Elektronische betaalsystemen

Dr.ir. B. Schoenmakers
DigiCash B.V.
Kruislaan 419, 1098 VA Amsterdam
telefoon (020) 592 99 99.
email berry@digicash.com

Banken, creditcard maatschappijen en andere financiële instellingen verwerken hun transacties al tientallen jaren elektronisch. Twee recente ontwikkelingen geven het vakgebied van het elektronisch betalen een nieuwe dimensie. Ten eerste is er de introductie van grootschalige chipkaartsystemen, waardoor vele nieuwe mogelijkheden voor off-line betalingen gecreëerd worden. Ten tweede creëert het vooruitzicht van elektronische commercie over het Internet een grote vraag naar betaalsystemen voor open netwerken. We bekijken een aantal betaalsystemen en bespreken kort de gebruikte technieken.

De komst van electronische apparaten waarop geld in een digitale vorm is opgeslagen is een teken voor het brede publiek dat elektronische geldsystemen werkelijkheid worden. Voorbeelden zijn telefoonkaarten, chipkaarten (smartcards), en PC's verbonden aan het Internet.
Technisch gezien zijn er natuurlijk veel verschillen met baar geld, zoals we dat kennen in de vorm van munten en bankbiljetten. Conceptueel staan dit soort *prepaid* systemen echter het dichtst bij wat mensen als elektronisch geld ervaren.

Aan de andere kant werken banken en winkeliers al jaren met elektronische systemen voor het verwerken van creditcard betalingen. En sinds een aantal jaren is het bijvoorbeeld in Nederland ook mogelijk om PIN betalingen te doen (Eng. debit cards). Dit zijn belangrijke voorbeelden van zogenaamde *payment by instruction* systemen. Kenmerkend is dat een betaling in feite bestaat uit een opdracht om geld over te maken van de ene bankrekening naar de andere. Dergelijke opdrachten moeten online afgehandeld worden door een bank of creditcard maatschappij om de winkelier te garanderen dat de klant over voldoende geld op zijn rekening beschikt.

Met het succes van postorderbedrijven en de uitgebreide handel per telefoon en fax in het achterhoofd staan veel partijen te springen om betaalsystemen die geschikt zijn voor het Internet. Meer algemeen is er een behoefte aan systemen voor open netwerken, dat wil zeggen netwerken waartoe in principe iedereen toegang heeft. Denk bijvoorbeeld ook aan kabelnetwerken, de publieke telefoonnetten, en de netwerken die daar weer bovenop gebouwd zijn. Om aan deze vraag te voldoen worden er een groot aantal voorstellen gedaan. In dit artikel zullen we een paar mogelijkheden nader bekijken. Vanuit de eindgebruikers gezien is het onderscheid tussen wel of niet prepaid een van de belangrijkste aspecten. Een heel scala aan technologishe aspecten maakt het vakgebied van elektronisch betalen echter een ingewikkelde doch interessante aangelegenheid.

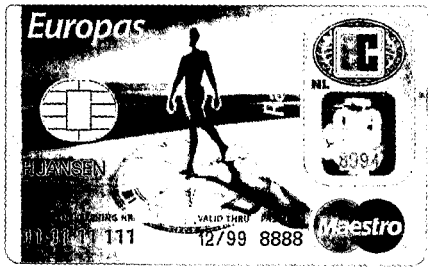
Cryptografie

Cryptografie speelt een grote rol in de moderne betaalsystemen. Zowel het vercijferen van boodschappen als het aantonen van de authenticiteit ervan wordt voor allerlei doeleinden gebruikt. Om een aantal redenen is de conventionele cryptografie, waarbij zowel de zender als de ontvanger van een vercijferd bericht beide over dezelfde geheime sleutel moeten beschikken, ontoereikend. Daarom wordt dit ook wel 'symmetrische' cryptografie genoemd. Bij de 'asymmetrische' cryptografie, beter bekend als public-key cryptografie, is dit probleem verdwenen: iedere partij behoeft slechts over een eigen geheime sleutel te beschikken. Interactie met andere partijen gaat op basis van de publieke sleutels van die partijen. Een belangrijk voortbrengsel is de digitale handtekening, die (a) door iedereen aan de hand van de publieke sleutel gecontroleerd kan worden en (b) alleen door de houder van de geheime sleutel gezet kan worden. Dit maakt een digitale handtekening in zekere zin bindend. Belangrijk is wel dat een geheime sleutel niet gestolen kan worden, en niet gebruikt kan worden zonder de toestemming van de eigenaar. Het uit 1977 stammende RSA systeem is het bekendste voorbeeld van een public-key cryptosysteem.

SET

De grote creditcard maatschappijen hebben hun eerdere inspanningen nu verenigd in het SET (Secure Electronic Transaction) voorstel. Mastercard en VISA waren hierbij de voortrekkers, waarbij uitgegaan is van de iKP betaalprotocollen zoals voorgesteld door onderzoekers van IBM. Aangezien SET verder door belangrijke software bedrijven als MicroSoft en Netscape gesteund wordt, is het de facto standaard voor creditcard (en verwante) betalingen over het Internet.

Het SET voorstel voorziet in een aantal niveau's van veiligheid. Het verkeer tussen de winkeliers en de creditcard maatschappij is in hoge mate beveiligd, gebruik makende van de digitale handtekeningen en encryptie waar nodig. Belangrijk hierbij is dat de gebruikte methoden aansluiten op het bestaande systeem. Het verkeer tussen de klant en de winkelier zal in eerste instantie niet zo zwaar beveiligd zijn. Maar het is in ieder geval wel zo dat het creditcardnummer en de verloopdatum van de kaart enkel in vercijferde vorm (en alleen leesbaar voor de creditcard maatschappij) worden verstuurd.



Figuur 1 – Om kleine bedragen kostendekkend af te kunnen handelen is het daarom interessanter om met prepaid systemen als Chipknip en Chipper te werken.

Het gebruik van public-key cryptografie heeft geen zin als er niet een infrastructuur is om publieke sleutels te certificeren. Een groot deel van het SET voorstel is dan ook gewijd aan het specificeren van een hierarchische structuur voor de certificerende authoriteiten. Een certificaat is feitelijk ook een digitale handtekening. Het idee is dat het vertrouwen in een publieke sleutel uiteindelijk neerkomt op het vertrouwen in de publieke sleutel die bovenaan staat in de hierarchie. De winkeliers worden allemaal in de hierarchie opgenomen. Voordat alle gebruikers ook in de hierarchie zijn opgenomen zal nog even duren. Dit verklaart waarom in eerste instantie met een lagere veiligheid voor de gebruikers gewerkt wordt.

Natuurlijk ligt er een enorme markt te wachten voor SET, en per definitie zal het geschikt zijn voor wereldwijde transacties. Maar er zijn ook punten waarop het systeem te kort schiet. Allereerst is er het simpele feit dat veel mensen geen creditcard willen of er zelfs niet voor in aanmerking komen. Verder is het zo dat voor kleine bedragen het gebruik van de creditcard niet kostendekkend is, Derhalve is er vaak een minimum bedrag vereist. Daarnaast is het duidelijk dat het ontvangen van betalingen alleen is voorbehouden aan winkeliers. Winkeliers hebben een speciale relatie met de creditcard maatschappij en moeten een bepaald percentage per transactie afstaan. In Japan loopt dit op tot 8%.

Chipknip/Chipper

PIN betalingen kunnen in principe als SET transacties worden afgehandeld. Dit geeft soortgelijke resultaten als voor creditcards. Om kleine bedragen kostendekkend af te kunnen handelen is het daarom interessanter om met prepaid systemen als Chipknip en Chipper te werken (zie figuur 1). Met deze voorbeelden blijven we dicht bij huis. Een prepaid systeem waarmee wereldwijd aan de weg wordt getimmerd is het Mondex systeem, waar Mastercard sinds een aantal maanden een belangrijk aandeel in heeft. In dit soort systemen geeft een teller op de kaart aan (opgeslagen in het EEPROM geheugen) hoeveel de kaart op dat moment waard is.

Ook voor de netwerkvarianten van Chipknip en Chipper zal het zo zijn dat het ontvangen van betalingen beperkt is tot winkeliers. Een technische reden hiervoor is dat deze systemen voornamelijk gebaseerd zijn op symmetrische cryptografie (zoals DES, de Data Encryption Standard). Zoals hierboven uitgelegd vereist dit dat de betaler en ontvanger over een gemeenschappelijke geheime sleutel beschikken. De voor de hand liggende oplossing om iedereen dezelfde geheime sleutel te laten gebruiken wordt over het algemeen als onvoldoende veilig beschouwd. Het 'breken' van een smartcard volstaat dan in principe om onbeperkt geld aan te maken. Ironisch genoeg, is dit precies wat Mondex doet om het mogelijk te maken dat elke gebruiker iedere andere gebruiker kan betalen door een off-line transactie (dus zonder dat de bank of een andere partij erbij betrokken is). Mondex overweegt dan ook om de betalingen tussen gebruikers onderling af te schaffen.

De standaard aanpak is dan ook om de symmetrie tussen betaler en ontvanger te verbreken. Chipknip en Chipper winkeliers hebben een apparaat met een ingebouwde SAM (Secure Application Module) nodig. De SAM bevat de masterkey, en het idee is dat het ontfutselen van deze key weer een stuk moeilijker is dan het breken van een smartcard. De geheime sleutels van de gebruikers worden van de masterkey afgeleid door diversificatie. Een manier is bijv. om het kaartnummer van de gebruiker te nemen, en dat tezamen met de masterkey in een cryptografische hashfunctie (zoals SHA, Secure Hash Algorithm) te voeren. De hashwaarde doet dan dienst als geheime sleutel.

Ecash™

Bij DigiCash werken we aan elektronische varianten van contant geld. In dit soort systemen passen we public-key cryptografie niet alleen toe om de veiligheid op algemene punten te verhogen, maar ook in het hart van het geldsysteem zelf. We gebruiken namelijk een speciale vorm van digitale handtekeningen om het geld zelf te representeren. Veel eigenschappen van de elektronische munten stemmen overeen met die van metalen munten. De authenticiteit van een munt, bijvoorbeeld, kan door iedereen worden vastgesteld. Verder is het zo dat kleine en grote aankopen met hetzelfde gemak gedaan kunnen worden. Alleen de bank beschikt over de geheime sleutel waarmee de elektronische munten gemaakt kunnen worden. De enige manier om geld te vervalsen is daarom het kopieren van bestaande munten. Voor een software-only ecash client is dit triviaal, maar de remedie is even triviaal: alle ontvangen munten worden in een database opgeslagen, en alleen niet eerder gebruikte munten worden geaccepteerd. Verder is het zo dat het betalen met elektronische munten werkelijk de enige manier is om de privacy van de gebruikers te waarborgen.

In het ecash™ systeem maken we vergaand gebruik van public-key cryptografie om een zeer hoog veiligheidsniveau te bereiken. Betalers en ontvangers maken hierbij gebruik van een client programma dat normaal in de achtergrond op hun PC draait. Via het Internet wordt er verbinding gelegd met een bank die ecash uitgeeft. Daar worden dan 'verse' munten opgehaald, die vervolgens voor later gebruik op de harde schijf worden opgeslagen. Met de munten kan betaald worden bij allerlei winkels die zich op het Internet presenteren. Het is echter ook mogelijk om aan een willekeurige gebruiker een betaling te doen (Eng. peer-to-peer payments). Desgewenst kan een betaling ook per email verzonden worden. Belangrijk is om op te merken dat het geld aan de winkelier (ontvanger) behoort zo gauw de betaling aankomt (en geldig wordt bevonden). Dit wordt in het Engels 'finality'

Tabel 1 – Een binair schema met k = 12 denominaties

e	3	5	7	11	13	17	19	23	29	31	37	41
D_e (f)	0,005	0,01	0,02	0,04	0,08	0,16	0,32	0,64	1,28	2,56	5,12	10,24

genoemd. Een dergelijke eigenschap geldt bijv. niet voor creditcard betalingen.

Ecash en meer algemeen de notie van elektronische of digitale munten is uitgevonden door David Chaum. Een unieke eigenschap van dit soort munten is dat het gebruik ervan in betalingen niets prijsgeeft over de identiteit van de betaler. Op het moment werken we met een aantal belangrijke banken en instellingen verspreid over de wereld die ecash uitgeven. Deze banken geven dus ecash uit aan hun klanten, die het vervolgens bij de aangesloten winkels kunnen gebruiken.

Ecash munten zijn een specifiek type RSA handtekeningen. Voor elke generatie munten genereert de ecash bank een 'verse' RSA sleutel. Deze bestaat uit een publiek bekende modulus N, de eerste k oneven priemgetallen $\{e_i\}_{i=1}^{k}$ = 3,5,7,... die als publieke exponenten fungeren, en de corresponderende geheime exponenten $\{d_i\}_{i=1}^{k}$. Elke exponent e correspondeert met een denominatie D_e, zie Tabel 1 voor een voorbeeld. De factorisatie van N moet geheim blijven, omdat aan de hand hiervan de geheime exponenten d_i worden bepaald. Voor de volledigheid vermelden we hoe dit laatste in zijn werk gaat. Laat p en q de priemfactoren van N (beide bijv. 384 bits lang). Het getal d_i is nu de multiplicatieve inverse van e_i modulo $\phi(N) = (p\text{-}1)(q\text{-}1)$. We noteren deze inverse als $1/e_i$. Om het bestaan van de inverse te garanderen moet de RSA modulus zodanig gekozen worden dat geen enkele e_i een deler is van $\phi(N)$, dus, $\text{ggd}(e_i,\phi(N)=1$ voor $i = 1,\ldots,k$. Dit is een normale restrictie voor RSA moduli. De conclusie dat $m^{d_i e_i} \equiv m \bmod N$ voor elke $m \in \mathbb{Z}_N$ is nu gerechtvaardigd, en deze eigenschap vormt de basis voor het RSA cryptosysteem.

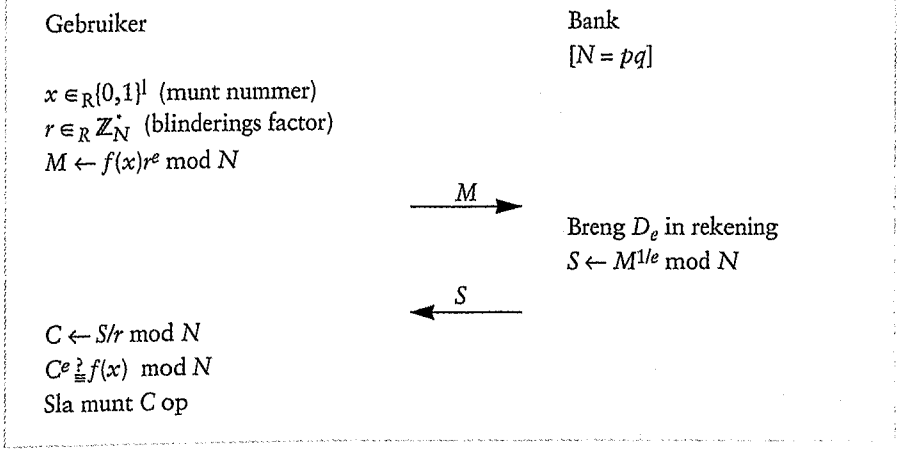
Een ecash munt C van denominatie D_e is nu een RSA handtekening van de vorm $C = f(x)^{1/e} \bmod N$, waarbij x een random gekozen getal is, en $f(x)$ een hier niet nader te specificeren expansie functie is. Het controleren van een munt op echtheid bestaat uit het berekenen van $C_e \bmod N$ en vervolgens nagaan of het resultaat van de vorm $f(x)$ is voor zekere x. We merken op dat voor de bank een munt volledig bepaald is door het getal x, en daarom slechts 10-20 bytes aan opslagruimte vergt.
De munten worden in een zogenaamd *blind signature protocol* opgenomen. Het protocol bestaat uit twee stappen zoals aangegeven in figuur 2. In het ecash systeem wordt dit protocol parallel uitgevoerd voor een groep munten ter waarde van het op te nemen bedrag. De onvervalsbaarheid van de ecash munten is net als de veiligheid van het RSA systeem zelf gebaseerd op het feit dat het onmogelijk wordt geacht om een RSA modulus van enkele honderden bits te factoriseren.

De verkregen munten kunnen vervolgens voor betalingen gebruikt worden. De belangrijke eigenschap van het opname protocol is nu dat een munt C niet in verband gebracht kan worden met het opname protocol waarin de munt C is gecreëerd en dus door welke gebruiker de munt is opgenomen. Op deze manier wordt de privacy van de gebruikers op een sterke manier gewaarborgd, omdat het zelfs onmogelijk is voor de bank om te onderscheiden of twee betalingen van *dezelfde* gebruiker komen of niet.
Het belang van deze sterke notie van privacy wordt duidelijk als we naar een voorbeeld kijken waarbij de privacy slechts berust op het gebruik van een pseudoniem. Stel u koopt volledig anoniem een telefoonkaart door deze contant te betalen. U zou dan kunnen denken dat u bij het gebruik van de telefoonkaart ook anoniem blijft. Echter, stel nu eens dat elke kaart een nummer heeft dat de telefoonmaatschappij gebruikt om er achter te komen of er niet gefraudeerd wordt (door te kijken of er op een kaart meer wordt gebeld dan de prijs van de kaart toestaat). Gegeven dit kaartnummer is het dan heel eenvoudig om de gegevens van alle telefoongesprekken die met deze kaart gemaakt zijn bij te houden. Soortgelijke files worden standaard bijgehouden voor elke telefoonnummer. In veel gevallen zal het nu zo zijn dat alsnog vastgesteld kan worden wie de telefoonkaart gebruikt heeft door beide databases met elkaar te vergelijken. Het gebruik van een pseudoniem (in dit geval het kaartnummer) is dus normaal gezien onvoldoende om de privacy van de eindgebruikers te beschermen.

Conclusie

Op het moment worden in het ecash systeem, net als bij SET, alle betalingen on-line geverifieerd. Door gebruik van smartcards of beter nog 'electronic wallets' is het mogelijk om betalingen ook off-line te doen, net

Figuur 2 – Chaum's opname protocol voor munt $C = f(x)^{1/e} \bmod N$ met waarde D_e



als bij Chipknip/Chipper systemen. Een dergelijke apparaat is bij DigiCash reeds ontwikkeld in het kader van CAFE, een Europees project. De bedoeling is uiteindelijk dat zo'n wallet zowel voor Internet betalingen als voor betalingen in de winkel of op straat gebruikt kan worden. Een belangrijk voordeel van de wallet is dat het een eigen toetsenbord en display heeft, en verder communiceert via infrarood. Op deze manier hoeft de wallet niet meer uit handen gegeven te worden tijdens betalingen. Door het gebruik van elektronische munten is de privacy dan op een unieke manier beschermd.

Elektronische betaalsystemen vormen slechts een deel van de oplossing om tot elektronische commerce te komen. Denk hierbij aan het tot stand komen van een bestelling en het vastleggen hiervan op een ondubbelzinnige manier. Om deze reden worden er voorstellen gedaan zoals in het SEMPER project (Secure Electronic Marketplace for Europe). Dergelijke projecten hebben ook tot doel om het gebruik van verschillende betaalmethoden naast elkaar mogelijk te maken, bijvoorbeeld SET naast ecash. Ook hier zijn extra veiligheidsmaatregelen nodig om te zorgen dat het geen probleem is dat klant en winkelier niet meer oog in oog staan, maar over een open netwerk communiceren.

Literatuur

D. Chaum, Blind signatures for untraceable payments. In D. Chaum, R.L. Rivest, and A.T. Sherman, editors, Advances in Cryptology - CRYPTO '82, pagina's 199-203, New York, 1983. Plenum Press.

Zie http://www.digicash.com.

M. Bellare, J. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, and M. Waidner. iKP - a family of secure electronic payment protocols. In First USENIX Workshop on Electronic Commerce, 1995.

Zie http://www.semper.org.

Zie bijv., http://www.mastercard.com and http://www.visa.com. @