

# De smartcard van

## Europese onderzoeksagenda voor smartcards

Het oktobernummer van (Smart) Cards in Business besteedde aandacht aan het onderzoek op het gebied van veiligheid en betrouwbaarheid van JavaCard smartcards bij de afdeling Informatica van de Nijmeegse Universiteit. Dit onderzoek vindt plaats binnen het Europese IST project VerifiCard. In Nederland werkt ook de Technische Universiteit Twente aan smartcards, namelijk binnen de informaticagroep gedistribueerde en embedded systemen. Beide universiteiten zijn eerder dit jaar betrokken geweest bij het opstellen van de nieuwe Europese onderzoeksagenda voor smartcards binnen het zogenaamde zesde kader programma. Voor de duidelijkheid: het gaat hier om de technisch-wetenschappelijke agenda voor smartcards, en niet de organisatorische of juridische. Bij deze een impressie van wat komen gaat...

'Brussel' beschouwt smartcards inmiddels als van strategisch belang voor Europa. Smartcards zijn in de jaren zeventig ontwikkeld in Europa; voornamelijk door het Franse bedrijf Bull, hoewel de eerste patenten staan op naam van de Duitser Jürgen Dethloff. Nog steeds zijn de meeste smartcardproducenten Europese (vooral Franse en Duitse) bedrijven. Ook in de daadwerkelijke toepassingen van smartcards - bankpassen, SIMs in GSMs, settop boxen, identiteitskaarten - loopt Europa (vooralsnog) voorop. Smartcards vormen een onderwerp waarmee Europa zich goed kan (en wil) profileren ten opzichte van de Verenigde Staten en Japan. De problemen op dit gebied vragen om een supranationale aanpak, niet alleen vanwege de omvang en de grootte van de bedragen die ermee gemoeid zijn, maar ook ter voorkoming van versnippering op natio-

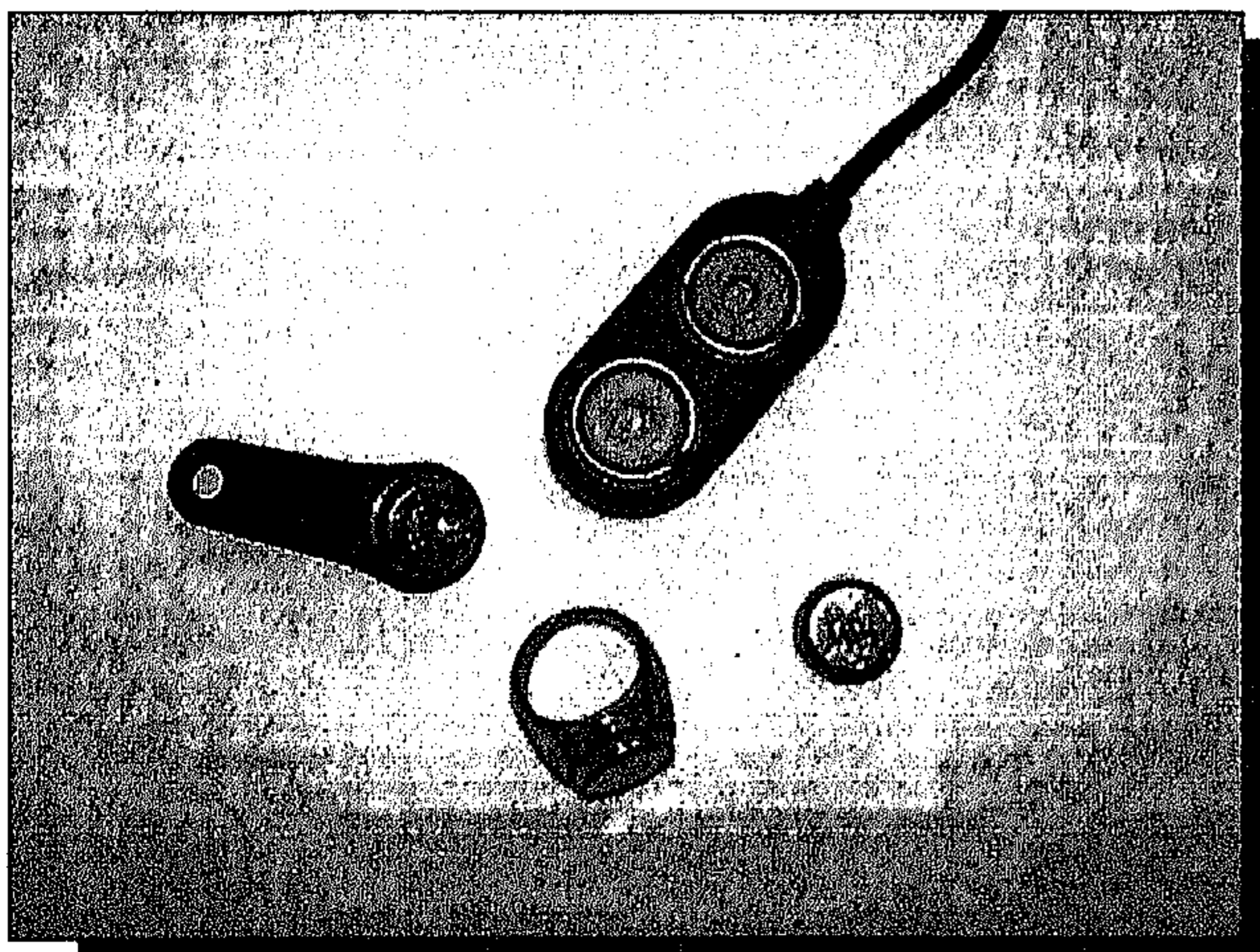
naal niveau (zowel technisch als organisatorisch).

### Europese kaders

De onderzoeksprogramma's van de Europese Gemeenschap (EG) zijn opgedeeld in zogenaamde kaders (frameworks), die vijf jaar duren. Op dit moment loopt het vijfde kader op zijn eind, en zijn de voorbereidingen voor het zesde kader in volle gang. Zo'n overgang is belangrijk omdat juist dan nieuwe thema's en programma's ingevoerd worden. Binnen deze context hebben ambtenaren van de EG in het voorjaar een consultatiebijeenkomst georganiseerd met Europese belanghebbenden op het gebied van smartcards. Deze bijeenkomst vond plaats op 23 mei in Brussel met vertegenwoordigers van bedrijven als Sagem, Infineon, Ericsson, Datacard, Philips, Giesecke & Devrient, Proton, Schlumberger, Gemplus, Sema, en Arttic én Pieter Hartel als enige vertegenwoordiger uit de Europese academische wereld. Omdat de bedragen waar het binnen dit zesde kader om gaat in de tientallen, zonet honderden miljoenen euro's lopen, zijn de belangen groot. Het is dus opmerkelijk dat vanuit de Nederlandse universitaire wereld zo'n grote invloed uitgeoefend kon worden. Aan de deelnemers van deze bijeenkomst was vooraf gevraagd een standpunt voor te bereiden

over 'de smartcard van het jaar 2010'. Daarbij diende vooral aangegeven te worden welke onderzoeksinspanningen daarvoor vereist werden geacht. Een samenvatting van de discussie is inmiddels beschikbaar op het web ([www.cordis.lu/ist/ka2/rptspolicyconf.htm](http://www.cordis.lu/ist/ka2/rptspolicyconf.htm)); wij lichten er enkele saillante punten uit.

Figuur 1: De iButton is permanent alert op geknoei



#### Aantoonbare veiligheid

In het algemeen vond men in de toekomst dat veel (meer) aandacht besteed dient te worden aan aantoonbare veiligheid, niet alleen van smartcards zelf, maar ook van de infrastructuur waarin deze kaarten gebruikt worden. Dit omwille van het nodige vertrouwen bij het publiek in op smartcards gebaseerde elektronische transacties (in e/m-commerce en e-government). In het bijzonder vond men dat meer geïnvesteerd dient te worden in betrouwbaarheid van software, boven op de bestaande investeringen in hardwarebeveiliging. Het gebruik van formele, wiskundige technieken werd door alle deelnemers als cruciaal gezien. Dit vergt een intensieve samenwerking tussen de Europese industrieën en universiteiten. Verder zullen smartcards steeds meer geheugen nodig hebben om meer en geavanceerdere toepassingen te kunnen ondersteunen. Daartoe moeten nieuwe geheugentechnologieën worden ontwikkeld, die weinig chipoppervlak nodig hebben, en weinig stroom verbruiken.

Met het steeds wijder verspreide gebruik van smartcards wordt het nog belangrijker dat de hardware 'tamper resistance' sterker wordt. Daarbij spelen nieuwe, slimme sensors een belangrijke rol, die kunnen detecteren wanneer er met de chip wordt geknoeid. Figuur 1 toont voorbeelden van de huidige generatie 'tamper resistant' JavaCards, maar dan in een iets afwijkende behuizing: de iButton. Een iButton kan

bijvoorbeeld in een ring of sleutelhanger verwerkt worden, heeft speciale sensoren en een batterijtje aan boord en is permanent alert op geknoei. Gewone smartcards beschikken nog niet over zo'n batterijtje op de kaart, en kunnen dus niet voortdurend waakzaam zijn tegen onbedoelde ingrepen.

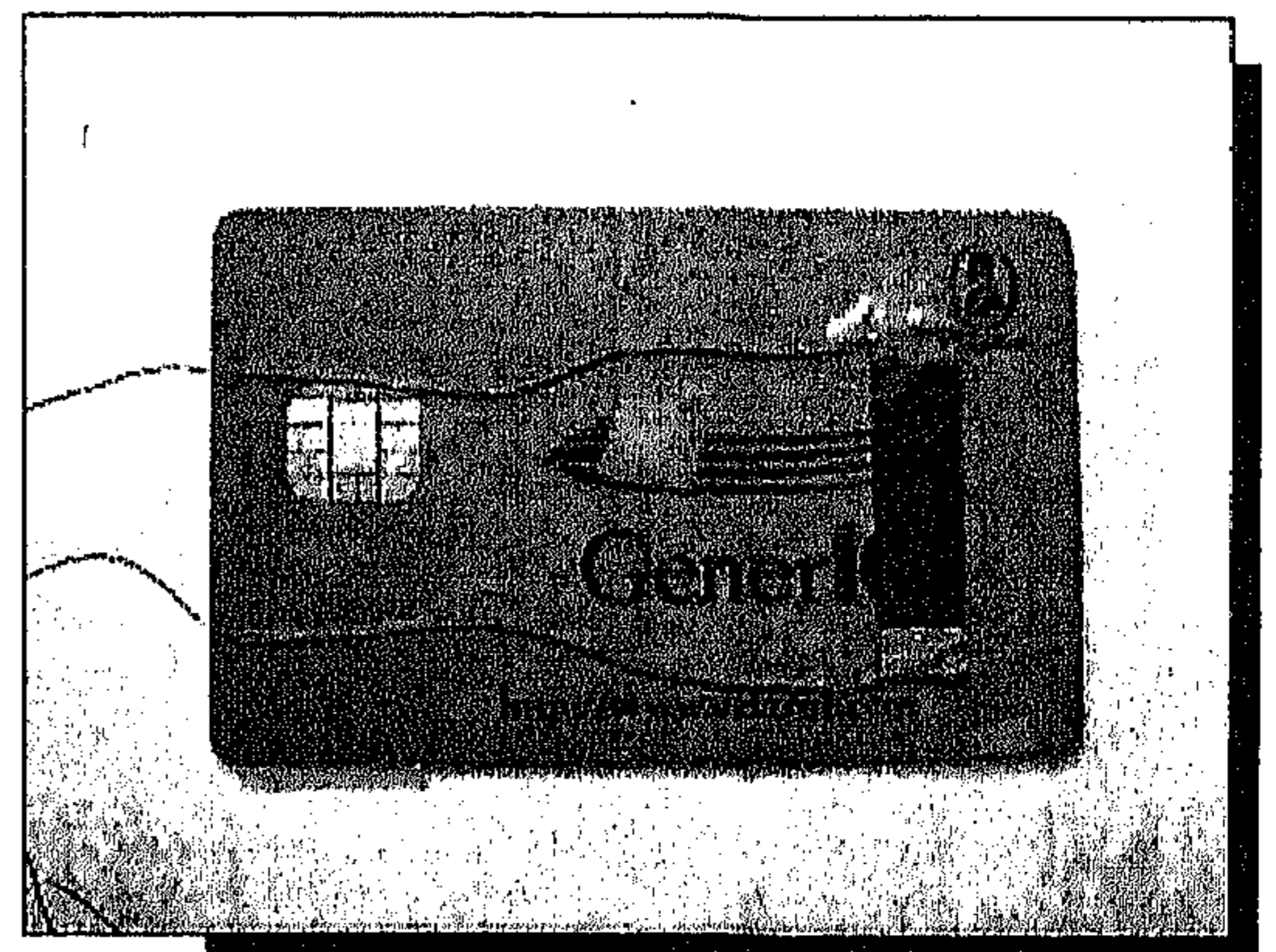
#### Besturingssystemen en systeemintegratie

Op de huidige generatie smartcards worden veelal speciale besturingssystemen gebruikt, die onderling niet compatibel zijn.

Met de komst van JavaCard is een belangrijke stap gezet op weg naar een standaard besturingssysteem voor smartcards. Deze ontwikkeling staat nog aan het begin; er moet nog veel werk worden verzet totdat er een algemeen geaccepteerde open source standaard ontstaat, die voldoende flexibiliteit toelaat voor het produceren van JavaCardproducten voor specifieke markten. Een smartcardapplicatie is meestal maar een klein (zeg 10 procent) onderdeel van een informatiesysteem, terwijl de veiligheid van het systeem als geheel misschien wel voor 80 procent van de smartcard afhangt. Er zijn nieuwe gereedschappen nodig om de integratie van de smartcard met de rest van het systeem te kunnen ondersteunen, waarbij de veiligheid van het geheel wordt gewaarborgd. Formele methoden zullen daarbij een grote rol spelen.

#### Ontwikkelinstrumenten en beveiliging

Een smartcard kan een uitstekend beveiligingsproduct zijn, maar de afnemers en hun klanten moeten natuurlijk wel overtuigd worden van de kwaliteit van de beveiliging. Er zijn nieuwe methoden en technieken nodig die sterke kwaliteitsgaranties ondersteunen, en die tegelijkertijd op een kosteneffectieve manier kunnen worden benut. Formele methoden toegespitst op de specifieke eigenschappen van smartcards zijn hierbij essentieel. Daarbij spelen zowel hardware als softwareverificatie een grote rol, en ligt er een belangrijke uitdaging voor het onderzoek om beiden te integreren. Omdat gebruikers hun smartcard altijd bij zich dragen, zullen zij in de regel hun eigen kaartje meer vertrouwen dan een willekeurige ATM of POS-terminal. De smartcard van de toekomst moet daarom meer zelfstandig, dus zonder medewerking van een terminal kunnen functioneren. Om dat mogelijk te maken zou de smartcard met een eigen ultraplattere batterij kunnen worden uitgerust en invoer/uitvoer faciliteiten. De componenten mogen maar heel weinig stroom verbruiken. Figuur 2 toont een prototype van een smartcard met een biometrische sensor.



Figuur 2: Dit prototype van een smartcard met biometrische sensor is ontwikkeld door Pieter Hartel en collega's van de Universiteit van Southampton.

#### Componenten, behuizing en materialen

Huidige smartcards bevatten slechts een chip en contacten of een antenne. Het inbouwen van meerder componenten vraagt om nieuwe montage technieken

# De smartcard van 2001

zodat de afzonderlijke componenten op een duurzame en goedkope manier kunnen worden verbonden. Productie van smartcards en smarttags in op de toepassing toegesneden maten en soorten verdient aandacht. Smartcards worden nu meestal van PVC gemaakt, hetgeen een milieuonvriendelijk materiaal is. Er is behoefte aan nieuwe materialen, die zowel bij productie als bij de verwerking van afval het milieu minder belasten. Ook de chipproductie belast het milieu en bij de verwachte grote aantallen waarin smartcards maar vooral ook smarttags

zullen worden geproduceerd, is er grote belangstelling voor alternatieve technologieën, bijvoorbeeld gebaseerd op polymeerelektronica.

## De smartcard van 2010

De deelnemers aan de vergadering over de smartcard van 2010 in Brussel schatten de investeringen op zo'n 320 miljoen euro. Hoeveel hiervan inderdaad door 'Brussel' geïnvesteerd gaat worden is op dit moment nog niet duidelijk. Veel zal natuurlijk ook afhangen van de kwaliteit van de voorstellen die binnen het nieuwe zesde kader ingediend gaan worden. Er lijken ruime mogelijkheden voorhanden voor zowel de Nederlandse industrie als de Nederlandse universiteiten.

Geïnteresseerden in mogelijke projecten kunnen hierover contact opnemen met de auteurs: pieter@cs.utwente.nl en bart@cs.kun.nl ●

*Pieter Hartel heeft ruime internationale ervaring op het gebied van smartcards en heeft recentelijk een half jaar gewerkt binnen SUN's JavaCard divisie in Cupertino, Californië. Verder is hij auteur van special issues over smartcards van de vaktijdschriften Future Generation Computer Systems en Computer Networks. Samen met Bart Jacobs, coördinator van het Verificard project, is Hartel nauw betrokken geweest bij de voorbereiding van de nieuwe Europese onderzoeksagenda op het gebied van smartcards.*

A d v e r t e n t i e

## Het succes van uw chipkaart zit in een goede organisatie.

Kwinta Essentia B.V. is een onafhankelijk bureau, gespecialiseerd in organisatie- & informatiseringsadvies en projectmanagement. Wij hebben ons toegelegd op het bieden van advies en ondersteuning bij het verbeteren van bedrijfsprocessen, onder andere met behulp van informatietechnologie. Daarbij maken wij ook gebruik van onze jarenlange expertise op het gebied van multifunctionele kaartconcepten.

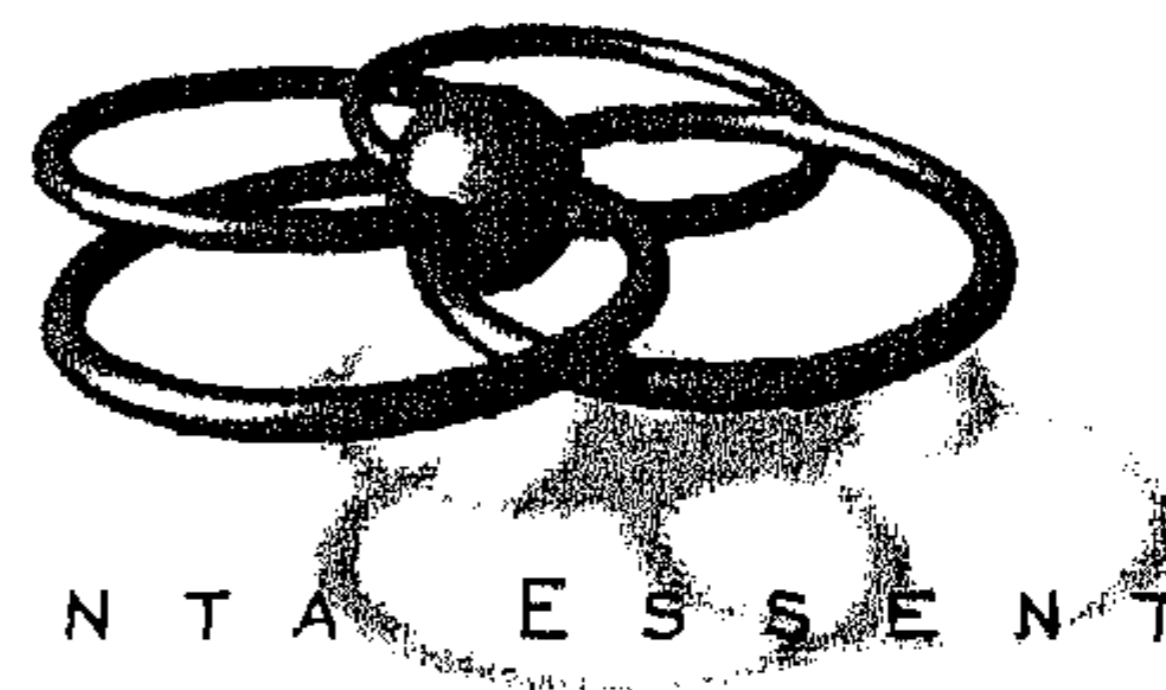
### Onze hoofdactiviteiten

- uitwerken van de informatiearchitectuur van geïntegreerde facilitaire bedrijfsprocessen en multifunctionele kaartconcepten;
- uitvoeren van haalbaarheidsonderzoeken voor innovatieve, technologische toepassingen;
- opstellen van bedrijfsplannen;
- project-en interim-management;
- verzorgen van trainingen.

### Expertise

Kwinta Essentia is in 1999 opgericht en is vanaf die tijd nauw betrokken bij de ontwikkelingen binnen het onderwijs ten aanzien van het herinrichten van processen als de registratie van aanwezigheid en afwezigheid, elektronisch betalen, fysiek toegangsbeheer en logisch toegangsbeheer.

Naast de sector onderwijs zijn de medewerkers van Kwinta Essentia al meer dan tien jaar actief binnen de sectoren Industrie, Verkeer en Vervoer, Gezondheidszorg, Telecommunicatie, Financiële en Zakelijke Dienstverlening.



K W I N T A E S S E N T I A

Kwinta Essentia B.V., Ambachtsweg 4 E, Maarsbergen, Postbus 93, 3970 AB Driebergen, Telefoon: 0343 52 16 98, Telefax: 0343 51 88 20, E-mail: info@kwintess.com