ELEKTRONISK BETALNING PÅ INTERNET

PayWatch 1997

Ulf Wingstedt (*redaktör*)
Mathias Axling
Peter Rosengren

Förord

PayWatch startade i februari 1997 på initiativ av Tidningsutgivarna (TU), bransch- och arbetsgivarorganisation för tidningar och andra företag i mediebranschen. TU:s syfte med PayWatch är att bevaka utvecklingen kring elektronisk betalning på Internet i Sverige och internationellt och via en webtjänst informera TU:s medlemsföretag och andra intresserade. TU gav Svenska Institutet för Systemutveckling (SISU) uppdraget att driva PayWatch.

PayWatch kommer även fortsättningsvis att bevaka utvecklingen som går in i en spännande fas där allt fler aktörer börjar få praktiska erfarenheter av elektronisk handel. 1998 är ett år då SET sätts i drift i Sverige och då system för mikrobetalningar börjar ta form. Utvecklingen kring smarta kort förutses få stor betydelse för betalning även på Internet och PayWatch kommer att följa händelserna noga. En länk till PayWatch webplats finns hos TU http://www.tu.se.

Under 1997 har nio nyhetsbrev producerats av PayWatch-redaktionen som bl a behandlat erfarenheter från svenska betalningslösningar, SET-standarden, smarta kort, upphovsrättfrågor och förtroende.. Ett urval av artiklar ur nyhetsbreven publiceras här i rapportform. Artiklarna har sammanfogats i ämnesrelaterade block och dessutom redigerats något. Rapporten riktar sig främst mot läsare som inte kontinuerligt följt PayWatchs rapportering på Internet och som vill ha en uppdatering av 1997 års viktigaste trender och händelser, liksom mot trogna PayWatch-läsare som önskar en sammanfattande rapport.

Artiklarna i denna rapport kan läsas fristående. Inom parentes anges det PayWatch-nummer som artikeln hämtats från.

Kista i februari 1998,

Ulf Wingstedt,

redaktör PayWatch 1997

Internetbetalning i Sverige

I början av 1997 hade en handfull pionjärer med Aftonbladet i spetsen börjat prova att ta betalt för elektroniska tjänster på Internet. Olika betalningssystem testades, allt från betaltelefonnummer till kreditkort via Cybercash och First Virtual. Men de stora förhoppningarna om en rejäl volymtillväxt för internethandeln i Sverige under 1997 kunde inte förverkligas.

Tvärtom avvecklade flera webplatser sina satsningar, däribland Aftonbladet och även Förenade Landsortstidningar (FLT). Vid årets slut framstod kreditkortsbetalning, krypterad eller öppen, som den vanligaste lösningen. Detta trots att tekniken inte accepteras av svenska banker utan kräver en utländsk bankkontakt vilket dock inte är svårt att ordna.

Vid årets slut presenterades deltagarna i den svenska SET-pilot som Visa koordinerar tillsammans med fyra svenska banker. Piloten kom igång i slutet av januari, drygt ett halvår efter plan.

Red.

Svenska sajter tar betalt på Internet (1/97)

Ett ökande antal svenska webplatser tar betalt för sina tjänster trots diskussionen om säkerhetsproblem. De som erbjuder fysiska varor enligt postordermodell måste självklart få betalt, men det finns även informationsleverantörer som går mot strömmen och istället för att bjuda ut information gratis, valt att ta betalt.

De typer av betalningssystem som är aktuella för en svensk internetbutik är:

- Kreditkort on-line, vilket är vanligt i USA men ännu sällsynt i Sverige pga svenska bankers hårdare regler.
- Betalorder via digital check eller postgiroöverföring (kontoöverföring)
- Betaltelefonnummer (0719-nummer), dvs man köper ett innehavsbevis (t ex en kod) via telefon och debiteras via telefonräkningen
- Off-line betalning av olika slag som t ex fakturering eller kreditkort off-line

Som synes är alla internetbutikens betalningssystem baserade på redan existerande motsvarigheter i den reella världen. I Sverige finns det idag möjlighet att ta betalt enligt alla systemen.

Det finns två huvudtyper av betalningssystem, dels slutna system, där säljare och köpare har en etablerad relation via t ex ett medlemskap, dels öppna system där en ny kund direkt kan handla utan krav på registrering eller andra förberedelser.

Ett exempel på ett slutet system på Internet är de sk "torg" eller Internet Malls där flera olika butiker finns samlade och där varje kund har ett enskilt uppsamlingskonto för inköp. I Sverige finns bl a Postens webplats "Torget" med detta upplägg, där betalningar samlas och kan

genomföras via postgiro, faktura eller kontokort. Betalningen görs dock inte på Internet utan via skriftliga handlingar.

Men flertalet svenska internetbutiker tillämpar öppna system och det är också de som är de mest intressanta för framtiden eftersom de gör köpbeslutet enklare för kunden och låter henne välja olika leverantörer.

Bland svenska webplatser med försäljning är de som baseras på en traditionell postordermodell vanligast. Postorderföretag som Ellos (http://www.ellos.se) och Clas Ohlson (http://www.clasohlson.se) visar sina varor i en webkatalog och tillhandahåller formulär för beställning. Betalning för varorna sker dock helt utanför Internet och med de traditionella systemen som faktura eller postförskott.

Även informationstjänster kan naturligtvis faktureras. Ett omtalat exempel är Sundsvalls Tidning (http://www.stonline.se/) som är den första svenska tidning som enbart gör sin webutgåva tillgänglig för betalande prenumeranter. Prenumerationen kan tecknas on-line, men betalningen sker mot skriftlig faktura.

Tjänster som bygger på fakturering är enkla att realisera och kräver litet i fråga om säkerhetsarrangemang. Den enda risker som måste hanteras är att beställningen är falsk och/eller mottagaren vägrar betala. Men eftersom riskerna är begränsade i fråga om de värden som riskeras och dessutom helt tas av säljaren, kan denna typ av betalning bidra till att undanröja kundernas tveksamhet inför att shoppa på Internet.

Men för postorderföretag som vill minska sina risker kan det göras genom att ta betalt direkt på Internet innan varan skickas. Ett svenskt exempel på denna utveckling är TV Shop (http://www.tvshop.se) som låter kunden betala med kreditkort. TV Shop använder en sk semisäker lösning där kundens kreditkortsinformation skyddas för insyn under överföringen på Internet med svag kryptering. TV Shop sköter dock inte kreditkortshanteringen i egen regi utan samarbetar med Förenade X AB (http://www.uni-x.se/), ett företag som hanterar semisäker kreditkortsbetalning för flera internetbutiker.

När det gäller informationstjänster är betalning on-line ännu mer intressant eftersom också varan ofta kan levereras via nätet, antingen i form av nedladdningsbara dokument eller i form av tjänster.

Den tidning som främst gått i bräschen för elektronisk betalning i Sverige är Aftonbladet som provat och använt flera olika betalningssystem parallellt. Under våren -97 hade man under en tid tre olika system i drift: Betaltelefon (0719) och kreditkort med den helt skyddade Cybercash-tekniken alternativt semisäker hantering via Förenade X AB (liksom TV Shop ovan). Dock valde Aftonbladet att så småningom avbryta användningen av de båda kreditkortslösningarna eftersom osäkerhet uppstod kring det juridiska ansvaret för eventuell förlust och missbruk av kunders kreditkortsnummer.

Osäkerheten gällde främst systemet via Förenade X där betalningstransaktionen i praktiken utförs på Förenade X:s webserver och inte Aftonbladets. Även om all känslig information överförs skyddat med kryptering till servern, så finns det risk att någon bryter sig in på Förenade X:s dator och det är då oklart huruvida det är Förenade X eller Aftonbladet, som tillhandahåller tjänsten, som står som ansvarig.

Att vissa kan ta betalt på Internet betyder dock inte att alla säkerhetsproblem lösts. Även om inte de omtalade kreditkortsnumren far kors och tvärs på Internet, så finns det många ytterligare aspekter på säkerhet att hantera, exempelvis kundens tillgänglighet till den informationstjänst hon betalt för. När morgontidningen inte kommer i brevlådan kan vi ringa

tidningen och få ett par nummer tillgodo som plåster på såren, men vem ringer man när nätet inte kan kopplas upp?

Trots alla möjliga problem och svårigheter med elektronisk betalning är det ändå nu som det är dags att sätta igång, inte minst för att skaffa erfarenheter. Det är viktigt att ha de nödvändiga systemen på plats och de grundläggande erfarenheterna gjorda när tillfället öppnar sig. Dessutom överdrivs problemen menar bedömare. Faktum är att "någon" därute faktiskt genomför vad de flesta säger inte kan göras.

Ulf Wingstedt

Svenska sajter kan ta kreditkort (2/97)

Ett i de verkliga livet mycket spritt betalningsmedel är kredit- och betalkorten. Dessa används också mycket för internetbetalning on-line, speciellt i USA där man sedan många år är van att använda kreditkort för köp via telefon och fax.

I Sverige har dock bankerna varit kallsinniga inför det amerikanska sättet att använda kreditkort. Bankerna har åsikten att en internetbutik idag inte uppfyller kraven på en säker hantering av kreditkortsinformation och tillåter därför inte sina företagskunder att ta emot kortnummer över Internet.

Men ändå finns det svenska företag som accepterar kreditkort på Internet. De få exempel som finns bland svenska företag bygger alla på att företaget, på något sätt, skaffat tillgång till ett konto i utländsk bank, typiskt i USA men även banker i andra europeiska länder som Norge eller Luxemburg. Den egna svenska banken kan dessutom ofta hjälpa till med att öppna konto i sin amerikanska filial.

Att behöva gå via utländska banker har naturligtvis en del nackdelar, förutom all extra administration. Exempelvis finns en valutarisk eftersom betalningen sker i det lands valuta där banken verkar. Ibland måste också priserna mot kunden sättas i dollar eller motsvarande.

Vid all kreditkortsbetalning är minst tre parter inblandade: kunden, handlaren och kortutgivaren. Vid en betalning måste därför information överföras genom hela kedjan, där det första steget är mellan köpare och handlare. Handlaren måste därefter i ett andra steg skicka informationen vidare till kortutgivaren för att få betalt. Denna informationsöverföring kan ske på olika sätt i olika lösningar där hela eller enbart delar av överföringen sker skyddat med kryptering.

Kreditkort direkt

En vanlig lösning på Internet idag är man direkt i webläsaren kan mata in kreditkortsnumret och därmed betala. I många enklare lösningar överförs numret helt oskyddat över Internet med risk för att någon ska avlyssna numret på vägen.

En bättre lösning är att använda de krypteringsmöjligheter som finns inbyggda i dagens webläsare. De flesta leverantörer av webservrar har varianter av produkterna som kan kryptera all information som överförs till en webläsare. Netscape Commerce Server är ett exempel där SSL (Secure Sockets Layer) används. När överföringen krypteras ser användaren det exempelvis som att ett blått streck visas i skärmens överkant och att nyckeln i nedre vänstra hörnet blir helt sammanfogad.

Krypteringen som sker med webläsarens inbyggda funktioner har fördelen att någon extra programvara inte behövs. Däremot kan numret ses i klartext av handlaren och det är omöjligt för kunden att vara helt övertygad om att handlarens hantering av kreditkortsnumret är helt

säker. Tillvägagångssättet kan jämföras med att använda kort i en restaurang, där kortet överlämnas från kunden till servitören på ett sätt som hindrar andra i restaurangen från att se kortnumret men där kunden tappar kontrollen över kortet när servitören tar det med sig till kassan bakom disken. Men, trots en viss risk, kan säkerhetsnivån vara helt tillräcklig för många tillämpningar.

Lösningar med direkt inmatning av kreditkortsnummer kan också användas av svenska företag, trots svenska bankers ovilja. Lösningarna bygger då på att en utländsk part används för själva korttransaktionen. Två svenska företag som erbjuder tjänster kring kreditkortsbetalning är internetleverantörerna Bahnhof (http://www.bahnhof.se) och Förenade X (http://www.uni-x.se).

Förenade X har byggt lösningar för TV Shop och Mediearkivet. Själva betalningsfunktionen ligger i dessa fall på Förenade X:s web-server och länkas in i handlarens tillämpningen. Förenade X tar hand om verifiering av kortnummer och ser till att pengar överförs från kundens kort till handlarens konto via utländsk kortinlösare. Tjänsten kostar mellan 5 och 9 procent av omsättningen beroende på volym enligt Förenade X.

Bahnhof hanterar dock inte betalningen självt, utan samarbetar med ett amerikanskt företag om det. När kunden klickar "betala" så ansluter hon till en server hos företaget Alpha Soft (https://www.alpha-soft.com) i USA där hela betalningen hanteras. För en svensk kund kan detta vara en nackdel. Även om kunden har förtroende för svenska företaget Bahnhof och dess varumärke kan hon komma att känna tveksamhet inför att betala hos Alpha Soft.

Jon Karlung som ansvarar för betalningstjänsten på Bahnhof tycker att riskerna kring denna typ av lösning överdrivs. Att använda en amerikansk kortinlösare kan tvärtom vara en fördel om man vänder sig till en global (läs amerikansk) kundkrets. Av den risk som ändå tas, faller den större delen på handlaren som riskerar att leverera utan att få betalt, påpekar Jon Karlung. Kundens riskexponering är mycket liten.

- Säkerheten för postorderföretag med fysiska varor är ändå mycket god, fortsätter Jon Karlung. Kreditkortets giltighet verifieras först så att inmatade uppgifter stämmer och dessutom kontrolleras att kundens angivna e-postadress är korrekt. Därefter görs en kontroll mot kortregister att det inte är spärrat och/eller täckning saknas samt att leveransadressen stämmer överens med kortinnehavarens adress. Först när allt är klart skickas varan.

För informationsprodukter som man önskar leverera utan fördröjning on-line kan dock inte hela kontrollen utföras direkt. - Men man kan ändå verifiera inmatade uppgifter och få en rimligt låg risk, menar Jon Karlung.

Bahnhof uppskattar uppsättningskostnaden för en mindre butik med ett 10-tal produkter till mellan 15 000 och 20 000 kronor. Sedan tillkommer en transaktionsavgift på 4,5%.

Större säkerhet med elektroniska plånböcker

I syfte att erbjuda en mer heltäckande säkerhetslösning för hela kedjan mellan kund och kortföretag har flera av de stora aktörerna som Mastercard, VISA, IBM, Microsoft m fl utarbetat en standard för kreditkortsbetalning som heter SET (Secure Electronic Transactions). Pilottester med betalningar enligt SET pågår för tillfället och färdiga tjänster beräknas finnas tillgängliga 1998. SET har ett brett stöd, även av svenska banker.

En av aktörerna bakom SET är det amerikanska företaget Cybercash (http://www.cybercash.com) som redan idag erbjuder en lösning som påminner om SET. Via en elektronisk plånbok som användaren installerar på sin dator kan man med Cybercash-tekniken överföra betalningsinformation på ett säkert sätt även förbi handlaren.

Kortinformationen tas om hand om Cybercash som är den som verifierar giltighet och ser till att pengar överförs.

Cybercash programvaror för internetbetalning kan kostnadsfritt laddas ner från Cybercash www-sajt. För att de ska kunna användas krävs dock konto i ett urval av amerikanska banker som samarbetar med Cybercash. Ett svenskt företag kan skaffa ett sådant konto i amerikansk bank om man har ett företag registrerat i USA.

Ulf Wingstedt

SET – uppgång och fall?

SET-standarden sågs av många som det som äntligen skulle kunna sätta internethandeln i rullning. 1997 kantades dock av förseningar, först av själva standardiseringen, sedan av realiseringen i det svenska pilotförsöket. När detta skrivs i februari 1998 sitter vi med facit i hand, den svenska SET-piloten startade i slutet av januari 1998 men under väntetiden har allt fler invändningar rests mot såväl kostnaderna bakom SET som mot den tekniska lösningen.

Urvalet av artiklar kring SET nedan speglar dels förväntningarna om vad en accepterad de facto standard skulle kunna innebära, dels att SET kanske inte får denna acceptans.

Red.

VISA testar säker kortbetalning i Sverige (1/97)

Den standard för säker hantering av kreditkortsköp på Internet som utvecklats av VISA och Mastercard i samarbete med mjukvaruföretag som Microsoft och IBM, SET (Secure Electronic Transactions), skulle varit i drift från årsskiftet 96-97 men har blivit försenad. Nu har dock pilotsystem satts i drift och provas av VISA i samarbete med nästan 40 europeiska banker, däribland fyra svenska, Handelsbanken, Sparbanken, S-E Banken och Postgirot.

- 1997 blir ett läroår för S-E Banken, säger Lena Lundholm som arbetar med strategisk affärsutveckling på S-E Banken. 1998 räknar vi dock med att på allvar kunna erbjuda våra företagskunder tjänster för säker korthantering via SET.

Den första kompletta pilotprojektet hade tidigare inletts i Danmark av PBS (danska bankcentralen) och IBM. För närvarande är ett bokförlag och ett försäkringsbolag användare av kreditkortstjänsten. Även Mastercard kommer att starta pilotsystem under 1997.

Det råder något delade meningar om huruvida SET är en förutsättning för internetbutiker eller ej. Medan vissa ser nuvarande bristande säkerhet som ett stort problem, ser andra de möjligheter till att ta betalt som faktiskt existerar via de vanliga systemen som fakturering, postförskott mm. En amerikansk undersökning utförd av Strategic Focus som intervjuat mer än 400 datachefer och utvecklare pekar dock tydligt ut säkerhetsfrågan som den enskilt största utmaningen vid utveckling av internettjänster. 55% ansåg säkerhetsbrister som det största hotet.

I väntan på SET (4/97)

SET, **som är den industristandard man hoppas ska skapa den nödvändiga ordning och stabilitet som krävs för att en elektronisk marknad ska ta fart, har dock inte ens hunnit bli klar innan man talar om utökningar och nya versioner. Det är inget gott tecken.**

I de pilottester av SET som startats under våren finns IBM med i flera. IBM satsar mycket på elektronisk handel med sin programvara NetCommerce och CommercePoint och är dessutom

en av de ledande företagen bakom SET. Den för Sverige närmaste SET-piloten är den som sedan årsskiftet körs i Danmark av just IBM tillsammans med Tele Danmark, Eurocard och förlaget Egmont. IBM har också nyligen släppt en ny version av NetCommerce där stöd för SET-transaktioner ingår vilket IBM är först med bland leverantörerna av programvara för Internethandel.

IBM är också inblande i den SET-pilot som körs i Japan tillsammans med Fuji Bank. Målet är att baserat på erfarenheterna från piloten sätta ett komplett system i drift vid årsskiftet och att på sikt nå drygt 100 000 kunder i Japan och utomlands.

Den japanska SET-piloten har dock rört upp känslorna bland IBM:s partners i SET-konsortiet. IBM och Fuji Bank har nämligen provat en variant av debetkortbetalning som inte täcks av SET-specifikation och har därmed på eget initiativ gjort en utökning av den föreslagna standarden. Även om IBM lovat föreslå utökning som en del av kommande SET-versioner, så är tilltaget en indikation på att ju närmare SET kommer, desto hårdare blir konkurrensen mellan parterna bakom SET. Leverantörsspecfika tillägg till standarder utarbetade av kommittéer har i andra sammanhang ställt till mycket problem och hindrat etablering av de facto standarder och denna typ av oreda är det sista det försenade SET-konsortiet behöver.

Som om inte ett hotande versionskrig vore nog, så har dessutom ett av grundfundamenten i SET ifrågasatts, nämligen den krypteringsalgoritm som ingår.

En representant för Mastercard, som också ingår i SET-konsortiet, skakade om SET-världen genom att kritisera och uttrycka oro kring krypteringsteknik från RSA. RSA är marknadsledande inom kryptering och håller viktiga patent. Problemet med RSA, enligt Mastercard, är att tekniken kräver allt längre nycklar för att inte kunna knäckas. SET kommer exempelvis att använda en nyckel av 1024 bitars längd vilket ger en mycket god säkerhet i dagsläget, men med de allt snabbare datorerna kommer den inte att räcka till i framtiden, en framtid som kanske ligger så nära som ett par år.

De allt längre nycklarna i RSA kommer tyvärr att medföra större behov av beräkningskraft för att kunna hanteras och häri ligger svagheten enligt Mastercard. Man pekar då hellre på en alternativ krypteringsteknik, sk elliptic curve cryptography (ECC), som utvecklats av företaget Certicom (http://www.certicom.com). Fördelen med ECC är att den kräver mindre av såväl processor som minne och passar därför bra i kombination med t ex smarta kort och andra enkla enheter. RSA, som nära nog har en monopolsituation idag, försvarar dock sin teknik och menar att ECC ännu är allt för outforskad för att ge säkerhet för mångmiljontransaktioner.

Den första versionen av SET som planeras att släppas den först juni har RSA-kryptografi som en integrerad del. Man talar nu om att i kommande versioner av SET ha en mer öppen och neutral arkitektur som tillåter flera olika krypteringstekniker. Mastercard hävdar att man redan gjort tester med ECC inom version 1 och vill öka takten för att få version 2 klar redan till årsskiftet.

Sannolikheten är alltså stor att version 1 av SET aldrig kommer att nå ut i tillämpning utanför pilottesterna och att det blir version 2 som kommer att utgöra grunden för de första kommersiella storsatsningarna, i bästa fall. Allt kunde varit frid och fröjd med det, men SET:s försening och svenska finansinstitutioners ovilja att ta sig an någon annan teknik än SET ligger som en våt filt över svenska satsningar på näthandel. Risken är att svenska företag hamnar på efterkälken i den globala konkurrensen på nätet.

Ulf Wingstedt

SET 1.0 provas i Sverige (5/97)

Den nya SET-standarden (Secure Electronic Transaction) är äntligen klar och nu vidtar omfattande pilotprojekt för praktiska test av SET-betalning över hela världen, även i Sverige. I bästa fall kan produktionssystem vara i drift till julhandeln.

SET (Secure Electronic Transaction) har tagit två år att utveckla, men är sedan länge accepterad som en de facto standard för kreditkortsbetalning på Internet. När de båda kortjättarna Visa och Mastercard slog sig samman om en gemensam standard följde resten av branschen efter och när version 1.0 nu är klar står även konkurrerande kortföretag som American Express och Diners Club bakom liksom banker över hela världen. Teknikleverantörerna med dataföretag som IBM, Microsoft, Oracle och Sun Microsystems i spetsen finns också där och har sedan länge varit inblandade i utveckling av SET-produkter.

Förhoppningarna är stora och SET anses allmänt kunna bli katalysatorn som får igång den slumrande handeln på Internet. En allmänt accepterad säker standard inger förtroende för systemet hos kunder och handlare och utgör en trygghet för dem som skall köpa och sälja på nätet. Dessutom innebär en standard att investeringar i inköp och utveckling av handelssystem blir mindre riskfyllda för handlare, banker och utvecklare av programvara.

Målsättningen bakom SET-arbetet har varit att ta fram en teknik som erbjuder lika bra eller bättre säkerhet som i befintliga system. SET använder därför stark kryptering som förhindrar att betalningsmeddelanden förändras eller avlyssnas. Krypteringstekniken i SET baseras på RSA och DES som båda är beprövade och noga testade under många års praktisk användning inom andra områden. Dessutom ingår att alla deltagare i en transaktion, dvs bank, handlare och kund, ska kunna identifieras på ett säkert sätt med hjälp av digitala ID-handlingar, sk certifikat. Det är främst certifikaten som ger SET en fördel framför konkurrerande lösningar vad gäller säkerhet.

Säker identitet

Användning av digitala certifikat kräver dock att en infrastruktur för att ge ut och verifiera certifikat finns på plats. Med tanke på att varje handlare och kund måste ha ett giltigt certifikat samt att dessa måste verifieras i varje transaktion måste ett certifieringssystem vara väl utbyggt och erbjuda mycket god prestanda (främst korta svarstider vid verifiering). Ett speciellt problem att lösa har varit hur ett certifikat utgivet av en instans kan verifieras av en annan. Det har tidigare funnits en oro över att driftsättningen av SET kan försenas av att certifieringssystemen saknas eller inte har tillräcklig kapacitet, men arbetet med certifieringssystemen har gått fort framåt.

Tidigare i vår valdes företagen Certco och Spyrus av Mastercard och Visa till uppdraget att konstruera det centrala kontrollsystemet för SET (Root Certificate Authority). Certifikaten utfärdas dock av olika instanser i en hierarki (sk Certificate Authorities, CA) men i toppen på denna finns den centrala instansen, som garanterar giltigheten i de certifikat som underställda instanser utfärdar. Utfärdare av certifikat är idag exempelvis specialistföretag som Verisign och GTE men även företag som Microsoft och kortföretaget American Express. Vi lär också få se svenska utgivare av certifikat, t ex Posten och andra. SET:s certifieringssystem vilar på att det centrala kontrollsystemet är absolut säkert och att en betrodd lösning nu är under utveckling är inte bara ett stort framsteg utan en förutsättning för att SET ska kunna användas i stor skala.

Svenskt pilotprojekt

Under sommaren kommer SET att testas i många olika pilotprogram över hela världen. Totalt handlar det om 60-70 pilotprogram med drygt 150 banker över ett 30-tal länder. Notabelt är

att pilotprogrammen främst genomförs i Asien och Europa där även en svensk del ska påbörjas under sommaren. Asiatiska regeringar som Singapore och Japan satsar hundratals miljoner dollar på att skynda på utvecklingen kring SET och elektronisk handel. Däremot har aktörerna i USA varit sena i starten.

I den svenska SET-piloten deltar fyra banker, Handelsbanken, Postgirot, S-E-Banken och Sparbanken Sverige, med en försöksverksamhet där upp till 8000 innehavare av Visakort från någon av bankerna ska kunna betala i närmare 30 svenska Internetbutiker som efterhand ansluter till projektet.

- Intresset för projektet är stort, både från köpare och säljare, berättar Ingemar Kjellberg, projektledare för den svenska SET-piloten som är en del av ett större europeiskt projekt i Visas regi med 38 europeisk banker i 16 länder inblandade. De svenska bankerna har gemensamt valt IBM som systemleverantör.

Visas SET-pilot har också en finsk gren som kommer att samordnas med det svenska försöket. 2000 finnar kommer att vara inblandade och kunna handla även i de svenska butikerna utöver de 20 finska som ska delta.

Även Mastercard/Europay genomför SET-piloter i Europa, bl a i Danmark där förlaget Egmont provat sedan årsskiftet. Pilotprojekt pågår också bl a i Irland, Spanien, Tyskland, Taiwan, Singapore, Japan och USA. Den förste amerikanske handlaren att prova SET var Wal-Mart Stores (http://www.wal-mart.com/) tillsammans med American Express. Ledande företrädare för inblandade företag har världen över köpt CD-skivor, böcker, Guinness öl, minnesfrimärken och svängborrar för att demonstrera SET i drift.

Inledningsvis har pilotprogrammen baserats på enskilda system där både kund och handlare haft samma bank med programvara från samma leverantör och certifikat från samma utgivare. I takt med att pilotprogrammen blir mer verklighetsnära kommer samverkan mellan olika system att bli allt mera viktig. Det är självklart så att exempelvis en S-E-Bankskund med Mastercard, en plånbok från Netscape och certifikat från GTE ska kunna handla av en handlare med konto i Nordbanken och certifikat från Verisign via IBM:s shoppingprogramvara.

I den svenska SET-piloten kan enbart Visakort användas, men under 1998 har man för avsikt att släppa på begränsningarna, både vad gäller antalet användare och vilka kort som kan tas emot.

Klart till jul?

Men det kommer dröja innan SET driftsatts på allvar. Tidigast under september kan man räkna med att de första godkända SET-systemen finns klara. När den kompletta specifikationen av SET nu finns klar måste alla utvecklare skriva ny programvara eller uppdatera befintliga system som överensstämmer med specifikationen. Ett program får dock inte kallas SET-kompatibelt om det inte testats av en speciell instans utsedd av SET-konsortiet. Denna instans har inte ens utsetts ännu och kommer därför inte att kunna starta sitt arbete förrän i september. SET-konsortiet hoppas kunna ha produktionssystem klara först till julhandeln 1997.

Man kan dock räkna med att alla användare har tillgång till en elektronisk plånbok med stöd för SET i framtiden. Konsumenternas elektroniska plånböcker kommer att färdigställas för SET efterhand och automatiskt ingå i populära programpaket. Exempelvis arbetar Netscape med Cybercash om en SET Wallet som ska ingå i kommande versioner av Communicator och även Microsoft kommer att bygga in en SET-plånbok i Explorer 4.0. Däremot måste konsumenten själv skaffa ett giltigt certifikat innan hon kan börja handla.

Den nya SET-tekniken måste också marknadsföras mot konsumenterna i syfte att minska misstron mot elektronisk betalning. En rejäl marknadsföringskampanj från kortföretagen och bankerna kring fördelarna med SET efterfrågas av handlare i USA. En sådan kampanj skulle kunna få stor betydelse och förändra inställningen till elektronisk handel om kända och betrodda företag ställer sig bakom.

Ulf Wingstedt, Mattias Axling

Cybercash förlorar första ronden (6/97)

Amerikanska företaget Cybercash hör till pionjärerna kring elektronisk handel på Internet. Företaget grundades redan i webbens barndom och hade snabbt prototyper klara med den egna SIPS-tekniken för kreditkortsbetalning med god säkerhet. Ganska snart fanns också en färdig produkt på marknaden, men därefter har det gått trögt.

Få företag har valt att satsa på Cybercash, varken banker eller butiker har valt Cybercash produkter. På den viktiga amerikanska marknaden för internethandel är Cybercash i princip osynligt, trots att ett stort antal företag säljer mot kreditkortsbetalning. Istället används enklare lösningar, ofta helt utan kryptering eller andra säkerhetsarrangemang, någon gång SSL-krypterat. Resultatet har blivit stora förluster för Cybercash. Nyligen hade aktiekapitalet återigen nästan förbrukats och riskkapitalister tvingades skjuta till nytt kapital. Trots misslyckande hittills finns det fortfarande investerare som hoppas på Cybercash.

En av de förhoppningsfulla är Jens Claesson, VD på det svenska företaget Pronoma som tillhandahåller en Cybercash-baserad betalningstjänst på den svenska marknaden. Det har hittills gått mycket trögt att få svenska företag att sälja med Cybercash, men när SET introduceras under hösten hoppas Pronoma att hela marknaden för elektronisk betalning ska skjuta fart. Cybercash planerar att SET-anpassa sin produkter under hösten.

Den gemensamma SET-standarden kommer att innebära stora förbättringar för både kunder och butiker, säger Jens Claesson. De användare som skaffat Cybercash SET-anpassade elektroniska plånbok kommer att kunna använda den mot alla SET-kompatibla serverprogram, t ex från IBM. På samma sätt kan butiker med Cybercash serverprogram ta betalt från kunder med andra elektroniska plånböcker som följer SET.

Förtvivlade kunder

Att kunderna ska kunna utnyttja elektroniska plånböcker från andra leverantörer kan kanske bli räddningen för Cybercash. Många kunder har nämligen haft problem med att få Cybercash plånbok att fungera på den egna datorn. - Vi har fått flera förtvivlade samtal från kunder som försöker köpa våra produkter på Internet men som inte lyckats installera Cybercash plånbok, berättar Mattias Hällström på SISU som ansvarar för betaltjänsten Virtual Workplace. - För oss som handlare var det mycket enkelt att komma igång med betalning, men vi har utan tvekan tappat kunder pga den höga tröskel som installation och handhavande av Cybercash plånbok innebär, fortsätter han.

Det är oklart varför inte Cybercash lyckats få ordning på programvaran. Flera av felen är av enkel karaktär och har varit kända länge, men inga nya korrigerade versioner har släppts. Cybercash nonchalans kring det som borde vara huvudprodukten tyder på att fokus ligger någon annanstans. Och även om det är tråkigt för de tjänsteleverantörer som försöker sälja på Internet med Cybercash idag, så kan Cybercash prioritering vara riktig på sikt, åtminstone för Cybercash. Marknaden för speciella elektroniska plånböcker för kreditkortsbetalning lär i praktiken försvinna när såväl Netscapes Communicator och Microsofts Internet Explorer

inom kort kommer att innehålla SET-anpassade plånboksprogram som standard. Till yttermera visso lär Cybercash vara företaget bakom Netscapes programvara.

På serversidan har det också varit skralt med framgångar. Cybercash serverprogram för internethandlare kommer att anpassas till SET, men konkurrenterna med IBM i spetsen har redan sin programvara klar. Det är symptomatiskt att Cybercash inte deltagit i en enda av de SET-piloter som nu körs över hela världen, nästan samtliga baseras på programvara från IBM (Commercepoint).

Den första ronden, den om kreditkortsbetalningar på Internet, förlorade alltså Cybercash klart till SET-konsortiets banker och dataföretag trots att man hade rejält försprång med en nästan lika god teknik. Det återstår att se hur det går i nästa rond, den som handlar om de digitala kontanterna för mikrobetalningar. Där ställer Cybercash redan upp med Cybercoins, bankerna och de stora dataföretagen har dock inte gått upp i ringen ännu.

Ulf Wingstedt

Julhandla med SET? (7/97)

Det svenska stora pilotprojektet där SET-transaktioner ska provas i praktiken har försenats men förhoppningen är fortfarande att man ska vara igång i god tid före julhandeln. Det berättar Susanne Krutrök, informationsansvarig för SET-projektet på S-E-Banken Kort.

Bakom det svenska pilotprojektet står fyra banker, Handelsbanken, Nordbanken, Postgirot Bank och S-E-Banken, som var och en kommer att ta med sig 10-15 nätbutiker och 2000 användare in i det storskaliga försöket. Syftet med provet är att skaffa praktiska erfarenheter av användning av SET-tekniken tillsammans med kunder. Provet kommer att utföras med Visas kreditkort och S-E-Banken kommer att vända sig till nuvarande kunder som har visakort och som dessutom använder bankens övriga internettjänster. På så vis får man användare med vana av Internet och kort, vilket är en fördel.

Hittills har S-E-Banken kontrakterat tio handlare att delta i provet, men trycket från marknaden är stort och många fler vill delta, inte bara i provet utan också i skarp drift. - Vi har dock valt att i provet enbart samarbeta med medelstora och större företag som har den IT-mognad som krävs för att kunna ta emot beställningar på Internet, säger Susanne Krutrök.

Det är fortfarande hemligt vilka företag som kommer att delta, men enligt S-E-Banken kommer de från olika delar av landet och ur olika branscher, allt för att visa på internethandelns generella karaktär.

SET-projektet kommer att använda programvara och tjänster från tre olika leverantörer. IBM står för kopplingen mellan Internet och de normala banknäten via en sk Payment Gateway som blir gemensam för de fyra bankerna och som kommer stå placerad hos IBM. Det irländska företaget Trintech kommer att leverera programvara för handlare och kunder, dvs ett POS-system (Point Of Sale) där handlaren tar emot kundens kortbetalning samt en elektronisk plånbok för kunden.

Provet ska enligt plan pågå under fyra månader med start i november. Men de tekniska förberedelserna har försenats och det är troligt att starten skjuts upp minst några veckor. Det är många aktörer och system som ska samordnas och allt måste vara på plats innan testet kan inledas.

Vem saknar SET? (8/97)

Introduktionen av SET i Sverige har försenats igen. Intresset för att delta i piloten är dock fortsatt mycket stort bland svenska företag. Men under tiden har behovet av SET börjat ifrågasättas av allt fler.

Driftsättningen av SET har kantats av förseningar och problem. Över hela världen har mindre pilotförsök genomförts under, men inget system finns i drift ännu. Orsakerna är flera men först och främst beror förseningen på att den grundläggande SET-standarden försenades vilket i sin tur medförde att leverantörerna av de program som krävs inte kunnat få fram lösningar i tid.

Det första svenska pilotförsöket med SET drivs av fyra banker, S-E-Banken, Postgirot, Handelsbanken och Sparbanken i samarbete med Visa. Den första SET-transaktionen beräknas nu äga rum under januari 1998.

- Den här gången kommer inte tidsplanen att förskjutas, säger Susanne Krutrök på S-E-Banken. Vi har haft problem med att inte kunna testa vissa viktiga programkomponenter eftersom de varit försenade från leverantören, men nu börjar allt komma på plats fortsätter hon.

Det är naturligtvis mycket viktigt att SET-systemen testas noggrant före driftsättning. Det handlar om att dels driftsätta helt nya system, men också att integrera dessa med befintliga transaktionssystem.

- Vi prioriterar en säker och stabil produkt över allting annat, vilket gjort att vi reviderat vår svenska tidsplan. Kortkunder och säljföretag som handlar över Internet måste veta att SET-standarden verkligen fungerar, säger Ingemar Kjellberg, projektledare för den svenska SET-piloten.

- Ur bankernas synvinkel är det dock ganska enkelt, berättar Susanne Krutrök. En kreditkortsbetalning via SET når oss från kortföretagens nät på samma sätt som vilken annan korttransaktion som helst. Vi vill dock kunna särskilja internetköpen från övriga kortköp för bättre säkerhet, fortsätter hon.

Ingen SET till jul

Men för de företag som hoppats sälja sina varor på Internet under hösten och inför julen är besvikelsen stor och man befarar minskad försäljning.

- Vi hade räknat med att från i slutet av november kunna sälja flygbiljetter och olika typer av paketresor över nätet, berättar Christer Forsberg, VD för Affärsresebyrån i Umeå som är ett av de företags som ska delta i SET-piloten.

För Affärsresebyrån ger deltagande i SET en möjlighet att nå ut till nya kunder över hela Sverige. Christer Forsberg ser i SET en chans att komma till rätta med ett av de största problemen för internethandeln, bristen på förtroende. Förutom säker handel menar han att själva användningen av SET ger nätbutiken ett gott anseende och är en signal till resenären att tryggt kunna handla. - Det kommer att sålla bort oseriösa företag vilket behövs i resedjungeln, tror Christer Forsberg.

För att kunna fungera som nätbutik med SET-betalning har Affärsresebyrån och alla andra deltagare i piloten tvingats skaffa och installera en programvara som kan ta emot korttransaktionen och skicka den vidare till Visa och bankerna för verifiering och inlösen.

Affärsresebyrån har redan idag ett sk självbokningssystem på Internet där kunden kan se vad han bokar, tider, priser, bokningsnummer mm. Det enda som saknats är betalningsfunktionen.

- De tekniska erfarenheterna så här långt är positiva, säger Christer Forsberg. Det har varit enkelt att integrera SET-programvaran med våra egna system, enda problemet har varit bristen på information om hur SET-motorn fungerar.

Skarp SET i Sverige

Det svenska SET-projektet har från början valt att skapa en pilotfas som var så lik den efterkommande produktionsfasen som möjligt. Ambitionsnivån i det svenska pilotprojektet har utgått från att man vill möjliggöra för ett flertal butiker och ett större antal Visa-kortkunder att delta redan i uppstartsfasen. Dessutom betyder detta att det svenska SET-projektet använder vad man kallar "skarpa" krypteringsnycklar baserade på den senaste versionen av SET (version 1.0) istället för att använda testnycklar baserade på testversionen av SET. Några europeiska länder har redan startat sina pilotfaser av SET-projektet, och dessa baseras på testnycklar som kan användas fram till november i år. Därefter måste alla testnycklar ersättas av produktionsnycklar, eller "skarpa" nycklar.

26 företag har hittills annonserats som deltagare i piloten. Företagen kommer från hela landet och ur olika branscher.

- Att så många välkända företag med intressanta produkter och tjänster kommer att delta är viktigt för att ge de 8000 kortkunder som också är med i pilotprojektet ett brett utbud att välja ifrån, menar Ingemar Kjellberg.

Men kanske mer anmärkningsvärt är att många av de större nättjänsterna saknas, speciellt de från tidningsvärlden. Till exempel finns varken DN eller Aftonbladet med, företag som i många andra sammanhang varit pionjärer för ny teknik och tillämpning på nätet.

Aftonbladet ligger lågt

- Vi har valt att ligga lågt med SET just nu, säger Henrik Barkefors från Aftonbladet som bl a arbetar med Aftonbladets, Svenska Dagbladets och Göteborgspostens tjänst Mediearkivet. Vi upplever att programleverantörerna har svårt att finna en bra form för att ansluta nya handlare. Vi vill inte skaffa ny teknik innan vi vet hur den ska hanteras.

Mediearkivet var en av de första i Sverige med att kunna ta emot kreditkort på Internet och använde både Cybercash lösning, som liknar SET, och vanlig krypterad mottagning. Men sedan i våras har båda systemen varit avstängda då Aftonbladet upptäckte oklara ansvarsförhållanden gentemot tjänsteleverantörerna för de risker som förknippades med korthanteringen.

Henrik Barkefors är inte ensam om att ifrågasätta behovet av SET. I teorin har de flesta leverantörer av program för säkerhet och betalning på Internet sagt sig stå bakom SET-standarden, men i praktiken är det få som har produkter färdiga eller ens under utveckling. Vissa systemleverantörer säger nu att några färdiga SET-anpassningar kommer det inte att bli tal om förrän mot slutet av 1998, andra vill inte ens ange ett datum längre.

Alternativet till SET är kreditkortsbetalning via SSL-krypterad förbindelse, en lösning som redan används och som enkelt kan utnyttjas av flera. SSL-krypteringen har dock två viktiga nackdelar gentemot SET, dels kan inte handlare och köpare säkert identifiera varandra, dels kan handlaren se kreditkortsnumret. Men SSL upplevs ändå av många som tillräckligt säkert. Jim Bidzos, VD för det kända säkerhetsföretaget RSA pekar till exempel på enkelheten i att använda SSL och det faktum att SSL-stöd finns i alla moderna nätbläddrare.

Inte bara SET för kortföretagen

SSL har också stärkt sin ställning under hösten då de båda kortföretagen Visa och Mastercard lanserat en ny policy (i USA) där kortinnehavare som använt kortet på Internet helt slipper ansvar för eventuella stölder. De båda kortföretagen har tidigare varit tveksamma till

internetbetalning som inte använder SET men detta verkar alltså vara på väg att vända. Ett ytterligare exempel på det är den webtjänst som Visa har tillsammans med Yahoo där webplatser med kortförsäljning listas. Ingen av dem använder SET.

Bland internetleverantörerna (sk ISP, Internet Service Provider) finns det allt fler som erbjuder SSL-betalning som en tjänst. I Sverige är det ISP:er som Förenade X och Bahnhof som har SSL-betalning via utländska partners men även utländska ISP:er kan användas direkt av svenska företag. Därigenom kringgår man svenska bankers ovilja att acceptera SSL. Ett färskt exempel är SSC Satellitbilds försäljning av satellitbilder mot kreditkort där Bahnhof förmedlat en SSL-lösning med en amerikansk korthanterare.

En del företag har dock varit skeptiska mot att lämna ifrån sig hanteringen av betalningarna till ISP:er som oftast är små datakonsultföretag utan tidigare erfarenhet av betalningssystem. Aftonbladet är ett exempel på detta. Men i takt med att internetbetalningar blivit allt mer accepterat har även större aktörer gett sig in på marknaden. En av världens största ISP:er, amerikanska PSINet har tillsammans med engelska Worldpay och National Westminster Bank nyligen lanserat en tjänst speciellt anpassad för internationell näthandel där man erbjuder internetbetalning med kreditkort där priser automatiskt kan konverteras mellan upp till 16 olika valutor.

SET kan innebära dyr affär

Ett annat hot mot SET:s vidare spridning är kostnaderna. För det första krävs stora investeringar av systemleverantörerna för att anpassa programvaror till SET-betalning, kostnader som självfallet hamnar hos köparen till sist. För det andra har vi bankernas kostnader som via en transaktionsavgift drabbar handlare och konsumenter, och till sist kortinnehavarnas avgifter för certifikat mm.

Företrädare för de banker som deltar i den svenska SET-piloten har nämnt avgifter för kortinnehavare på mellan 50 och 100 kronor. De svenska säljföretagen kan också komma att behöva betala en några kronor högre transaktionsavgift än för andra kreditkortsbetalningar. Transaktionsavgiften är speciellt viktig eftersom den sätter en gräns för hur små belopp som lönsamt kan hanteras. Bankerna nämner här belopp mellan 100 och 200 kronor som nedre gräns.

Bland systemleverantörerna är det alltså fortfarande få som lanserat SET-anpassade system. IBM hör dock till den exklusiva skara som idag säljer SET-färdiga butikssystem för Internet. IBM:s billigaste lösning riktad mot små och medelstora företag heter Net.Commerce START och kostar kring 5000 dollar.

Ulf Wingstedt

Deltagarna i svenska SET-piloten (8/97)

När SET-piloten äntligen lanserades fanns följande företag med bland handlarna:

24 Store http://www.24store.com	Adlibris http://www.adlibris.se
Affärsresebyrån i Umeå http://www.affarsresor.com	Akademibokhandeln http://www.akademibokhandeln.se
Apollo Resor http://www.apollo.se	Bonnier Online http://www.bokhandeln.com
City	Doro

http://www.gmp.se/city	http://www.doro.se
Dustin http://www.dustin.se	ETC Produktion http://www.etc.se
Euroflorist http://www.euroflorist.se	Expressfood http://www.expressfood.kf.se
Gant Stores http://www.gant.com	Interflora http://www.interflora.se
Medströms Multimedia http://www.kiosken.com	NK Hallen http://www.nk.se
Nokia/Geab http://www.shop.nokia.se	Peak Performance http://www.peakperformance.se
Per Dahlberg Elektronik http://www.pdeab.se/	Ring Up http://www.ringup.se
SJ http://www.sj.se	Telia http://www.telia.se
Ticnet http://www.ticnet.se	Vasaloppet http://www.vasaloppet.se
Videobutiken http://www.ideobutiken.se	Åhlens Multimedia http://www.ahlens.se

Förtroende och bedrägeri

Förtroende en nyckelfråga (4/97)

En av de starkaste trenderna inom Internethandeln just nu handlar om förtroende. Framväxten av en marknad på nätet är kanske inte så mycket ett utslag av en informationsekonomi som en förtroendeekonomi, en ekonomi som baseras på de senaste landvinningarna inom teknik och information. Tillväxten inom förtroendeekonomin baseras främst på möjligheten att säkra förtroendefulla relationer mellan handelsparter och i mindre utsträckning på teknik.

Elektronisk handel på Internet är förmodligen det mest tydliga exemplet på vad en marknad baserad på förtroende kan innebära. I undersökning efter undersökning är det tydligt att konsumenter upplever säkerhetsbrister vara det största hindret mot att handla på Internet. CommerceNets senaste undersökning pekar till och med på en ökad misstro. Ändå är det ett faktum att det redan nu är enkelt att bygga lösningar för betalning på Internet som är långt säkrare än exempelvis de kreditkortstransaktioner som vi dagligen gör i vardagslivets restauranger och butiker. Nätet har blivit en säker marknadsplats, men konsumenterna känner osäkerhet, de saknar förtroende.

Hur kan man då komma i den avundsvärda positionen att ha marknadens förtroende? En bra början är naturligtvis att äga ett inarbetat globalt varumärke som redan inger förtroende. Tidningar som Financial Times eller, på vår lokala marknad, Dagens Industri har det väl förspänt jämfört med de nya och små företagen som vill in på nätmarknaden. Men det man inte har får man skaffa sig!

I USA har konsumentorganisationen Better Business Bureau (BBB, http://www.bbbonline.org) tagit ett initiativ som man hoppas ska skapa ökat förtroende för Internet som marknadsplats. BBB har ett certificeringsprogram där godkända webhandlare får ett sigill i form av en GIF-bild att visa på webplatsen. Konsumenter kan klicka på bilden och få upp en sida med information om företaget i fråga, bakgrund, antal år i branschen, styrelse mm. Hela processen har inbyggda säkerhetskontroller för att försäkra att inte sigillet används av någon som inte certifierats av BBB.

BBB menar att initiativet är viktigt för att det bekräftar för potentiella köpare att Internet är "på riktigt". Internet är ett nytt medium där konsumenterna inte får de traditionella ledtrådarna

om handlarens ärlighet genom att se varorna och butiken eller prata med en expedit. BBB tror att drygt 3000 webplatser kommer att ha sigillet före årskiftet 97-98.

Ett liknande initiav kommer från Electronic Frontier Foundation och CommerceNet och kallas eTrust (http://www.etrust.org). Här handlar det om skapa förtroende kring det informationsutbyte som äger rum mellan kund och webplats. Många känner oro inför vad som händer med den information de frivilligt och/eller ofrivilligt lämnar ifrån sig när en webplats besöks. Det kan handla adressinformation men också loggar av vad man köpt, läst, laddat hem mm.

Som medlem i eTrust deklarerar man klart och tydligt, också via ett sigill, att man följer eTrust policies. Informationsutbyte kan ske på några olika nivåer:

	*Anonymt. Ingen information samlas med undantag för ev. fakturering och systemadministration*
	*Ingen insamlad information delges tredje part. Informationen används enbart för direkt kundtjänst.*
	*Tjänsten kan delge information till [Image] tredje part förutsatt att man talar om vilken information som kommer spridas, till vem och i vilket syfte.*

Företaget Verisign är ledande leverantör av digitala ID-handllingar för Internethandel. Alla innehavare av digitala ID:n kommer nu att få del av ett försäkringsprogram som ersätter förluster som beror på att den digitala ID-handlingen missbrukats av utomstående. Försäkringen kostar inget extra för kunden utan är ett sätt för Verisign att ta ansvar för sin produkt och dessutom visa vilket förtroende man själv hyser för sina lösningar.

Kombinationen av teknik, avtal och försäkringar är ett mycket bra sätt att bygga förtroende inför de nya lösningarna och om fler leverantörer tog samma ansvar för sina respektive lösningar skulle utan tvekan förtroendet för Internethandeln öka.

Att Internethandel nu handlar om att bygga förtroende är naturligtvis helt i linje med utvecklingen i samhället i övrigt där förtroendetrenden utvecklats under många år t ex genom kvalitetssäkringsprogram, utveckling av kundservice mm. Ett aktuellt exempel på vad förtroende kan innebära är barnmatstillverkaren Findus misstag att förneka förekomsten av utländskt kött i några leveranser barnmat. Den direkta faran för svenska barn var naturligtvis minimal, men konsekvenserna av att förtroendet för Findus produkter minskat kan bli betydande.

Enligt managementgurun Peter Keen handlar dagens informationssystemutveckling i grunden om att bygga förtroenden. Är det dags att byta IT mot RT, relationsteknologi?

Ulf Wingstedt

Säkrare för banker med fler bitar (5/97)

De amerikanska exportbegränsningarna för säker kryptering mildras nu för bankerna som kan erbjuda säkrare lösningar. På sikt kommer det även komma andra branscher till godo.

Amerikanska myndigheter lättar gradvis på de exportrestriktioner som hindrat amerikanska företag att exportera programvara med stark kryptering. Nyligen har såväl Microsoft och Netscape som ett antal mindre företag fått tillstånd att exportera krypteringsteknik med upp till 128-bitars nycklar för bank- och andra finanstillämpningar. Såväl datorindustrin som kongressen har tryckt på för att restriktionerna ska minskas.

Nyckellängden är helt avgörande för hur svårt det är att knäcka ett krypterat meddelande. Det tidigare gränsen har legat på 40-bitars nycklar, en nyckellängd som idag tämligen enkelt kunnat knäckas genom den sk "brute force" metoden, dvs att vanliga datorer sammankopplade i nätverk gissar sig fram. Den inbyggda kryptering som hittills funnits i bl a Netscapes och Microsofts Internetprodukter för export har alltså haft enbart 40-bitars nycklar.

128-bitars nycklar ger en avsevärd förbättring gentemot nuläget. För varje ytterligare bit i nyckeln fördubblas nämligen antalet möjliga kombinationer vilket gör att en 128-bits nyckel kan anta drygt 3*10E26 (en trea följt av 26 nollor) fler kombinationer.

Bara för banker

Netscapes produkter ska redan finnas klara med den nya krypteringen och Microsoft kommer att uppdatera sina produkter under de närmaste månaderna. Tidigare exporttillstånd för längre nycklar har alltid varit kopplade till ett tvång att deponera "huvudnyckeln" hos amerikanska myndigheter. Så är inte fallet denna gång men det finns ändå en begränsning, den starkare krypteringen förbehålls banker och andra finansiella aktörer. Det betyder att serverprogramvara med stark kryptering enbart kommer säljas till denna användarkategori, däremot kommer alla användare att få 128-bitsversioner av nätbläddrarna Communicator och Internet Explorer. Microsoft förväntar sig dock ytterligare lättnader under sensommaren och att man då kan erbjuda stark kryptering även till andra finansiella institutioner som försäkringsbolag och mäklare.

Utvecklingen mot allt längre nycklar drivs på av dataindustrin. Ett exempel är krypteringsföretaget RSA som ligger bakom en av de mest använda krypteringsalgoritmerna med samma namn. RSA utlyste i januari i år en tävling där de erbjöd 10 000 dollar till den som kunde knäcka ett meddelande krypterat enligt den konkurrerande krypteringstekniken DES. DES har sedan 1977 varit officiell standard för kryptering för bl a banker och använder en 56-bitars nyckel.

Knäckte koden

Den 17 juni, efter nära fem månader, kunde den rätta nyckeln tas fram och DES var knäckt. Vinnaren Rocke Verser skrev ett program som gissade nycklar och distribuerade sedan programmet till så småningom tiotusentals datorer hos frivilliga. Den rätta nyckeln togs fram av en enkel PC, Pentium 90.

Om vi i en framtid får miljontals krypterade transaktioner varje dag på nätet, så är det inte sannolikt att en liknande satsning från tio tusen hackers kan äga rum. Däremot ökar datorresurserna också snabbt och för bibehållen god säkerhet med dagens krypteringsalgoritmer måste nyckellängderna ökas.

Det knäckta DES-kryptot var alltså uppbyggt av en 56-bitars nyckel. I SET, den kommande standarden för kortbetalningar på Internet som bl a kortföretagen och bankerna står bakom,

används också DES för huvuddelen av krypteringen med en nyckel som bara är åtta bitar längre. Med motsvarande datorresurser som Rocke Verser lyckades samla ihop skulle det ta ca 100 år att knäcka ett SET-meddelande. Men, som sagt, datorerna blir allt snabbare.

Full säkerhet är dock inte enbart en fråga om avancerad kryptering. FBI har avslöjat en större stöld av kreditkortsnummer i Kalifornien. Stölden utfördes av en 36-årig hacker, Carlos Salgado, också han från Kalifornien.

Salgado bröt sig via Internet in i en Internetleverantörs dator där han installerade ett program som avlyssnade när Internetleverantörens kunder avgav användarnamn och lösenord. Med hjälp av denna information kunde han sedan komma vidare och stjäla hela registret med nära 100 000 kreditkortsnummer. Salgado spårades av FBI och avslöjades när han försökte sälja bytet till en FBI-agent.

Händelsen är allvarlig och visar med all önskvärd tydlighet att säkerheten fortfarande är bristfällig på många håll. Det kanske mest besvärande i hela historien är att Salgado inte ens kan anses som en speciellt talangfull hacker. Enligt FBI har han använt program som nästan vem som helst kan skaffa via Internet.

För företagen som sysslar med elektronisk handel kunde det blivit en PR-mässig katastrof, men reaktionerna har ändå inte blivit speciellt stora. Många är medvetna om att det finns brister i dagens system och att vi får räkna med en del gropar på vägen mot elektronisk handel. Det finns fortfarande många som använder föråldrade och bristfälliga säkerhetslösningar och inte kan skydda den information de lagrar på ett tillförlitligt sätt.

Stölden visar också på behovet av moderna och mer sofistikerade betalningssystem som Cybercash och SET-baserade lösningar där ingen känslig information kommer handlaren till del. Problemet med den vanligaste betalningsmetoden på Internet idag, att föra över kreditkortsnummer via krypterade förbindelser som SSL, är att även om själva överföringen är skyddad så finns ingen kontroll över att inte handlaren hanterar den överförda informationen slarvigt. Salgado skulle sannolikt inte kunnat stjäla kortnumren om Internetleverantören haft ordning på säkerhetsrutinerna.

Ulf Wingstedt

Säkra kort

Framtiden ligger i korten (7/97)

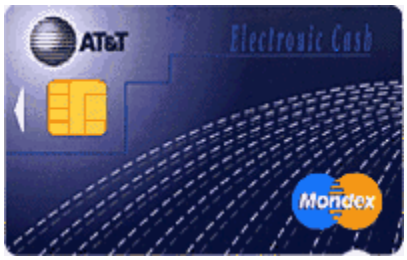
Betalning på Internet med kreditkort lär så småningom helt hanteras via SET-standarden. Däremot är det fortfarande osäkert hur betalning med digitala kontanter kommer att gå till. En intressant möjlighet är de smarta korten som med låga transaktionskostnader och stor spridning kan ta denna del av betalningsmarknaden på Internet.

Den egentligen enda framgångsrika betalningstekniken på Internet hittills baseras på kreditkorten. Den stora fördelen har varit att man direkt haft en mycket stor kundkrets som redan har kreditkort, internetbetalningen har därmed kunnat utnyttja en redan befintlig infrastruktur. Kreditkorten har dock även en stor nackdel, de kan inte lönsamt användas för små belopp. Gränsen för när kreditkort blir användbara brukar sägas ligga strax under 50 kronor. Dessutom finns det stora grupper användare på Internet som inte vill eller får använda kreditkort, t ex ungdomar under 18 år. Det finns därför behov av ett system för digitala kontanter, ett system som påminner om kontantbetalning i vanliga kiosker och butiker.

Under de senaste åren har flera system för digitala kontanter tagits fram och provats, men inget har lyckats slå igenom. Det kanske allvarligaste problemet har varit att dessa system helt baserats på Internet och inte varit möjliga att använda i den vanliga butiken. Den kritiska massan för att etablera en helt ny infrastruktur har helt enkelt inte funnits.

Kreditkorten visar vägen

Den framgångsrika användningen av kreditkort visar nu vägen, det handlar om att få ett system för digitala kontanter som kan användas såväl i butiken som på Internet. Bäraren av den datakraft som realiserar systemet förväntas bli de smarta korten (Smart Cards) som sedan en tid tillbaka introduceras i allt fler tillämpningar över hela världen.



Ett smart kort är ett plastkort stort som ett traditionellt kreditkort, men där kortets magnetremsa bytts ut mot elektroniska kretsar av samma typ som finns i datorer. Smarta kort används redan nu inom en mängd områden. Vanligast i Sverige är Telias telefonkort och smarta kort kommer på sikt att helt ersätta de kort med magnetremsor som nu används för olika former av kredit-, betal- och bonuskort. De smarta korten är dyrare än magnetkorten att tillverka (i dagsläget 3 – 5 dollar för ett smart kort mot 60 cent för ett magnetkort), men erbjuder många andra fördelar.

Den vanligaste typen av smarta kort är sk kontaktkort (Contact Card), som känns igen på de sex kontaktytorna mitt på kortet. Men det finns även kort utan synliga kontakter som får sin ström genom induktion och som därmed kan aktiveras beröringsfritt. Termen smarta kort är egentligen något missvisande, då det finns flera olika typer av kort som är mer eller mindre "smarta". Den enklaste typen är den som används i telefonautomater och bara innehåller "passivt" minne och fast logik för att styra funktionen. Ett telefonkort kan exempelvis enbart användas för att ringa i Telias automater tills markeringarna tagit slut, därefter kan kortet kasseras.

De kort som med rätta kan kallas smarta innehåller även en liten mikroprocessor som kan utföra beräkningar och styra kortets beteende. En funktion som kan realiseras i sådana kort är en elektronisk plånbok som kan fyllas på med digitala kontanter. Kort med elektroniska plånböcker provas sedan en tid i Sverige i några stora pilotförsök bl a i Uppsala, Kalmar och Halmstad där butiker och kiosker via speciella kortterminaler kan ta emot digitala kronor som betalning.

Bättre säkerhet med smarta kort

Smarta kort är säkrare än mjukvarubaserade lösningar och magnetkort. Informationen på kortet är kodad och kan inte avläsas ens genom att utifrån avläsa kortets minneskretsar. Kortet kan till exempel användas för att identifiera parterna vid en transaktion. De koder som identifierar parterna finns då endast på kortet och kan inte läsas utifrån eller manipuleras. Fördelar gentemot dagens magnetkort är bland annat minskad datatrafik eftersom säkerhetskontrollen kan ske lokalt vid betalning. Dessutom kan kortet skräddarsys för olika ändamål, till exempel förses med olika kredittak för olika kundgrupper, spärras för användning i ej godkända butiker eller automatiskt upphöra att gälla vid en viss tidpunkt.

Smarta kort kan även användas off-line, vilket gör att de kan användas där direkta nätförbindelser inte är tillförlitliga eller för dyra. Kort från engelska Mondex kan till och med användas för direkt överföring av kontanter mellan två individer.

Smarta kort kan även användas i andra tillämpningar som ej inbegriper pengar, främst för att lagra personliga certifikat (ID:en) och därigenom användas för identifiering. Till exempel kräver SET-standarden för kreditkortsbetalning att parterna kan identifieras och ett system där certifikaten lagras på smarta kort istället för på användarens PC har presenterats av en företagsgrupp. Också ett svenskt projekt kallat "Strategisk samverkan" arbetar på att utveckla smarta kort som kan användas för identifiering. Projektet drivs av Posten, bankerna och Telia.

Sätt allt på ett kort

Ett smart kort behöver heller inte enbart användas för endast ett ändamål. På ett och samma kort kan flera olika tillämpningar finnas, som elektronisk plånbok, identitetskort, telefonkort, kollektivtrafik, kundtrohetsbonus och SIM (Subscriber Identity Module) för mobiltelefoner. Sådana flerfunktionskort finns redan för ett flertal tillämpningar. Som exempel kan nämnas MobilSmart, en tillämpning från Postgirot Bank, där GemXplore SIM-kort används för att administrera konton och göra utbetalningar från kundens mobiltelefon. Man kan också använda kortet för att lagra annan information, som adressbok och kalender. Det är bara minneskapaciteten på kortet som begränsar. För en bra sammanställning av olika smarta kort och deras användning, rekommenderas ett besök på URL:en http://www.smartcard.co.uk/cgi-bin/everett/library.pl.

Samma kort som används för att betala i butiker kan alltså också användas för handel på Internet. Det som krävs för att kunna handla är att en kortläsare ansluts till datorn. Även om datorer med kortläsare ännu är sällsynta, så kan det väntas bli standardutrustning för persondatorer. Drivkraften bakom detta är inte enbart elektronisk handel, utan att de smarta

korten med fördel kan användas för certifikat och identifiering av användare även i andra sammanhang som t ex behörighetskontroll vid inloggning. Bland annat har HP och Microsoft sagt sig ha tangentbord med inbyggda kortläsare på gång.

Kortläsare i form av PC Card-dosor för bärbara datorer har också tagits fram där det smarta kortet kan skjutas in i ett fack i PC Card-dosan. För de stationära skrivbordsmaskinerna kan kanske en billig lösning vara en kombinerad kort- och diskettläsare. Ett diskettliknande fodral sköter avläsningen av kortet, fodralet kan i sin tur skjutas in i datorns diskettläsare.

Jämfört med konkurrerande mjukvarubaserade lösningar som E-cash, Millicent m fl för kontant betalning kan många av problemen lösas med smarta kort, t ex kontroll av dubbelspendering, nödvändigheten av central clearing av transaktionen och att de mjukvarubaserade systemen endast kan tillämpas för internethandel. Kortbaserade system blir också portabla och inte låsta till användarens dator.

Många problem lösta

Att bygga ny infrastruktur tar tid. De smarta korten har en mer än 20-årig historia bakom sig utan att hittills lyckats etablera sig utanför nischtillämpningar, varför skulle det lyckas nu? Det första problemet man fått bukt med är tillverkningspriset som länge var mycket högre än för kort med magnetremsa. Det andra problemet var, och är fortfarande i viss mån, att olika leverantörers kort ej kan användas tillsammans, de är inte kompatibla. Nu har dock marknadsstandarder börjat falla på plats, inte minst Java Card-specifikationen som gör det möjligt att köra javaprogram på kort från olika leverantörer. Det är samma teknik som gör att Java Applets kan köras på olika datorer som används i de smarta korten. Kortföretaget Visa är ledande aktör bakom Java Card, medan konkurrenten Mastercard står bakom en annan lösning, Multos. Båda alternativen har dock brett stöd på marknaden och det återstår att se om det finns plats för två lösningar, eller om de kommer att förenas.

Arbetsgruppen PC/SC, en sammanslutning av en lång rad ledande företag ur data- och kortbranscherna, har i december 1997 släppt den första versionen av en plattformsoberoende specifikation av hur smarta kort kan integreras med persondatorer. Standarden är ett stort steg mot bred användning av smarta kort.

Med tanke på att PC/SC-gruppen samlat alla stora dator- och programtillverkare inklusive Microsoft, IBM och Sun samt kortföretagen Siemens-Nixdorf, Gemplus m fl lär uppslutningen kring standarden bli god. Vi kommer därför under 1998 se många nya produkter och lösningar som använder smarta kort på PC. Till exempel kommer Hewlett-Packard att släppa ett tangentbord med läsare för smarta kort enligt PC/SC under första kvartalet 1998. Den första plattform som kommer att innehålla en realisering av PC/SC-standarden blir Windows i 32-bitsversion (95 & NT)

Det tredje problemet har varit bristande engagemang från de stora aktörerna på den finansiella marknaden, främst kortföretagen med Visa och Mastercard i spetsen och bankerna. Även detta ändras dock nu. Exempelvis har Visa bestämt sig för att med början tidigt nästa år börja byta ut alla kort med magnetremsa mot smarta kort av flerfunktionstyp. Mot slutet av 1998 förväntas 2-3 miljoner kortinnehavare i USA att ha de nya korten och mer än 200 miljoner över hela världen kommer att ha smarta visakort år 2001, dvs en tredjedel av alla visakort ska då vara utbytta.

Skeptiska handlare

I Sverige har flera banker varit inblandade i stora pilotförsök som omfattat hela städer. Erfarenheterna därifrån är dock blandade. Medan bankerna är positiva och verkar bestämt sig för att driva på införandet av smarta kort, så uttrycker majoriteten av handlarna skepsis mot korten. Vanligen var kort populära till en början, men efter en tid minskade användningen av korten till mycket låg nivå. ICA-handlare i Uppsala säger att efter nio månaders användning så sker mindre än en halv procent av omsättningen via kontantkortet.

Erfarenheterna från pilotförsöken ger att man i princip är nöjd med de tekniska lösningarna, men huvudorsaken till handlarnas missnöje är att ekonomin blir för dålig. Förutom att tvingas hyra eller köpa kortläsare tillkommer en avgift per transaktion som överstiger kostnaden för hantering av de vanliga mynten och sedlarna. Dessutom minskar kundernas användning av kontanter bara i liten utsträckning.

Ytterligare problem vid införande av en ny infrastruktur för små betalningar är att alla apparater som läsk-, godis-, telefon- och parkeringsautomater måste byggas om eller bytas ut.

För bankerna är det dock bara en tidsfråga innan de smarta korten är här. De jämför med de tio år som krävdes för bankomaterna att accepteras. För att bryta dödläget provar man dock nya lösningar, främst är flerfunktionskorten lovande. Med ett gemensamt kort för kredit- och kontantbetalning slipper kunden skaffa fler kort och handlaren behöver bara en kortläsare.

Den tekniska utvecklingen ger också kort med allt bättre prestanda och vi kan vänta oss att få se fler och fler tillämpningar på samma kort. Kombinationer av olika tjänster kommer att bli allt vanligare. I framtiden hägrar, för vissa, ett anpassningsbart universalkort för alla typer av tillämpningar: ID-kort, passerkort, betalkort, kollektivtrafik, patientjournal, telefonkort, mobiltelefoner och samtidigt adressbok, kalender eller varför inte personliga inställningar för bilen. Det gäller bara att inte tappa bort det.

Mattias Axling, Ulf Wingstedt

Mikrobetalningar

Megavinster från mikrobetalningar (3/97)

Användningen av kreditkort blir allt vanligare världen över. Siffror från Visa anger att enbart Visa-kortet handhar 8,5% av värdet av alla personliga inköp i USA under sista kvartalet 1996. Det är en ökning med en hel procent från samma period bara ett år tidigare. Antalet transaktioner ökar än snabbare med 40% för betalkorten under 1996.

Även på Internet är kreditkorten den vanligaste betalningsformen. Otaliga är de sajter som säljer såväl hårda varor som informationstjänster och som tar emot kreditkortsnummer on-line. Det finns också flera tämligen etablerade system för kreditkortsbetalning i drift, Cybercash, SSL m fl.

Men kreditkorten har en ibland avgörande nackdel, transaktionsavgiften. För varje korttransaktion får handlaren betala en avgift till kortutgivaren som beror dels av transaktionsbeloppet, dels av en fast avgift. Avgifterna är visserligen små, typiskt någon procent, men speciellt den fasta delen omöjliggör effektivt en lönsam hantering av försäljning till låga priser. Generellt sett kan först belopp över 30 kronor bli lönsamma för kreditkortsbetalning.

Att sälja på Internet till låga priser, eller sk mikropriser, är något som diskuteras intensivt bland internethandlare in spe. Det är en spridd uppfattning att konsumenternas tveksamhet inför att handla på Internet minskar om varje inköp i sig inte är kostsamt. Man talar om "pay-per-view" där t ex en tidning skulle kunna ta några få ören, eller till och med delar av ett öre, för varje artikel läsaren klickar fram.

Sådana mikrotransaktioner ligger naturligtvis långt under gränsen för när kreditkortsbetalning är lönsam. Möjligen kan man med någon sorts uppsamlingsfunktion ta hand om många mikrobetalningar som samlat debiteras användarens kort (jämför markeringarna på teleräkningen), men annars måste alternativa betalsystem användas, system som bygger på elektroniska kontanter. Och intresset för mikrobetalningar är stort, optimisterna ser en mångmiljardmarknad att ta hand om.

Siffrornas magi

Det totala värdet av alla transaktioner med små belopp är överväldigande. Enligt undersökningsföretaget FutureScan görs 300 miljarder kontantinköp varje år i USA och Visa uppskattar värdet för alla kontantinköp under 10 dollar till mer än 1 800 miljarder dollar. Vilken handlare som helst skulle vara nöjd med en mycket liten andel av dessa transaktioner!

Men den digitala ekonomin är annorlunda. Även om man skulle kunna köpa en chokladbit för en femkrona är det ingen som accepterar 30 kronor för frakt och expeditionskostnad plus att chokladen kommer fram först tre dagar senare. Därför fokuseras intresset mot produkter som kan levereras automatiskt direkt över nätet, musik, filmer, textdokument etc.

Hur stor är då en mikrobetalning? Eftersom begreppet mikrobetalning har blivit ett positivt värdeord menar de flesta systemleverantörer att de hanterar mikrobetalningar idag, även om

beloppen kan vara tämligen stora. Låt oss införa ett nytt begrepp, minibetalning, och använda följande skala:

- Betalning:50 - 500 kronor
- Minibetalning:5 - 50 kronor
- Mikrobetalning: under 5 kronor

Enligt vår skala blir kreditkort aktuellt först i övre delen av minibetalningar. Även det e-postbaserade betalningssystemet från First Virtual hamnar över gränsen för mikrobetalningar. Orsaken är en avgift om två procent av köpesumman plus 29 cent per transaktion. First Virtual rekommenderar själva inte att systemet används för belopp under en dollar.

Dyrt att mikrobetala med telefon

Inte heller betaltelefonnummer (0719-nummer) är lämpade för mikrobetalningar. Betaltelefonnummer används av flera av de svenska pionjärerna vad gäller betalning på Internet, t ex Mediearkivet och några av porrtidningsförlagen, och innebär att kunden köper ett lösenord genom att ringa ett betaltelefonnummer. Priserna styrs till viss del av vad som är möjligt att hantera via betalnumren och kan ligga mellan 5 kronor och 700 kronor, men det är bara en del av priset mot kund som når handlaren.

För att sätta upp en internettjänst med betalning via telefon anlitar man helst ett konsultföretag som är specialister på betaltelefontjänster för att hantera transaktionerna. Konsultföretaget säljer lösenord till kunden som denne sedan kan använda som betalningsbevis på nätet. Handlaren får sin ersättning från konsultföretaget.

Per Ummer från Mediasvar, ett konsultföretag som erbjuder betaltelefontjänster, berättar att ca 85% av priset mot kund efter moms kvarstår efter Telias avdrag. Därefter avgår Mediasvars transaktionskostnad som vanligen varierar mellan en och fem kronor per lösenord beroende på hur mycket arbete som krävs av Mediasvar.

I praktiken är det först när priset mot kund närmar sig 30 kronor som betaltelefonnummer kan ge lönsamhet. Med uppsättningskostnader och andra avgifter kan det ändå bli så lite som tio kronor kvar till handlaren, dvs 70% bort.

Ett av problemen med mikrobetalningar är att kostnaden för att utföra transaktionen måste vara lägre än transaktionens värde. När transaktioner med delar av ören ska hanteras i stort antal krävs extremt effektiv användning av kommunikationsnätverk och datorkraft. Egentligen är det samma problem som drabbar kreditkorten även om beloppen där är större, hanteringen måste finansieras (samt ge vinst till kortföretagen).

Inga av de idag mest etablerade systemen kan alltså hantera mikrobetalningar. Hoppet står istället till ny och ännu oprövad teknologi, de elektroniska kontanterna.

Infopengen lockar

Under senare år har flera förslag till system baserade på elektroniska kontanter, eller infopengar, förts fram. Inget system har dock ännu etablerats på marknaden. Först ut var holländska DigiCash där användaren förvarar sina infopengar, ecash, som mynt representerade av krypterade sifferserier i en plånboksprogramvara i datorn. Trots flera års pilotförsök har fortfarande enbart ett fåtal banker gett ut ecash, däribland en finsk bank. Transaktionskostnaden för att hantera ecash beräknas vara endast ca ett öre, men det finns en osäkerhet över de verkliga kostnaderna för att hantera stora mängder ecash, speciellt som varje mynt används enbart en gång varefter det måste växlas in hos utgivande bank. Banken måste dessutom hålla reda på att inte samma mynt används flera gånger, all sådan hantering kostar självfallet pengar som i slutändan måste tas ut av konsumenten.

Forskningsprojektet NetBill från amerikanska universitetet Carnegie-Mellon riktade från början in sig mot mikrobetalningar (minst ca 30 öre) och har utvecklat ett system för främst informationsförsäljning. Systemet hanterar inte bara själva betalningen utan också leverans av varan, med kontroll av att betalningen först ägt rum. NetBill kräver att både kund och handlare har konto på NetBill-servern och att kunden installerar ett speciellt program. Visa har intresserat sig för NetBill som nu ska provas i begränsad omfattning för informationsförsäljning inom universitetet. De beräknade transaktionskostnaderna är låga, 10-20 öre, men även här finns tveksamhet pga de stora krav på kommunikations- och datakraft som krävs för att realisera systemet. NetBill är också ännu otestat under verkliga förhållanden.

Ytterligare ett system som befinner sig på försöksstadiet är Millicent från Digital. Millicent skiljer sig något från övriga system genom att det kan utnyttja flera parallella utgivare av infopengar vilket minskar belastningen på centrala servrar. Transaktionskostnaden beräknas bli mycket låg, mindre än ett öre styck. Digital talar också om möjligheten att inte bara kunden ska kunna betala handlaren, utan att också kunden ska kunna få betalt för prestationer som t ex att läsa en annons.

Cybercash har kompletterat sin elektroniska plånbok med infopengar, sk Cybercoins. Systemet bygger på att kunden sätter in pengar på ett konto hos Cybercash som sedan debiteras för köp. Cybercash är förhållandevis dyrt i drift, ca två kronor per transaktion, vilket gör det till ett gränsfall om mikropriser (< 5 kronor) kan hanteras lönsamt.

Billigare med smarta kort

En uppstickare bland systemen för elektroniska kontanter är de som baseras på sk smarta kort, Smartcards. Ett smart kort liknar ett kreditkort, men har försetts med en mikroprocessor istället för magnetremsa och kan därför fås att uträtta avancerade operationer. De smarta korten används redan som exempelvis telefonkort, men också som elektronisk plånbok där försök pågår i bl a flera svenska städer. De har dock inte ännu använts praktiskt på Internet, men smartcardbaserade system är på gång.

En av fördelarna med de smarta korten är att de förenklar processen att verifiera kundens identitet och hanteringen av infopengarna som kan lagras direkt på kortet. Identitetskontrollen kan ske off-line istället för on-line vilket minskar kommunikationsbehovet och därmed transaktionskostnaden.

Ett smartcardbaserat system kommer från engelska Mondex. Mondex-systemet har används i den fysiska verkligheten och tillåter till och med att två kortinnehavare överför kontanter sinsemellan, utan inblandning från någon central instans. Mondex, som nyligen förvärvats av Mastercard, har inlett samarbete med telekombolaget AT&T som ska använda Mondex-kort för internetbetalning i den betalservice de erbjuder sina kunder. Mondex-delen ska provas under sommaren och planeras att sättas i drift till hösten om allt går väl.

Men för att använda smarta kort krävs speciell hårdvara, en kortläsare som idag inte ingår i var mans PC. Detta problem kommer dock att lösas menar företrädare för dataföretaget Hewlett-Packard (HP). Enligt vad för HP säger i tidningen InfoWorld kommer tangentbord med inbyggda kortläsare att finnas från tillverkare som Microsoft, HP och Gemplus före årsslutet. Dessutom har lösningar presenterats där en kortläsare kan användas i form av ett PC-kort eller via diskettläsaren (i ett speciellt fodral i diskettstorlek).

Den långa raden av oförenliga betalningssystem som vi diskuterat ovan kan naturligtvis i sig vara ett hinder för utbredning av etablerade system. Varje system har sina brister och fördelar, sina egna konventioner och lösningar. Inget system kommer heller ännu i närheten av de

gamla hederliga metallmyntens enkelhet. Men ett större problem är att det fortfarande är oklart om det faktiskt finns en marknad för mikrobetalningar på Internet.

Vinnande affärsmodell saknas

Hittills saknas framgångshistorier där internetbutiker lyckats få megavinster från mikrobetalningar. Tvärtom, som redovisas i tidningen Wired, utrycker flera amerikanska företag tveksamhet inför en affärsmodell som baseras på informationsprodukter till mikropriser. En handlare medger, föga förvånande, att "få kunder har elektroniska pengar".

Patrick Toner, från databasvärden Lexis-Nexis anser vidare att det är bättre att fakturera kunden en månadsavgift, för en prenumeration, än att ta några kronor per dokument. Administration och annan hantering blir mycket enklare. Och en handlare måste naturligtvis fråga sig om det inte blir enklare att finansiera en tjänst genom att sälja några annonser än att ta fem öre per dokument av tiotusentals kunder och köptillfällen. Speciellt som det överhuvudtaget visat sig svårt att få internetanvändare att betala för något som förväntas vara helt gratis.

Dessutom, mikropriser tenderar att ge "mikromarginaler", dvs handlarens vinst på varje såld vara är mycket liten. Det innebär att en vinst mycket snabbt kan ätas upp av brister i systemen som leder till att kunder ringer och klagar, kräver support osv.

Men naturligtvis står vi också inför en hönan-eller-ägget situation, dvs så länge inget finns att köpa är ingen intresserad av att skaffa ett betalsystem och vice versa. För att dödläget ska kunna brytas krävs att en dominerande marknadsaktör etablerar en standard. Förmodligen är det enbart bankerna och kortföretagen som har kraften och förmågan att genomföra det.

Ulf Wingstedt

Skydda upphovsrätt på Internet

Sälj i digitala kuvert (6/97)

Flera kommersiellt fungerande lösningar för kontrollerad försäljning av digitala verk och varor börjar se dagens ljus. Med hjälp av de nya lösningarna ska handel med digitala varor över nätet skjuta fart. De närmaste åren kommer flera konkurrerande system för försäljning av digitala varor att introduceras.

Skyddande av ägande- och upphovsrätter för digitala varor har alltid varit ett problem för företag inom program-, medie- och innehållsindustrin, men Internets utveckling har gjort att problemen kommit i fokus på ett helt annat sätt än tidigare. De företag som idag äger och utvecklar stora mängder med digitala varor - musik, film, tidningar, fotografier, kurser och inte minst programvaror - tvekar att erbjuda dessa direkt på Internet. Om den som bekostat utvecklingen av en digital vara inte kan kontrollera hur den används och därmed säkerställa intäkter från nyttjandet så minskar snabbt ägarens intresse.

Nu pågår på flera håll ett intensivt arbete kring teknik och arkitektur för sk IPR-hantering (Intellectual Property Rights). Internet har radikalt förenklat spridningen av digitala varor och det handlar nu om att vända detta till sin fördel istället för att se enkel och snabb kommunikation och distribution som ett hot. Den tekniska utvecklingen är inriktad mot att ta fram dels teknik för att skydda upphovsrätter, dels infrastruktur för att kontrollera och mäta användning och samla in betalningar till de som äger rättigheterna. Ett komplett system som täcker in alla dessa delar kallas ett ECM-system - Electronic Copyright Management Systems.

Uppmuntra kopiering

Det största problemet kring IPR är inte, som man kanske kan tro, stöld av digitala varor från upphovsmannen. Istället är det den illegala vidarekopieringen som man måste kunna få bukt med, dvs att en kund som på lagligt sätt köpt en vara som han sedan skickar vidare till andra, illegalt. Men att hindra den första kunden från att skicka kopior vidare vore dumt, snarare bör man få de nya mottagarna att betala de också!

Denna modell brukar kallas superdistribution, det vill säga det är kunderna själva som sköter distributionen åt leverantören enligt en "mun-till-mun"-princip. Först när man försöker packa upp varan på den egna datorn behöver man betala. Tillvägagångssättet minskar också risken för problem med kunder som betalt men inte lyckats hämta hem varan samtidigt som den enkla och billiga distributionsmetoden kan leda till ökad försäljning. Möjligen kan superdistribution komma att bli modellen för framgång på informationsmarknaden. Men för att en sådan distributionsmodell ska kunna fungera krävs en väl fungerande infrastruktur av ECM-system.

Principerna för ECM-system är ganska enkla. Rättighetshavaren (författaren, kompositören, förläggare, programutvecklare etc) förser sina alster med "omslag" som anger hur det får

nyttjas. Det handlar om en uppsättning användningsregler som styr hur alstret kan användas och de kostnader som är förknippade med användandet. Alstret och reglerna stoppas in i någon form av virtuellt paket, kuvert eller behållare och krypteras. Sedan gäller det att ha en pålitlig infrastruktur där alla ingående systemkomponenter kan tolka och respektera de regler som följer med det upphovsrättskyddade objektet.

De system som finns eller är under utvecklingen skiljer sig åt i hur avancerade användningsregler som kan uttryckas, typ av paket och hur "pålitlig" infrastrukturen egentligen är. Inget system kan idag göra anspråk på att vara komplett. Tre kommersiellt tillgängliga infrastrukturer finns redan: IBM:s Cryptolope, svenska Buyonet från företaget med samma namn och Intertrusts DigiBox.

Sälj i digitala kuvert

IBM har utvecklat systemet Cryptolope. En digital vara, t ex en artikel levereras via nätet i ett krypterat "kuvert" (därav namnet Cryptolope). Kuvertet kan hämtas och lagras på hårddisken utan att kunden betalar för varan. Kuvertet innehåller förutom varan även prisinformation, det vill säga kuvertet "vet" vad det kostar att bli öppnat. När användaren bestämmer sig för att öppna det och titta på artikeln startar en hjälp-applikation till webläsaren där man anger sitt användarnamn och lösenord. Cryptolope-systemet bygger på att alla köpare är registrerade hos den som garanterar systemet, i dagsläget IBM. Hjälp-applikationen kommunicerar sedan med en server som kontrollerar att användarnamn och lösenord är giltigt.

Servern skickar tillbaka en krypteringsnyckel som gör att hjälpapplikationen kan öppna kuvertet. Därefter öppnas själva artikeln i webläsaren och först då sker betalningstransaktionen. Allt sker automatiskt utan att användaren ser vad som händer under ytan.

En poäng är att Cryptolope-kuvert kan kopieras och skickas vidare till någon annan, t ex med e-post. Om den personen då öppnar kuvertet får han i sin tur betala. Förutsättningen är förstås att han också har Cryptolope installerat. På så vis uppmuntrar Cryptolope till att informationen kopieras och sprids samtidigt som ägaren kan tjäna pengar varje gång information används.

Cryptolope används idag i IBM:s egen Web-tjänst InfoMarket men har ännu inte spridits vidare av IBM.

IBM samarbetar också med Xerox i syfte att kunna beskriva upphovsrätter och affärslogik i mer detalj. Exempelvis vill man kunna definiera regler som att "De två första sidorna får läsas fritt, sidan 1 får fritt kopieras. Bild 1 är gratis, bild 2 kostar 15 kronor".

Bygg värdekedjor

En annan lösning är DigiBox från Intertrust. Den fungerar ungefär på samma sätt som Cryptolope. En "skapare" tar sitt verk plus en uppsättning upphovsregler och stoppar in dem tillsammans i ett DigiBox-paket. DigiBox-paketet som är krypterat placeras sedan på en försäljningsserver hos en distributör. Denna kan i sin tur lägga till sina egna användningsregler och betalningsinformation. Detta är en speciell finess i DigiBox som gör att det går att bygga upp värdekedjor, där olika aktörer tjänar pengar genom att göra sina egna tillägg eller anpassningar. Från försäljningsserver kan användarna sedan komma åt olika DigiBox-paket.

När paketen väl öppnas och materialet nyttjas så informeras både en användningsserver och en finansiell server. Användningsservern samlar ihop och summerar användningen av ett visst objekt och skapar sedan rapporter som skickas till distributörer och upphovsmännen. Den

finansiella servern hanterar betalningar och ser till att pengar flyttas från användarens konto till upphovsmannens konto.

Precis som Cryptolope stödjer DigiBox superdistributionsmodellen. För närvarande finns DigiBox tillgängligt i form av ett utvecklingsverktyg för Windows 95 och Windows NT.

Svenska aktörer

Svenska Buyonets betalnings- och distributionssystem påminner om Cryptolope och Digibox. Via nätet kan kunden ladda hem den önskade varan i form av en körbar applikation. Applikationen hanterar betalningen och kan därefter packa upp varan. Kunden kan utan krav på registrering hos Buyonet välja mellan att betala via nätet med kreditkort, via faxad betalorder eller vanlig banköverföring och det går därigenom att undvika Internet som betalningsförmedlare om det uppfattas som osäkert.

- De flesta väljer att betala on-line, berättar Freddy Tengberg, VD på Buyonet. Hela 85% av kunderna har hittills valt betalning on-line medan resten är jämt fördelade på de övriga betalningssätten.

Buyonet använder brittiska National Westminster Bank för att ta emot kreditkort på nätet. Svenska banker tillåter som bekant inte korttransaktioner på Internet men bankvalet styrdes också av andra egenskaper.

- Buyonet riktar sig till en global kundkrets och vi vill kunna ge kunderna möjligheten att betala i lokal valuta, säger Freddy Tengberg. National Westminster Bank är den enda bank vi träffat på som inte är begränsad till det egna landets valuta vilket är en stor fördel, fortsätter han.

När en köpare utför en betalning med kreditkort on-line krypteras den först med SSL och skickas sedan till Buyonets server. Där packas kortinformationen om och skickas vidare på en privat ISDN-förbindelse till banken som verifierar kortet och utför transaktionen. Inom fyra sekunder brukar Buyonet få svar om köpet är godkänt eller ej och kan därefter ge kunden en kodnyckel för att "låsa upp" varan. Systemet är förberett för att kunna använda SET-standarden när den finns klar. Hittills är Buyonet själva de enda användarna av systemet i det programvaruhus som de driver på nätet. Planer finns dock på att licensiera tekniken vidare.

Ytterligare en spännande svensk lösning kommer från det svenska företaget OptiTech och kallas MediaDNA. MediaDNA bygger på Java och principen är att digitala varor bäddas in i en typ av "intelligenta objekt" som har en uppsättning beteenderegler på samma sätt som DigiBox-paketen. MediaDNA är fortfarande under utveckling och finns ännu inte som färdig produkt.

Även om de lösningar för IPR-hantering som är på gång inte fullständigt löser alla upphovsrättsproblem så är de ett gott steg på vägen. Ett viktigt delmål är att det åtminstone ska vara enklare att vara laglig än olaglig när man kopierar från nätet.

Peter Rosengren, Ulf Wingstedt

ID-kort för Internet

De nödvändiga certifikaten (9/97)

En av de viktigaste grundstenarna i den infrastruktur för öppen elektronisk handel på Internet som nu sakta tar form är säker identifiering av de parter som deltar i en transaktion. För flertalet kommande säkra betalningsfunktioner, däribland SET, är en digital ID-handling en förutsättning men redan idag kan sådana ID-handlingar, eller certifikat, köpas och användas på Internet för att realisera olika säkerhetsfunktioner.

Ett certifikat kan liknas vid en ID-handling och är ett digitalt dokument som innehåller information om utfärdaren, innehavaren och dennes krypteringsnycklar. Ett certifikat installeras och används tillsammans med andra program som t ex webläsare, e-postprogram eller webservrar som förpackar det i ett ofta enkelt användargränssnitt.

Det är fortfarande ovanligt att Internetanvändare och tjänsteleverantörer är innehavare av certifikat. Det är dock enkelt att skaffa ett certifikat för att till exempel göra det möjligt att skicka och motta krypterad e-post eller för identifiering på olika webplatser. Ett certifikat utgör också grunden för att kunna signera digitala handlingar med digitala underskrifter.

Det går snabbt att skaffa ett certifikat. Certifikaten utfärdas av företag som erbjuder detta som tjänst, ofta direkt på Internet. De utfärdande företagen kallas Certificate Authorities (CA) och den marknadsledande CA:n är amerikanska Verisign, ett företag som är specialiserat på digitala ID:n och som bl a både Netscape och Microsoft i första hand länkar till när det gäller att skaffa certifikat till sina webläsare. Proceduren är enkel. Genom att fylla i ett formulär där man uppger e-postadress, namn och några övriga uppgifter skapas ett certifikat som automatiskt installeras i exempelvis den webläsare som används vid registreringen. Det hela tar mindre än en minut att genomföra.

En CA utfärdar inte bara certifikat, utan är också kontrollant av att de är giltiga. Ett certifikat som används på Internet ska alltid vara möjligt att få verifierat av utfärdande CA.

Certifikat ger förtroende

Användning av certifikat har stora möjligheter att skapa det förtroende mellan handelsparter som krävs för att Internethandel ska komma igång på allvar. Genom att parterna visar varandra sina certifikat vet kunden att köpet sker från rätt nätbutik och säljaren vet att kunden är den han utger sig för att vara. Frågan om förtroende mellan handelsparterna överförs alltså till en betrodd tredje part, CA:n. Men när vilket företag som helst kan agera CA, vilkas certifikat kan man ha förtroende för?

Infrastrukturen för certifikat befinner sig i sin linda men växer sakta fram "organiskt" och styrs inte av någon central auktoritet eller myndighet i något land. Istället sköts hanteringen av marknadens aktörer och marknadsstandarder etableras och accepteras av alla stora leverantörer av programvara och tjänster som normalt inte har intresse av att konkurrera i denna fråga.

Det förtroende ett certifikat inger, dess styrka, bygger i grund och botten på hur väl innehavarens identitet kontrollerats av utfärdaren. Kontrollen kan utföras efter en rad olika metoder och med varierande noggrannhet beroende på respektive CA:s metoder, men också på de förtroendekrav som certifikatet ska uppfylla. En etablerad princip har blivit att dela in certifikaten i klasser beroende på styrka och därmed användningsområde. De sk klientcertifikaten som är de certifikat som är avsedda för användare av tjänster (personer) delas in i tre klasser.

Med Verisign som exempel är klass 1-certifikatet det enklaste med lägst styrka. Ett sådant kan man få ganska lätt, då det enda detta certifikat garanterar är att innehavaren verkligen har tillgång till en viss e-postadress. Namnet som är kopplat till certifikatet behöver inte ens vara innehavarens eget och ingen namnkontroll sker. Men kan ett sådant enkelt certifikat verkligen användas till något vettigt? Jo, redan klass 1 kan användas för att t ex signera och kryptera e-post eller för registrering och inloggning på de webplatser som stödjer certifikat.

Ett klass 2-certifikat kan användas för samma saker som klass 1 men här kontrolleras även innehavarens identitet, dvs att e-postadressen hör ihop med det angivna namnet som måste vara innehavarens. Personuppgifter kontrolleras av lämplig tredje part, där Verisign använder sig av Equifax som kan sägas vara en amerikansk motsvarighet till svenska DAFA/SPAR-registret.

Ett klass 2-certifikat ska även kunna användas för identifiering vid elektronisk handel och innehåller därför kreditkortsnummer. Ett sådant certifikat gör det alltså möjligt att avgöra om en person verkligen är innehavare av ett visst kontokort eller ej.

Klass 3-certifikaten är ännu starkare men kan inte skaffas direkt på nätet eftersom de kräver att identiteten personligen verifieras av tredje part som kan intyga identiteten. Denna bekräftelse skall sedan sändas till CA tillsammans med ansökan. Tillvägagångssättet påminner mycket om t ex Postens kontrollprocess bakom Postens vanliga ID-kort.

Samma klass – men olika styrka

Styrkan i certifikat av samma klass skiljer sig tyvärr åt beroende på utfärdande CA:s kontrollmetoder. Ett exempel är Thawte Consulting som har ett system där all information om användaren registreras och kontrolleras innan något certifikat överhuvudtaget utfärdas, oavsett vilken typ det är. Certifikatet kopplas till användarens nationella ID-kod (NIC), vilket i Sverige innebär personnumret. Företaget ämnar beivra missbruk av systemet genom att stämma missdådaren och/eller dennes arbetsgivare på stora summor. Hos Thawte är alltså användarens identitet kontrollerad även för klass 1-certifikat vilket ger ett starkare certifikat jämfört med Verisigns av samma klass.

Certifikat av klass 3-styrka är avsedda att användas för bank-på-nätet-tjänster och kommer att användas i Visas svenska SET-pilot med ett 30-tal nätbutiker och 8000 användare. Säker betalning med kreditkort enligt SET-standarden förutsätter att såväl köpare som säljare kan verifieras via certifikat. I Visas SET-pilot används certifikat från just Verisign som förmedlas till deltagarna via de svenska bankerna Handelsbanken, Postgirot, S-E-Banken och Sparbanken som gör erforderliga identitetskontroller. Piloten beräknas starta i slutet av januari 1998.

Utöver nämnda klasser av certifikat finns även andra för olika ändamål som för handel företag emellan på Internet (EDI). Speciella certifikat finns också för webservrar där man önskar använda den idag vanligaste betalningsmodellen på Internet, SSL-krypterad överföring av kreditkortsnummer. Ett servercertifikat är nödvändigt för att SSL-kryptering ska fungera eftersom certifikatet innehåller den viktigaste av de krypteringsnycklar som används.

Verisign har ansökningsformulär om servercertifikat för företag på Internet. Om företaget finns registrerat i Dun & Bradstreet databas kan man fullfölja registreringen online. Annars kan man sända organisationsnummer och för respektive land lämpliga handlingar och intyg med fax eller post till Verisign. Tillvägagångssättet ger ett certifikat med styrka motsvarande klass 3 för klientcertifikaten.

För att undvika totalt kaos med tusentals olika inbördes konkurrerande CA organiserar man sig i hierarkier där man via en topp-CA inbördes kan verifiera varandras certifikat. En sådan lösning kan dock ge problem med flaskhalsar i nätverkskommunikationen om t ex alla SET-transaktioner skulle behöva verifieras av Verisign i USA.

Arbete pågår också för att möjliggöra korsverifiering mellan olika CA-hierarkier vilket skulle innebära att varje CA:s certifikat skulle kunna verifieras av samtliga andra CA och det skulle bl a kunna reducera problemen med flaskhalsar. En intressant möjlighet som öppnas här är att exempelvis en arbetsgivare agerar CA för sina anställda och via korsverifiering gör certifikaten användbara globalt. Enligt företaget Entrust och övriga företag som stödjer detta system (bl a Bell, Cisco, GTE CyberTrust, Hewlett-Packard, IBM, Netscape) kommer denna modell att fungera bättre rent praktiskt eftersom varje CA som utfärdar certifikat kan kontrollera de som ansöker bättre än vad till exempel Verisign kan göra nu. Det kan dock noteras att Verisign inte står med på listan över företag som tycker att det här är en bra idé…

Det finns flera svenska företag som är tänkbara som CA. Självfallet är dagens ID-utgivare aktuella med Posten i spetsen men även bankerna och många dataföretag som WM-Data, Enator och AU System.

Ett certifikat för varje program och dator

Kostnaden för att erhålla ett certifikat varierar med styrkan. Ett klass 1-certifikat kostar knappt tio dollar, ett klass 2-certifikat knappt 20 dollar per år hos Verisign. Men då ingår även en försäkring som täcker innehavarens eventuella ekonomiska förlust eller annans missbruk av det digitala ID:et. Det är också troligt att vissa mycket betrodda CA kommer att kunna ta ett högre pris än mindre trovärdiga aktörer. Bankerna kan också komma att inkludera avgiften för certifikaten i allmänna avgifter för internethandel.

Den juridiska styrkan hos certifikaten och därmed de lösningar som baseras på dessa är fortfarande oklar. En digital signatur anses t ex ännu inte ha samma status som en namnteckning (frågan kartläggs just nu av svenska regeringen). Men informellt skulle man kunna jämföra klass 1-certifikat med ett medlemskort. Den du visar certifikatet för vet att det är samma person varje gång, men vet inte säkert vem du är. Ett klass 3-certifikat kan jämföras med en ID-handling, även om den inte är giltig som en sådan idag. Och liksom med de vanliga fysiska ID-handlingarna varierar styrkan med utfärdarens trovärdighet och kontrollsystem.

I jämförelsen med vanliga ID-handlingar och certifikat finns dock en viktig skillnad, certifikaten är inte alls lika "flyttbara" utan knyts inte bara till en viss e-postadress eller individ utan till en kombination av dessa plus den dator och det program certifikatet ska användas med. Om man t ex vill använda både Netscape och Internet Explorer på två olika datorer krävs fyra olika certifikat, eller om man önskar använda olika kreditkort från olika datorer krävs ett certifikat per kreditkort och dator.

En sådan begränsning i flyttbarhet är självfallet inte acceptabelt i en framtid när användning av certifikat krävs från allt fler tillämpningar. Det är också en kostnadsfråga. En möjlig framtid lösning kan dock bli de smarta korten som väntas få stor betydelse som bärare av digitala certifikat som då knyts till ett visst smart kort med kreditkortsnummer mm som innehavaren kan bära från en dator till en annan.

Ett smart kort kan alltså fungera som både "vanligt" ID-kort och som plattform för elektroniska transaktioner, till exempel underskrift av kontrakt med digitala signaturer. SET-certifikat kan t ex utfärdas tillsammans med kreditkortet och lagras på själva kortet. Spridning och användning av smarta kort ökar nu snabbt över hela världen och de stora kreditkortsföretagen planerar att under de kommande åren byta ut alla de magnetkort som nu används mot smarta kort.

Ulf Wingstedt & Mattias Axling