekommendation 1994 att endast kreditinstitut bör kunna få utgivarstatus för kortbaserade medel. Argumentet var att dessa medel i ekonomisk mening var att betrakta som inlåning. Oavsett dessa skillnader, är alla dock överens om att hot mot stabiliteten skulle kunna uppstå om omfattande säkerhetsbrister och/eller otillräcklig tillsyn av utgivarna förekom. Följderna skulle kunna bli stora problem med förtroendet från allmänheten för elektroniska betalningssystem.

Omfattningen av riskerna beror till stor del på hur utbredda systemen är. Förutom de spridningsfaktorer som diskuterades ovan finns det andra ekonomiska aspekter som avgör graden av acceptans för de nya produkterna. Grundläggande är hur pass väl de uppfyller pengarnas traditionella funktioner: som betalningsmedel, som värdebevarare och som värdemätare. Betalningsmedelfunktionen är viktigast om ambitionen finns att systemet ska få en viss bredd.

Elektroniska pengarnas användbarhet som **betalningsmedel** bestäms i sin tur av graden av acceptans i samhället. Även om det låter som ett cirkelresonemang så är detta en känd problematik. För att användarna ska efterfråga elektroniska pengar i stor omfattning måste det finnas ett stort antal potentiella användningstillfällen i form av butiker med nödvändiga terminaler mm - men för att butikis innehavarna ska vilja göra de nödvändiga invester-

ingarna krävs det att de kan räkna med en stor kundbas. I det sammanhanget är de föreslagna systemens begränsade transferabilitet en nackdel. För både butiksinnehavare som för kunder är det pris de måste betala för de nya produkter i termer av avgifter och förlorade ränteinkomster (jfr. vanliga bankmedel) ett viktig övervägande. Utgivarna har klart överlägsna incitament i form av float-intäkter och minskande kostnader för kontant-hantering som de får genom dessa instrument. Vinsterna beräknas dock inte vara stora i en första period då investeringsutgifterna är höga samtidigt som kundbasen är liten. För banker som är utgivare är också den hårdnande konkurrensen om kunderna drivande. Säkerheten är självfallet ett avgörande acceptanskriterium för alla inblandade parter.

Elektroniska pengarnas funktion som **värdebevarare** är beroende av dels tekniska faktorer: hållbarhet och teknisk tillförlitlighet som till exempel att någon teknisk störning inte leder till att de elektroniska värdeenheter plötsligt blir obrukbara, dels risken att utgivaren går i konkurs. En minst lika angelägen aspekt för centralbanker är risken för överutgivning av pengar med de följer det kan få för inflationen. När banker blir utgivare finns incitament till överutgivning eftersom de får floatintäkter på utgivna pengar. Enskilda institut (till skillnad från centralbanker) behöver inte ta hänsyn till en ökad penningmängds negativa konsekvenser på prisnivån. Marknadskrafterna kan å andra sidan komma att klara detta problem själva. Alltefter-som elektroniska pengar blir lönsammare som produkter kommer konkurrensen mellan utgivarna om konsumenterna att hårdna. Kampen om kunderna kan komma att tvinga fram räntebetalningar på utgivna pengar. Ökad konkurrens mellan utgivande institut kan leda till att de tvingas betala allt högre räntor på utgivna pengar vilket minskar vinstmarginalerna, dvs. skillnaden mellan de floatintäkter som utgivarna får på utgivna pengar och de räntor som de måste betala konsumenterna, minskar. Processen fortgår tills man uppnår en punkt där floatintäkterna blir lika stora som ränteutbetalningarna. Därmed försvinner de ekonomiska incitamenten till att ge ut mera pengar.

Många menar därför att de penningpolitiska farhågorna är starkt överdrivna. Bankerna har visserligen ekonomiska incitament att öka utgivningen av elektroniska pengar. Denna ökning av skuldsidan möjliggörs av en motsvarande ökning av tillgångssidan genom ökad utlåning. Men detta kan aldrig ge upphov till en ohämmad kreditexpansion så länge kreditefterfrågan är räntekänslig och det finns en centralbank som kan styra räntan. Allmänheten skulle inte heller absorbera obegränsade mängder av elektroniska pengar eftersom efterfrågan på pengar också är räntekänslig. Räntan är pengarnas alternativa kostnad och den är under centralbankernas kontroll.

Från övervakningssynvinkeln är effektiviteten i betalningssystemet en viktig centralbanksangelägenhet. På den fronten finns det övervägande goda ny-

heter. En stor potential av effektivitetsvinster finns att hämta i system med elektroniska pengar. För alla typer av Internet-betalningar sjunker transaktionskostnaderna dramatiskt. Beräkningar i USA visar att kostnaden för en typisk banktransaktion är ca. 1,00 USD, för en uttagsautomat är motsvarande siffra ca. 0,25 USD medan kostnaden för en Internet transaktion är ca. 0,01 USD¹⁰. Minskade transaktionskostnader räknas som ett av de starkaste motiven bakom bankernas intresse i Internet-banking. Framväxten av en stor global marknad över Internet ska också betraktas som en positiv utveckling som kan vara tillväxt- och handelsbefrämjande, med stora besparingar i termer av sök-, informations- och transaktionskostnader för alla parter. Utvecklingen av digitala betalningssystem som lämpar sig väl för det mediet är en nödvändig förutsättning för att det väntade genombrottet för elektronisk handel ska kunna ske.

Säkerhet

Både nätverksbaserade och kortbaserade system kan ge upphov till allvarliga säkerhetsrisker. Den största risken ligger i möjligheten för individer att föra in elektroniska värdeenheter i systemet utan att motsvarande belopp tagits ut från utgivande bank. Detta är förstas fråga om förfalskning av pengar vilket i sig inte är ett nytt problem. En ny komplikation uppstår emellertid eftersom äkta och falska elektroniska värdeenheter är omöjliga att skilja från varandra. Om falska pengar inte upptäcks när de används vid första betalningen kommer bankerna inte heller att göra det förrän de inser att det löses in mer elektroniska pengar än vad det finns täckning för.

Det finns två sätt genom vilken förfalskning kan ske. Antingen kan falskt elektroniskt värde skapas eller så kan ett äkta värdeenheter användas vid flera transaktioner, så kallat multipelt spenderande. För att lyckas med detta måste man på ett eller annat sätt kunna manipulera de anordningar där de elektroniska enheterna lagras, kretsen i korten, butiksinnehavarnas terminaler eller en dators minne. Den allvarligaste risken skulle uppstå om utgivande bankers krypteringsnycklar kunde avslöjas eftersom det skulle kunna ge möjlighet till förfalskning i stor skala. Enskilda konsumenter kan också drabbas om de mekanismer som skyddar deras behållningar brister. Elektroniska data kan också avledas eller stjälas från den "äkta" mottagaren under själva överföringen över telekommunikationsnät. I det sammanhanget är öppna nätverk som Internet mindre säkra än privata finansiella nätverk och kräver därmed omfattande säkerhetsåtgärder.

¹⁰ Siffrorna är hämtade från "Report on Electronic Commerce", Business Research Publications, Sep.1996.

Allvarliga brister i säkerheten kan leda till att "falska" enheter förs in i systemet och att allmänheten tappar förtroende för elektroniska pengar och bestämmer sig för att lösa in sina behållningar.

Riskerna hanteras i varierande grad i de olika systemen med hjälp av åtgärder som syftar att i första hand förebygga och i andra hand upptäcka och minimera vidden av faktiskt genomförda bedrägerier. Åtgärderna av förebyggande karaktär är oftast baserade på olika typer av **krypteringsteknologier**. I vissa fall - smarta kort till exempel - kompletteras krypteringen med att hårdvaruskydda lagringen av elektroniska värdeenheter. Detta gör manipulationen av data mycket svårt. En anordning som är motståndskraftig mot manipulation kan till exempel automatiskt radera alla elektroniska data vid otillbörlig användning. Även om sättet på vilket säkerheten hanteras skiljer sig mellan systemen, finns vissa säkerhetsegenskaper som anses vara kritiska för att upprätthålla en tillfredställande säkerhetsnivå. Dessa är:

- Konfidentialitet: med vilket menas skydd mot avlyssning av meddelanden¹¹. Detta är mycket viktigt när känslig finansiell information som till exempel kreditkortnummer skickas över öppna nätverk.
- Säker identifikation: användarna skyddas mot att individer utför transaktioner eller skickar meddelanden i någon annans namn.
- Integritet av meddelanden: syftar på skydd mot manipulation eller substitution av sända meddelanden. Garanterar att det meddelande som mottagaren får är detsamma som avsändaren skickat.
- Icke-förnekande: skyddar användarna mot att deras motparter i en transaktion förnekar att de själva gett auktorisation för transaktionens genomförande.

De tre sista egenskaperna brukar sammanfattas under kravet på "bestyrkande av äkthet" (authentication). Uppfyllandet av det kravet är första försvarslinje för att förhindra införseln av falska pengar i systemet. Framförallt måste terminaler kunna förvissa sig om att de kommunicerar med äkta betalningsinstrument som inte manipulerats, vare sig det är en dator eller ett kort. Detta sker med hjälp av krypteringstekniker och krypteringsnycklar. Kryptering är en teknik som används för att skydda en viss informations konfidentialitet och är allmänt mycket effektiv i att förhindra otillbörlig användning av elektronisk data. Den bygger på matematiska algoritmer som används för att chiffrera och dechiffrera meddelanden samt nycklar som används för att åstadkomma själva chiffrerings- och dechiffreringsproces-

¹¹ Elektroniska betalningar består av överföringar av digitala meddelanden över nätverk.

sen¹². För att kunna bestyrka sin äkhet måste ett betalningsinstrument kunna visa för terminalen att det känner till den utgivande bankens hemliga krypteringsnyckel. Terminalen måste också ha kännedom om den hemliga nyckeln för att kunna verifiera äkheten.

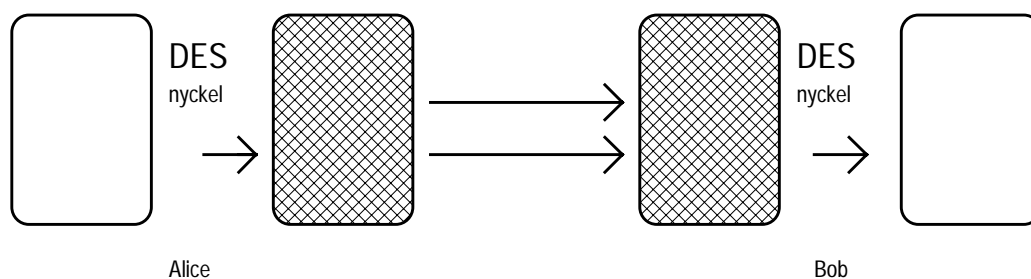
Det är viktigt att de åtgärder som är inbyggda i systemet kan stå emot en så kallad "replay attack". Man kan nämligen lura en terminal att den kommunicerar med ett äkta betalningsinstrument om man återanvänder ett tidigare betalningsprotokoll som avlyssnats och spelats in i en utskrift. För att komma undan det problemet använder sig de flesta systemen av ett så kallat "challenge-response" protokoll. Terminalen "utmanar" betalningsinstrumentet att bestyrka sin äkhet genom att presentera den med en slumpgenererad siffra på vilken en förbestämd beräkning måste tillämpas. Endast med hjälp av den korrekta nyckeln kan kalkylen beräknas. Betalningsinstrumentet slutför kalkylen och skickar över resultatet till terminalen som verifierar att det fått ett korrekt svar och därmed att den kommunicerar med en äkta motpart. Själva nyckeln överförs emellertid inte.

Sättet på vilket terminalen(eller mottagande betalningsinstrument) kontrollerar svaret och äktheten bestyrks skiljer sig åt mellan system som bygger på symmetrisk respektive asymmetrisk kryptering.

Symmetrisk kryptering bygger i allmänna drag på att båda parter i en transaktion delar på en hemlig nyckel vilket innebär att chiffrerings- och dechiffreringsnyckel är identiska. Säkerheten i sådana system är beroende av att den hemliga nyckeln inte avslöjas. Data Encryption Standard (DES), är ett exempel på en sådan teknik. Den utvecklades av IBM och används ofta för att uppnå både konfidentialitet och äkhetsbestyrkning. Säkerheten i de flesta kortbaserade system baseras på DES.

Ett allmänt exempel på hur symmetrisk kryptering fungerar: Det finns två transaktionsparter, Alice och Bob. Alice vill skicka Bob ett krypterat meddelande. Alice krypterar med DES nyckeln och skickar det chiffrerade meddelande till Bob. Bob dechiffrerar meddelandet från Alice med samma DES nyckel. Vem som helst som har kännedom om nyckeln kan också läsa meddelandet.

¹² BIS; Security of Electronic Money; 1996.



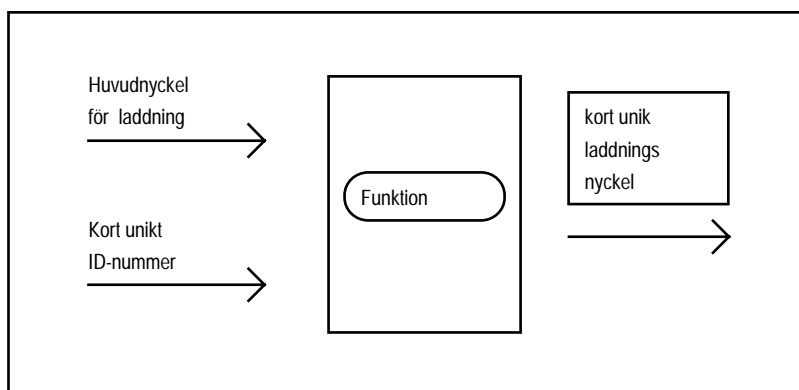
När äkthetsbestyrkande baserad på symmetrisk kryptering görs måste terminalen eller motparten i transaktionen ha kännedom om betalningsinstrumentets hemliga nyckel för att kunna räkna ut det rätta svaret på utmaningskalkylen och jämföra det med det erhållna. Den svaga länken i systemet är förvaringen av den hemliga nyckeln. Eftersom det är så viktigt att ingen kommer åt den hemliga nyckeln måste både terminaler och betalningsinstrument måste vara så konstruerade att de kan motstå manipulationsförsök. Nycklarna är hårdvaruskyddade och förvaras in i en krets som byggs in i korten och terminaler. Att båda parter i transaktionen delar på samma nyckel gör också att symmetriska krypteringssystem är mindre bra på att skydda användarna mot insider brott eller mot att deras transaktionsmotparter förnekar att transaktionen auktoriserats. Ena parten skulle kunna manipulera ett erhållt meddelande till sin fördel. Från den synvinkeln är det också viktigt att symmetriska system kompletteras med hårdvaruskydd mot manipulation.

Även om tämligen säkra manipulationshinder byggs in i alla betalningsinstrument- och anordningar vore systemet alltför sårbart om alla delade på samma nyckel. Vidden av konsekvenserna av att den nyckeln komprometteras vore så omfattande att ett sådant system skulle vara otänkbara. En lösning vore att olika betalningsinstrument hade olika nycklar men då skulle skalbarheten vara ett problem, dvs. systemen skulle aldrig kunna bli någorlunda omfattande. Det är omöjligt för terminaler att lagra ett stort antal nycklar.

Eftersom symmetriska krypteringssystem är sårbara för attacker på den hemliga nyckeln, finns det internationella principer eller standard för nyckelhantering. En av dessa principer är att använda olika nycklar för olika funktioner, en för laddning, en för inköp, o.s.v. Dessutom ska nycklar vara terminal- och kortspezifika så att om en nyckel komprometteras begränsas den potentiella förlusten till just det kortet eller terminalen. Man övervinner skalbarhetsproblem som nämndes ovan genom att använda ett system av huvudnycklar och härledda nycklar. Terminaler lagrar inga hemliga nycklar men istället en huvudnyckel som är slumpgenererat och som installeras av banken.

De kortspezifika nycklarna härleds från huvudnycklar när kortet görs personligt, d.v.s när användaren införskaffar kortet. Härledningen sker för varje funktionspecifik nyckel.

Grafiskt:



För att till exempel härleda den kortspezifika laddningsnyckeln tillämpas en aritmetisk funktion på en kombination av laddningsfunktionens huvudnyckel och kortets identifikationsnummer. Det resulterar i den kortspezifika laddningsnyckeln. Varje gång kortet används för laddning kan banken läsa kortets ID-nummer och med hjälp av huvudnyckeln och samma funktion beräkna det laddningspecifika numret.

För att ytterligare öka säkerheten används förutom kort- och funktionspecifika nycklar så kallade engångsnycklar. Engångsnycklar är en speciellt typ av härledda nycklar. Dessa härleds vid varje transaktionstillfälle från de kortspezifika inköpsnycklarna i kombination med kortets transaktionsnummer (varje kort har en inbyggt mätare som räknar transaktionerna). Terminalerna, försedda med lämpliga huvudnycklar, läser av kortets transaktionsnummer och inköpsnycklar och räknar ut en engångsinköpsnyckel. Nya transaktioner kräver nya nycklar¹³.

System med härledda nycklar övervinner problemet med att behöva installera ett ohanterligt antal nycklar i terminaler och framförallt risken med överföring av den hemliga nyckeln vid varje transaktion. Den sårbara punkten är huvudnyckeln¹⁴. Om en obehörig kan knäcka denna så kan den också simulera ett äkta betalningsinstrument.

¹³ BIS; Security of Electronic Money; 1996.

¹⁴ IEEE SPECTRUM; D. Chaum and S. Brands; Minting electronic cash; feb. 1997.

Asymmetrisk kryptering, också kallad "publik nyckel" eller RSA-teknologi¹⁵ övervinner problemet med hemliga nycklar. Den bygger på en rad krypteringsmetoder, bland annat ett system av nyckelpar och envägsfunktioner. Envägsfunktioner är konstruerade så att inversen är mycket svår att beräkna. Nyckelpar av publika och privata nycklar är länkade till varandra genom envägsfunktioner. Den publika nyckeln offentliggörs och den privata nyckeln hålls hemlig tack vare att kunskap om den publika nyckeln inte avslöjar någonting om den privata. Äkthetsbestyrkande sker fortfarande med en "challenge-response" protokoll. Svaret på utmaningen räknas ut med hjälp av den privata nyckeln, skillnaden ligger i att terminalen eller mottagaren verifierar att svaret är korrekt med hjälp av en matchande publik nyckel.

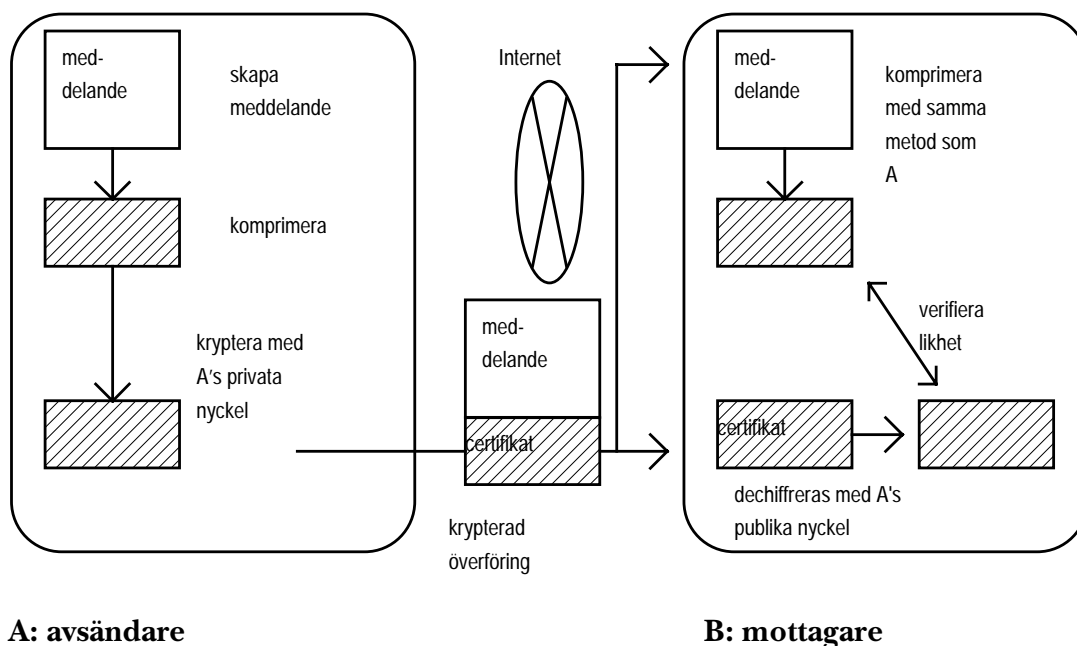
När användarna identifierar sig med hjälp av sina privata nycklar sägs det att de använder sig av **digitala signaturer**. En digital signatur uppfyller samma funktion i elektroniska meddelanden som handskrivna signaturer i pappersbaserade dokument. Man bevisar avsändarens identitet på ett sådant sätt att denne inte kan förneka sin signatur i efterhand. Eftersom digitala signaturer inte kan förfalskas och enbart användarna har kännedom om egna nycklar, löser denna teknik problemet med förnekande av genomförda transaktioner.

Bestyrkande av äkthet med digitala signaturer görs på följande sätt. Avsändaren komprimerar meddelandet med hjälp av speciell mjukvara och krypterar det komprimerade meddelandet med den egna privata nyckeln. Denna del är den digitala signaturen- också kallad digital certifikat- som bifogas till det ursprungliga meddelandet och överförs. Mottagaren verifierar den elektroniska signaturen genom att dechiffrera det komprimerade meddelandet med hjälp av avsändarens publika nyckel. Han komprimerar det ursprungliga meddelandet med hjälp av samma mjukvara och jämför det med det erhållna komprimerade meddelandet. Om de är identiskt lika kan mottagaren vara säker på att avsändarens identitet och på att meddelandet inte modifierades under överföringen¹⁶.

¹⁵ Rivest-Shamir-Adleman är namnen på de som utvecklade tekniken på MIT och som sedermera skapade ett eget bolag, RSA Data Security Inc.

¹⁶ Hitachi Research Institute; Electronic Money: Its Impact on Retail Banking and Electronic Commerce; F.I.A. Financial Publishing Company; 1997.

Grafiskt:



Hanteringen av krypteringsnycklar och digitala certifikat är fortfarande en potentiellt svag länk. Till exempel kan publika nycklar förfalskas. Av den anledningen uppstår behovet av neutrala organisationer vars funktion är att kontrollera nyckelhanteringen samt att garantera att rätt person har rätt nyckel. Det finns olika sätt att lösa detta på. Utgivande banker kan själva påta sig den rollen eller så kan den överlämnas åt specialinrättade certifierande myndigheter, så kallade "Certification Authorities" (CA). När certifikationsrollen lämnas över åt en tredje part finns för närvarande två alternativa system. Antingen hanteras det av en "betrodd tredje part", som är privata företag som opererar under internationellt överenskomna standards eller så kan statliga myndigheter ta på sig den rollen. De digitala certifikaten kan innehålla information om användarens namn, publika nyckel, giltighetsdatum samt namnet på den certifierande myndigheten.

RSA-teknologin används av nätverksbaserade- och Internetanpassade kortkortssystem. Bland dem räknas *e-cash*, *CyberCash* och *SET*. Den är lämplig för Internetsystem eftersom öppna nätverk kräver mer omfattande säkerhetsåtgärder. Praktiskt taget alla kortbaserade system baseras främst på DES-teknologin. Många smarta kort system säger sig vilja uppgradera sig till RSA men det är tveksamt huruvida detta är praktiskt genomförbart. Fördelen med symmetrisk kryptering är att transaktionerna processas mycket snabbare och kostnaderna per transaktion är lägre än om asymmetrisk kryptering används. En typisk korttransaktion tar cirka 20 sekunder att processa med

RSA-teknologi men mindre än en sekund med DES. Likaså framställningskostnaden för ett RSA-baserat kort är cirka 150 SEK, men bara 20 SEK för ett DES-baserat kort¹⁷.

Oavsett vilket krypteringssystem som används beror säkerheten i hög grad på längden på krypteringsnycklarna och på hur lagringen av krypteringsnycklarna hanteras. En viktig säkerhetsåtgärd är att använda krypteringsalgoritmer som utsätts för regelbundna granskningar av kryptoanalytiker. Krypteringsstyrkan testas genom att beräkna den tid och resurser som krävs för att knäcka en viss algoritm. Denna varierar med nycklarnas längd. För symmetriska system, rekommenderas idag nycklar på minst 90 bitar¹⁸. Nycklar på 128 bitar anses vara säkra mot avkodning en lång tid framöver. Asymmetriska system kräver längre nycklar. Nycklar på 1024 bitar anses erbjuda en mycket hög säkerhetsnivå idag. En ofta gällande säkerhetsprincip baseras på att minska de ekonomiska incitamenten till brottslighet. Enligt den principen bör säkerheten uppnå den nivå som innebär att kostnaden av att knäcka krypteringsalgoritmen vida överstiger den potentiella vinsten.

Syftet med krypteringsteknologin är att förhindra bedrägerier eller förfalskningar. Det finns emellertid en andra försvarslinje som går ut på att upptäcka brott efter att det skett. Ett exempel på sådana upptäcksåtgärder är statistiska analyser av betalningsflöden som underlättar upptäckt av onormala betalningar. Detta kan göras med hjälp av avancerad datateknologi, ofta tillämpningar av s.k. artificiell intelligens eller neurala nätverk. Dessa är tekniker som används för att åstadkomma inlärning av vissa mönster över tiden och som idag är vanliga inom kreditkort branschen. Med hjälp av dessa metoder kan betalningsflöden analyseras på olika nivåer. På övergripande system nivå, kan man lära in sig det normala dagliga mönstret av utgivning och inlösen. De normala betalningsflöden som tillfaller varje handlare kan också analyseras. Varje större avvikelse från normen leder mer detaljerade undersökningar¹⁹. Beträffande upptäcksmöjligheter av falska pengar eller andra typer av brott, är riskerna lika mycket avhängiga av systemens funktionssätt som av den använda tekniken.

Egenskaper som transaktionsanonymitet och transferabilitet mellan användarna är eftertraktade av konsumenterna men utgör samtidigt riskfaktorer. Spårbarheten av transaktionerna till transaktionskällan är en mycket viktig säkerhetsåtgärd när det gäller att upptäcka bedrägerier. Alla kortbaserade system tillåter spårbarhet, dock inte nätverkssystem som e-cash. Transferabiliteten tillsammans med icke-spårbarhet kan underlätta för andra typer av

¹⁷ Information från Jan-Olov Brunila från FöreningsSparbanken.

¹⁸ En grupp programmerare och forskare har nyligen lyckats knäcka en 56-bitar lång DES nyckel, som idag används för att skydda de flesta finansiella transaktioner. Wall Street Journal 19 Jun 1997.

¹⁹ BIS; Security of Electronic Money; 1996

brott som penningtvätt och skattefusk. Framförallt för system som är Internetanpassade kan dessa egenskaper höja risknivån eftersom de samtidigt erbjuder möjligheten till blixtnabba betalningar över landgränserna.

Säkerheten hos kortbaserade system²⁰ har kartlagts i den tidigare nämnda rapporten från BIS som kom ut 1996. I den dras slutsatsen att de nya systemen erbjuder en ganska hög säkerhetsnivå jämfört med den som gäller för traditionella betalningssystem. Det poängteras att säkerheten inte kan garanteras av någon specifik åtgärd eller teknik hur avancerad den än må vara. Viktigt i sammanhanget är snarare vilken kombination av åtgärder som väljs, för vilken typ av transaktioner, hur systemet administreras, formerna för produktion och distribution, interna kontroller m.m. Det påpekas också att systemens säkerhet bör uppgraderas kontinuerligt. Systemens säkerhetsaspekter bör också löpande granskas av lämplig tillsynsmyndighet.

²⁰ Ibid.

Några olika system

Systemen beskrivs nedan enligt den struktur som presenterades under avsnittet om indelningsgrunder. Kontobaserade system beskrivs först och därefter kontantbaserade system. Fakta om systemen har inhämtats från Web-information från aktörerna själva och från annat material²¹.

Kontobaserade system

FIRST VIRTUAL

First Virtual anser att det inte finns någon teknologi som kan övervinna de säkerhetsrisker som ett öppet nätverk innebär. Inte ens den starkaste krypteringen är tillräckligt säker p.g.a. risker med t.ex. "trojansk häst" angrepp. Det anses vara relativt lätt att smyga in ett program i någons dator som kopierar till exempel kreditkortsinformation i det ögonblick de skrivs ner, innan man hinner kryptera för överföring. FV påstår sig ha utvecklat ett virus som automatiskt kopierar sådan information samt att de har provat detta på alla existerande kryptobaserade system. Enligt deras utsago har alla visat sig sårbara för denna typ av anfall²². FV påstår att deras system, av den anledningen, är överlägset ur säkerhetssynvinkel. Känslig information skickas inte över nätet. Istället håller FV en databas med alla användares kontokort eller kontoinformation. Användarna (både säljarna och kunderna) måste registrera sig hos FV och får vid registreringstillfället ett ID-nummer som de använder för identifikation vid transaktioner och som inte kan kopplas till något fysiskt finansiellt instrument. Kontokortsinformation skickas per fax eller telefon vid registrering.

Alla meddelanden mellan säljare, kund och FV sker via e-mail. Fördelen är att det inte finns behov av speciell mjukvara eftersom man utnyttjar Internet för informationsutbyte som rör själva transaktionen. Själva avvecklingen av transaktioner sköts av FV genom existerande säkra nätverk. Det finns registreringsavgifter och säljarna betalar också en fast avgift plus en andel av transaktionsbeloppet vid varje transaktion.

Transaktionsegenskaperna liknar i allt väsentligt ett vanligt kontokortköp. Kunden är anonym inför säljaren under själva transaktionen eftersom han bara identifierar sig med ett ID-nummer. Transaktionen är dock fullständig

²¹ Dr. Andreas Schöter, Rachel Willmer; inter://trader, "Digital Money Online. A Review of Some Existing Technologies". Feb.1997. Olika artiklar i "Technology and the Electronic Economy" februari nummer av tidningen IEEE Spectrum. Hitachi Research Institute; Electronic Money: Its Impact on Retail Banking and Electronic Commerce; F.I.A. Financial Publishing Company.

²² CyberCash säger sig ha utvecklat en metod för att undvika problemet.

spårbar eftersom FV har information om varje transaktion och ID-numret är kopplad till ett vanligt bankkonto. Transaktionerna sker on-line.

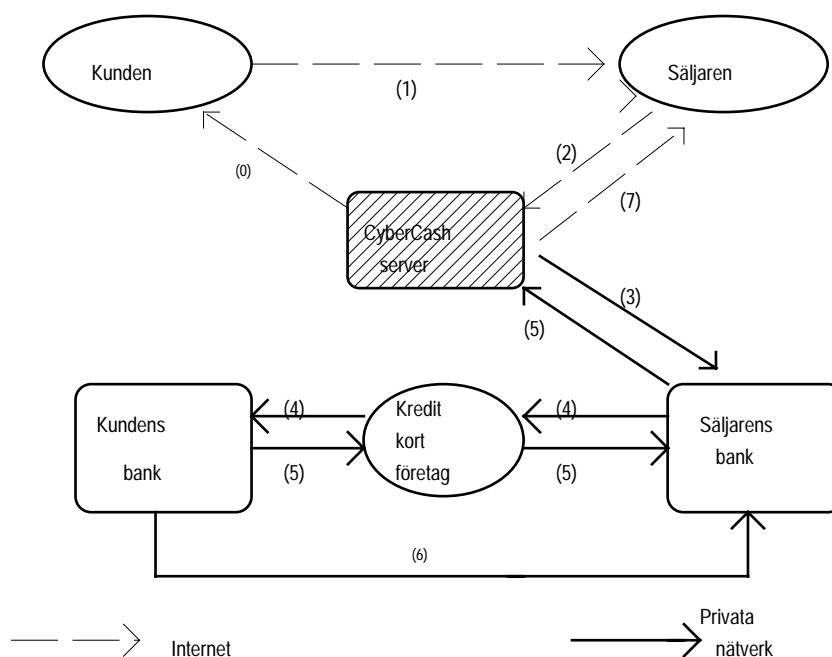
CYBERCASH

CyberCash liknar FV i den meningen att det också utnyttjar existerande finansiella nätverk men i CyberCash behöver både säljaren och konsumenten speciell mjukvara. Den andra skillnaden är att all kommunikation mellan transaktionsparterna och CyberCash sker i krypterad form. Detta beror på att kreditkortnummer skickas över Internet och måste därmed skyddas med krypteringsteknologi. CyberCash servern dekrypterar information innan den överförs till handlarens bank men då sker överföringen genom säkra kommunikationslinjer. Annars liknar transaktionen en vanlig betalning med kreditkort. En fördelaktig skillnad är att tack vare krypterad information förblir kundens kontokortsinformation hemlig för säljaren.

CyberCash fungerar som en intermediär (gateway) mellan säljaren och dennes inlösande bank. Kunden använder sig av mjukvaran "CyberCash wallet" för att generera en krypterad betalningsorder som skickas till säljaren.

Krypteringstekniken bygger på en kombination av symmetrisk och publik nyckelteknologi med 1024 bitar RSA nycklar. Avsändaren krypterar meddelandet med en hemlig nyckel som i sin tur krypteras med mottagarens publika nyckel. Denne lägger till sin digitala signatur och skickar vidare till CyberCash servern. Där tas transaktionen bakom Internets brandväggar, dekrypteras och skickas vidare till handlarens bank. Banken kommunicerar med kundens bank för auktorisation. Svaret skickas sedan till CyberCash. Hela transaktionen sägs ta cirka 15-20 sekunder. Transaktionsparterna identifierar sig med hjälp av digitala certifikat som de utbyter med varandra i varje skede av transaktionen. Transaktionerna är fullständigt spårbara och sker on-line.

Grafiskt:



(0) Kunden laddar ner mjukvaran CyberCash Wallet över Internet. Säljaren har en CyberCash Merchant Server. Bådas mjukvara innehåller transaktionshantering, transaktionslagrings system samt elektroniska certifikat och krypteringssnycklar.

(1), (2) Kunden krypterar sitt kreditkortnummer med Wallet och skickar det till säljaren som skickar i krypterad form till CyberCash.

(3) CyberCash servern avkrypterar informationen och skickar över till säljarens bank över säkra linjer.

(4), (5), Auktorisationsförfarande mellan kundens- och säljarens bank. Auktorisationen skickas till CyberCash servern som informerar säljaren.

(6), (7) Avveckling, elektroniskt kvitto .

Källa: Hitachi Research Institute.

Fördelarna för bankerna är att de utnyttjar befintliga säkra nätverk och för säljarna att det förlitar sig på existerande bankrelationer. Eftersom det underliggande finansiella instrumentet är ett kontokort lämpar det sig inte för små transaktioner. Av den anledningen har CyberCash lanserat två nya betalningsinstrument som ska ingå i CyberCash Wallet, nämligen CyberCoin och CyberCheque (CyberCheque är inte igång ännu men beräknas lanseras under 1997). CyberCoin sägs vara ett mikrobetalningssystem men den lägsta transaktionsgränsen är 25c som är en rätt hög gräns för att vara ett mikrobetalningssystem. Anledningen till den höga gränsen är att systemet använder asymmetrisk kryptering som fördyrar transaktionen. Dessutom måste handlarna betala en transaktionsavgift. Värdet är inte fritt transfererbart.

Samarbetspartner till CyberCash Inc är MasterCard, Visa Netscape, Sun, AOL, Comuserve, HP, IBM, Apple och RSA. 80 % av USA's banker kan

idag använda sig av systemet. De har i dagsläget 400 000 plånböcker ute på marknaden. CyberCash har fått tillstånd av den amerikanska regeringen för export av krypteringsteknologin vilket förbättrar deras globaliseringsmöjligheter²³.

SET (SECURE ELECTRONIC TRANSACTIONS)

SET är en gemensam teknisk standard utvecklad av Visa och MasterCard, men varje kortföretag planerar att utveckla sin egen produktversion av betalningssystemet. SET är en mängd protokoll som ger enhetliga standards för varje steg av den elektroniska handels- och betalningsprocessen och som beskriver kommunikationen mellan kunden, säljföretaget och banksystemet över Internet. Specifikationerna är öppna vilket innebär att det är fritt för vem som helst att utveckla egen mjukvara enligt SET protokoll. American Express har nyligen annonserat sin avsikt att följa SET standards.

SET och CyberCash fungerar på samma sätt och använder sig av samma krypteringsteknologi, dvs. en kombination av symmetrisk och publik nyckelkryptering med digitala certifikat. Certifikaten är ett behörighetssystem som avspeglar ingångna avtal mellan parterna. Det förutsätter i sin tur existensen av en hierarki av certifieringsmyndigheter. Fördelen för bankerna jämfört med CyberCash systemet är att de har större kontroll över systemet.

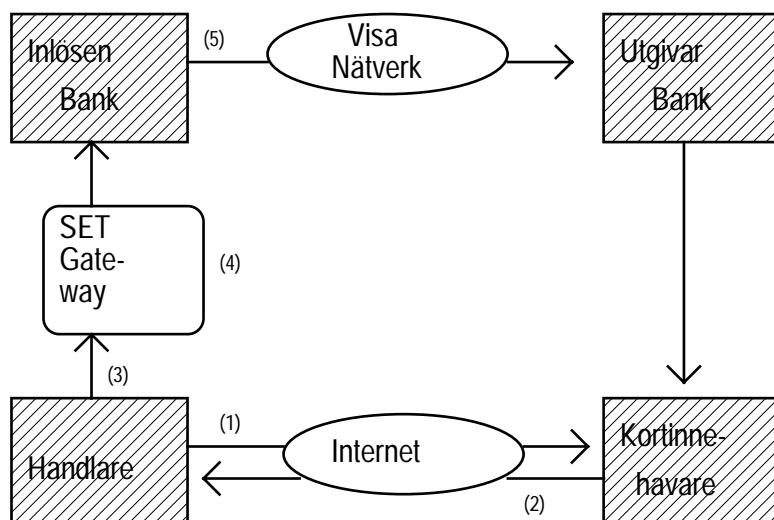
Tekniken är inte lämplig för små betalningar dels på grund av det inriktar sig på kontokortsbetalningar, men också på grund av att varje transaktion kräver ett utbyte av ett antal nycklar och certifikat vilket fördyrar transaktionen. Flera kända teknologiföretag samarbetar med Visa och MasterCard i SET projektet. Bland andra Microsoft, IBM, Netscape, Veriphone, GTE, Terissa Systems, SAIC och Verisign. Enligt flera bedömare anses SET vara det system som sannolikt kommer att dominera marknaden för Internetbetalningar.

Ett pilotprojekt i Sverige syftar till att använda SET standard för Internetbetalningar. I projektet ingår Sparbanken, S-E Banken, Handelsbanken, PostGiro Bank samt 38 utländska banker. Visa Interactive har huvudnyckeln och varje bank erhåller sin bankspecifika certifikatnyckel. Bankerna själva distribuerar de privata kund- respektive säljarnycklar²⁴. Bankerna samarbetar kring den gemensamma Payment Gateway som är gränsnittet mellan Internet och banksystemet och uppfyller samma funktion som CyberCash servern.

²³ Hitachi Research Institute; Electronic Money: Its Impact on Retail Banking and Electronic Commerce; F.I.A. Financial Publishing Company.

²⁴ Enligt information från Jan Olof Brunila på Sparbanken.

Grafiskt:



- (1) På kundens anmodan skickar handlaren beställningsblanket över Internet.
 (2) Kunden aktiverar sin plånbok genom att trycka på "Pay"knappen och väljer vilket kort han ska betala med. Han skickar sin beställning och krypterad köptransaktion till handlaren genom att trycka på "OK".
 (3) Handlaren behåller beställningsblanketten, signerar och krypterar kundens krypterade köpuppgifter med sin egen privata nyckel och skickar det vidare till Payment Gateway.
 (4) Meddelandet flyttas ut från Internet miljön bakom säkra brandvägar, avkrypteras och skickas vidare till inlösen i detsedvanliga formatet genom det egna nätverket.
 (5) Auktorisationsförfarandet mellan inlösen och utgivaren går till på det sedvanliga sättet²⁵.

I väntan på SET satsar Posten Torget på ett system för betalning med kort över Internet som liknar First Virtuals. De som handlar med det systemet måste vara medlemmar i Torget, en Internet baserad marknad som funnits i ett år där konsumenterna kan köpa livsmedel, dataprodukt, kläder, resor, m.m. Antalet medlemmar är uppe i 40 000. Inga kreditkortsnummer lämnas ut över nätet. Konsumenten ger Torget en fullmakt som ger Posten rätt att dra pengar från kontot. Själva fullmakten skickas inte heller över nätet men brevledes. Posten Torget fungerar som mellanhand mellan säljaren och konsumenten och tar hand om både betalningen och leveransen. Postens avsikt med den nya tjänsten är att få igång postorderförsäljningen över nätet.

²⁵ Marie-Noël Tardivel; Svenska Handelsbanken; Konferensen "Smarta Kort & Elektronisk Betalning"; nov. 1996.

Kontantbaserade system

NÄTVERKSBASERADE SYSTEM

E-cash

E-cash är ett mjukvarusystem som utvecklats av det holländska företaget DigiCash med inriktning på anonyma nätverksbetalningar. Värdet lagras lokalt i användarens dator men systemet förutsätter att användaren har ett konto med ett e-cashutgivande bank från vilket uttag kan göras. Värdet representeras av elektroniska mynt, d.v.s transaktioner bokförs inte i termer av krediteringar eller debiteringar av ett saldo som i de flesta smarta kort system. De elektroniska mynten är egentligen slumpgenererade siffror som representerar ett visst värde och som baseras på publik-nyckel teknologi.

Asymmetrisk krypteringsteknologi är första försvarslinje mot förfalskning. Det finns två olika protokoll för hur denna teknologi tillämpas i praktiken. Det ena gäller on-line system vilket e-cash är. Det andra protokollet gäller för off-line kortbaserade system och det är det som används i CAFE²⁶. Mynten verifieras för äkthet med hjälp av en publik nyckel som matchar den utgivande bankens privata nyckel. Säkerheten är avhängig av att bankens privata nyckel/digitala signatur förblir okänd.

Till skillnad från andra system erbjuder denna teknologi fullständig anonymitet i den meningen att mynten inte kan länkas till vare sig individer eller transaktioner. Andra system erbjuder någon slags "pseudoanonymitet": alla betalningar utförda med ett visst betalningsinstrument kan länkas samman och vid några transaktioner till exempel laddning länkas betalningsinstrumentet till individen. Här garanteras anonymiteten med hjälp av ett avancerat krypteringsparadigm kallad "blindning" genom vilken användarna kan skydda sin identitet när de skickar mynten till banken för verifiering. Återigen skiljer sig teknikerna åt beroende på om transaktionerna sker on-line eller off-line.

On-line protokollet fungerar på följande sätt:

Uttag: användarens mjukvara skapar mynten med hjälp av en slumpnummargenerator som förser dem med ett serienummer och förblindar dem. Förblindningsproceduren innebär att användaren tillämpar en matematisk funktion på mynten som skymmer serienummerinformationen från banken. Användaren skickar de förblindade mynten till banken med förfrågan om uttag. Banken signerar mynten digitalt, skickar dem till användaren och debiterar dennes konto. Användaren tar bort förblindningen men behåller bankens signatur.

²⁶ CAFE är ett system utvecklat i EU-kommissionens regi. Mer information om det finns under avsnittet om kortbaserade system.

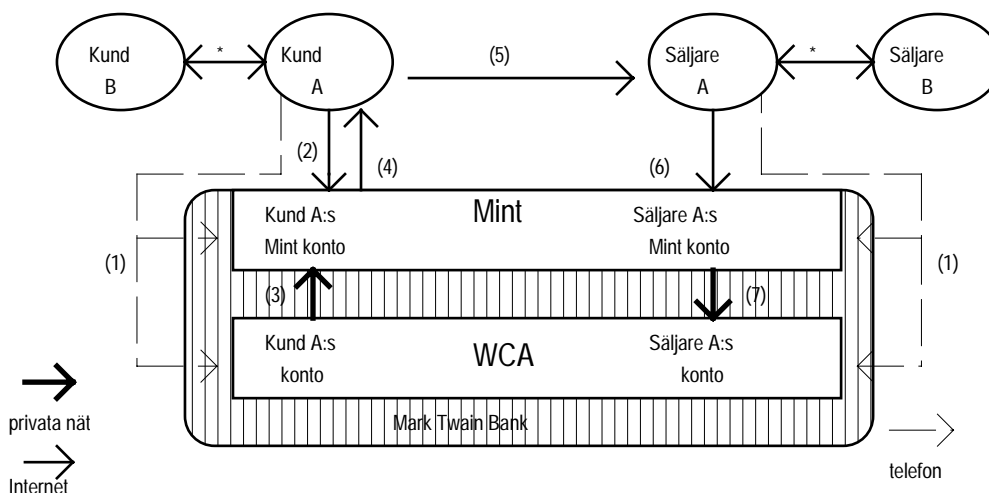
Betalning/insättning: användaren betalar med mynten genom att överföra dem över nätet. De krypteras inför överföring. Mottagaren skickar mynten vidare till banken. Eftersom mynten var förblindade när uttagsförfrågningen skedde kan inte banken veta vem betalningsavsändandaren är, men banken kan dock känna igen sina mynt när de presenteras för verifiering eftersom de innehåller bankens digitala signatur. Banken verifierar den egna digitala signaturen och verifierar att mynten inte använts tidigare genom att kontrollera myntens serienummer mot en central databas. Banken bokför mynten som använda, krediterar betalningsmottagarens konto och informerar denne. Om mynten redan var använda instruerar banken betalningsmottagaren att inte acceptera betalningen. Källan till bedrägeriförsök spåras dock inte. Betalningsinstrumentet, mjukvaran i det här fallet, behöver inte vara motståndskraftigt mot manipulation eftersom betalningar kontrolleras on-line²⁷.

Systemet har testats i några år med en egen testvaluta, s.k. "Cyber-Bucks". Dessa kan inte växlas till nationella valutor men kan användas inom Internet-handel. Numera ges e-cash ut i USA av Mark Twain Bank, i Europa av Finlands Eunet och av Deutsche Bank samt i Australien av Advance Bank, alla i sina respektive valutor. Enligt Mark Twain's tillämpning av systemet kan mynt som inte använts skickas tillbaka till bankkontot, så kallad "World Currency Access" (WCA). Så länge som värdeenheter befinner sig i bankkontot täcks de också av insättningsgaranti. När kunden vill göra ett uttag av elektroniska pengar måste först medel i WCA omvandlas till elektroniska enheter vilket sker i en mellanstation eller elektroniskt konto kallat för "Mint"²⁸.

²⁷ D. Chaum, S.Brands; "Minting electronic cash"; IEEE SPECTRUM.

²⁸ Hitachi Research Institute; "Electronic Money: Its Impact on Retail Banking and Electronic Commerce"; F.I.A. Financial Publishing Company.

Grafiskt:



(1) WCA som är vanliga bankkonto öppnas av kunder och säljare. Samtidigt öppnas virtuella konto i Mint.

(2), (3) Efter förfrågning om uttag av elektroniska pengar överförs fonder från WCA till Mint.

(4) Elektronisk värde laddas i kundens PC.

(5) Elektronisk värde överförs till säljarens PC över Internet.

(6), (7) Elektronisk värde överförs till säljarens Mint konto, kan omvandlas till kontanter om så önskas.

* Elektronisk värde kan också överföras mellan kunder och säljare sinsemellan.

Källa: Hitachi Research Institute.

Sammanfattningsvis är transaktionerna i detta system anonyma och fritt transfererbara mellan individer som är anslutna till systemet. De sker online eftersom mynten måste auktoriseras av banken. Det faktum att banken måste kontrollera varje spenderat mynt skulle kunna bli en flaskhals i systemet om det blir tillräckligt utbrett.

KORTBASERADE SYSTEM

Det finns flera system över hela världen, de flesta av vilka fortfarande befinner sig på ett utvecklings- eller teststadium. Det finns tre system som är världsomfattande: Mondex, Proton och Visa Cash. Det finns två europeiska projekt: CAFE och Clip.

En allmän översikt av systemen och aktörerna bakom följer²⁹:

System	Aktörer	Kort i omlopp
Mondex (världsomfattande)	MasterCard och stora banker i fem kontinenter ³⁰	50 000 i olika pilot tester
Proton (världsomfattande)	American Express och banker	12 000 000 under 1997 (2 000 000 under 1996)
Visa Cash (världsomfattande)	Banker medlemmar i Visa	2 000 000 i över ett tiotal länder
Clip (europeisk)	Banker medlemmar i Euro-pay	50 000 i pilot tester
Danmont (Danmark)	Danmont, danska banker och dansk telekombolag	1000 000 än så länge enbart engångskort
CAFE (europeisk)	ESPRIT ³¹ , Siemens, Digi-cash, Gemplus, mm	små pilot tester, ca 2000 kort

Proton

Proton är det största smartkortssystemet för närvarande. Systemet används i åtta länder och har flera operationsdugliga system på plats och kort i omlopp än alla andra system tillsammans. Det är utvecklat av BANKSYS som är en förening av belgiska banker. Teknologin har sålts under licens till ban-

²⁹ Carol Hovenga Fancher, IEEE SPECTRUM, "Electronic Payments".

³⁰ NatWest, Midland, Royal Bank of Canada, Canadian Imperial Bank of Commerce, Hongkong Shanghai Banking Corporation, Wells Fargo, Chase Manhattan, First Chicago samt 10 stora banker i Australien.

³¹ ESPRIT är EU-Kommissionens forskningsprojekt. Nyligen avslutat.

ker i Schweiz, Canada, Holland, Australien, Tyskland, Sverige och Brasilien. Det är för närvarande Sveriges enda system för elektroniska pengar. Varje lands system har ett eget namn. American Express har licens för världsomfattande användning.

Säkerheten bygger på dynamisk trippel DES-kryptering (symmetrisk kryptering) och har designats i enlighet med specifikationerna från Europay, MasterCard och Visa. En trippdubblad DES-algoritm höjer krypteringsstyrkan jämfört med en vanlig DES-algoritm. Tre skilda krypterings- och avkrypteringsoperationer genomförs med hjälp av en längre DES-nyckel.

Varje bank har sin egen huvudnyckel från vilken kort- och funktionspecifika nycklar härleds (se Säkerhet). Engångsnycklar används för varje inköp och bestyrkande av äkthet sker genom en "challenge-response" protokoll mellan terminaler och betalningsinstrument.

Systemet har profilerats som ett alternativ för kontanter vid småbelopps-transaktioner (under USD 15) inom detaljhandel, parkeringsplatser, kiosker m.m. Det kan inte för närvarande användas för nätverksbetalningar. För inskaffande av kort måste kunden registrera sig hos en kortutgivande bank som vid utgivande kontrollerar kundens identitet. Kortet är personligt och kan inte överlåtas utan speciell fullmakt. Kunden tilldelas en personlig PIN-kod som används för uppladdning av kortet. Uppladdning kan endast ske genom personligt besök i banken eller från särskilda laddautomater. Det finns också ett utvecklingsprojekt tillsammans med Telia kring framtida laddningsmöjligheter hemifrån antingen via datorer eller smarta telefoner. Det finns en övre gräns för laddningsbart belopp (i Sverige SEK 1 500) och antalet laddningstillfällen är begränsat per tidsperiod. Kortets giltighetstid är tidsbegränsad. Om kunden tappar sitt kort förlorar han det värde som finns kvar i kortet eftersom spärllistor inte kan upprättas.

Vid transaktioner utförs ingen identitetskontroll, dvs användaranonymitet garanteras. Transaktioner är dock spårbara till kortet eftersom korten kopplas till ett bankinternt skuggkonto där alla transaktioner registreras. Eftersom individen är kopplad till korten skyddas inte konsumenten från banksyn. Dennes anonymitet gentemot handlaren är däremot garanterad. Syftet med skuggkontot är att höja säkerheten för utgivaren och möjliggöra upptäckt av bedrägeri eller förfalskning. Denna situation skulle uppstå om inlösande bank presenterar Protonenheter till utgivande bank för betalning och det skulle visa sig att skuggkontot inte har tillräckligt saldo för att täcka utförda transaktioner. Säljställets terminal kommunicerar med inlösande bank så att Proton enheterna överförs till ett angivet konto. Transaktionerna sker off-line, ingen kommunikation behövs med utgivande bank för verifikation. Betalningar kan inte göras mellan individer eller från kort till kort.

Värdet kan endast överföras mellan kortinnehavare till säljarstället och där-
efter måste det lösas in³².

I Sverige har Proton systemet³³ lanserats av Nordbanken och Sparbanken. S-
E Banken anslöt sig senare och ytterligare ett antal banker tycks vara intres-
serade att ansluta sig. De tre nämnda bankerna har tillsammans över 70%
av den svenska bankkortmarknaden både som inlösare och som utgivare
vilket också är den främsta drivkraften bakom deras samarbete. Även om
Protonteknologin är gemensam för de tre, kommer bankerna att konkurre-
ra med egna kortutgivningar. Systemen kommer att vara interoperabla, en
nödvändig förutsättning för att lyckas nå upp till "kritiska massan".

Användarna erhåller ingen ränta på pengarna i den elektroniska plånbo-
ken. Bankerna behåller floatintäkterna som används för finansieringen av
systemet. Räntedelen motsvarar högst 10% av intäkterna. Resten är inkomst-
er från avgifter från kortinnehavarna samt transaktionsavgifter för butiker-
na.

Systemet har testats sedan hösten 1996 i Uppsala och Halmstad samt i Gal-
lerian i Stockholm med upp till 20 000 användare. Under 1997 har Cash
kortet varit igång i ovan nämnda städerna samt i Västerås, Kalmar, Norrkö-
ping, Umeå och Sundsvall. Under senhösten kommer en större provlans-
ering att ske i Helsingborg, Örebro, Östersund samt Allingsås. En utvärde-
ring av den första provlanseringen har gjorts. Från bankernas sida
rapporteras goda resultat, medan företrädare från handeln varit kritiska.
Lärdomarna från testerna är att kortsystemet bör utvecklas vidare för att
göra korten mer attraktiva för kunderna. Flera funktioner borde kunna
ingå i korten, exempelvis kombineras med vanliga bankkort. Bättre ladd-
ningsmöjligheter - hemifrån via PC och anpassning till digitala nätverk - an-
ges även som prioriterade utvecklingsområden.

Mondex

Mondex är ett smartkort system utvecklat av Mondex International och som
ursprungligen ägdes av NatWest, Midland Bank och British Telecom. Nu
finns ytterligare 15 banker världen över som deltagare men aktiemajorite-
ten (51 %) köptes av MasterCard i november 1996. Som i fallet med Proton
och andra kortbaserade system har Mondex utvecklats med tanke på trans-
aktioner i detaljhandeln men det är tekniskt möjligt att använda Mondex
kortet även för Internetbetalningar. Detta sker med hjälp av ett kortläsare
som kopplas till datorn. Distansbetalningar kan också utföras med hjälp av

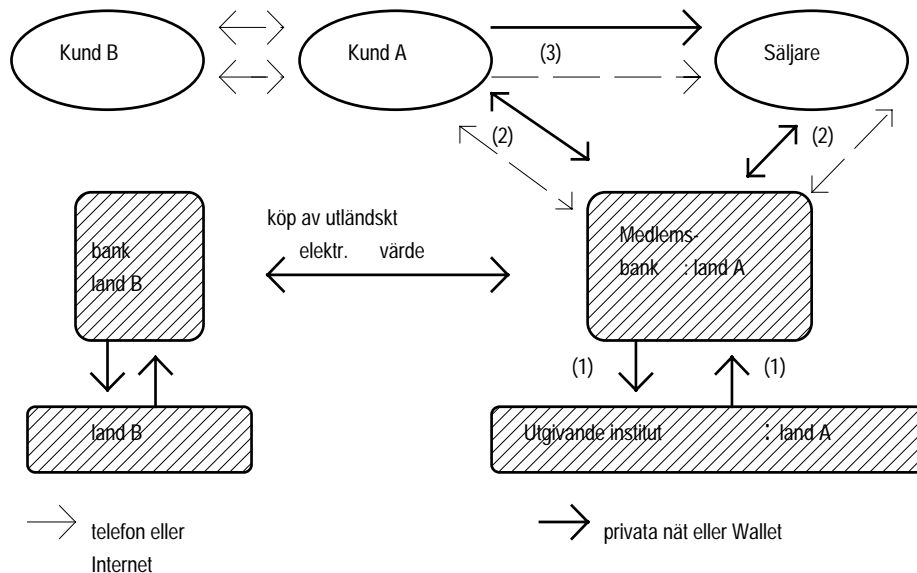
³² Informationen om Proton har hämtats från två källor: "A survey of existing e-commerce
solutions" samt information utlämnat av Finansinspektionen.

³³ I Sverige heter systemet Cash kort.

en Mondex-kompatibel smart telefon. Samma gäller för uttag från- eller insättningar i utgivande respektive inlösende bank.

Ett särdrag hos Mondex som skiljer det från övriga kortsystem är att transferabiliteten inte begränsats. Handlaren kan välja mellan att lösa in Mondexenheter eller använda de för betalningar till andra Mondex anslutna användare. Innehavare kan också överföra elektroniskt värde till varandra med hjälp av en børs som ser ut som en miniräknare och som används för att överföra pengar från kort till kort. Tanken är att systemet ska kunna hantera fem olika valutor men än så länge fungerar det enbart med varje lands egen valuta.

Mondexteknologin bygger på en kombination av symmetrisk och asymmetrisk kryptering. Säkerheten garanteras av digitala signaturer som genereras av kretsen i korten och som bestyrker betalningsinstrumentens äkthet för varandra. Mondex erbjuder bara partiell anonymitet. Precis som i fallet med Proton behöver inte användarna identifiera sig vid transaktionstillfället men transaktionerna är spårbara till betalningsinstrument och terminal. För närvarande lagrar korten uppgifter om de tio senaste genomförda transaktioner medan terminaler har kapacitet för att lagra uppgifter om de 300 senaste genomförda transaktioner. Avsikten är att öka revisionspåretslängd i takt med att kraftfullare kretsar introduceras. I likhet med alla andra kortsystem sker transaktionerna off-line. En grafisk representation av transaktionsflöden med Mondex:



(1) Utgivande institut ger ut elektroniska värdeenheter till varje lands medlemsbank i utbyte mot kontomedel.

(2) Mondex korten kan laddas via ATM, Mondex telefon och snart även via Internet.

(3) Kunden kan överföra värdet till säljaren med hjälp av Mondex anpassade terminaler, med Mondex telefon eller via PC. Värdet mellan individer kan överföras med hjälp av Mondex telefoner eller Mondex Wallet.

Källa: Hitachi Research Institute.

Pilottester av Mondex pågår för närvarande i Storbritannien (Swindon, Exeter och York), Nya Zeeland, USA, Kanada och Hongkong.

VisaCash

VisaCash är Visas eget smartkortssystem som kom ut och testades under OS 1996 i Atlanta. Systemet baseras på och utvecklas under licens av Danmont, den teknologi som utvecklades och används i Danmark³⁴. Resultaten av testen sägs ha varit mycket goda vilket väl kan stämma med tanke på den snabba spridningen som det har fått i förhållande till dess relativt korta existens (se tabell 1). Det finns både engångs- och laddningsbara kort. Kortet sägs vara kompatibelt med EMV-standard. EMV är en arbetsgrupp skapad av Europay, MasterCard och Visa. Dess mål är att utveckla standard för chip kort och terminaler som möjliggör internationellt interoperabilitet.

VisaCash skiljer sig från Mondex i att värdet inte fritt kan transfereras mellan användarna. Flödet av värdet går från kund till säljare och sedan till banken för inlösande. Anonymitet garanteras också i samma grad som Proton och Mondex, vilket innebär att transaktioner är spårbara

CAFE

CAFE står för "*Conditional Access for Europe*" och är ett av EU-kommissionens forskningsprojekt som startade 1992. Målet för projektet var att utveckla en elektronisk börs-teknologi som skulle fungera som betalningsinstrument, accessanordning för informationstjänster och identifikationskort. Syftet var inte att komma fram med en kommersiellt gångbar produkt utan snarare att utveckla en öppen arkitektur (system och systemspecifikationer) som var tillgänglig för alla som ville utveckla egna produkter.

Systemet använder asymmetrisk kryptering med samma krypteringsprinciper som används i e-cash systemet och kallas kort-versionen av e-cash . Transaktioner sker dock off-line. Transaktionsprotokollet liknar e-cash systemet men skiljer sig från detta i två avseenden. Betalning och insättning är skilda i tiden, dvs. betalningsmottagaren accepterar mynten innan banken verifierar och kontrollerar för multipel spendering, vilket sker först när betalningsmottagaren överför pengarna till banken för insättning. Eftersom verifiering och kontroll sker i efterhand kräver det protokollet andra säkerhetsåtgärder. Betalningsinstrumentet måste vara motståndskraftigt mot manipulation och källan till bedrägeri måste kunna spåras samtidigt som anonymiteten bevaras. Det förnämnda åstadkoms med hårdvaruskydd, dvs. tillämpas på kortbaserade system. Upphävandet av anonymitet vid dub-

³⁴ Hitachi Research Institute; Electronic Money: Its Impact on Retail Banking and Electronic Commerce; F.I.A. Financial Publishing Company.

bel spendering åstadkoms genom att avkräva betalningsavsändaren identifikationsinformation. Denna information är delad i två bitar. När myntet används korrekt, d.v.s bara en gång, räcker inte denna information till för att identifiera avsändaren. Vid upprepat spenderande av samma mynt avslöjas dock avsändaren.

Flera valutor kan hanteras. Den teknologi på vilket systemet baseras tillåter dock inte transferabilitet av värdet mellan individerna. Transferabilitet skulle medföra att mynten måste "bli större" (ackumulera mera bitar) varje gång värdet byter ägare. Detta beror på att mynten måste innehålla information om varje individ som har använt dem för att banken ska ha behålla kapaciteten att spåra de individer som använder samma mynt flera gånger³⁵. Transferabilitet är heller ingen önskvärd egenskap i system där förfalskning eller upprepat spenderande upptäcks efter att det skett. Ju flera gånger ett dubbelt använt mynt har transfererats desto längre tid tar det att upptäcka det.

Denna teknologi är för tillfället alldeles för dyr, men teknologikostnaderna förväntas sjunka och göra CAFE systemet konkurrensdugligt inom några år³⁶. Systemet har pilottestats i Bryssel mellan oktober 1995 och februari 1996 enligt systemrapportörerna med goda resultat. Försöket har förlängts med gemensam finansiering av EU-kommissionen och Commercial Bank of Greece.

Clip

Clip är ett smartkort system utvecklat av Europay. Det är EMV kompatibelt och är ett av de första kortbaserade system som använder RSA-säkerhetsteknologi³⁷. Systemet ska möjliggöra betalningar med flera valutor. Enligt planerna ska kontantfunktionen kombineras med vanliga bankkortfunktioner och även integreras med SET-standard för att möjliggöra Internet betalningar. Systemet befinner sig fortfarande på ett initialt försöksstadium.

Det är värt att notera sammanfattningsvis att de stora internationella kortföretagen verkar ha positionerat sig så att de kan täcka större delen av marknaden för elektroniska betalningar. Visa och MasterCard anses av många ha stora chanser att vinna spelet om Internet-betalningar med SET, där även American Express har anslutit sig. De täcker också marknaden för smarta

³⁵ L. Law, S. Sabett, J.Solinas; "How to Make a Mint: The Cryptography of Anonymous Electronic Cash"; The American University Law Review; April 1997.

³⁶ Conditional Access for Europe, Esprit Project EP 7023; Background information and status of the trial.

³⁷ Per Lindström, Europay Sweden AB; "Nya möjligheter med Kombikort: ökad säkerhet och internationell användbarhet".

kort. American Express står bakom Proton, Visa har VisaCash och MasterCard äger Mondex.

Marknaden för smarta kort är intressant för kortföretagen inte enbart för att säkerhetsteknologin sänker "bedrägerikostnaderna", utan också för att det ger dem möjlighet att delta i marknaden för kontanttransaktioner, där de tidigare varit exkluderade³⁸.

Det bör noteras att för att kortbaserade system ska bli utbredda behövs det en kraftig investering i infrastruktur. Befintliga terminaler måste bytas ut. Produktionen av själva korten sker också till väsentligt högre kostnader än fallet är med magnetkort. För närvarande varierar priserna för smarta kort producerade av de tre största korttillverkare (Gemplus, Schlumberger och Bull) inom intervallet USD 1-20. Motsvarande kostnad för magnetkort ligger mellan 10-20 cent³⁹.

³⁸ Enligt Visas egna estimat uppgår det årliga värdet för kontanta transaktioner -ofta små sådana- i världens 29 största ekonomier till USD 8,1 biljoner.

³⁹ Electronic Payments, IEEE SPECTRUM.

Klassificering av systemen

En klassificering av elektroniska betalningsmedelssystem enligt de indelningsprinciper som angavs i avsnitt 2 kan illustreras i följande matris:

	On-line	Off-line
Spårbara	Kontobaserade First Virtual CyberCash SET	Smarta kort Mondex (en viss grad av transferabilitet) Proton VisaCash
Anonyma	Nätverksbaserade e-cash fullständig transferabilitet	Smarta kort CAFE ingen transferabilitet

Motsvarande klassificering för icke-elektroniska betalningsmedelssystem skulle ge följande matris:

	On-line	Off-line
Spårbara	Checkar kontokort giro	
Anonyma		Sedlar och mynt

Kontomedel hamnar i samma klass oavsett om de är digitala eller ej. För kontanter är jämförelsen mer tvetydig. Den enda elektroniska system som hamnar i samma kategori som sedlar och mynt är CAFE men det är ingen produkt utan snarare en teknologi som skulle kunna användas i produktutveckling. En stor skillnad mellan CAFE teknologin och fysiska kontanter är att CAFE inte tillåter transferabilitet. Mondex och e-cash ligger nära kontantbegreppet i flera avseenden men skiljer sig i andra. Alla nämnda system är överlägsna sedlar och mynt i det att betalningar inte behöver ske "face-to-face". Inget system tillåter dock omedelbar avveckling, och till skillnad från fysiska kontanter är förbetalda instrument inte legala betalningsmedel - de representerar bara ett löfte från en bank om att betala eller lösa in en skuld. Ur den aspekten skiljer sig inte elektroniska pengar, kortbaserade eller nätverksbaserade, från traditionella kontomedel.

Sammanfattning och slutsatser

Elektroniska betalningsmetoder finns i två huvudkategorier av system, *kontobaserade* respektive *kontantbaserade* system. Båda är relativt nya och bygger på sofistikerade tekniska lösningar. Den första kategorin innebär introduktionen av nya, effektiva metoder för access till och hantering av medel på konto, dvs. en delvis ny form för traditionell, kontobaserad betalningshantering. Den andra kategorin brukar betecknas som elektroniska pengar på grund av att de i vissa hänseenden liknar fysiska kontanter, om än i varierande grad. Inom kontantbaserade system finns i sin tur två underkategorier, kort- respektive nätverksbaserade system. Skillnaden ligger i var de elektroniska värdeenheter lagras fysiskt; i en integrerad krets inbyggd i själva kortet i det första fallet eller i en dators hårddisk i det andra.

Lite förenklat är nätverksbaserade system närmare kontantbegreppet än "genomsnittliga" kortsystem. Detta kan påstås med säkerhet om jämförelsen görs mellan det enda världsomfattande nätverkssystemet, e-cash, och det nuvarande största kortsystemet, Proton. Betalningar med e-cash är anonyma och icke-spårbara vilket innebär att konsumentens anonymitet garanteras inför både säljare och utgivande bank. Dessutom är värdeenheter transfererbara mellan individer. Kortssystem tillåter å andra sidan att transaktioner kan ske off-line, något som annars bara är möjligt med kontantbetalningar. Distinktionen mellan off-line och on-line transaktioner är dock intressant bara i den mån det påverkar transaktionskostnaderna. Detta är knappast fallet för nätverksbetalningar på grund av att telekommunikationskostnader är oerhört låga, åtminstone så länge det finns ledig kapacitet på nätet.

Cash-kortet, det svenska systemet för elektroniska pengar, baseras på Proton-teknologi. Nordbanken, S-E-Banken och Sparbanken är utgivande banker. Flera andra banker tycks också vara intresserade. Projektet befinner sig dock fortfarande på pilotstadiet.

Elektroniska betalningssystem aktualiserar flera centralbanksrelevanta frågor, både från ett penningpolitiskt perspektiv och från ett stabilitetsperspektiv. En utbredd substitution av sedlar och mynt till förmån för elektroniska pengar minskar centralbankens s.k. seigniorageintäkter i motsvarande grad. Om centralbankernas förmåga att självfinansiera sina aktiviteter kraftigt försämras, kan detta inverka - eller uppfattas inverka - negativt på deras oberoende från den politiska processen i utformningen av penningpolitiken. Informationsvärdet av penningmängdsaggregaten kan också minska om andra än kreditinstitut uppträder som utgivare och inga statistiska rapporteringskrav på dessa införs.

Vidden av dessa problem, som idag är obetydliga, beror i hög grad på hastigheten med vilken elektroniska pengar kan tänkas spridas och omfattningen av denna spridning. På den punkten verkar den allmänna uppfattningen vara att detta kommer att bestämmas om, och i så fall när, man når en kritisk massa av användare. Gör man det kan tillväxten bli explosionsartad och substitutionen av fysiska kontanter omfattande. Dessa frågor kräver dock en närmare analys. Några intressanta aspekter i det sammanhanget är förekomsten av s.k. nätverksexternaliteter, d.v.s att nyttan för individen av att ansluta sig till ett system ökar med antalet redan anslutna individer, samt stordriftsfördelar och andra produktionsekonomiska särdrag hos systemen.

En viktig faktor skulle kunna vara utvecklingen av den digitala Internetmarknaden. Där behövs nya betalningsinstrument, eftersom inga redan existerande betalningsinstrument är särskilt användbara. Om några av de nya produkterna kan tänkas kunna vinna spelet om Internetbetalningar har dessa också möjlighet att nå den kritiska massan på en global nivå. Som det ser ut idag verkar det dock som om det är traditionella kontobaserade metoder i ny elektronisk skepnad som har de bästa chanserna. Elektroniska kontanter får dock ett bättre utgångsläge om de samtidigt är användbara både på nätet och ute i detaljhandeln. Det är dock inte klart från vilket håll - från kortsidan eller från nätverkssidan - som en sådan sannolik konvergensprocess kommer att startas och drivas.

Från stabilitetsperspektivet är säkerheten den stora frågan. Det gäller att skapa system som är rimligt säkra ur bedrägeri- och förfalskningssynvinkel och som kan förtjäna och behålla allmänhetens förtroende. Detta har, givet att systemen får allmän utbredning, också betydelse för stabiliteten i det samlade betalningssystemet. Säkerheten skiljer sig mellan olika system. Nätverkssystemet e-cash och kreditkortbetalningar med SET baseras på avancerade asymmetriska krypteringsalgoritmer medan kortssystem använder symmetrisk kryptering eller en kombination av båda. Krypteringstekniken kan kompletteras med "tamper resistant" hårdvara vilket är fallet för smarta kort. Även om det är viktigt att hårdvaruskydda informationen är valet av krypteringsalgoritm avgörande för säkerheten. Systemens säkerhetsåtgärder måste ständigt uppgraderas. Dock är det så att säkerhet kostar pengar, vilket gör det ännu viktigare att säkerhetsaspekter kontinuerligt bevakas från myndighetshåll.

Stabilitetsperspektivet rymmer också andra frågor. En som varit mycket omdebatterad i EMI och andra internationella fora är vilka som ska få vara utgivare. Det synsätt som dominerat i den europeiska centralbanksvärlden och som kom till uttryck i EMI-rekommendationen från 1994, innebär att enbart banker ska få ha utgivarstatus, grundat på uppfattningen att de elektroniska värdeenheter är att betrakta som inlåning. Eftersom inlåning är förbehållet kreditinstitut och deras verksamhet är reglerad med syfte att nå

upp till en viss stabilitetsstandard, skulle detta vara ett enkelt och logiskt sätt att garantera fortsatt stabilitet. Samtidigt skulle man på så sätt undvika att belasta banksektorn med orimliga konkurrensvillkor. Mot detta står framför allt det amerikanska synsättet att kravet på bankstatus är för restriktivt och att det skulle kunna strypa marknadens innovationsförmåga. Dessutom finns det EU-länder som utifrån existerande lagstiftning inte betraktar de elektroniska värdeenheter som inlåning.

Om man tittar på vad marknaden själv åstadkommit så visar det sig att enbart kreditinstitut i praktiken agerat som utgivare. Teknologi-, data- och telekommunikationsföretag utvecklar den nödvändiga teknologin som sedan säljs till banker eller stora kortföretag under licensavtal. En rimlig tolkning är att denna arbetsfördelning anses vara den mest fördelaktiga av marknadsaktörerna själva, eftersom bankerna redan besitter den expertis och trovärdighet som kan garantera allmänhetens förtroende för de nya betalningssystemen. En annan bild som skymtar fram är att redan idag är konkurrenssituationen ganska begränsad. Visa, MasterCard och American Express är dominerande inom både smarta kort och elektroniska kreditkortbetalningar. Själva kostnadsstrukturen i de elektroniska betalningssystemen med mycket höga fasta kostnader och relativt låga rörliga kostnader talar för uppkomsten av en oligopolistisk marknad.

Om denna bild med en marknad som domineras av några få stora aktörer och med kreditinstitut som utgivare är korrekt, skulle den reflektionen kunna göras att den faktiska samhällsekonomiska kostnaden - till följd av att vissa potentiella utgivare stängs ute - av en reglering av det slag EMI förordat inte är så stor som man skulle kunna befara. En fri-konkurrens marknad med många jämstarka aktörer och med låga etableringströsklar är inte en realistisk framtidsbild oavsett hur regleringen kan komma att se ut. Med andra ord kan ifrågasättas om den stundtals intensiva diskussionen kring utgivningsrätten är särskilt relevant i praktiken. Ett måhända större problem med en begränsning av utgivningsrätten kvartstår dock för de system som används över Internet eller andra nät över landsgränserna. Detta skulle kunna kräva en global samordning av regelverken, något som kan vara svårt att åstadkomma. I annat fall kan så kallat regleringsarbitrage komma att uppstå och utgivare från mer regleringsinriktade länder kan komma att slå ut.

Referenser

BIS, Implications for Central Banks of the Development of Electronic Money, 1996.

BIS, Security of Electronic Money, 1996.

Business Research Publications, Report on Electronic Commerce, Sep. 1996.

D. Chaum & S. Brands, Minting Electronic Cash, IEEE SPECTRUM, Feb. 1997.

E-Commerce, A Survey of Existing E-Commerce Solutions,
URL: <http://www.internet-banking.com/>

C. Fancher, Electronic Payments, IEEE SPECTRUM, Feb. 1997.

Hitachi Research Institute, Electronic Money: Its Impact on Retail Banking and Electronic Commerce, F.I.A Financial Publishing Company, 1997.

L. Law, S. Sabett, J. Salinas, How to Make a Mint: The Cryptography of Anonymous Electronic Cash, The American University Law Review, vol. 46. Apr. 1997.

M. ter Maat, The Economies of e-cash, American Bankers Association.

Dr. A. Schöter, R. Willner, Digital Money Online: A Review of Some Existing Technologies, Feb. 1997.

T. Tanaka, Possible Economic Consequences of Digital Cash, Columbia University, New York.

M. Tardivel, Svenska Handelsbanken, Konferensen om Smarta Kort och Elektronisk Betalning, nov. 1996.

Företagsinformation

CAFE, Conditional Access for Europe, Esprit Project EP 7023.
URL: <http://www.cordis.lu/esprit/src/w4w19.htm>

CyberCash,
URL: <http://www.cybercash.com>

First Virtual, E-Commerce, URL: <http://www.internet-banking.com>

Mondex, URL: <http://www.mondex.com>

Proton, E-Commerce; A survey of existing e-commerce solutions,
URL: <http://www.internet-banking.com>

VisaCash; URL: <http://www.visa.com>

SET, E-Commerce, URL: <http://www.internet-banking.com>

Ordlista

Mikrobetalningar: ett nytt begrepp som uppstått i Internetsammanhang. Det är tillämpligt på handel med digitala varor som anses kunna prissättas inkrementellt eller per bit på samma sätt som vatten eller elektricitet. Det är fråga om mycket små betalningar, det kan röra sig om några ören.

Kryptering: tekniker utvecklade genom tillämpning av matematisk teori som syftar till att skydda datas konfidentiella karaktär, garantera dess äkthet och bibehålla dess integritet. Det finns två huvudtekniker för kryptering och avkryptering av data. DES-teknologi eller symmetrisk kryptering använder samma nyckel (eller kod) för både kryptering och avkryptering. RSA-teknologi eller asymmetrisk kryptering använder nyckelpar, en för kryptering och en för avkryptering. Dessa nycklar är relaterade till varandra på ett sådant sätt att man inte kan sluta sig till den ena nyckel genom kunskap om den andra. En digital signatur är en praktisk tillämpning av asymmetrisk kryptering som uppfyller samma funktion på elektroniska meddelanden som en handskriven signatur på ett pappersbaserat dokument, nämligen att garantera den signerande partens identitet och dennes godkännande av dokumentet.

Off-line: i system av elektroniska pengar, en transaktion som inte kräver kommunikation mellan betalningsinstrumentet och ett centralt datasystem för kontroll eller godkännande.

Transaktioner som kräver kommunikation med en central datasystem för godkännande sägs ske on-line.

Revisionspår: bokföring, som går att följa, av alla transaktioner som genomförts med hjälp av olika betalningsinstrument och terminaler.

Spårbarhet: anger i vilken utsträckning transaktioner eller transfereringar av pengar kan spåras till den som initierade betalningen eller till mottagaren.

Transfererbarhet: anger i vilken utsträckning elektroniska pengar kan överföras mellan betalningsanordningar (instrument och terminaler) utan inblandning av en central myndighet eller institut.