Privacy

David Chaum was een van de *founding fathers* van het moderne cryptografieonderzoek, de wetenschap van de digitale veiligheid. Hij had visionaire ideeën over elektronische privacy en richtte een spin-offbedrijf op, DigiCash. Het bedrijf was zijn tijd ver vooruit en ging later failliet. Chaums ideeën worden echter nog steeds gebruikt door onderzoekers.

Elektronische privacy

Waarom was Chaum zo bezorgd over elektronische privacy? Hij voorzag aan het begin van het informatietijdperk al dat organisaties steeds meer gegevens zouden verzamelen en koppelen. Banken zouden willen weten of iemand zijn rekeningen betaalt voordat ze een lening verstrekken en een belastingdienst zou kunnen nagaan of iemand te veel uitgeeft voor zijn inkomen. Organisaties, vreesde Chaum, kunnen onderling gegevens uitwisselen over het betaalgedrag van klanten, zonder dat die kunnen nagaan of de gegevens correct zijn. Soms komen klanten pas achter een fout als een bepaalde dienst wordt geweigerd. Verder vroeg de onderzoeker zich af wie bij de betaalgegevens kan komen: is het systeem te kraken? Chaum wilde daarom een anoniem betaalsysteem ontwerpen dat niet alleen veilig was voor de geldverstrekkers maar ook voor de klant en diens privacy.

Blind signatures

De uit de Verenigde Staten afkomstige onderzoeker ontwierp technieken om de privacy van betalers te garanderen, gebaseerd op *blind signatures*. Een klant kan digitale bankbiljetten lenen bij een bank, *e-cash*, door zelf een honderdcijferig serienummer van een biljet te genereren dat hij versleuteld aan de bank opstuurt. De bank herkent de zender aan diens digitale handtekening en tekent ongezien (blind) het elektronische bankbiljet zodat het geldig wordt. De bank kent het serienummer dus niet. Als de klant onder een pseudoniem het biljet uitgeeft bij een winkel en de winkelier laat het geld op zijn rekening bijschrijven, weet de bank niet dat de klant juist bij deze winkelier iets gekocht heeft. Het is veilig omdat er steeds andere digitale handtekeningen nodig zijn, zodat afluisteren geen zin heeft. Verder zijn er lage transactiekosten, waardoor e-cash uitermate geschikt is voor kleine betalingen.

Chaum: visionair op het gebied van elektronische privacy

DigiCash

Om geen belangenverstrengeling te hebben tussen het publiek gefinancierde onderzoek en commerciële zaken richtte Chaum in 1990 het bedrijf DigiCash op, waarna hij in 1993 het CWI verliet. De overheid en investeerders waren zeer onder de indruk van de geavanceerde technieken. Gilde Investments en bijvoorbeeld Nicholas Negroponte, oprichter van het MIT Medialab in de Verenigde Staten, staken geld in de onderneming. Verschillende banken probeerden het systeem uit. In Amerika werd ook een vestiging opgericht, maar uiteindelijk ging het bedrijf failliet. Chaums ideeën – ook toepasbaar op rekeningrijden en elektronisch stemmen – worden echter nog steeds gebruikt. Ronald Cramer, hoofd van de huidige cryptografiegroep op het CWI, zegt: 'Tegenwoordig staat individuele privacy wel eens onder druk in het internationale maatschappelijke veld. Chaums thema heeft dus nog niets aan relevantie ingeboet, eerder gewonnen.'

Links
www.chaum.com
www.cwi.nl/pna5
www.iacr.org

Annette Kik,
wetenschapsvoorlichter van het Centrum voor Wiskunde en Informatica (CWI) in Amsterdam (www.cwi.nl). E-mail: Annette.Kik@cwi.nl.