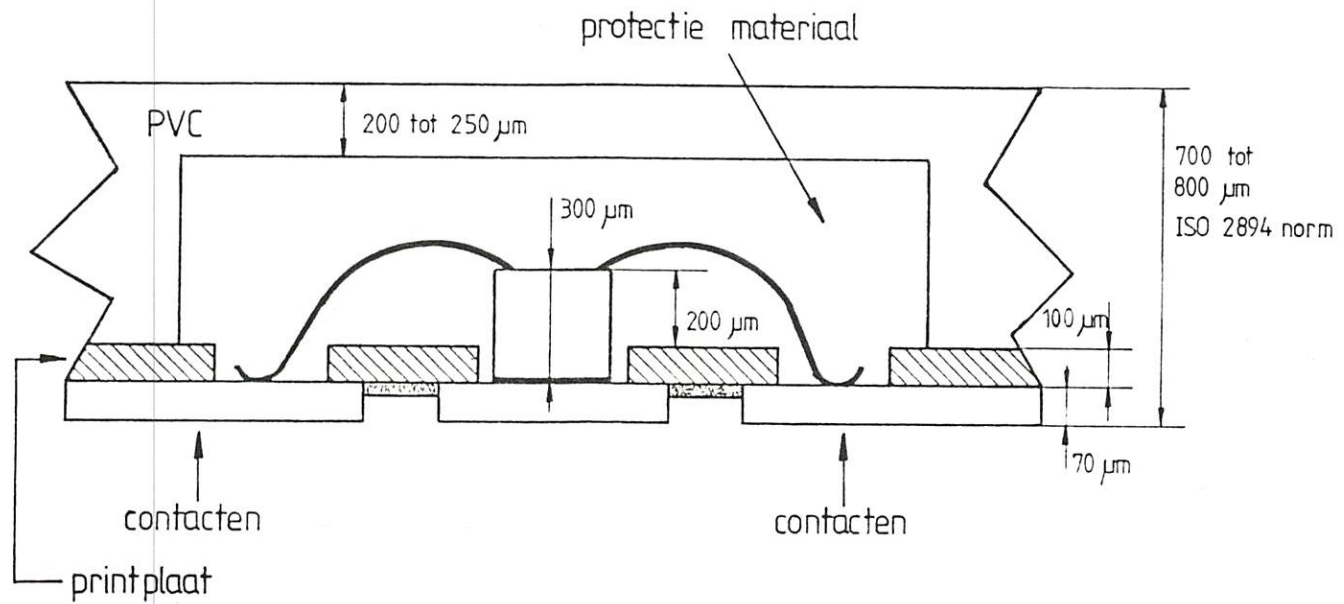


DE SMART CARD ALGEMEEN



Samengesteld door: E.R. Lekanne gezegd Deprez
C. Bolt

2 Woord vooraf.

Omdat de chipkaart technologie de laatste jaren een enorme vlucht heeft genomen, hebben we gemeend een leemte te moeten vullen. Met name de smart card technologie is erg belangrijk omdat daarmee vele beveiligingsmethoden mogelijk zijn, daardoor is deze bij uitstek geschikt voor toepassingen in het betalingsverkeer.

Omdat de Hogeschool Utrecht, vestiging Hilversum, aandacht wil schenken aan deze technologie werd opdracht gegeven om een algemeen onderzoek in te stellen. Dit heeft geresulteerd in een overzicht van de in Nederland belangrijkste bedrijven op het gebied van de smart- en chip kaart technologie.

In dit rapport wordt de nadruk gelegd op een algemene overzicht van deze technologie. Er wordt in hoofdstuk 6 ingegaan op de technische samenstelling van de smart card. In hoofdstuk 7 worden de standaardisatie commissies op dit gebied beschreven. In hoofdstuk 8 wordt beschreven hoe de smart card binnen het ATF4 gaat functioneren. Hoofdstuk 9 beschrijft van een aantal landen de fabrikanten met hun produkten op dit gebied, waarbij de Nederlandse fabrikanten vollediger zijn uitgewerkt dan de buitenlandse. De lopende projekten worden in hoofdstuk 10 behandeld, waar met name veel aandacht besteed wordt aan het chipcard projekt in Woerden.

Dit rapport is daarom zeer geschikt voor iedereen die zich wil gaan verdiepen in de smart card technologie.

3 Samenvatting.

Het blijkt uit de vele bedrijven uit het buitenland dat er in Nederland nog niet zoveel gewerkt wordt met de smart card. In Japan bijvoorbeeld wordt de smart card al op grootte schaal toegepast in het dagelijks leven. In Frankrijk blijkt men ook op grootte schaal deze smart card te gebruiken. De smart cards worden toegepast voor het betalen van boodschappen tot het betalen van de metro. In hoofdstuk 9 is duidelijk te zien dat Japan en Frankrijk de meeste bedrijven hebben op dit gebied. Bij het uitkomen van dit rapport schrijven de kranten bijna elke dag wel een artikel over chip kaart in het betalingsverkeer. De chipkaart voor het betalen van de dagelijkse boodschappen wordt o.a. getest in Woerden. Hoe dit projekt is opgezet en wat de resultaten zijn wordt beschreven in hoofdstuk 10. Een heel belangrijk aspect voor de invoering van de smart card is de standaardisatie. In dit rapport is dan ook geprobeerd een duidelijk beeld van deze standaardisaties te geven. Hoe de smartcard gebruikt kan worden wordt in hoofdstuk 8 beschreven. In dit hoofdstuk wordt de smart card toegepast in het toekomstige ATF4 net. Hieruit volgen dan ook duidelijk de voordelen van de smart card. In hoofdstuk 11 zijn alle geïnformeerde partijen met naam, adres en telefoon vermeldt. Hierdoor is dit rapport een naslag werk geworden voor mensen die zich verder willen verdiepen in deze technologie.

4 Inhoudsopgave.

	bladzijde: -----
1 Voorblad.	1
2 Woord vooraf.	2
3 Samenvatting.	3
4 Inhoudsopgave.	4
5 Doelstelling	5
6 Inleiding.	6
6.1 Verschillende geheugen typen.	7
6.1.1 Het ROM-geheugen.	7
6.1.2 Het EPROM-geheugen.	8
6.1.3 Het EEPROM-geheugen.	8
6.1.4 Het RAM, SRAM en DRAM-geheugen.	8
6.2 De Smart card.	8
6.3 De communicatie.	9
6.4 De Super smart card.	10
7 Standaardisatie.	10
8 Applicatie: De smart card in het vierde generatie autotelefoonnet.	15
9 Fabrikanten.	21
9.1 Japanse bedrijven.	21
9.2 Franse bedrijven.	23
9.3 US bedrijven.	25
9.4 Overige bedrijven.	26
9.5 Nederlandse bedrijven.	29
9.5.1 Philips.	29
9.5.2 Bull.	32
9.5.3 B.V. Technisch Adviesbureau Annokkee.	32
9.5.4 DigiCash b.v..	33
9.5.5 Etrometa.	33
9.5.6 NEDAP N.V..	35
9.5.7 Intercai.	35
10 Projekten in binnen- en buitenland.	37
10.1 Projekten in Japan.	37
10.2 Projekt in Nederland.	38
10.3 Projekt in Denemarken.	47
11 Adressenlijst van geïnformeerde bedrijven.	48
12 Conclusie.	54

5 Doelstelling.

Doelstelling van het projekt wat gehouden zal worden over Smart- en Super Smartcards.

Het opzoeken van leveranciers en hierbij contactpersonen creëren.

Het bekijken van de stand van zaken wat betreft de winst en toekomstverwachtingen.

Het bekijken van de Techniek wat betreft Interfacing, opbouw en afmetingen van de kaart.

Het bekijken van allerlei toepassingen.

6 Inleiding.

Er worden in dit verslag twee technologieën gebruikt, deze twee technologieën worden geciteerd uit het verslag van economische zaken "Chipcards en Elektronische labels: een verkenning":

- Chipcard-technologie: de technologie waarbij een chip met in elk geval een geheugen, maar vaak tezamen met computer-processing capaciteit, met andere woorden tezamen met "intelligentie", compact wordt ondergebracht in kaartvorm; de chipcard is daarmee een (simpele) computer in de meest portable vorm zonder (volledige) in- en uitvoer-mogelijkheden van zichzelf: een "computer" die dus niet los gezien kan worden van een infrastructuur waarbinnen hij kan functioneren.
- Identificatie-technologie: technologie waarmee ondubbelzinnig de identiteit en eventueel uniciteit van een object of persoon kan worden vastgesteld; in de studie van economische zaken richtte men zich op identificeren met behulp van portable chips, ofwel ondergebracht op een kaart dan wel in andere vorm.

Voor de "intelligente" vorm van de chipcard wordt meestal de term "smart card" gebruikt. Het zal duidelijk zijn dat de smart card zowel voor identificatie doeleinden gebruikt kan worden als voor andere doeleinden, zoals beveiligde opslag van gegevens of geld. De identificatie-technologie kent ook chipcard technologie zonder card maar wel met gebruikmaking van portable chips. Dit gebeuren zal nauwelijks in dit verslag worden besproken, wel is er in de bijgevoegde documentatie folder materiaal omtrent dit soort technologie beschikbaar. Deze vorm van identificatie wordt wel elektronische labels genoemd. In de engelstalige literatuur worden deze elektronische labels vaak aangeduid met "(smart) tags", resp. "(smart) tokens". In deze technologie kent de tag talloze vaak zeer compacte vormen.

De meest simpele chipcard bevat alleen digitaal geheugen. Deze kaart wordt dan ook memory kaart genoemd. Er kan onderscheid worden gemaakt in éénmalig beschrijfbaar en herschrijfbaar geheugen.

De smart card bevat zijn eigen processor waardoor de kaart niet alleen kan "onthouden", maar ook intelligente functies kan verrichten. De smart card is veelal geen meer-chipcard omdat deze over het algemeen minder goed te beveiligen zijn, de verbindingen tussen de verschillende chips zijn af te tappen.

De super smart card heeft dezelfde mogelijkheden als de smart card, maar bezit op de kaart een eigen display en toetsenbord. De gegevens die in de chip zijn opgeslagen zijn direct voor de kaarthouder zichtbaar te maken. De informatie wordt dan zichtbaar na het intoetsen van een PIN-code.

Het blijkt dat er een grote verscheidenheid is aan maten van de kaart. Dit kan vertaald worden in het al of niet voldoen aan de maten van ISO standaard.

	niet ISO	ISO formaat
memory card	ja	ja
smart card		ja
supersmart card	ja	

tabel 1: Het wel of niet voldoen aan de ISO norm.

6.1 Verschillende geheugen typen.

De verschillen tussen de typen chipkaarten hebben ook betrekking op de wijze waarop de geheugens kunnen worden beschreven.

	eenmalig beschrijf baar	herschrijf baar	blijvende inhoud	zonder voeding gaat inhoud verloren
ROM	ja		ja	
(S/D) RAM		ja		ja
EPROM	ja	ja	ja	
EEPROM		ja	ja	

tabel 2: Indeling voor verschillende geheugen typen.

6.1.1 Het ROM-geheugen.

(Read Only Memory)

Dit type geheugen kan maar éénmalig beschreven worden, de inhoud is dan wel blijvend.

In de begin toestand bestaat het onbeschreven ROM-IC uit allemaal logische enen. Als men nu gegevens in het geheugen wil schrijven dan kunnen m.b.v. een ultra violette lichtbundel de gewenste transistors (de logische enen) worden doorgebrand. De doorgebrande transistors vormen de logische nullen. Eenmaal doorgebrande transistors kunnen niet meer worden hersteld. Het beschrijven van het ROM-geheugen is een proces dat door de fabrikant zal moeten worden uitgevoerd. Dit betekent dat de gebruiker een volledige beschrijving moet geven van wat er in het geheugen moet komen te staan en op welke plaats. De gebruiker zelf kan dus niet een ROM programmeren, en derhalve ook geen wijzigingen of aanvullingen aanbrengen.

6.1.2 Het EPROM-geheugen.

De EPROM (Electrically Programmable ROM) is evenals de ROM een type geheugen dat eenmalig beschreven kan worden. Het verschil met de ROM technologie is dat het geheugen elektrisch wordt beschreven. Voor het eenmalig beschrijven van de kaart heeft men een hogere spanning nodig dan de normale voedingsspanning van de kaart. In sommige gevallen worden zgn. powerdrivers op de chip aangebracht, zodat men kan volstaan met de normale voedingsspanning voor de chip.

De gebruiker kan zelf het EPROM geheugen programmeren. Alleen met UV-licht kan het geheugen worden gewijzigd, maar de kaart wordt zodanig geconstrueerd dat UV-licht niet kan binnendringen.

6.1.3 Het EEPROM-geheugen.

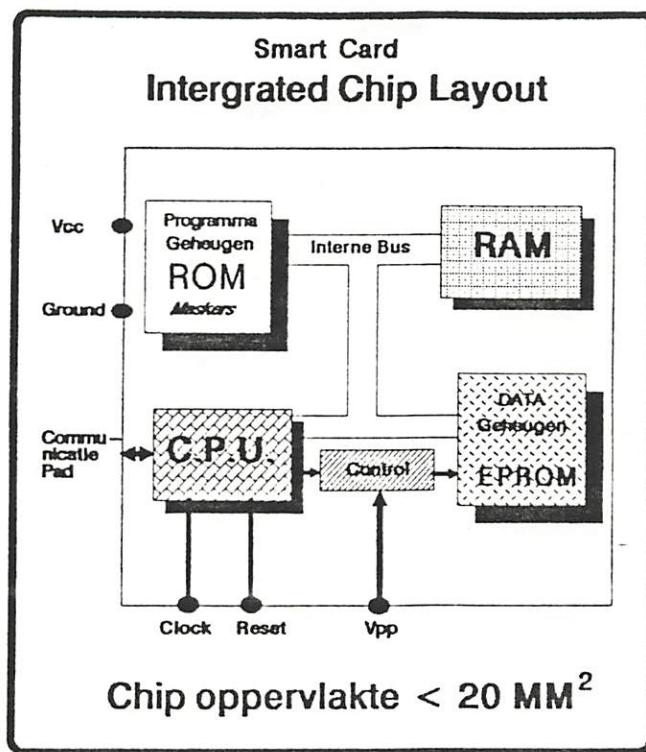
Het EEPROM-geheugen (Eraseable EPROM, ook wel E2PROM genoemd) is een geheugen dat meerdere malen beschreven kan worden, waarbij de data opslag niet verloren gaat als de spanning wegvalt. De chip wordt identiek aan de EPROM elektrisch geprogrammeerd waarbij de extra benodigde spanning of extern of intern via power drivers wordt geleverd. Het geheugen kan door de gebruiker zodoende zelf worden beschreven en herschreven.

6.1.4 Het RAM, SRAM en DRAM-geheugen.

Het RAM-geheugen behoort tot het type geheugens dat ook meerdere malen beschreven kan worden. De opgeslagen informatie gaat echter verloren als de voedingsspanning niet meer aanwezig is. Het voordeel is het grote geheugen en de snelle toegangstijden tot dit geheugen in vergelijking met bijvoorbeeld EPROM en EEPROM. RAM wordt vaak gebruikt als werkgeheugen in computers. Een Static-RAM is nog sneller dan RAM en wordt gebruikt voor zeer grote geheugenchips. De Dynamic-RAM technologie biedt mogelijkheden tot een groot aantal Mbytes per mm².

6.2 De Smart card.

De smart card chip bevat een CPU en één of meer verschillende geheugengebieden. De functie van de CPU is het regelen van de gegevensstroom van en naar de verschillende geheugengebieden. Met de CPU kunnen natuurlijk ook rekenkundige bewerkingen worden uitgevoerd.



In het ROM geheugen komt de systeem software van de CPU te staan. De grootte van het ROM geheugen loopt van 1 Kbyte tot ongeveer 6 Kbyte. Het RAM is een veel kleiner geheugen, ongeveer 1 Kbytes, en doet dienst als werkgeheugen. Het (E)EPROM geheugen wordt gebruikt voor de applicatie software en opslag van datagegevens.

6.3 De communicatie.

De communicatie kan direct of indirect zijn. De directe oplossing maakt gebruik van de contacten en zal een direct elektrisch contact zijn. De indirecte oplossing kan bestaan uit een microgolfverbinding of andere oplossingen. De microgolfverbinding wordt toegepast bij de contactloze kaart, dit soort kaarten worden toegepast bij tolwegen. Bij microgolft technieken spelen ook de dikte van de kaart mee, hoe hoger de frequentie hoe dunner de kaart. Een andere oplossing kan zijn met een infraroodzender. Voor de directe communicatie zijn er op de smart card 8 contacten aangebracht. Twee van deze contacten hebben nog geen functie en kunnen in de toekomst eventueel gebruikt worden.

6.4 De Super smart card.

Deze kaart heeft buiten de chip van de smart card nog een uitleesvenster en een toetsenbordje. De kaart beschikt dus over een contact- en een user-interface. De mogelijkheden met deze kaart zijn legio. Het is een computer op credit card formaat met beeldscherm en toetsenbord. Het is mogelijk om een heleboel extra's te bieden: memo's, klok, lijst van transac-

ties, agenda enz. Deze kaarten moeten nog wel onderzocht worden op veiligheid, omdat het via slijtage van de toetsen mogelijk is om de PIN-code te achterhalen. Het blijkt dat er maar een paar bedrijven op de hele wereld met deze kaart bezig zijn, dit komt onder andere door de prijs van deze kaart en het veiligheidsaspect.

7 Standaardisatie.

Er blijken diverse standaarden te bestaan. Zo is er de in Japan belangrijkste standaard de JEIDA (Japan Electronic Industry Development Association) standaard. In Frankrijk is de belangrijkste standaard de AFNOR standaard. In Nederland is de belangrijkste standaard de ISO standaard. In de United States bestaat nog de PCMCIA (Personal Computer Memory Card International Association). De JEIDA en de PCMCIA werken samen aan een gelijke standaardisatie van IC memory kaarten. In onderstaande tabel word alleen de JEIDA aangegeven welke de zelfde is als de PCMCIA standaard. INTAMIC is een internationale standaardorganisatie club die aanbevelingen doet aan ISO. Deze INTAMIC standaard, die uit de bancaire wereld komt, is in de diverse landen bekend.

De standaardisatie heeft betrekking op de fysieke eigenschappen en elementaire communicatieprotocollen.

Het grondwerk voor de standaardisatie begon begin tachtiger jaren onder andere vanuit de bancaire wereld (Intamic). Dit wordt nu voortgezet in de Technische commissies 68 en 97 van ISO. Diverse aanbevelingen zijn reeds tot ISO norm verheven, andere hebben reeds een DIS (Draft International Standard) status of DP (Draft Proposal) status bereikt. Men kan zonder overdrijving stellen dat de standaardisatie grootschalige produktie van smart cards en smart card apparatuur nu reeds mogelijk is.

Standaards relevant voor smart cards zijn: (de onderstreepte standaards zijn aangekocht door de schrijvers van dit rapport)

JEIDA - version 3 : Of the IC Memory Card Guidelines - adress the hardware specifications. Deze versie is gemaakt door JEIDA met acceptatie van de PCMCIA. In deze versie worden 5 typen IC Memory kaarten gesproken. Eén van deze type is het 68 pins byte geadresseerde type IC Memory kaart welke in the JEIDA version 4 uitvoerig wordt uitgewerkt.

JEIDA - version 4 : Of the IC Memory Card Guidelines - deze versie is door de JEIDA en PCMCIA samen gemaakt met als basis de oude JEIDA standaard version 3.

part 1 : Standardisation of the I/O features to support peripherals such as modems in the card

part 2 : Standardisation of DRAM card

part 3 : Standardisation of cards with a wide range of operating voltage

part 4 : Definition of a world-wide common logo

(trade mark). Dit logo is:

ICMC

- part 5 : Specifications for programming EPROM and EEPROM cards
- ISO 7810 : Identification cards - Physical characteristics
- ISO 7811 : Identification cards - Recording technique -
- part 1 : Embossing
 - part 2 : Magnetic stripe
 - part 3 : Location of embossed characters on ID-1 cards
 - part 4 : Location of read-only magnetic tracks - Tracks 1 en 2
 - part 5 : Location of read-write magnetic tracks - Track 3
- ISO 7812 : Identification cards - Numbering systems and registration procedure for issuer identifiers
- ISO 7813 : Identification cards - Financial transaction cards
- ISO 7816 : Identification cards - Integrated circuit(s) cards with contacts -
- part 1 : Physical Characteristics standaard
 - part 2 : Dimensions and location of the contacts standaard
 - part 3 : Electronic signals and transmission protocols draft standaard
 - part 4 : Standardisation of the common application so that they can be used for any application and be understood unambiguously by any terminal and any IC card.
- ISO 8583 : Financial transaction card originated messages - interchange message specifications. Waarschijnlijk is er van deze versie ook een toevoeging verschenen.
- ISO 9992 : Financial transaction cards - Messages between the integrated circuit card and the card acceptor device -
- part 1 : Concepts and structures draft standaard
 - part 2 : Functions
 - part 3 : Messages (Commands and responses)
 - part 4 : Common data for interchange
 - part 5 : Data element organisation
- ISO 10202: Identification cards - Security architectures of financial transaction systems using Integrated Circuit Cards -
- part 1 : Card life cycle draft proposal
 - part 2 : Transaction Process draft proposal
 - part 3 : Cryptographic Key Relationships draft proposal
 - part 4 : Security Modules in IC Card

- part 5 : applications in financial industries
Algorithms for use in Integrated
Circuit Cards
- part 6 : Cardholder Verification Security
- part 7 : Key management and a Systems Overview

ISO 10373 : Deze standaard is een toevoeging op de ISO 7816 part 1. Dit gedeelte bevat gegevens met betrekking tot contactloze kaarten. Tevens staan hier voor alle type kaarten test methodes in.

ISO 10536 : Deze standaard is een toevoeging op de ISO 7816 part 1. Dit gedeelte bevat toevoegingen op de physical characteristics of the IC card with contacts. Hierin staan bijvoorbeeld: bescherming tegen ultra violet licht, bescherming tegen x-rays en statische elektriciteit.

Het blijkt dat ETSI (European Telecommunications Standards Institute) ook bezig is met het standaardiseren van IC cards. Deze groep kreeg de taak om een Europese standaard te definiëren voor multi-application cards en kaart terminals in telecommunicatie services en de bijbehorende testing procedures. Onderstaand is een lijst weergegeven van enige standaarden die reeds zijn uitgekomen.

- ETSI 9000 : Requirements for IC cards and terminals for telecommunication use -
- part 1 : General description (version 2)
 - part 2 : Security framework (version 4)
 - part 3 : Application independent card requirements (version 6)
 - part 4 : Application independent card related terminal requirements (version 5)
 - part 5 : Payment methods (auto-billing, purse, use of bank cards)
 - part 6 : Telecommunication features

ETSI GSM 11.11 : Deze aanbeveling is opgemaakt voor een IC kaart die ingebed is in mobiele telefoon applicaties. Deze ingebedde IC kaart wordt een SIM (Subscriber Identity Module) kaart genoemd. Er worden twee typen kaarten geproduceerd:

- IC card SIM (heeft dezelfde maten als de normale plastic kaart)
- Plug-in SIM (de Plug-in kaart is een verklein de normale plastic kaart, omdat hij voor zeer kleine telefoon apparaten gebruikt wordt)
- In deze version 3.5.0 staan de Specifications of the SIM-ME Interface.

CEN (Comité Européen de Normalisation). Deze organisatie heeft verschillende werkgroepen opgericht die als doel hebben de ISO standaarden verder uit te werken. Eén van die doelen is de tolerantie bepalen, bijvoorbeeld de tolerance ranges for IC

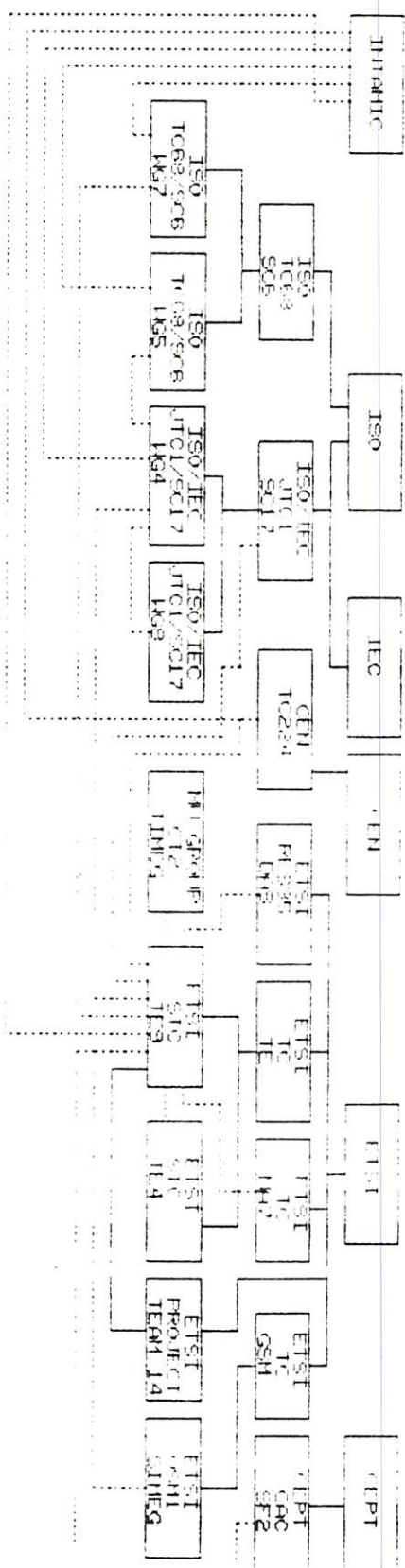
cards. Een ander doel is de ergonomical specification.

IEC (International Electronic Commission) werkt samen met ISO.

De FSSCF (Financial Sector Standards Co-ordination Forum) is een initiatief van ECPS (European Council for Payment Systems, met de bedoeling dat de bancaire wereld de aanbevelingen van de CEN kon coördineren. Het levert aanbevelingen aan de raad van de ECPS en de leden van de ECSAs (European Credit Service Associations).

Een overzicht tussen de verschillende IC card standaardisatie groepen is op de volgende bladzijde weergegeven.

ENT DORSEAD TONAT DE PERULES NUSSEN OF ATPO-DILLING - CHADWORTH-DISABLE - COMPTON-IES



Transgangalisatone is a member of the

Hierarchical relationships were also examined using the same methodology.

- CTN : Comité Européen de Normalisation
- CTPT : Conférence Européenne des Administrations des Postes et Télécommunications
- ETSI : European Telecommunications Standardisation Institute
- GSM : Groupe Spécial Mobile
- IEC : International Electrotechnical Commission
- ITU-T : International Telecommunication Union - Telecommunication Standardisation Organisation
- ITU : International Telecommunication Union
- ITU-R : Radiocommunication Sector
- ITU-S : Services and Systems
- ITU-TG : Telecommunication Group
- ITU-TT : Terminal Equipment
- ITU-TE : Telephone
- ITU-TS : Telephony Service

8 Applicatie: De smart card in het vierde generatie autotelefoonnet.

Binnen PTT Telecom wordt het nieuwe net inmiddels betiteld als ATF-4, internationaal spreekt men van het GSM-systeem. Dit autotelefoonnet zal uiteindelijk heel Europa gaan bestrijken. Het net gaat een groot aantal faciliteiten en diensten aanbieden: van automatisch terugbellen bij bezet tot en met videotex en facsimile. De smartcard fungeert in ATF-4 als abonnee-identiteitsmodule en is datgene wat de gebruiker krijgt als hij zich op het net abonneert. Dankzij deze smartcard zal de abonnee vanaf elke willekeurige terminal gebruik kunnen maken van de diensten die het GSM-systeem biedt; door heel Europa en voor eigen rekening. De smartcard speelt bovendien een cruciale rol in de beveiliging van het netwerk en draagt er in belangrijke mate toe bij dat de privacy van de gebruikers gewaarborgd is.

Persoonsgebonden telecommunicatie wil zeggen dat abonnees altijd voor eigen rekening gesprekken kunnen voeren en ontvangen, waar men ook in Europa is en vanaf elke willekeurige terminal. Ook voor het vaste telefoonnet wordt momenteel een dergelijk systeem van persoonlijke telecommunicatie voorbereid (het blijkt nu nog wel toekomstmuziek te zijn). Ook hierin zal de smartcard een essentiële rol spelen. Kort gezegd komt het hierop neer:

- de abonneegegevens bevinden zich niet meer in de lokale centrale in de vorm van de huisaansluiting, maar zijn in de vorm van persoonsgebonden gegevens in internationaal gekoppelde databases opgeslagen; deze databases worden met een smartcard geactiveerd,
- telefoontoestellen zullen overal in Europa voorzien kunnen worden van smartcardlezers,
- thuis, op bezoek bij vrienden of op de vakantiebestemming... overal kan de smartcard met een telefoontoestel worden ingelezen, het netwerk weet hierdoor waar de abonnees zich bevinden,
- voor eigen rekening kan nu overal vandaan gebeld worden,
- zonder extra doorschakelapparatuur in de lokale centrale kunnen gesprekken bovendien op elk willekeurig adres in Nederland of elders in Europa worden ontvangen,
- vaste telecommunicatie wordt dankzij de persoonlijke telecommunicatie dus veel "mobiel".

Dit nieuwe netwerk maakt digitale radiocommunicatie mogelijk in het gebied rond 900 Mhz. Het gebied dat het netwerk bestrijkt is daartoe verdeeld in een groot aantal cellen met een diameter variërend van circa 1.5 tot 30 km.

Elk van die cellen beschikt over een vast zend/ontvangststation (Base Station) dat de gesprekken, van en naar de abonnees in de cel, verwerkt. Als een abonnee zich tijdens het gesprek van de ene naar een andere cel verplaatst, wordt alle noodzakelijke informatie naar die andere cel doorgesluisd (hand-over) zonder dat de abonnee er iets van merkt.

GSM biedt niet alleen telefonie maar een heel scala aan diensten.

Deze diensten zijn globaal in drie categorieën te verdelen, van elke categorie worden bovendien enkele voorbeelden gegeven.

- Netwerkdiensten: datacommunicatie- en telefonieverbindingen. Netwerkdiensten:
 - circuit geschakelde duplex asynchrone data verbindingen met snelheden van 300 tot 9600 bits/seconde,
 - pakket geschakelde duplex synchrone data verbindingen met snelheden van 2400 tot 9600 bits/seconde,
 - circuit geschakelde 3.1 kHz audio verbindingen.
- Telediensten: telefonie, noodoproepen, videotex, tele fax en korte berichten dienst. Met deze laatste dienst kan een kort bericht van 180 octetten naar een abonnee worden verstuurd. Het netwerk fungeert hierbij als "store and forward" centrum. De zender krijgt een bevestiging van ontvangst.
- Aanvullende diensten: nummeridentificatie, presentatie van het telefoonnummer van degene die belt, doorschakelen van binnenkomende gesprekken of doorschakelen onder bepaalde condities (bijvoorbeeld altijd, alleen bij geen antwoord of uitsluitend bij bezet), wachtgesprek (indicatie van een binnenkomend gesprek tijdens het lopende gesprek), kostenindicatie (indicatie op display van de kosten van een gesprek).

De beveiligingsfaciliteiten dienen ertoe misbruik van het netwerk te voorkomen en de privacy van de abonnee te beschermen.

- Om misbruik van het netwerk tegen te kunnen gaan, worden abonnees die toegang wensen eerst geauthenticeerd; met andere woorden hun identiteit wordt geverifieerd. Dit geschiedt als volgt: als een abonnee via het GSM-systeem een verbinding wil opzetten, wordt eerst zijn abonnee-identiteitsnummer richting netwerk gestuurd waarna met behulp van cryptografische technieken gecontroleerd wordt of deze geclaimde identiteit authentiek is. Dat abonnee-identiteitsnummer waarover hierboven gesproken wordt, is de zogenaamde IMSI (International Mobile Subscriber Identity), een uniek 15-cijferig nummer dat iedere gebruiker toegekend krijgt als hij zich op het GSM-systeem abonneert.
- Om de privacy van de abonnees te beschermen wordt hun identiteit (in de vorm van de IMSI) steeds vertrouwelijk behandeld. Dit komt erop neer dat de IMSI overal waar dat mogelijk is, door een tijdelijk nummer vervangen wordt. Dit zogenaamde TMSI (Temporary Mobile Subscriber Identity) bestaat uit een kort nummer dat alleen voor een beperkte periode en in een beperkt gebied (een cel) geldig is.
- Tevens wordt ter bescherming van de privacy de communicatie over het radiopad vercijferd. Dit geldt zowel voor de gebruikersdata (gespreksinhoud) als voor de signaalsdata.

Door deze beveiligingsfeatures wordt het voor derden vrijwel onmogelijk om op illegale wijze van het netwerk gebruik te maken of om gebruikers te "tracen". Ook zal het in GSM nage-nog onmogelijk zijn om gesprekken tussen de abonnees af te luisteren.

Ten behoeve van de beveiligingsfuncties zijn behalve maatregelen in het netwerk, ook een aantal veiligheidsvoorzieningen in de GSM-terminal nodig. Deze terminal wordt in het GSM-wereldje wel het Mobile Station (MS) genoemd, waarmee dan de autotelefoon of de pocketline (zaktelefoon) van de abonnee wordt bedoeld. Realisatie van deze beveiligingsfuncties in het MS zelf zou echter betekenen dat daarin vertrouwelijke informatie en geheime cryptografische algoritmen opgenomen moeten worden. Omdat het MS onder de categorie randapparatuur valt en in de meeste landen door allerlei fabrikanten geleverd zal gaan worden (na type-goedkeuring), geeft dit een probleem ten aanzien van de beveiliging. Dit probleem is opgelost door in de specificaties het Mobile Station (MS) functioneel en fysiek in tweeën te splitsen:

- een abonnee-identiteitsmodule genaamd de SIM (Subscriber Identity Module);
- het resterend deel genaamd de ME (Mobile Equipment).

De ME bevat voornamelijk bedieningsfuncties voor de gebruiker en functies die nodig zijn voor de communicatie met het netwerk en met de abonneeidentiteitsmodule (SIM). De SIM is feitelijk geen randapparatuur maar onderdeel van het netwerk en valt daarmee onder verantwoordelijkheid van de netwerkbeheerder. Alle gebruikersspecifieke data zijn in deze module opgeslagen. Daarnaast bevat de SIM nog alle noodzakelijke functies om de gewenste beveiligingsfaciliteiten uit te voeren. Voor de "echte randapparatuur" (ME) is er naast de interface voor het radiopad met het netwerk, dan ook een tweede interface gestandaardiseerd namelijk met dat deel van het netwerk dat zich in de terminal zelf bevindt, de SIM (m.a.w. de smartcard).

Het van de ME loskoppelen van alle abonnee-specifieke informatie en functies, heeft voor elk van de betrokken partijen een aantal voordelen.

-De industrie. De ME kan gefabriceerd worden zonder dat daarin een soort security box geïnstalleerd hoeft te worden. De randapparatuur kan daardoor in heel Europa verkocht worden, zonder dat er aan specifieke eisen en procedures van netwerkbeheerders moet worden voldaan ten behoeve van de abonnementen-uitgifte. Dankzij het invoeren van de SIM kan de Mobile Equipment (ME) na algemene type-goedkeuring dus in heel Europa op de markt worden gebracht.

-De netwerkbeheerder. Voor de netwerkbeheerders wordt de uitgifte van de abonnementen een stuk eenvoudiger. In plaats van talloze ingewikkelde procedures met de verschillende apparatuurfabrikanten af te moeten spreken (voor het laden van geheime en gevoelige functies en informatie), kan nu worden volstaan met het rechtstreeks aan de gebruikers leveren van een kleine draagbare veiligheidsmodule (in de vorm van een "slimme kaart").

Deze veiligheidsmodule bevat alle relevante functies en informatie. Het uitgeven van abonnementen in de vorm van deze SIM kan hierdoor geheel in eigen beheer gebeuren.

-De gebruiker. Voor de abonnees betekent de aparte identiteitsmodule dat hij of zij niet noodzakelijk een eigen randapparaat (ME) hoeft te kopen, maart dat gebruik kan worden gemaakt van openbare, gehuurde of geleende randapparatuur. Een abonnee hoeft ook niet steeds zijn eigen auto- of zaktelefoon mee op reis te nemen, om toch op eigen rekening te kunnen bellen en gebeld te worden. Elke willekeurige ME volstaat, waar in Europa de abonnee zich ook bevindt. In feite si de SIM-concept dus de eerste persoonsgebonden vorm van telecommunicatie.

Voor de SIM module bestaan twee uitvoeringsvormen. De belangrijkste hiervan is de smartcard. De smartcard is het ideale middel om de benodigde functionaliteit te realiseren. Het is een kleine, makkelijk mee te nemen en zeer flexibele "security box" met een gestandaardiseerde interface op fysiek, mechanische en elektrisch niveau. Een tweede uitvoeringsvorm is de zogenaamde mini-smartcard. Dit is in feite een gewone smartcard waarbij een groot gedeelte van het plastic rond de chip en de contacten is weggesneden. De mini-smartcard is geïntroduceerd omdat er kleine draagbare zaktelefoons op de markt zullen komen waarvan de maatvoeringsmogelijkheden niet ingeperkt mogen worden door de standaardafmetingen van de creditcard. Voor de huidige mobiele netten zijn bijvoorbeeld al kleine zaktelefoons op de markt die smaller zijn dan de breedte van een creditcard. Van de mini-smartcard is het overigens niet de bedoeling dat deze telkens uit de terminal gehaald gaat worden, maar semipermanent in de ME wordt aangebracht. Het gebruik in verschillende ME's van de mini-smartcard zal derhalve niet gauw voorkomen en is bovendien ook niet zo nodig omdat een abonnee zijn kleine zaktelefoon meestal toch met zich mee zal dragen. Een niet te verwaarlozen nadeel van de mini-smartcard is dat deze, door het minder flexibele karakter en de buiten GSM niet gestandaardiseerde afmetingen, in de toekomst ongeschikt zal zijn voor multifunctionele doeleinden (multi service card).

De smartcard wordt binnen GSM/ATF-4 voor een tweetal taken ingezet:

- het realiseren van beveiligingsfuncties,
- de opslag van abonnee-specifieke data.

De beveiligingsfuncties die de smartcard vervuld, hebben als doel:

- 1 -de authenticatie van de gebruiker door middel van een PIN procedure,
- 2 -de authenticatie van de smartcard door het netwerk,
- 3 -een sessiesleutel te genereren die gebruikt wordt voor het versleutelen/ontcijferen van de data over het radiopad.

De eerste beveiligingstaak van de smartcard is mee te draaien in de procedure die een ongeoorloofde toegang tot het netwerk tegengaat. Dit gebeurt door de identiteit van de abonnee te verifiëren.

Dit verifiëren van de abonnee-identiteit vindt in twee stappen plaats. Allereerst wordt door de smartcard aan de hand van een PIN-procedure de identiteit van de gebruiker geverifieerd. De kaart controleert of de PIN die de geclaimde abonnee via de ME aan de kaart aanbiedt ook de correcte is, waarbij verondersteld wordt dat alleen de "echte abonnee" deze juiste PIN kent. De PIN kan door de abonnee overigens zo vaak als deze dat wenst, veranderd worden. In tweede instantie verifieert het netwerk via een ingewikkelde procedure vervolgens de identiteit van de smartcard, waarbij gebruik wordt gemaakt van een in de smartcard geprogrammeerde geheime abonneesleutel, de al eerder genoemde IMSI en TMSI (abonnee-identiteitsnummers) en een sessiesleutel waarmee data kunnen worden versleuteld en ontcijferd. De PIN is 4 tot 8 cijfers lang. Als aan de smartcard achtereenvolgens tot drie keer toe een verkeerde PIN wordt aangeboden, blokkeert de kaart zichzelf. Het maakt daarbij niet uit hoeveel tijd er tussen de pogingen zit en of de kaart tussentijds een keer verwijderd is uit de ME. Een geblokkeerde kaart hoeft echter niet direct weggegooid te worden maar kan weer ontsloten worden met een zogenaamde "unblocking key". Deze "unblocking key" is acht cijfers lang en kan niet veranderd worden. Nadat de "unblocking key" achtereenvolgens 8 keer verkeerd is aangeboden wordt de kaart echt onbruikbaar en kan weggegooid worden. Hoe met deze "unblocking key" omgegaan wordt, kan en zal per netwerkbeheerder verschillen. Eén mogelijkheid is dat de netwerkbeheerder deze sleutel in eigen beheer houdt. Een abonnee wiens kinderen bijvoorbeeld met de kaart hebben gespeeld en deze hebben geblokkeerd, zal dan terug moeten naar de netwerkbeheerder om de kaart weer bruikbaar te maken. Een tweede mogelijkheid is het aan de abonnee zelf meegeven van de "unblocking key", met het verzoek deze sleutel op een veilige plaats te bewaren. Deze laatste optie zal waarschijnlijk in Nederland gekozen worden.

Behalve het realiseren van de beveiligingsfuncties heeft de smartcard als tweede taak om alle gebruikersspecifieke data op te slaan. Het betreft hier data ten behoeve van:

- het netwerk,
 - de diensten,
 - "Mobile Station" features.
- Voor het netwerk is in de smartcard ten eerste de opslag nodig van de data voor de authenticatie-procedure (de geheime abonneesleutel, de abonnee-identiteiten IMSI en TMSI en de sessiesleutel). Tevens bevat de smartcard informatie waarmee het opzetten van een verbinding met het netwerk kan worden versoepeld.
- Ten behoeve van een tweetal GSM-diensten bevat de smartcard eveneens informatie: voor de teledienst "korte berichten dienst" en voor de aanvullende dienst "kostenindicatie". Om de abonnee in staat te stellen te allen tijde "korte berichten" te ontvangen, biedt de smartcard opslagruimte aan een willekeurig aantal van dergelijke aan de abonnee gezonden berichten. Willekeurig aantal slaat op het feit dat elke netwerkbeheerder zelf kan bepalen hoeveel dit er zullen zijn.

Dit zal voornamelijk bepaald worden door de grootte van het opslaggeheugen van de in de smartcard toegepaste chip en het beslag dat andere faciliteiten op dit geheugen zullen (gaan) doen. Voor de dienst kostenindicatie is op de kaart eveneens geheugenruimte gereserveerd. Hierin kunnen de kosten per gesprek of cumulatief opgeslagen worden. Bij de aanvullende dienst kostenindicatie wordt door het netwerk een indicatie aan de ME gegeven, waarmee deze de kostprijs van het gesprek kan berekenen.

- Tot slot wordt op de kaart informatie opgeslagen voor enkele Mobile Station (MS-)features. Eén van de features is de mogelijkheid tot het gebruik van verkorte kiesnummers op de terminal. De lijst met de verkorte kiesnummers staat hierbij op de kaart opgeslagen, waardoor een gebruiker zijn zelf-samengestelde lijst altijd op elke terminal beschikbaar heeft.

opm. De standaard die voor bovenstaand SIM-module geldt is beschreven in ETSI GSM 11.11.

9 Fabrikanten.

9.1 Japanse bedrijven.

Bedrijfsnaam	Produkt/services
- Asahi Chemical Industry Co., Ltd	:kontakt IC-card, 8-bit CPU, 2Kbyte EEPROM, ISO
- NTT Datacommunication	:kontakt SX en SA-type, 2Kbyte en 8Kbyte EEPROM apparatuur voor geheimcode als optie
- Oki-Denki Corporation	:kontakt IC-kaart en "low-cost" kaart, 8-bit CPU, 2Kbyte EEPROM, 125 byte EEPROM of EPROM, optie magneetstrip
- Kyodo Printing	:kontakt IC-card, 8-bit CPU, 2Kbyte of 8Kbyte EEPROM
- Shoei Printing	:kontakt IC-card, 8-bit CPU, 0.5Kbyte of 2Kbyte of 8Kbyte EEPROM, communicatie 7600 bps
- Dai Nippon Printing	:algemene IC-kaart of grote geheugenkaart of "low-cost" kaart, 8-bit CPU, 0.5Kbyte of 1Kbyte of 2Kbyte of 8Kbyte of 16Kbyte of 32Kbyte EEPROM, ISO
- Toshiba	:TOSMART(kontakt IC-card), 8-bit CPU, 8Kbyte EEPROM. TOSCA(kontaktloze kaart), bevat transciever
- Toppan Printing	:kontaktloze IC-kaart, 8Kbyte EEPROM. Multi-use IC-kaart, kontakt one-chip IC-kaart, 2Kbyte of 8Kbyte EEPROM, two-chip IC-kaart, 32Kbyte
- Hitachi Maxell	:IE-2 en IE-8 kontakt kaart, 2Kbyte of 8Kbyte, ISO
- Fujitsu	:MB98301 kontakt kaart, 8-bit CPU, 8Kbyte EEPROM, 2-chip kaart, 27 commando's (file toegang, controle commando's e.d.)
- NEC	:kontaktloze IC-kaart RF-remote ID systeem, microgolg, met communicatie afstand van 0-2 meter, ID-label (8Kbyte RAM of 128 byte EEPROM of 32 byte ROM

Bedrijfsnaam	Produkt/services
- Arimura Giken	:Supplies the ACT range of contact-equipped and contactless cards; includes a 16 kilobit EEPROM single-chip card.
- Casio Microcard	:Originally developed a 64 kilobit EPROM card for use in MasterCard's West Palm Beach trial location. Other versions since designed.
- Matsushita Denka	:Miniature (hand-held) reader/writer device
- Mitsubishi Electric	:Extensive range of EEPROM equipped smart cards as well as SRAM memory cards (non-microprocessor) under the 'MELCARD' title.
- Omron	:Yet another variation of the 'visual card' development. Previously developed an electronic cash register system with builtin smart card reader.
- Panasonic/Matsushita	:Recently announced a 16 kilobit EEPROM-equipped card.
- Tokyo Tatsuno	:Specialists in a range of reader/writers.
- SPOM	:Komt voort uit Dai Nippon Printing en Bull CP8. Deze firma levert een geheugenkaart van 1 K bit EEPROM, en kaarten met CPU: 4K, 16K, 64K en 256K bit EEPROM. De kaart voldoet aan ISO 7816/1 en 7816/2. De voedingsspanning bedraagt 5 V. De clock frequentie is 4.9125 Mhz. De transmissie methode is Half Duplex, asynchroon. De transmissie snelheid bedraagt 9600 bps.

9.2 Franse bedrijven.

Bedrijfsnaam	Produkt/services
Alcatel CAMP	:Automatic toll and fare-collection systems.
Cap Gemini Sogetti	: 'MULTICAM' software for smart card/videotex systems.
Crouzet	: Smart card payphone and the 'MONOTEL' EFT equipment.
CSEE	: Electronic payment terminals.
CKD	: Hand-held certifiers and 'SECURITEL' - a remote ID and certification system.
Connectral	: Specialisers in card acceptor devices.
Electronique Serge Dassault	: Turn-key public payphone system; teller and ticketing machines.
Honeywell Bull	: Manufactures full range of 'CP8' smart cards and products including readers and personalisation equipment.
Ingenico	: 'ISOCAM' mixed chip/magnetic stripe EFT-PoS terminals and software.
Logicam	: Systems supplier of hardware and software for payment, physical and logical access applications.
MET (Matra Ericsson Telecom)	: Physical access controls.
Monedata	: Reader/writers for combined chip/magnetic stripe cards.
RTIC (Philips)	: 'LECAM' smart card reader for use with Minitels (the French PTT's videotex terminal).
Schlumberger Industries Smart Cards Systems Division	: Major supplier of payphone cards and payphone terminal equipment as well as a full range of PoS terminals for mixed cards.
Segime Industrie	: Supplies system software for videotex/smart card applications and for PC based personalisation plus a software 'toolbox' package 'SEGIMTEL'.
Groupe Segin	: Customisation and personalisation processes for smart cards.

Bedrijfsnaam	Produkt/services
SGS-Thomson	:Major European supplier of microprocessors for smart cards - wired logic, NMOS and CMOS products.
Sligos	:Specialising in payment and transaction processing services plus on-line authorisation services as well as systems engineering. Recently designed the health-care software for Carte Santé.
SYD (Synergie Informatique et Developpement)	:Systems design in medical and healthcare applications.
Telesystemes	:Systems integrator under the 'Signetique' trademark with information security as a major application.
TRT-TI	:One of two suppliers of the Carte Bancaire 'mixed' card, also pioneered DEC cryptographic use in smart cards and manufactures readers and payment terminals.
Unidel sécurité	:Developed 'Clematic CP8(TM)', physical access control system with relevant 'tool-box' support products including personalisation kit.
Gemcard	:Most recent entrant is a spin-off of SGS-Thomson preparing a family of smart cards using both EPROM and EEPROM technology.

9.3 US bedrijven.

Bedrijfsnaam	Produkt/services
ASI (Applied Systems Institute)	:Systems integrator currently involved in both the Dept. of Agriculture's Peanut Quota and Tobacco Quota programmes.
AT&T	:Developed a proprietary contactless card system. One version the 'E-Card' is being extensively trialled as a business traveller's payphone service.
Battelle Memorial Institute	:System developer currently designing a system for the 'Individually carried record' Dept. of Defense (dog-tag) project.
Datakey Corporation	:Distinctive by virtue of its novel 'key'-shaped carrier, these devices offer both memory and logic capabilities.
GeneSys Data Technologies	:A subsidiary of LifeCard International and Blue Cross-Blue Shield specialising in medical/healthcare applications.
Intellicard	: 'Active' card development aimed at security and financial applications.
Logicard	:Supplies both Casio and proprietary smart card products including a 16 kilobit EEPROM version as well as PoS transaction terminals.
MCTI (MicroCard Technologies)	:Honeywell Bull's US subsidiary of Multimil, Switzerland. Supplier to the US Dept. of Defense container-tracking project.
Paymatec Schlumberger	:This US subsidiary of the French company is providing the card technology for the Tobacco Quota trial using a 4 kilobit reprogrammable card as well as small quantities of 32 kilobyte memory cards.

Bedrijfsnaam	Produkt/services
Personal Computer Card Corp.(PC3)	:Offers a range of kit including reader/writers and high-volume card initialiser and OEM smart cards - 64 kilobit programmable and non-programmable versions.
Sillcocks Plastics International	:Traditionally a magnetic stripe card manufacturer now developing a range of smart card products. Part owner of PC3.
SCI (SmartCard International Inc.)	:Developed first working 'active' card for Visa's prototypes. Now offers proprietary range of card products - ULTICARD (active), MAGNACARD (passive) as well as reader/writers and systems integration services.

9.4 Overige bedrijven.

Bedrijfsnaam	Produkt/services
<u>Australië</u>	
AES (Associated Electronic Services) Ltd.	:Located in Perth, Western Australia, has developed 'DATAFARE' smart card products for public transport applications using Dai Nippon chips. Voor technische specificaties zie SPOM Japan
Electronic Transactions Pty. Ltd.	:This Australian subsidiary of Schlumberger (France) operates Australia's first smart card manufacturing facility. The M64 offers 64 kilobits EPROM, 32 kilobits ROM and 2 kilobits RAM.

Bedrijfsnaam	Produkt/services
<u>Finland</u>	
Otatieto	:The OTACARD being used in the field trial in the Helsinki University of Technology; the 'OTA 2000' project card contains 64 kilobits of EEPROM and its current being up-graded to a single-chip version.
TT Innovation	:This Helsinki-based systems house is shortly to offer a range of US-developed smart card products.
<u>Italië</u>	
Monetica Spa	:A joint venture between Sligos and Enidata - current projects comprise design/implementation of both the Rome University and Lombardy banking projects.
<u>United Kingdom</u>	
De La Rue Systems Ltd.	:Leading international security printer now offering smart card products based on Hitachi EEPROM chips for primary application in security sector.
Fraser Williams	:London-based computer services company offering design/implementation of smart card systems directed at computer security and the financial sector.
GEC Card Technology Ltd.	:Smart cards and terminal devices based on contactless technology with 64 kilobit EEPROM capacity. Non-ISO thickness being followed by ISO standard size card.
Honeywell Bull UK	:Offers range of CP8 products - cards plus ancillary equipment. Supplying healthcare trials in south-west England.
National Physical Laboratory & British Technology Group	:Developed and licensed the 'intelligent token' for logical access using RSA cryptographic techniques.

Bedrijfsnaam	Produkt/services
Oakwood Design	:Manufacturer of precision plastic card production equipment has recently developed an automated chip-in-card production line.
Smart Card International (Europe)	:UK-based subsidiary of US SmartCard International currently involved with ULTICARD evaluation by Thomas Cook Ltd. et al.
<u>West Duitsland</u>	
Amphenol Tuchel Electronics	:Design and development of smart card reader/writers.
Giesecke & Devrient	:This West German security printer is now supplying a combined smart card and magnetic stripe security module equipped with PIN pad and display as an add-on to conventional terminals.
Nixdorf Computers	:Is offering various security-related solutions including fingerprint identification utilising Bull's CP8 and Indentix fingerprint scanners as well as a PC entry security facility.
Siemens	:Supplier to the Regensburg (Bavaria) EFT-PoS Trial funded by West German banks; a novel feature is the involvement of two smart cards (user and retailer) in every transaction.

9.5 Nederlandse bedrijven.

De Nederlandse fabrikanten worden uitvoeriger beschreven omdat naar deze bedrijven onderzoek is gedaan.

De bedrijven die worden beschreven zijn:

- 9.5.1 - Philips,
- 9.5.2 - Bull,
- 9.5.3 - Annokkee,
- 9.5.4 - DigiCash b.v.,
- 9.5.5 - Etrometa,
- 9.5.6 - NEDAP,
- 9.5.7 - Intercai.

9.5.1 Philips.

Levert drie type smart cards: D1, M4, D2 en de TB100 smart card. Verder levert Philips standaard software pakketten voor deze smart card. Daarnaast leveren zij de PE 111 Smart Card lezer en schrijver, de PE 117 en PE 118. De laatste twee zijn beveiligings apparaten die in de PC geïntegreerd gebruikt kunnen worden. Deze apparaten zijn voorzien van software die het mogelijk maakt om wederzijdse authentication te verkrijgen, dit geldt ook voor de dan eventueel aangesloten netwerken.

De Philips D1 kaart.

De Philips D1 smart card is een general purpose smart card. De beveiliging is gebaseerd op het DES algoritme dat geïmplementeerd is in het programma geheugen van de chip. De kaart kan tot 256 verschillende services zones bevatten. Een service zone bevat een blok data en is speciaal voor één service. Een speciale set van sleutels kan aan elke zone worden toegevoegd. Mogelijkheden (volgens Philips):

- PIN wijzigen zo vaak als de gebruiker maar wil,
- persoonlijke extra mogelijkheden op aanvraag,
- instructie set bevat sleutel management functies speciale functies om session keys of master keys te generen.
- intern wordt gebruik gemaakt van het DES algoritme om een hoge mate van beveiliging te bereiken.

Technische eigenschappen D1 smart card:

Standaard:	ISO 7810 tot 7816
Afmetingen:	0.78 mm X 85.60 mm X 53.98 mm
Plastic Logo:	klant afhankelijk
Magnetic stripes:	ISO 1, ISO 2, ISO 3 (optioneel)
Electronica:	Mono-chip 8-bit microprocessor, gebruikersgeheugen van 8Kbits
Contacten:	Hoge of lage ISO positie
PIN control:	-Monitored door sleutel chip micro-programma. -geen PIN code is mogelijk

-meerdere PIN wijzigingen mogelijk

Beveiligings Keys: -maximum 12 sleutels
 -2 sleutels maximum per zone
 -flexibel sleutel management door:
 -generen van sessie sleutels
 -grote verscheidenheid aan master sleutels

Algoritme: Ingebouwd DES algoritme
 ECB, CBC, CFB modes zoals gedefinieerd in de standaarden.

Applications: -Data beveiliging
 -Informatie toegangs controle
 -Fysische toegangscontrole
 -Draagbare file
 -Onderhouds file, produktie kaart
 -Financiële transacties

De Philips D2 kaart.

Deze kaart is een hoog beveiligde Multi-service smart card. Deze kaart heeft net als de D1 kaart een ingebouwd DES algoritme. Deze kaart heeft een beveiligings architectuur die verschillende speciale functies die gebruikt worden op computer mainframes.:

- In cijferschrift overbrengen van sleutels voordat de werkelijke transmissie van de gevoelige data plaats vindt
- Grote verscheidenheid aan geheime sleutels
- Tijdelijk generen van sessie sleutels behorende bij verschillende data processen
- Random generator voor ondubbelzinnige wederzijdse authenticatie tussen card en server.
- MAC (Message Authentication Code) berekening.

Technische eigenschappen D2 smart card:

Standaard: ISO 7816/1-2-3-4

Afmetingen: 0.78 mm X 85.60 mm X 53.98 mm

Plastic Logo: klant afhankelijk

Magnetic stripes: ISO 1, ISO 2, ISO 3 (optioneel)

Electronica: Mono-chip 8-bit microprocessor, gebruikersgeheugen van 32Kbits (EPROM)

Contacten: Hoge of lage ISO positie

PIN control: -geen PIN code is mogelijk
 -meerdere PIN wijzigingen mogelijk

Beveiligings Keys: -6 basis sleutels
 -2 sleutels maximum per zone
 -flexibel sleutel management door:
 -generen van sessie sleutels
 -grote verscheidenheid aan master sleutels

Algoritme: Ingebouwd DES algoritme: 440 bits/sec
 -ECB volgens ANSI X3.92
 -MAC volgens ANSI X9.9

Applications:

- Data beveiliging
- Informatie toegangs controle
- Werkstation beveiliging
- Boot control
- Fysische toegangscontrole
- Draagbare file
- Onderhouds file, produktie kaart
- Financiële transacties

De Philips TB100 kaart.

Deze kaart heeft de laatste technologieën in zich. Elektronisch Erasable Memory, Data File Memory Management, krachtige op DES gebaseerde beveiligings architectuur. De architectuur en de low power HCMOS chip maken deze kaart zeer geschikt voor een wijde range van applicaties.

Technische eigenschappen TB100 smart card:

Standaard:	ISO 7810, 7811, 7816-1 tot 7816-3
Afmetingen:	0.80 mm X 85.60 mm X 53.98 mm
Plastic Logo:	klant afhankelijk
Magnetic stripes:	ISO 1, ISO 2, ISO 3 (optioneel)
Electronica:	Mono-chip 8-bit 68HC05 microprocessor, gebruikersgeheugen van 3Kbytes EEPROM, 6Kbytes ROM, 128bytes RAM
Contacten:	Volgens ISO 7816-2 positie
PIN control:	-geen PIN code is mogelijk -meerdere PIN wijzigingen mogelijk
Beveiligings Keys:	-6 basis sleutels -2 sleutels maximum per zone -flexibel sleutel management door: -generen van sessie sleutels -grote verscheidenheid aan master sleutels
Algoritme:	Ingebouwd DES algoritme: 440 bits/sec -ECB volgens ANSI X3.92 -MAC volgens ANSI X9.9
Applications:	-Data beveiliging -Informatie toegangs controle -Werkstation beveiliging -Boot control -Fysische toegangscontrole -Draagbare file -Onderhouds file, produktie kaart -Financiële transacties -Elektronische portemonnee

9.5.2 Bull.

Dit bedrijf vervaardigd de CP8 kaart. Deze kaart kan voor verschillende applicaties gebruikt worden. De microcomputer van de CP8 is een zelf programmeerbare chip. Er zijn verschillende kaarten te onderscheiden onder de CP8 kaart.

EPROM (bits)	8K	16K	64K	
EEPROM (bits)				24K
MASKS	M4	M9	M9 MP	M9
ROM (bytes)	1.6K	2K	6K	6K
CPU (bits)	8	8	8	8
Technologie	HMOS	HMOS	HCMOS	HCMOS

De kaart bezit een eendraads asynchrone bidirectionele interface welke voldoet aan de ISO norm 7816-3. Het masker kan vergeleken worden met het operatings systeem van een computer. Zoals te zien in bovenstaande tabel bestaan er 3 verschillende maskers. Het M4 masker is het meest gewone masker dat gebruikt wordt voor kleine geheugens. Het M9 masker kan werken met veel grotere geheugencapaciteiten, en ondersteunt ook het gebruik van EEPROM's. Het MP/ADF masker (Multi-purpose/Application Data File) is ontwikkeld met het oog op de in de toekomst te gebruiken multi-applicatie kaart. Deze maakt het mogelijk om met onafhankelijke applicaties van de zelfde kaart gebruik te maken, met hun eigen files en beveiligings regels. Buiten het vervaardigen van de CP8 kaart levert Bull bijbehorende software en hardware apparatuur. De produktie van deze kaart is de laatste jaren enorm gestegen. Dit is goed te zien in de tabel op blz. 32 van de bijgevoegde documentatie "13 questions about Bull CP8 "The Microcomputer card"".

9.5.3 B.V. Technisch Adviesbureau Annokkee.

Deze firma is importeur van COTAG. COTAG is een engels firma die identificatie kaarten maakt. Deze hoogfrequent tags worden gebruikt voor identificatie van mens, artikelen en dieren. COTAG levert ook de benodigde apparatuur om deze kaarten te kunnen uitlezen. De COTAG systemen worden veel verkocht voor fysieke toegang tot specifieke ruimten. Een lees antenne wordt dan naast de deur geplaatst, deze antenne staat in verbinding met een centrale regelaar.

9.5.4 DigiCash b.v..

Dit bedrijf werkt met een smart card die voorzien is van het RSA algoritme. Dit algoritme is langzamer maar nog veiliger dan het DES algoritme. Eigenschappen van deze kaart zijn niet bekend. De kaart wordt veel gebruikt voor financiële applicaties omdat deze een hoge graad van beveiliging moeten hebben.

9.5.5 Etrometa.

Deze firma is importeur van het australische bedrijf AES (Associated Electronic Services limited), welk onder anderen het datafare 2000 systeem ontwikkelde. Dit datafare 2000 systeem is gebaseerd op een smart card (zie SPOM JAPAN), welke wordt gebruikt als waardekaart. Het systeem is geschikt voor vervanging van de strippenkaart. De smart card wordt tegen een eventuele betaling van statiegeld uitgereikt aan de reizigers. De waarde of het saldo van de kaart kan, al naar gelang het gebruik, steeds worden aangevuld. Om de benodigde functies te kunnen realiseren bevat de smart card als het ware drie kompartimenten:

- een "elektronische beurs",
- een strippenkaart/meerritten kaart of een abonnement,
- een notitieboekje.

In het kompartiment "elektronische beurs" wordt het saldo, de waarde, van de kaart geregistreerd. De regelmatige reiziger kan een abonnement of een meerrittenkaart (strippenkaart) kopen en betalen met kontant geld of met "geld" uit de elektronische beurs: het saldo op de kaart. In het kompartiment "abonnement" wordt dan het traject en de periode waarvoor het abonnement geldig is geregistreerd. Bij gebruik als meerritten kaart wordt op dezelfde manier betaald en wordt in dit (tweede) kompartiment het traject en het aantal gekochte of nog beschikbare ritten geregistreerd. In het kompartiment "notitieboekje" wordt het gebruikt van de kaart geregistreerd. Dit betreft reizen waarvoor een afzonderlijk plaatsbewijs is gekocht en reizen op een meerrittenkaart, eventueel ook de reizen die met gebruik van een abonnement zijn gemaakt.

In geval van verlies of diefstal van een smartcard, die een aanzienlijke waarde kan vertegenwoordigen, kan het verlies voor de klant beperkt worden door de kaart te blokkeren. De klant moet daartoe het verlies van de kaart melden aan het vervoersbedrijf. De kaart wordt dan op een attentielijst geplaatst. De informatie van deze attentielijst wordt aan de bestuurders van alle voertuigen meegegeven bij het aanvangen van hun dienst door middel van de bestuurder smart card. Een reiziger met een dergelijke kaart kan dan signaleerd worden door het voertuigapparaat.

Het vervoerbedrijf dat een dergelijke smart card uitgeeft kan besluiten andere organisaties medegebruik toe te staan. Dit kan bijvoorbeeld een parkeergarage zijn. Deze moet dan ook over een apparaat beschikken waarmee in het apparaat zelf en in de smart card van de klant de betalingen ten laste van het kaartsaldo worden geregistreerd. Deze organisatie verzamelt aldus de gegevens van alle betalingen te haren gunste en kan deze vervolgens bij het vervoerbedrijf declareren. Ook kan een dergelijke organisatie met de aanwezige apparatuur zorgen voor de aanvulling van het saldo van een kaart, het daarvoor ontvangen geld moet dan worden afgedragen aan het vervoerbedrijf. In zo'n geval ligt het voor de hand dat het vervoerbedrijf de apparatuur in beheer houdt en deze bijvoorbeeld verhuurt.

Er is een compleet pakket software-hulpmiddelen beschikbaar voor de operationele ondersteuning van de kaartverkoopapparatuur. Dit zijn programma's die uitgevoerd kunnen worden met behulp van een standaard personal computer en die, naast de eerder genoemde analyse van het kaartgebruik, voorzien is in functies zoals:

- onderhoud van administratie en bestand van kaarthouders
- onderhoud van de attentielijst (verloren of gestolen kaarten)
- onderhoud tarieven en tariefsysteem
- keuze van opties, instelling van de apparatuur wijzigen.

Datafare 2000 is naast een kaartverkoop en betaalsysteem ook een marketinginstrument. Op basis van het geregistreerde kaartgebruik kan een vervoerbedrijf een goed inzicht krijgen in de vervoersvraag.

Flexibiliteit en differentiatie in tarieven evenals speciale tarieven voor bijzondere gelegenheden zijn mogelijk met "Datafare 2000".

Met "Datafare 2000" is eenvoudige afrekening en betaling van afzonderlijke kaartjes mogelijk naast het gebruik van abonnementen of meerrittenkaarten/strippenkaarten.

"Datafare 2000" is klantvriendelijk door de mogelijkheid de smart card te laten blokkeren in geval van verlies of diefstal en door de mogelijkheid reizigers een "kassabon" te geven bij elke kaarthandeling of op verzoek een overzicht te printen met gegevens van de laatste kaarthandelingen.

"Datafare 2000" maakt samenwerking mogelijk tussen verschillende vervoersbedrijven, waarbij elk vervoerbedrijf een eigen herkenbaar kaartmodel uitgeeft via eigen verkooppunten. De hoofdstroom van de kaartverkoopopbrengst bereikt hierdoor meteen zijn bestemming.

Het gebruik en de ontwaarding van een kaart is niet beperkt tot één vervoerbedrijf. Reizigers kunnen daardoor met dezelfde kaart met verschillende vervoersbedrijven reizen. De bedrijven kunnen elkaar de diensten aan reizigers met een kaart van een zusterbedrijf op basis van het automatisch geregistreerde kaartgebruik in rekening brengen. Deze verrekening kan rechtstreeks tussen de vervoersbedrijven onderling worden afgehandeld.

9.5.6 NEDAP N.V..

NEDAP produceert in Groenlo de XS card. Dit is een identificatie kaart voorzien van een onuitwisbare 64-bits code. De XS kaart bevat geen interne energiebron maar ontvangt zijn energie uit de antennespoel tot op een afstand van ca. 70 cm (e.e.a. afhankelijk van afmetingen en inbouwmogelijkheden van de antennespoel). De XS kaart is leverbaar in verschillende uitvoeringen: als sleutelhanger en in de vorm van een creditkaart. Voor het werken met dit type kaart zijn een zender en ontvanger noodzakelijk.

Eigenschappen van deze zender/ontvanger:

- Ongemoduleerde zender met 120 Khz draaggolf,
- voldoet aan alle internationale PTT-voorschriften,
- instelbaar zendniveau,
- afstemming met behulp van LED-array,
- ontvanger voor de teruggemelde signalen van de XS-card,
- aansluiting voor diverse antennespoelen d.m.v. 300 Ohm lintkabel (max. afstand t.o.v. de zender is 10 m).

Toepassingen van deze kaart zijn fysische toegangscontrole en identiteits controle. NEDAP heeft met deze kaart een Ski Card systeem gemaakt, waarmee de XS-card dienst doet als Ski pas. NEDAP maakt deze identiteits XS-card ook in capsule vorm zodat hij geschikt is om bij dieren onder de huid geïnjecteerd te worden. De andere vormen van deze XS-card kunnen zo zijn dat ze geschikt zijn voor logistieke problemen. Het NEDAP-GIS systeem bevat de XS-card in kleine blokjes die geschikt zijn om op goederen bevestigd te worden. Hierdoor is op ieder moment bekend waar artikelen zich bevinden. Dit soort identificatie is ook geschikt voor automatische productie machines die geheel automatisch stukken gereedschap moeten verwisselen. Op elk stuk gereedschap wordt dan een XS label aangebracht.

9.5.7 Intercai.

Intercai, opgericht in 1979, is een adviesbureau op het gebied van telecommunicatie en telematica. In deze snel groeiende en ook anderszins zeer dynamische markt neemt Intercai een voor-aanstaande plaats in. Deze positie is te danken aan een duidelijke profilering, die is gebaseerd op met elkaar samenhangende bedrijfskenmerken:

- onafhankelijkheid,
- actief op het hele terrein van telematica,
- expertise in zowel technische als beleidsadviezen,
- know-how op het gebied van projectmanagement en beheer van telematica-infrastructuren,
- kennis van en actief op de Europese markt.

Intercai is gevestigd in: Nederland, België, Duitsland, het Verenigd Koninkrijk, Zwitserland, Italië, Tsjecho-Slowakije, de Sovjet Unie en in de toekomst ook op Curaçao.

Het dienstenpakket van Intercai ziet er als volgt uit:

- technische advisering,
- beleidsadviesing,
- projectmanagement,
- facilities management,
- opleidingen,
- speciale kennis.

Intercai heeft in opdracht van het ministerie van Economische Zaken een technologie verkenning gedaan met als titel: "Chip-cards en Elektronische labels: een verkenning".

De conclusie van het rapport luidt: Het rapport pleit er niet voor dat de Nederlandse overheid het voortouw neemt om deze chipcard-infrastructuur ook in ons land te creëren. Aanbevolen wordt om het initiatief te laten bij anderen, en een groeipad uit te zetten van geringe naar grotere complexiteit. Infra-structuren ontstaan dan op basis van in samenhang gebrachte minder complete bouwstenen.

De begeleidingscommissie van het onderzoek voegt daar nog aan toe: "Voor de overheid is het bevorderen van infrastructuur een gegeven. Maar daarmee kiest de overheid bijna voortdurend voor projecten die te groot, te moeilijk, te complex zijn en te vroeg worden gestart".

De Nederlandse samenleving zou op den duur schade ondervinden als ze niet aansluit op die nieuwe ontwikkelingen. Chipcard-technologie, en de in het rapport eveneens behandelde technologie van elektronische labels, mogen dan ook niet veronachtzaamd worden.

10 Projekten in binnen- en buitenland.

In dit hoofdstuk worden projecten vermeld van IC kaarten met verschillende standaardisaties.

10.1 Projekten in Japan.

Projecten in Japan:

- Kodak to market industrial-use hi-vision compatible CCD cameras in Japan,
- NTT markets ISDN terminal adapters,
- Japan industrial Journal/October 29, 1991, Tuesday/page 1 COMLINE-CTE/page 2,
- Risho Kogyo to expand production of PCBs for telephone IC cards,
- Komatsu nears development of unmanned dump truck system,
- NTT markets new display phone,
- AT&T, Nipponese to cooperate in IC card business,
- Matsushita to market 16-bit Notebook PC,
- NTT to lend 100,000 "Angel Note" data terminals,
- Shin Nippon Kohan markets business-use telephone with LC Display,
- Matsushita electric markets Notebook-size PC,
- Proside to market IC card data storage device, PC,
- CSK to market communications IC card for electronic organizer,
- Telemation Association to standardize multifunction IC card telephone,
- JSB, Sanyo and Kankaku develop multi-function telephone terminal,
- NTT developing color still image transmission systems,
- JAL develops image transmission system,
- Fujitsu markets 32-bit Notebook-size PC,
- Hitachi Maxell to market expansion memory for Toshiba PC,
- Sharp develops communications card, compact modem for electronic Notebook,
- Adtech develops IC card interface for NEC PC's,
- Sharp to market application development IC card for electronic Notebook,
- Fujitsu markets small Japanese WP,
- Ascii to supply IC memory card BIOS on OEM basis,
- Toshiba to test, market IC card system,
- Fujitsu to supply Notebook-size PC's to its sales department,
- Oki Electric to produce non-contact IC cards for FA use,
- Ricoh markets new laser printers,
- Sharp Expects to sell 1.5 Million electronic Notebooks this year,
- Ascii markets IC card software for NEC Notebook-size PC,
- Toshiba markets new PC's,
- Canon to market facsimile machine with IC memory card,

- Hitachi sales to market electronic Notebook,
- Niigata engineering develops asphalt finisher,
- Toshiba, Fuji Photo Film's standard for digital still cameras likely to be approved,
- NTT Data Communications develops computer communications encryption system,
- Publishers develop software for Kyocera electronic Notebook,
- NEC HE markets electronic Notebook software.

Opmerking : Bij bovenstaande projecten wordt vaak de JEIDA standaard gebruikt, deze beschrijft een 68-pins Memory kaart.

10.2 Projekt in Nederland.

Chipcard-proef in Woerden.

Op 1 november 1990 is in Woerden een experiment van start gegaan. Het is een experiment van winkeliers, banken en consumenten met een nieuwe wijze van betalen: elektronisch. Niet meer in de winkel afrekenen met gegarandeerde cheque of betaalkaart, creditcard of contant geld, maar met een chipcard. Het Economisch Instituut voor het Midden- en Kleinbedrijf (EIM) begon in opdracht van het Hoofdbedrijfschap Detailhandel met een verkennend onderzoek naar de bruikbaarheid van elektronisch betalen en de eisen, te stellen aan het toe te passen systeem. Naar aanleiding van de rapportage van het EIM trad het Hoofdbedrijfschap Detailhandel in overleg met de Raad voor het Betalingsverkeer van de gezamenlijke banken en met de Postbank. Dat eerste verkennende overleg werd uiteindelijk een samenwerkingsverband, dat een stuurgroep[, de stuurgroep Chipcard-proef Woerden geheten, met de uitvoering van de proef belastte. In de Stuurgroep zijn thans het Hoofdbedrijfschap Detailhandel (HBD), alle banken, inclusief de Postbank, de Consumentenbond en het Ministerie van Economische Zaken vertegenwoordigd. De Nederlandsche Bank heeft een waarnemerszetel. Deze Stuurgroep heeft in de loop van 1986 de mogelijkheden en problemen rond de beoogde proef onderzocht. Het nu in Woerden gestarte Chipcard-experiment is het resultaat van dat onderzoek. Voor advies gedurende het gehele project en voor coördinatie is KPMG door de Stuurgroep ingeschakeld.

De Stuurgroep bestaat uit de volgende leden:

- | | |
|-----------------------|--|
| -C.A. Klomp RA, | directeur Automatiseringscentrum IDETA B.V.; namens het Hoofdbedrijfschap Detailhandel; voorzitter Stuurgroep, |
| -R.M.M.G. van Bergen, | secretaris KNOV voor werkgevers detailhandel, |
| -W.J. van Gelder, | lid Tweede Kamer (PvdA), vertegenwoordiger werknemers, |
| -M. de Kool, | namens Hoofdbedrijfschap Detailhandel; secretaris Stuurgroep, |

- | | |
|--------------------|---|
| -J.C. Enters, | directeur Raad voor het Beta-
lingsverkeer, |
| -J.F.L. Hazelet, | directeur BankGiroCentrale, |
| -H. Hoffman, | Hoofd Ontwikkeling Particulier
Betalingverkeer Postbank, |
| -C.H.M. Hoogkamer, | beleidsmedewerker Consumenten-
bond. |

De plaats Woerden is uitgekozen omdat de plaats representatief moest zijn voor Nederland en hij moest ook niet al te groot zijn: de kosten voor de aan te schaffen apparatuur en chip-cards konden daardoor binnen zekere grenzen blijven. Daarnaast diende de middenstand divers te zijn samengesteld en moesten er voldoende banken zijn. En ten slotte was de centrale ligging van belang. Er zijn in Woerden ongeveer 25.000 particuliere cliënten van de Postbank, de algemene banken, de Rabo- en de spaarbanken.

Doelstellingen van de proef:

De proef is opgezet met als doel ervaring op te doen met elektronisch betalen op grote schaal in de detailhandel. De opgedane ervaring zal worden vertaald in:

- Het verkrijgen van inzicht in de mate van acceptatie van elektronisch betalen en de verandering in het gebruik van betaalmiddelen door de consument,
- het bepalen van de mate van acceptatie van elektronische betalingen door de detailhandel, hetgeen tot uitdrukking kan worden gebracht in verbetering van en/of inzicht in de verhouding kosten en baten, verbetering van doorlooptijden aan de kassa, bedieningsgemak, beveiliging en vermindering van de kans op fraude,
- het verkrijgen van inzicht in de voordelen van gebruik van de chipcard als medium voor elektronisch betalen, hetgeen tot uitdrukking kan komen in:
 - verbetering van beveiliging door de mogelijkheden voor verwerking van functies door de chipcard zelf,
 - lagere kosten van de terminal door het verleggen van betaalfuncties naar de chipcard,
 - lagere verwerkingskosten van transacties door het betaalproces, mogelijk, "off-line" uit te voeren, dat wil zeggen: beperking van gebruik van datacommunicatie voorzieningen en centrale computerkosten,
 - korte responsietijden waardoor het betaalproces kan worden versneld.

De volgende systeemeisen zijn aan de proef gesteld:

- Er wordt uitsluitend gebruik gemaakt van de chipcard,
- er wordt gebruik gemaakt van de nieuwste chipcardtechnologie (hoge capaciteit, multi-functioneel),
- voor de functionaliteit van de beveiliging wordt gebruik gemaakt van het zogenaamde twee kaarten-principe: één systematiek voor alle banken,
- de toepassing zal zoveel mogelijk aansluiten bij internationale (ISO- en Intamic-standaards) en nationale (Interbancair Autorisatie Protocol) standaards,
- bij de start wordt de proef beperkt tot één functie: de elektronische cheque,

- alle kredietwaardige consumenten worden op de proeflocatie toegelaten (maximaal 20.000 kaarten),
- alle detaillisten worden uitgenodigd op de proeflocatie (maximaal 220 betaalautomaten),
- van de financiële instellingen zullen uitsluitend de RBV banken en de Postbank deelnemen aan de proef,
- maximale beschikkingsruimte:
Iedere cliënt krijgt op de proeflocatie in principe de beschikking over een chipcard/betaalkaart. Per cliënt wordt zijn/haar beschikkingsruimte vastgesteld, mede afhankelijk van de voorwaarden van de bank. Deze maximale beschikkingsruimte (bijvoorbeeld f2.000,-- per maand) wordt opgeslagen in de cliënten-chip en automatisch verhoogd tot het vastgestelde maximum, zodra de eerste betaling plaatsvindt in een nieuwe periode,
- de betaling:
De detaillist krijgt de beschikking over een betaalautomaat met een handeenheid voor toetsenbord/beeldscherm/chipcard-lezer. De betaalautomaat bevat een opslagcapaciteit (schijfruimte) van 128K, een printer, een datacommunicatie-eenheid en een journaalrol. De betaalautomaat is verbonden met een afzonderlijke eenheid voor de cliënt, een zogenaamde pinpad met beeldscherm en toetsenbord.

In de betaalautomaat vinden de volgende controles plaats:

- Echtheidscontrole (authenticiteit),
- pin-verificatie,
- controle op aanwezigheid op de zwarte lijst (in de betaalautomaat),
- controle op voldoende beschikkingsruimte in de consumentenkaart,
- afhankelijk van de situatie in een beperkt aantal gevallen on-line controles. In geval van on-line controle wordt verbinding gemaakt met de Postbank en de Bankgirocentrale (BGC),
- Na positieve autorisatie van de betaling wordt de transactie:
 - weggeschreven in het transactiedagbestand (in betaalautomaat),
 - weggeschreven naar de consumenten-chip,
 - uitgeprint voor de cliënt (transactiebon),
 - doorslag vastgelegd op de (papieren) journaalrol.

Enkele onderscheidende kenmerken tussen magneetstripkaart en chipkaart zijn:

	<u>magneetstripkaart</u>	<u>chipkaart</u>
kosten	circa f1,--	circa f25,-- verwachting circa f10,-- of f15,-- op grote schaal
verwerking levensduur	on-line enkele jaren	off-line verwachting enkele jaren
betrouwbaarheid	redelijk	onzeker (ervaring ontbreekt, verwachting is hoog)
kosten datacom- municatie	hoog	laag
kosten betaalautomaat	circa f6.000,-- tot f10.000,--	f3.000,- / f7.000,-- perspectief op grote schaal f1.500,--
security	hoog	hoger
multifunctionaliteit	niet/nauwelijks	ja
verwerkingssnelheid (doorlooptijd)	traag	snel
gebruikersvriende- lijkheid	hoog	hoger (zelf uitlezen saldo en transacties)

Hoofdleverancier van de kaarten en betaalautomaten is Schlumberger Industries B.V. in Gorichem, onderdeel van Schlumberger Industrie France. Het bedrijf heeft met name in Frankrijk, waar de chipcard-technologie in een vergevorderd stadium verkeert, een belangrijke positie als leverancier van apparatuur voor elektronisch betalingsverkeer verworven. De onderneming produceert gemiddeld 1,5 miljoen chipcards per maand. Zij heeft met name een belangrijke rol gespeeld bij de ontwikkeling van het nieuwe type chipcard dat in Woerden gebruikt wordt.

Consumentenvoorwaarden:

Hoewel de kansen op misbruik en fraude bij een chipcard minimaal zijn, wordt voor alle zekerheid een regeling ontworpen. Deze ziet er in grote lijnen hetzelfde uit als de regeling die voor het elektronisch betalen gaat gelden.

Eigenschappen Schlumberger chipcard:

- chipcard beschikt over ADF-software en ingebouwd DES algoritme
- twee technologieën chipcards worden gebruikt in de proef, te weten: de EEPROM-chipcard met 16K geheugen die dienst doet als detaillistenbeveiligingskaart, en de EPROM-chipkaart met 64K geheugen die dienst doet als cliëntenkaart.
In de EPROM kaart kunnen éénmalig 500 betaaltransacties worden opgeslagen, waarna moet worden overgegaan tot aanschaf van een nieuwe kaart.
- De beveiliging is uitgevoerd volgens het zogenaamde twee kaarten-concept zoals dit binnen ISO en Intamix is aanbevolen. In de proef is dit concept gerealiseerd door communicatie tussen de cliëntenchip en detaillistenchip. Echtheidscontrole, PIN-verificatie, saldocontroles, encryptieberekening en vaststelling van transportcodes worden uitgevoerd binnen beide chips. De sleutels voor deze verwerkingen zijn opgeslagen in beide chips, voor elke kaart afzonderlijk. Deze sleutels worden dagelijks gewisseld. Voor de encryptie van berichten voor veilig transport van en naar de chips wordt gebruik gemaakt van het DES-algoritme, dat is opgeslagen in de chip. De communicatieverbinding tussen de detaillist en Datatrafic wordt verkregen d.m.v. telefoonhuurlijnen. Deze lopen vanuit de zaak van de detaillist naar een PAD-toegangspoort tot het datanet dat naar de verwerkingscomputer leidt. In de proef is afgezien van clustering van de betaalautomaten. Dit betekent dat voor elke detaillist een even groot aantal telefoonhuurlijnen wordt gebruikt als het aantal afgenomen betaalautomaten.

Evaluatiemiddelen.

De Stuurgroep interesseert zich voor de technische resultaten, het functioneren van de hardware, de snelheid van de transactieverwerking, de kracht van de beveiliging, de convenience voor de detaillist en consument, het gebruik van de uitleesfaciliteit etc.

Op de volgende belangrijke vragen worden uitkomsten verwacht:

- gegevens over feitelijke transacties: hoeveel en waar (op winkelniveau en per branche), voor welke transactiebedragen, hoe vaak off-line en on-line, gebruiksfrequentie per kaart, aantal kaarten dat in het geheel niet wordt gebruikt;
- oordelen van consumenten over het praktische gebruik en de substitutie-effecten op andere betaalinstrumenten, over de gebruiksrisico's;
- oordelen van de detaillisten over de toepassing, de administratieve afwikkeling en zo mogelijk over de bedrijfseconomische betekenis;
- informatie uit de Helpdesk over storingen en afwikkelingsproblemen.

Het feitelijke marktonderzoek is uitbesteed aan het EIM (Economisch Instituut voor het Midden- en Kleinbedrijf). Voor het veldwerk onder de consumenten, die een drietal keren worden 'gehoord', is de Nederlandse Stichting voor Statistiek (NSS Marktonderzoek) ingeschakeld. Vijfhonderd consumenten worden in interviews voor de zogeheten nulmeting met liefst 55 vragen bestookt. De nulmeting onder de detaillisten wordt door het EIM zelf verzorgd. Op de volgende belangrijke vragen worden uitkomsten verwacht:

- de aard van de winkel,
- de omzet van deze winkel,
- de frequentie van de bestedingen naar klassen van aankoopbedragen (de Stuurgroep wil weten of de chipcard ook een gebruikskans heeft voor kleinere en zelfs de kleinste bedragen die onder de huidige omstandigheden en in alle landen cash worden voldaan),
- de verdeling van de verschillende betaalinstrumenten,
- de door de detaillisten ingeschatte voor- en nadelen van het elektronisch betalen.

Een vraag die eveneens in het onderzoek naar voren komt: de kosten- en besparingsgevolgen van de toepassing van de chipcard.

De tussenbalans.

Van de totale omzet in Woerden werd 7% met de chipcard betaald. Het marktaandeel van de contante betalingen is sinds de start van de proef met 4% gedaald, evenals het marktaandeel van de cheques. Het bleek dat 93% van de gebruikers de chipcard gemakkelijker vindt dan andere betaaltvormen en dat meer dan 60% van deze groep consumenten voor voortzetting van de proef is. Van de winkeliers bleek ruim 60% tevreden.

Achtergronden van de chipcard proef:

- 200 winkels aangesloten;
- Schlumberger heeft een order gehad van 224 terminals;
- de deelnemingskosten voor de detaillist bedragen een symbolische contributie van f25,-;
- het OVD (Opleidingsinstituut voor de Distributie) zorgde voor de opleidingen van detaillisten en personeel;
- er werden 5 uitleesterminals geïnstalleerd;
- op twee van deze uitleesterminals kan een print-out gemaakt worden;
- in een kaart kunnen maximaal 500 transacties worden vastgelegd;
- onderhoud en reparaties worden verzorgd door ESCON (een technisch servicebedrijf).

Feitelijke gegevens van de chipcard proef:

- op 28 augustus 1990 waren op 170 winkellokaties 209 terminals geïnstalleerd;
- daarnaast waren 15 terminals in voorraad voor uitbreiding;
- in juli 1990 waren er bij bankcliënten 7.595 chipcards uitgezet. Dit is 47% van de 16.245 oorspronkelijke benaderde rekeninghouders;

-in de maanden mei t/m augustus 1990 vonden gemiddeld in totaal 7500 transacties per week plaats. Dit is gemiddeld 36 transacties per terminal en 44 transacties per lokatie per week. De frequentie-verdeling om deze gemiddelden ziet zeer scheef. Gemeten in één recente maand ziet dit er als volgt uit:

- minder dan 24 transacties per week: 56% van de terminals;
- meer dan 24, doch minder dan 48 transacties per week: 20% van de terminals;
- meer dan 48, doch minder dan 96 transacties per week: 14% van de terminals;
- meer dan 96, doch minder dan 192 transacties per week: 8% van de terminals;
- meer dan 192 transacties per week: 2% van de terminals.

De gemiddelde waarde van de transacties bedraagt ca. f50,-; -percentage on-line transacties bedraagt in de praktijk ca. 6%;

- tijdens sluitingstijd van de winkel worden de terminals door het centrale verwerkingssysteem van Datatraffic via de telefoonverbinding benaderd. Voor de tijdige verwerking van de transacties in de rekeningen-courant van de betrokken cliënten, zowel debet als credit, is een hoog slaagpercentage van het uitlezen noodzakelijk. In de maanden t/m augustus bedroeg dit percentage 98,3;
- het aantal behandelde technische storingen die tot interventie van de onderhoudsdienst nopen, ligt de laatste maanden op 10 à 15 per week;
- het aantal contacten met chipcardhouders bedraagt rond 60 per week, waarbij aan de orde zijn: algemene informatie, melding van verloren passen, gebruik van de uitleesterminals voor raadpleging van transacties, bestedingsruimte en wijziging van de PIN, klachten over de afrekening, deblokken kaarten na 3xfoute PIN, wijziging bestedingsruimte, inleveren van kapotte chipcards, etc;
- het aantal niet-gebruikte chipcards bedraagt maandelijks circa 50%;
- geschat is dat 25 à 30% geheel niet deelneemt aan het systeem;
- voor diegene die de kaart wel gebruiken werden in de maanden maart t/m juli gemiddeld 8,5 transacties per kaart genoteerd;
- er zijn grote verschillen bij de houders:
 - ca. de helft hanteert de kaart minder dan 5 maal per maand,
 - ruim een kwart 6 tot 10 maal per maand,
 - en een kwart meer dan 10 maal per maand,
 - en er zijn absolute toppers met meer dan 60 transacties per maand;

-Tabel Chipcard-bestedingen naar branche:

	Aandeel transacties	Aandeel geldomzet	Terminal produktivi- teit *
Dagelijkse artikelen (food, drogisterij, e.d.)	ca. 58%	ca. 49%	274
Textiel en schoeisel	9	15	70
Elektro en woning	3	6	22
Overige detailhandel	26	26	152
Ambachten en diensten	3	3,5	83
Gemeente (1 terminal)	nihil	nihil	nihil

* Het aantal terminals is niet gelijk over de verschillende branches verdeeld. De terminalproduktiviteit is het aantal transacties per terminal per maand (cijfers juni 1990).

Duur responsietijden:

In de eerste aanleg werd een zeer korte responsietijd bij off-line transactie-afhandeling niet gerealiseerd. Gemeten werden off-line tijden van 45 seconden en on-line tijden van zelfs 65 seconden. Deze tijden staken ongunstig af bij het tijdsbeslag van de on-line magneetstriptoepassing (circa 35 seconden) en bij de gemiddelde tijd die contante betaling vergt (30 à 35 seconden). Na enige wijzigingen door Schlumberger waarbij iets werd gedaan aan hard- en software aanpassingen en enige procedurewijzigingen bleek de responsietijd minder dan 30 seconden te bedragen.

Kaartuitval:

Een uitvalspercentage van circa 5 procent gaf aanleiding alle in voorraad zijnde kaarten aan een aparte kwaliteitstest te onderwerpen. Daarbij zijn "de zwakke broeders" uit het bestand verwijderd. Verwacht werd dat de in gebruik zijnde kaarten die problemen hadden met onstabiele chips en/of zwakke verbindingen, zichzelf "uitspuwden" en werden vervangen door goede exemplaren.

Oordeel detaillisten:

Het oordeel van de detaillisten is van de start af aan gemiddeld positief gebleven. De gemiddelde waarde van de chipcard-transacties steekt echter gunstig af ten opzichte van het gemiddeld bestedingsbedrag voor alle aankopen: ca. f50,- t.o.v. f23,30. Naar geldswaarde vormen de chipcard-betalingen derhalve ruim 8% van de totale geldomzet. Bij de grootwinkelbedrijven met veel klanten en grote kassadruk komen relatief hoge chipcard-omzetten voor en is het elektronisch betalen een uitdrukkelijk gewenste ontwikkeling, die voor de dienstverlening aan de winkelende klant hoogst belangrijk is.

Consumenten:

De tegenvallende chipcard-omzet wordt geweten aan de terughoudendheid van de consumenten en aan de te geringe promotionele actie van de projectorganisatie naar de gebruikers. Bij de projectleiding leeft echter twijfel of de verlangde gedragsverandering, d.w.z. substitutie van betaling met gegarandeerde betaalmiddelen en contant geld, met publicitair geweld kan worden afgedwongen. Moet niet eerder gerekend worden op geleidelijke penetratie van de chipcard-betalingen door een van lieverlee groeiend besef, dat deze betaalwijze gemakkelijk, veilig en door de detaillisten gewenst is? Al meer dan 20 jaar hebben miljoenen Nederlandse bankcliënten gegarandeerde cheques en girobetaalkaarten op zak; in Woerden vindt voor "slechts" 11,4% van de betalingen in de detailhandel een cheque of girobetaalkaart zijn weg over de toonbank. Dan is 4% in driekwart jaar voor de chipcard nog zo slecht niet. In de nulmeting is reeds gebleken dat de aanval op de gevestigde oordelen van de niet-aanvragers van chipcards weinig kansen zou maken. 61% van deze respondenten vond de huidige betaalmiddelen toereikend en had grote voorkeur voor contante geldbetalingen. Als aanvulling op de bestaande middelen zagen zij de chipcard niet zitten. 73% van de "weigeraars" verklaarde destijds zeker niet in de twee proefjaren overstag te zullen gaan, 24% antwoordde: "wellicht ja". Het matig gemiddelde gebruik heeft ook te maken met de personen en met de gezinssituatie van de chipcard-houders. Tweederde van de huishoudens heeft meer dan één chipcard in bezit, mogelijk mede daardoor gebruikt één vijfde de kaart af en toe en een kwart vermoedelijk geheel niet. Daarnaast werkten technische storingen in het begin van de proef nog wat door en gaven ook de te lange responsietijden aanleiding tot terughoudendheid bij consumenten. Tenslotte blijkt ook de attitude van het winkelpersoneel van belang; als bij de cassières onwennigheid, onzekerheid of vrees voor verwarring bij storing ontstaat, dan wordt al gauw naar andere betaalmedia verwezen. Niettemin blijkt bij de tussenmeting van mei/juni dat de meerderheid van de chipcard-gebruikers hun vertrouwen in de nieuwe kaart hebben behouden. En zelfs als er voor betaald moet worden - 'niet te veel: f25,- is het maximum' - blijven deze consumenten aanhangers van het elektronisch betalen. De meeste chipcard-houders maken blijkens de tussenmeting geen gebruik van de uitleesterminals.

Slotbeschouwing chipcard projekt in Woerden:

De deelnemers in de projectorganisatie en met name de detailhandelsvertegenwoordigers en de banken zijn het nog niet over de vraag eens: wat moet er met het systeem gebeuren? en vooral ook: wat moet er met het elektronisch betalen in Woerden gebeuren? Gebleken is dat een voldoende aantal consumenten positief staat tegenover het elektronisch afrekenen en zullen vragen in Woerden daarmee te kunnen doorgaan. Of dat met de chipcard-technologie dient te geschieden, hangt voor de detaillisten af van het uiteindelijk aantal klanten dat daarvan gebruik zal willen maken en van de systeemkwaliteiten (snelheid, betrouwbaarheid, veiligheid en kosten).

Voor de consumenten zal het afhangen van beschikbaarheid, veiligheid en niet te hoge kosten. De technologie is hierin geen relevante grootheid, behalve wanneer nieuwe functies kunnen worden ingezet, die niet met de magneetstriptechnologie te realiseren zijn. Die nieuwe functies ontbreken echter in het Woerdense systeem. Het is niet ondenkbaar dat de Stuurgroep al of niet onder de bestaande projectorganisatie zal overwegen de proef te continueren met één of enkele nieuwe functies. Deze beslissing is echter eerst te nemen na uitvoering van een grondige analyse van de mogelijkheden, na een feasibility-beoordeling van deze functies door de detailhandelsorganisaties en de banken, en na gebleken bereidheid een dergelijke nieuwe ontwikkeling te financieren. De Woerdense proef moet niet worden beoordeeld in termen van succes of mislukking in de gebruikelijke betekenis van het woord. Het doel is inzicht te krijgen. Dat inzicht zal in ruime mate worden verworven. De actieve deelnemers aan beide zijden van de winkeltoonbank in de "Kaasstad" geven blijk van een positieve appreciatie van het elektronisch betalen met de chip-card.

10.3 Projekt in Denemarken.

Volgens een brief van AES uit Australië, heeft Denemarken besloten om op nationale basis een smartcard te introduceren voor het betalen van kleine uitgaven. Het nationale plan heeft betrekking op het publieke transport, parkeren, automaten en andere faciliteiten die op klein geld draaien. De kaart wordt het persoonlijk eigendom van de houder, zoals de credit kaart, de houder is in staat om de kaart te laden met een bepaald bedrag en hiermee zijn betalingen in bovenstaande apparaten te verrichten. De firma AES gaat dit systeem leveren, omdat ze zeggen de enige firma te zijn die een vervoerssysteem levert op basis van een smartcard. De twee grootste openbaarvervoers ondernemingen, Värmlandstrafik AB (VTAB) en Karlstad Lokaltrafik (KLAB), bezitten gezamenlijk zo'n 250 bussen. AES heeft na een proefperiode een contract gekregen van \$2 miljoen, voor het leveren van een op smartcard gebaseerd ticket systeem. Zo'n 25.000 passagiers gaan gebruik maken van dit systeem voor hun dagelijkse reisbehoeften. Het totaal gereisde bedrag wordt maandelijks van de rekening afgeschreven. Voor deze mogelijkheid heeft AES, bank debit database software.

11 Adressenlijst van geïnformeerde bedrijven.

Doormiddel van symbolen achter de naam van het bedrijf, of achter de naam van een persoon, wordt de vorm van contact duidelijk gemaakt.

Philips Nederland B.V. [#,*,@]
Communicatie- en Informatiesystemen.

Maanweg 156
Postbus 16830
2500 BV Den Haag
t.n.v. Ing. L. Snel
Senior Consultant
Tel(zaak): 070 - 3483071
 070 - 3482643
Tel(privé): 070 - 3203886
Telefax : 070 - 3482828
Telex 32245 ptis nl

Siemens [#]
Den Haag
t.n.v. de heer Nieuwenhuis
Tel: 070 - 3332383

Etrometa [#,*,@,
Meet- en Registratietechniek.
Kerkewal 49
Postbus 132
8400 AC Gorredijk
t.n.v. Ir. G. de Boer
Technisch Manager
Tel: 05133 - 3435
Telefax: 05133 - 3112

N.V. Nederlandsche Apparatenfabriek "Nedap" [#,*,@]
Oude Winterswijkseweg 7
Postbus 6
7140 AA Groenlo
t.n.v. de heer C. Kluit
Tel: 05440 - 71111
Telefax: 05440 - 62745

TNO [#]
Den Haag
t.n.v. de heer Meulemans
Tel: 070 - 3264221

DigiCash b.v. [#,*,@]
Kruislaan 411
1098 SJ Amsterdam
t.n.v. de heer David Chaum
Tel: 020 - 5922242
Tel(CWI): 020 - 5924169

BULL Nederland n.v. [#,*,@]
 Hoogoorddreef 66-68
 Postbus 22859
 1101 BE Amsterdam Zuidoost
 t.n.v. de heer C. Aalbrecht
 Consultant new projekts
 Tel(Algemeen): 020 - 5652111
 Tel(direkt): 020 - 5652419
 Tel(privé): 03403 - 79780
 Telefax: 020 - 5652950

B.V. Technisch Adviesbureau Annokkee [#,*,@]
 Veersedijk 97
 3341 LL Hendrik Ido Ambacht
 Postbus 280
 3340 AG Hendrik Ido Ambacht
 t.n.v. de heer P.E. Annokkee
 Directeur
 Tel: 01858 - 16100
 Telefax: 01858 - 16167

Ministerie van Economische Zaken [#,*,@]
 Bezuidenhoutseweg 30
 Postbus 20101
 2500 EC 's-Gravenhage
 t.n.v. mevrouw A.P. van der Geest
 Tel(algemeen): 070 - 3798911
 Tel(direkt): 070 - 3798820
 Telex 31099 ecza nl
 Telefax: 070 - 3474081

Intercai Utrecht b.v. [#,*,@,@]
 Einsteindreef 123-125
 Postbus 9256
 3506 GG Utrecht
 t.n.v. de heer Heidkamp [#]
 Tel: 030 - 631780
 t.n.v. de heer J.N.L. Akkermans [#,*,@]
 Hoofd beleidsadvisering
 t.n.v. de heer J. Ijtsma [#,*,@]
 Senior security adviseur

Nederlands Normalisatie-instituut [#,*,@]
 Postbus 5059
 2600 GB Delft
 t.n.v. mevrouw Zetzema
 Tel(algemeen): 015 - 690390
 Tel(direkt): 015 - 690256
 Telefax: 015 - 690190
 Telex 38144 nni nl

International Association for Microcircuit Cards "Intamic"
Mercury House, Triton Court [*,@]
14 Finsbury Square
London EC2A 1BR Engeland
t.n.v. de heer J. Tunstall
General Secretary
Tel: 071 711 6200
Facsimile 071 256 5527

SMART CARD -A Technology Impact Report [!]
T002
Februari 1989
Frost & Sullivan, Inc.
106 Fulton Street
New York, New York 10038
(212) 233-1080
FAX: (212) 619-0831

SMART CARDS Moet de school zeker hebben. [!]
principles, practice, applications.
Roy Bright.
Ellis Horwood Edition ISBN 0-7458-0374-1
Halsted Press Edition ISBN 0-470-21159-8

SPOM JAPAN CO.,LTD. [ø-AES,@]
26-8 Nando-cho
Shinjuku-ku
Tokyo 162
Telefoon: 81-3-266-2132
Telefax : 81-3-266-2239

AES (Associated Electronic Services LTD) [#,@]
249 Balcatta Road
Balcatta
West Australië
Australië 6021
P.O. BOX 234
Tuart Hill W.A.
Australië 6060
Telefoon: 344-3255
Fax : 344-3448950
Telex : AA92686
t.n.v. de heer K Gibson
Director Marketing

KPMG Klynveld Management Consultants [#,*,@]
Euclidislaan 1
3584 BL Utrecht
t.n.v. de heer J.A.M. van Schaik
Telefoon: 030-525211
Telefax : 030-525200

GEMPLUS Card International [*,@]
Z.E. de la Plaine de Jouques
B.P. 100
13881 Gemenos Cedex Frankrijk
t.n.v. de heer E Meniere
Export Manager
Telefoon: 33-42325124
Fax : 33-42325029

Chipcard projekt in Woerden [#,@,@]
Jan de Bakkerstraat 10
3441 EE Woerden
t.n.v. de heer H. Rudelsheim
Algemeen projektleider
Telefoon: 03480-23144

Royal Netherlands Embassy [*,@]
3-6-3 Shibakoen
Minato-ku
Tokyo 105 Japan
t.n.v. de heer P.J. Schalkwijk
Technisch Wetenschappelijk Attaché
Telefoon: 03-5401-0425
Fax : 03-5401-0429

U.S. & Foreign Commercial Service [#,@]
(Amerikaanse ambassade)
Lange voorhout 102
2514 EJ Den Haag
t.n.v. de heer M. Armitage
Telefoon: 070-3109209
Fax : 070-3632985

CCS Credit Card Software Inc. [ø-Amerikaanse ambassade,*]
900 Winderley Place
Suite 200
Maitland, Florida 32751
Telefoon: 407-660-0343
Fax : 407-875-8367

NMB Postbank [#]
t.n.v. de heer Vught
telefoon: 020-563902
t.n.v. de heer Goudriaan
(expert op het gebied van beveiliging)
telefoon: 020-5639111
020-5636331

ABN [#]
t.n.v. de heer v. Daalen
telefoon: 020-6289393

Akzo Systems [#,*]
Postbus 450
6710 BL Ede (Gld.)
t.n.v. de heer v. Grootel
telefoon: 08380-74444

Texas Instruments [#]
Amsterdam zuid-oost
telefoon: 020-5602911
(doen alleen transponders)

PTT [#]
Den Haag
t.n.v. de heer J. Frankhuizen
(richt smartcard commissie op binnen PTT)
Telefoon: 070-3432311
t.n.v. de heer H.J.W.M. van de Pavert
(expert op het gebied van ATF4)
Telefoon: 070-3325811

IBM [#]
Amsterdam
Telefoon: 020-5133111
IBM informatienummer: 06-0343

Postbank [#]
Leeuwarden
Telefoon: 058-449111

VISA [#]
Amsterdam
Telefoon: 020-5205911

VISA-International [#]
P.O. Box 253 London
w8 5TE Engeland
t.n.v. de heer R. Cullen
telefoon: 09-44-71-9378111
direkte lijn: 09-44-71-7955403

RATP (franse metro) [#]
Parijs
Telefoon: 140464141

Claudia Sträter [#]
(willen niets zeggen)
Stammerhove 1
1112 VA Diemen
t.n.v. de heer Boxel
Telefoon: 020-6954041

Ahold [#]

(zeggen niets met smartcard te doen, maar krijgen er wel subsidie voor?)

Postbus 33

1500 EA Zaandam

t.n.v. de heer J. Burggraaf

Telefoon: 075-599111 (alleen s'maandags)

Betekenis van de symbolen achter de bedrijfsnaam:

*	= schriftelijk contact,
#	= telefonisch contact,
@	= persoonlijke ontmoeting,
⊙	= informatie van toegestuurt gekregen,
⊙-...	= via informatie van gehad,
!	= ingezien.

opm. De symbolen mogen ook naast elkaar voor komen.

12 Conclusie.

De toekomst van de smart card is nog onzeker omdat andere technologieën nog in onderzoek zijn. Bij dit soort technologieën denk ik dan aan: optical card, stem herkenning, iriscope, gedigitaliseerde handtekening en beeldherkenning. Het is duidelijk dat bovengenoemde toekomstige technologieën op den duur de smart card kunnen inhalen als deze laatste te duur blijkt te zijn, of als de introductie stuit op tal van organisatorische invoeringsproblemen. Het blijkt dat de meeste fabrikanten hun experimenten met de smart card tijdelijk hebben stop gezet omdat na vooronderzoek bleek dat een groot projekt niet of nauwelijks resultaat op zou leveren. De hoofdvraag blijft telkens of de smart card technologie het gaat winnen van de toekomstige technologieën. Er zijn wat dat betreft twee extreme situaties mogelijk:

- 1) Deze situatie treedt op als smartcards zeer grote winst qua mogelijkheden en kosten-baten bieden t.o.v. de bestaande technologieën en moeiteloos kunnen worden ingevoerd binnen bestaande organisaties. Dit houdt dan wel in dat de voortgang van toekomstige technologieën stagneren of blijven de kosten ervan veel te hoog. De penetratiegraad van de smartcard zal dan hoog zijn totdat er vervangingsinvesteringen voor verouderde technologie aan de orde zijn.
- 2) Dit extreem treedt op als smart cards weinig of onvoldoende functionele meerwaarde kunnen bieden ten opzichte van bestaande technologie, kostbaar blijven en snel worden ingehaald door nog meer biedende technologieën. Deze situatie kan ook optreden als de introductie op tal van organisatorische invoeringsproblemen stuit. In dit stadium is het zelfs denkbaar dat de technologie bij gebrek aan een "kritische omvang" zal worden overgeslagen.

In de huidige situatie heeft de smart card enige voorsprong op de toekomstige technologieën, maar heeft nog geen penetratiegraad die boven de "kritische omvang" uitkomt. In bepaalde gevallen blijkt de smart card zowel qua beveiliging als qua mogelijkheden een meerwaarde te bieden. Maar het blijft belangrijk om telkens weer de zelfde vragen te stellen:

- a) Welke vernieuwing en verbetering is in het geding door toepassing van de smart card?
- b) In welke bedrijfstakken zijn de voordelen het grootst, zodat deze het meest belang hebben bij een snel introduceren van de smart card?
- c) Zal een keuze voor de smart card de (internationale)(concurrentie)positie van partijen kunnen wijzigen?
- d) Hoe zijn Nederlandse partijen, qua kennis, innovatie bereidheid en organisatorische kracht en souplesse voorbereid op deze smart card?
- e) Wat is de positie van Nederlandse partijen aan de aanbod zijde van de smart card? En welke rol spelen Nederlandse onderzoeksinstellingen bij de verdere ontwikkelingen, c.q. zouden die moeten spelen?
- f) Welke gebruikers reactie en maatschappelijke acceptatie is te verwachten?

g] In welke mate kan de smart card bijdragen aan de noodzaak privacy te waarborgen in een informatiemaatschappij?

Op het moment van dit schrijven blijken er al weer heel wat projekten in voorbereiding te zijn. Zo blijkt de PTT een speciale groep opgericht te hebben, die zich moet bezighouden met de smartcard in de telefonie. Zo blijkt er een city card projekt er uiteindelijk toch te komen. De overheid schijnt ook aardig achter deze plannen te staan gezien de subsidiepot die het komende jaar zo rond de 11 miljoen gulden gaat bedragen.