

Stichting Maatschappij, Veiligheid en Politie

De chipkaart: een publieke zaak

Veiligheidsaspecten van de chipkaart

Standpunt van de Stichting Maatschappij, Veiligheid en Politie
en samenvatting van het rapport

Dordrecht, september 1998

Chipkaart en onveiligheid: standpunt van de SMVP

Enkele jaren geleden bracht de Stichting Maatschappij, Veiligheid en Politie een rapport uit met als titel 'Toekomst gezocht'. Het rapport bevatte een analyse van de ontwikkelingen waarmee de politie de daaraan voorafgaande jaren was geconfronteerd en formuleerde aanbevelingen voor de toekomst. Uiteraard heeft de stichting ook zelf de uitvoering van een aantal van die aanbevelingen ter hand genomen. Eén van de aanbevelingen benadrukte het belang van meer toekomstgericht werken: probeer in te schatten welke ontwikkelingen te verwachten zijn en anticipeer daarop met beleidsmaatregelen, zodat mogelijk negatieve gevolgen zoveel mogelijk worden voorkomen. Dit was een aanbeveling waar de divisie Centrale Recherche Informatie van het Korps landelijke politiediensten op aansloeg. In het kader van het 75-jarige bestaan van de Fraudecentrale van de CRI werd een congres georganiseerd over de chipkaart. Eén van de thema's die op het congres ter sprake kwam was de toekomstige ontwikkeling van de chipkaart. De SMVP beloofde toen op dit terrein een project te zullen starten. Dit rapport is de inlossing van die belofte. Een breed samengestelde projectgroep heeft de achterliggende periode de problemen rond de ontwikkelingen van de chipkaart in beeld gebracht en een aantal aanbevelingen geformuleerd. Het bestuur van de Stichting Maatschappij, Veiligheid en Politie spreekt haar dank uit jegens de projectgroep voor het diepgaande rapport dat zij heeft vervaardigd. Een bijzonder woord van dank voor de secretaris, de heer drs. A. Kuijvenhoven, als commissaris van politie verbonden aan de regiopolitie Rotterdam-Rijnmond voor het vele werk dat hij heeft verzet om dit rapport te realiseren.

Hierna is een samenvatting van het rapport weergegeven, met daarin uiteraard ook de belangrijkste aanbevelingen. De aanbevelingen zijn onderwerp van gesprek geweest binnen het bestuur van de SMVP. Het bestuur van de stichting meent dat, gelet op de rol van de stichting op het raakvlak van overheid en samenleving, een aantal aanbevelingen meer in het bijzonder moet worden benadrukt. Het bestuur heeft deze aanbevelingen geformuleerd als een standpunt van de stichting en publiceert dit standpunt hier tegelijk met en voorafgaand aan het rapport.

De projectgroep gaat ervan uit dat het gebruik van de chipkaart, nu en in de toekomst, zal leiden tot criminaliteit, maar dat het niet te verwachten is dat deze criminaliteit enorm zal groeien. De huidige vormen van misbruik van de chipkaart geven daartoe geen aanleiding en de ontwikkelingen rond de beveiliging gaan zo snel dat het niet waarschijnlijk is dat het misbruik explosief zal groeien. Wel is een waarschuwing op zijn plaats voor een drietal nieuwe risicotypen. In de eerste plaats zal er naar verwachting sprake zijn van nieuwe vormen van misbruik. Technologische ontwikkelingen oefenen een onweerstaanbare aantrekkingskracht uit op sommigen om de mogelijke zwakke punten daarin op te sporen, ook zonder de behoefte aan persoonlijk voordeel. Zo gaat het bij veel hackers alleen om de kick. In de tweede plaats zal het bij de chipkaart in de toekomst steeds minder uitsluitend gaan om het financiële aspect. Kenmerkend voor de chipkaart is dat malversaties ook spelen op bijvoorbeeld het terrein van de manipulatie van (persoons)gegevens. Dat laat zich onder meer denken bij medische gegevens en bij examenresultaten. In de derde plaats waarschuwt de projectgroep ervoor dat, ook als de criminaliteit niet enorm zal groeien, het afbreukrisico desondanks erg groot kan zijn. Immers, als mensen hun vertrouwen in chipkaarten verliezen, zal hun bereidheid om ze te gebruiken dalen. Het zal niet de eerste keer zijn dat een chipkaartproject om die reden moet worden stopgezet. Terecht stelt de projectgroep daarom het maatschappelijk vertrouwen centraal. Het bestuur van de SMVP onderschrijft die keuze.

In het rapport wordt geconstateerd dat er inmiddels al een veelheid aan beveiligingsmaatregelen is genomen. Niet alleen in technische- en organisatorische zin; ook ten aanzien van het

gebruik. Terecht stelt het rapport dat maatregelen om misbruik van chipkaarten te voorkomen altijd ontoereikend zullen zijn: alles is te kraken. Dat is een verstandig uitgangspunt, zo heeft de recente geschiedenis geleerd. Steeds weer blijken avonturiers op lumineuze ideeën te komen waarmee beveiligingen worden doorbroken. Maar de vraag hoeveel misbruik er zal plaats vinden hangt sterk af van de moeite die kwaadwillenden zich bereid zijn zich te getroosten: kraken is niet altijd lonend. Het kraken van chipkaarten kan zo ingewikkeld zijn, zoveel deskundigheid vereisen en zoveel kosten met zich mee brengen, dat het rendement niet opweegt tegen de investeringen. Het is belangrijk maatregelen te nemen tegen misbruik; de dam die moet worden opgeworpen tegen misbruik moet hoog zijn. Desondanks zullen er altijd onverwachte ontwikkelingen mogelijk blijven. Het kritisch volgen daarvan is onontbeerlijk om te voorkomen dat nieuwe vormen van misbruik ons plotseling overvallen. Hoewel in het rapport de potentiële risico's van de chipkaart centraal staan, mag niet worden vergeten dat de invoering van kaartsystemen ook grote veiligheidsvoordelen kunnen hebben, bijvoorbeeld bij vormen van fraude die jegens de overheid worden gepleegd. Invoering van de burgerservicekaart zal naar verwachting dergelijke vormen van fraude aanzienlijk terugdringen.

Een verantwoorde ontwikkeling van de chipkaart, waarbij risico's en maatschappelijke voordelen in een redelijk evenwicht ten opzichte van elkaar staan, is van groot belang. Een te hoog niveau van beveiliging, zeker wanneer de gebruiker daarbij zelf een belangrijke rol speelt (pincodes, passwords), kan het gebruik in de praktijk ingewikkelder maken en daarmee veel gebruikers afschrikken. Een te laag niveau van beveiliging verhoogt het risico van misbruik en, als burgers te vaak worden geconfronteerd met negatieve gevolgen, tot schrikreacties en weigering de chipkaart te gebruiken. Keuzen inzake beveiliging zijn altijd dilemma's. Gelet op de verwachte ontwikkelingen rond de gebruiksmogelijkheden van de chipkaart is het van groot belang te zoeken naar een optimum tussen gebruiksgemak en veiligheid. De basis van alle maatregelen moet echter worden gevormd door maatschappelijk vertrouwen. Om dat te garanderen is een breed pakket aan maatregelen vereist. Dat vindt zijn neerslag in het grote aantal aanbevelingen in het rapport, achttien in totaal, die vooral zijn gericht op de vraag welke maatschappelijke discussies er moeten plaats vinden en welke stappen er moeten worden gezet om de groei van het chipkaartgebruik verantwoord te laten plaats vinden.

Het bestuur van de SMVP acht het verheugend dat er veel aandacht wordt besteed aan beveiligingsaspecten die samenhangen met het gebruik van de chipkaart. De oprichting van het Nationaal Chipkaartplatform enige jaren terug is in dat verband een belangrijk winstpunt. Wel meent de SMVP, in aansluiting op de mening van de projectgroep, dat de komende jaren een aantal nieuwe stappen moet worden gezet om de verdere groei te ondersteunen:

In de eerste plaats moet aandacht worden besteed aan de *positie van de gebruiker*. Naarmate de technologie op steeds meer terreinen als het ware over gebruikers wordt uitgestort, met steeds meer gevolgen voor het dagelijks leven en steeds meer risico's, wordt het des te belangrijker om aandacht te schenken aan de positie van die gebruiker, met name ook de waarborgen voor de privacy. De ontwikkelingen op het gebied van de chipkaarten worden vooral beïnvloed door de grote spelers op het terrein van het bedrijfsleven en door de overheid. Weliswaar wordt rekening gehouden met de gebruikers, maar dan toch vooral 'voor u, over u en zonder u'. De gebruiker moet er maar op vertrouwen dat het allemaal goed loopt. De SMVP schaart zich daarom volmondig achter de suggesties om de gebruiker de mogelijkheid en het recht te geven om de gegevens op de chipkaart te laten controleren door een onafhankelijk orgaan met een daaraan gekoppelde klachtenprocedure, om een onafhankelijke geschillenregeling vast te stellen en een vrijwaringsregeling te ontwerpen bij het einde van het gebruik van de chipkaart.

In de tweede plaats is vereist dat een aantal *organisatorische voorzieningen* wordt getroffen die de verdere ontwikkelingen kunnen ondersteunen. Onafhankelijk toezicht is een belangrijke voorwaarde voor een evenwichtige positie van alle betrokkenen. De SMVP meent dat de overheid moet nagaan of een aparte organisatie moet worden opgericht om dit toezicht uit te oefenen. Het rapport verwijst daarnaast terecht naar het belang van een informatiepunt, waar overheid en bedrijfsleven samen werken aan de oplossing van de grote hoeveelheid problemen, vaak praktisch - soms fundamenteel, en dat als vraagbaak kan dienen voor derden. Met organisatorische voorzieningen wordt niet alleen bedoeld op het oprichten van nieuwe organisaties; het gaat ook om nadere afspraken rond procedures, met name waar het de vaststelling van identiteitsgegevens betreft, de systematiek van beveiliging en het recht van de gebruiker van de kaart om de daarop vermelde gegevens te kunnen raadplegen en, onder voorwaarden, wijzigen. Dit zijn afspraken die zowel de overheid als de branche regarderen. Een adequate organisatie van de branche is noodzakelijk om alle belangen die een rol spelen evenwichtig te kunnen afwegen.

In de derde plaats is het van belang om een *maatschappelijke discussie* op een aantal terreinen te stimuleren. Er moeten nog tal van belangrijke keuzen worden gemaakt. Dat betreft onder andere de multifunctionaliteit van chipkaarten: hoeveel functies mag een chipkaart hebben en zijn alle functies verenigbaar op een kaart? Hoe wordt de privacy gereguleerd? Inzake beveiliging is het met name de vraag in hoeverre biometrie maatschappelijk acceptabel is en welke vormen van biometrie de voorkeur verdienen. Biometrie, in enigerlei vorm, zal naar verwachting onontkoombaar zijn. De vraag is vooral wanneer en hoe. Het is niet ondenkbaar dat, als deze discussie niet vanuit de overheid wordt vormgegeven, er vanuit de branche maatregelen zullen komen om die discussie te omzeilen, bijvoorbeeld door aantrekkelijke financiële arrangementen voor te stellen: 'u krijgt 10% korting op de chipkaart als van uw handpalm gebruik mag worden gemaakt'. De stichting acht het maatschappelijk belang van de discussie, waarbij met name aandacht is vereist voor de gevolgen op langere termijn, te groot om die aan de branche zelf over te laten.

Tenslotte, in de vierde plaats, zullen de technologische ontwikkelingen op het gebied van de chipkaart *consequenties hebben voor politie en justitie*, met name in de sfeer van de opsporing. Traditionele opsporingsmethoden, zoals het af luisteren van een telefoon, zullen in de toekomst minder gemakkelijk worden als gevolg van het gebruik van GSM-kaarten. Het rapport wijst daar terecht op. Politie en justitie moeten tijdig energie steken in de mogelijke consequenties die daarvan het gevolg zijn.

De SMVP hecht eraan dat bij alle ontwikkelingen rekening wordt gehouden met de verwachte voorschriften op Europees niveau. Op een terrein dat zoveel directe gevolgen heeft voor de burger moeten de beleidsontwikkelingen op Europees en op nationaal niveau op elkaar zijn afgestemd.

De stichting gaat ervan uit dat er ook in de komende jaren sprake zal zijn van misbruik van chipkaarten. En dat daarbij steeds nieuwe mogelijkheden zullen worden ontdekt om met de gegevens op chipkaarten te manipuleren. Maar duidelijk is dat heldere afspraken en een goed stelsel van voorzieningen ertoe zullen leiden dat de risico's sterk kunnen worden teruggedrongen.

Mr Pieter van Vollenhoven,
voorzitter Stichting Maatschappij, Veiligheid en Politie

Samenvatting

Een samenleving is gebaseerd op vertrouwen. Dat vertrouwen moet worden onderhouden. En dat onderhoud is een gezamenlijke verantwoordelijkheid voor alle maatschappelijke partijen. Technologische ontwikkelingen gaan snel, en dat maakt dat die verantwoordelijkheden soms moeilijk zijn waar te maken. Dat geldt ook de chipkaart. Die speelt een steeds grotere rol, en zal dat in de toekomst naar verwachting in nog sterkere mate gaan doen. De chipkaart bevat steeds meer informatie en kent steeds meer mogelijkheden.

De snelheid van de ontwikkelingen en de omvang ervan maakt veel mensen onzeker. Zij missen de oude vertrouwde persoonlijke contacten en kunnen moeilijk wennen aan de anonieme, door de techniek gedomineerde transacties die in steeds grotere delen van onze samenleving gewoon worden. Daar komt bij dat gebruiksrisico's (beroving, verlies, vergeten van pincode) bepaald niet denkbeeldig zijn. Dit leidt ertoe dat een aanzienlijk aantal mensen de technologie niet gebruikt, met name ouderen. Maar niet alleen zij. Recente ontwikkelingen laten zien dat burgers bij nieuwe toepassingen steeds weer tot een afweging komen van nut en risico en dat zij bij wijze van spreken per keer besluiten of het verstandig is om de chipkaart te gebruiken. De moeizame groei van chipper en chipknip laat zien dat de consument een machtige vinger in de pap heeft door simpelweg te weigeren te participeren. Bovendien, als er sprake is van teveel misbruik, zullen steeds meer mensen huiverig worden om over te gaan tot het gebruik van de chipkaart, en zal de maatschappelijke druk om andere informatiedragers te (blijven) hanteren groot zijn. Dat wordt versterkt door misbruik, zeker wanneer de schade van het misbruik aanzienlijk is.

Ontwikkelingen

Ondanks het feit dat niet elke nieuwe toepassing erin gaat als zoete koek, is het aantal toepassingen de laatste jaren sterk gegroeid, hoewel minder spectaculair dan enkele jaren geleden werd verwacht. Toch is een verdere groei te verwachten, bijvoorbeeld onder invloed van ontwikkelingen in andere landen, groeiende technische mogelijkheden, en niet in de laatste plaats de marktbelangen van betrokken bedrijven.

Belangrijke ontwikkelingen vinden plaats op het terrein van de elektronische portemonnee, de klantenkaarten van grote bedrijven, kaarten voor gebruik in het openbaar vervoer (die hier en daar zelfs de strippenkaart al vervangen), de zorgkaarten in de gezondheidszorg, studentenkaarten, asielzoekerskaarten en de burgerservicekaart. Met name dit laatste is een belangrijk initiatief omdat het hier om een echt identiteitsdocument gaat. Ook in de communicatie tussen gemeente en burger zal deze kaart een belangrijke rol spelen. Op het niveau van de Europese Unie houdt men zich bezig met de invoering van verschillende typen zorgkaarten, mede in verband met de daaraan gekoppelde privacy-problemen.

Veel vragen rond de toekomst van de chipkaart moeten nog worden beantwoord: hoeveel kaarten zal de gemiddelde persoon straks met zich dragen? Hoe multifunctioneel worden de kaarten? De chipkaart gaat naar verwachting een steeds belangrijker rol in onze samenleving spelen. Maar de potentiële gevaren die eraan zijn verbonden mogen niet worden onderschat. Als die gevaren niet adequaat worden beheerst, kan dat leiden tot het aan tasten van het maatschappelijk vertrouwen. Hoe voorkomt men (on)eigenlijk gebruik van de van de kaart? En hoe voorkomt men dat de persoonlijke gegevens ter beschikking komen van derden?

Bij veiligheid gaat het om een afweging tussen het gewenste, het mogelijke en het betaalbare: wat is veiligheid waard? Technische mogelijkheden veranderen, de behoeften aan veiligheid eveneens. Bovendien is sprake van grote individuele verschillen. Bij de beantwoording van die vragen spelen alle partijen, kaartuitgever, kaartacceptant en kaarthouder een rol. Er is een grote vrijheid van partijen, waarbij de kaartuitgever de belangrijkste rol speelt.

Soorten chipkaarten

Chipkaarten kunnen worden onderscheiden in drie verschillende typen. In de eerste plaats de *anonieme* kaart, zoals de telefoonkaart. Het is een document aan toonder, dat wil zeggen dat iedereen die over de kaart beschikt er ook feitelijk gebruik van kan maken. De andere typen kaarten zijn persoonsgebonden. Er zijn relatief lichte vormen van persoonsgebondenheid, waarbij de bezitter van de kaart niet echt wordt geïdentificeerd maar min of meer als partij wordt beschouwd. Men spreekt van *pseudonimiteit*. Voorbeelden hiervan zijn de pinpas, de GSM-kaart, de klantenkaart en diverse vormen van zorgpassen. De kaart is gekoppeld aan een persoon, maar wie de beschikking heeft over de kaart en een of meer gegevens (pincode, naam en adres) kan er gebruik van maken. Koppeling van de kaart aan de persoon is hier in feite een kwestie van vertrouwen. Er vindt immers geen echte identificatie plaats. In de derde plaats zijn er de *identiteitskaarten*, waarbij het voor de maatschappelijke rol van de kaart van groot belang is dat de identiteit van degene die de kaart gebruikt en degene aan wie de kaart oorspronkelijk is uitgereikt overeenstemmen. Voorbeelden van identiteitskaarten zijn op dit moment de asielzoekerskaart, burgerservicekaart en in de toekomst het rijbewijs en het paspoort. Identificatie bij het uitreiken van de kaart is bij dit laatste type kaart van groot belang. Wanneer een chipkaart wordt gebruikt als identiteitsdocument, als paspoort, als rijbewijs, maar ook als het bijvoorbeeld gaat om toegang tot beveiligde gebouwen, dan is het van groot belang te weten dat de kaarthouder is wie hij zegt te zijn.

Dat het onderscheid niet alleen een theoretische zaak is, blijkt uit ervaringen in Duitsland waar een chipkaart werd ingevoerd in het kader van de sociale verzekeringen, beveiligd met een pincode. Mensen gingen echter zoveel elkaars pin gebruiken dat het gehele chipkaartstelsel moest worden beëindigd. Er was gekozen voor pseudonimiteit terwijl het maatschappelijk gebruik identiteit vereiste.

Elk type kaart vereist aparte vormen van beveiliging. Bij de anonieme kaart staan technische beveiligingen centraal. Veel andere mogelijkheden zijn er niet. Er moet niet kunnen worden gemanipuleerd met de bedragen (het tegoed op de kaart moet met andere woorden niet illegaal kunnen worden verhoogd). Iemands identiteit blijft buiten beschouwing. De kaarthouder heeft grote vrijheid: hij kan de kaart overdragen. Maar misbruik is gemakkelijk: het ontvreemden van de kaart is voldoende. Omdat het in de praktijk om relatief kleine bedragen gaat, zijn er in het dagelijks gebruik niet al te veel problemen, zij het dat misbruik, bijvoorbeeld bij telefoonkaarten, nogal eens voorkomt.

In gevallen van pseudonimiteit is sprake van meer soorten beveiliging en vinden er meer controles plaats. Men kan onder meer denken aan de pincode. De kaartuitgever is soms verplicht de 'identiteit' te controleren (bankpas), maar gebruik van zo'n pas kan in principe plaats vinden zonder dat er een redelijke zekerheid is dat de gebruiker ook degene is van wie de rekening is. De beveiliging is het meest complex bij de identiteitskaarten. Persoonsverwisseling moet worden voorkomen. Identiteitskaarten zijn kaarten die door de overheid worden uitgegeven. Alleen de overheid kan de identiteit onderzoeken en vaststellen. In uitzonderlijke gevallen kunnen ook particulieren worden aangewezen. Wanneer het gaat om identificatie is grote zorgvuldigheid vereist. Dit stelt hoge eisen aan betrouwbaarheid en veiligheid. De identiteitsdocumenten fungeren vaak als bewijs voor identiteit en zijn daarom aantrekkelijk voor fraude. De overheid hoopt door middel van de invoering van chipkaarten (met name de burgerservicekaart) een belangrijk deel van de fraude die thans plaats vindt te verminderen.

Misbruik van chipkaarten

Het kan op veel manieren mislopen bij het gebruik van chipkaarten: toeval, nonchalance in het gebruik (bijvoorbeeld het uitlenen van pincodes en passwords), technische gebreken (bijvoor-

beeld door veroudering of een slechte kwaliteit materialen), maar ook bewust misbruik. Ook dat kan door nonchalance ontstaan (het uitlenen van kaarten of het zoekraken), maar ook door vervalsen, door het ontvreemden van pincodes of passwords, het kraken van beveiligingscodes. Door koppeling van bestanden en door de mogelijkheden om via één systeem toegang krijgen tot andere systemen (stapelning) worden de risico's van misbruik steeds groter. Daardoor kunnen mensen bijvoorbeeld met één enkele vervalsing op tal van terreinen onrechtmatig voordeel behalen. De openlijke discussies die op het Internet plaats vinden over het misbruik laten zien dat er een aanzienlijke groep belangstellenden is. Vaak niet eens zozeer uit gewin als wel, net als bij het hacken, om slimmer te zijn dan de beveiligingsmaatregelen.

De ervaring heeft geleerd dat alles is te kraken; het punt is alleen dat het lang niet altijd lonend is. Beveiligingsmaatregelen moeten een optimum nastreven, geen maximum. Daarbij is ook de maatschappelijke hanteerbaarheid van belang: zodra de kaart te ingewikkeld wordt in het gebruik haken veel mensen af. Alleen al het feit dat iemand verschillende pincodes moet onthouden (giromaatpas, chipper of chipknip, GSM, password voor de computer thuis en op het werk) maakt dat de bereidheid om al die beveiligingsmaatregelen serieus te nemen alleen maar kleiner wordt.

Bij misbruik gaat het voor een deel om reeds langer bestaande problemen, zoals de fraude met creditcards. De bedragen die daarmee zijn gemoeid zijn onbekend, maar dat het om grote bedragen gaat is zeker. De vraag of creditcards een rol zullen spelen bij witwassen wordt, na een uitgebreide studie, door het Europees Monetair Instituut ontkend: de registratie van transacties met elektronisch geld, die thans te allen tijde plaats vindt, biedt voldoende waarborgen tegen witwassen. Maar nieuwe technologieën leiden ook tot nieuwe vormen van misbruik, zoals het voorbeeld dat enkele maanden geleden in de pers stond: met een aantal in Duitsland geblokkeerde pinpassen werd geld gehaald uit geldautomaten in Nederland. De risico's worden onder meer groter, omdat de kaarten steeds meer mogelijkheden bieden. De oudere kaarttypen konden alleen worden gebruikt om te lezen, nieuwere kaarten bevatten intelligente chips waarop de informatie ook kan worden gewijzigd en de nieuwste ontwikkeling is die van de multiservice kaarten, die voor geheel verschillende doelen kunnen worden gebruikt: openbaar vervoer, financiële transacties, toegang tot gebouwen, het lenen van boeken en het vastleggen van studieresultaten, om maar eens enkele voorbeelden te noemen. Naarmate de mogelijkheden om met gegevens op kaarten te manipuleren moeilijker worden, zal de neiging kunnen ontstaan om, bijvoorbeeld door industriële spionage, de noodzakelijke gegevens te verkrijgen gedurende het productieproces.

Los van de potentiële gevaren voor criminaliteit, geldt als probleem dat de ontwikkelingen op het terrein van de telecommunicatie steeds mobieler en anoniemer worden en dat er steeds meer aanbieders op de markt komen. Dat heeft aanzienlijke gevolgen voor de opsporing van strafbare feiten. Niet alleen het afluisteren wordt technisch steeds moeilijker, dat geldt zelfs de vraag bij welke telecommunicatiemaatschappij men terecht moet. Het oprichten van een informatiepunt waarin alle betrokken overheidsdiensten en particuliere bedrijven samen werken aan de oplossing van deze problemen is van groot belang, al was het maar om de kosten van de benodigde investeringen enigszins te beperken. Daarnaast verdienen de juridische regelingen rond de bevoegdheden van politie en justitie op dit nieuwe terrein nog de nodige aandacht.

Maatschappelijk vertrouwen

Het behoud (of soms zelfs het verkrijgen) van maatschappelijk vertrouwen vereist steeds meer aandacht. Voorlichting is daarbij belangrijk, maar vooral beveiliging. De beveiliging omvat een breed scala van uiteenlopende maatregelen: in de eerste plaats is de kwaliteit van het materiaal van belang voor levensduur en bruikbaarheid in de praktijk. In de tweede plaats de

scheiding van de verschillende fasen van het productieproces, zodat wordt voorkomen dat medewerkers van productiebedrijven de kans krijgen om te malverseren als de kaart eenmaal in gebruik is. In de derde plaats, en dat is voor dit rapport het meest belangrijk, de beveiliging van het gebruik. Die beveiligingen zijn voor een belangrijk deel technisch van aard (het aanbrengen van fire-walls in computersystemen, het toepassen van cryptografie), en voor een ander deel hebben zij te maken met identificatie- en verificatieprocedures. Naarmate het aantal en het gebruik van kaarten toe zal nemen, is de verwachting gewettigd dat het gebruik van pincodes en passwords minder in de aandacht zal komen te staan; ook thans is het immers al gebruikelijk dat iemand de pincode ergens opschrijft, immers, 'je weet maar nooit...'

Beveiliging wordt aanmerkelijk verbeterd als gebruik wordt gemaakt van een systeem dat twee kenmerken vergelijkt. Dat is onder andere het geval bij biometrie, waarbij twee unieke persoonlijke kenmerken (*geen* persoonlijkheidskenmerken) met elkaar worden vergeleken. Op zichzelf is biometrie niet nieuw. De pasfoto en de handtekening zijn voorbeelden. Maar biometrie bestaat uit meer: fysieke kenmerken (vingerafdruk, handpalmvergelijking, iriscopie) en gedragskenmerken (de handtekening). De fysieke biometrie is over het algemeen te prefereren, omdat vervalsing minder gemakkelijk is. Bovendien moet een onderscheid worden gemaakt tussen anonieme en gepersonaliseerde biometrie. In het eerste geval wordt alleen gecontroleerd of de gegevens op de chipkaart overeenkomen met de gegevens van een persoon (wie hij dan ook is). In de gepersonaliseerde biometrie gaat het erom de gegevens te koppelen aan een bepaalde persoon. Biometrie is, hoe belangrijk ook, een in maatschappelijk opzicht overigens zeker geen onweersproken ontwikkeling. Velen krijgen het gevoel dat Big Brother zich wel erg dichtbij bevindt. Een maatschappelijke discussie over de toelaatbaarheid is van groot belang.

Er zijn diverse stappen gezet om de ontwikkeling van en rond de chipkaart zo goed mogelijk te begeleiden: de oprichting van het Nationaal Chipkaart Platform en de Richtlijnen van het Nederlands Normalisatie Instituut, zijn daar belangrijke voorbeelden van. Hoewel de overheid ook in de toekomst een belangrijke rol zal spelen bij maatregelen die een veilig gebruik van de chipkaart moeten garanderen. Het vermogen van de overheid om al deze maatschappelijke ontwikkelingen te beïnvloeden wordt relatief klein geacht.

Aan de overheid worden hoge eisen gesteld waar zij zelf gebruik gaat maken van de chipkaart. Gelet op de technische mogelijkheden en de (relatief en op lange termijn bezien) geringe hoeveelheid kosten, ligt het voor de hand de chipkaarttechnologie door de overheid een belangrijk instrument bij haar taakuitoefening wordt.

Aanbevelingen

Het rapport neemt vertrouwen als uitgangspunt voor haar redenering en de aanbevelingen. Dat vertrouwen eist primair een aantal organisatorische maatregelen, die betrekking hebben op de burger:

- mogelijkheid om gegevens op een chipkaart door een onafhankelijk orgaan te laten controleren;
- een onafhankelijke geschillenregeling;
- een vrijwaringsregeling bij het einde van het gebruik;
- een toegankelijke klachtenprocedure;
- de mogelijkheid van aangepaste regelingen voor bepaalde categorieën van de bevolking (bejaarden, invaliden).

Daarnaast is vereist dat allen die betrokken zijn bij de ontwikkeling en de uitgifte van chipkaarten (de branche) een aantal maatregelen neemt. Dit betreft met name de organisatie van

onafhankelijk toezicht op de ontwikkelingen. Ook dient de branche afspraken te maken over bepaalde procedures die worden gehanteerd, bijvoorbeeld inzake:

- de wijze waarop persoonsgebonden gegevens worden opgenomen; het ontwikkelen van een uniform stelsel van regels van identiteitsvaststelling, waarbij gemeenten een centrale rol dienen te spelen;
- de systematiek van beveiliging (verhouding tussen ‘technische’ en ‘menselijke’ beveiliging) en de te hanteren procedures;
- Hoe de verhouding moet zijn tussen de verantwoordelijkheden van de overheid en particulieren, wanneer deze laatsten als ‘poortwachters’ worden ingezet. Als particulieren worden ingeschakeld dient te worden gezorgd voor voldoende kennis en bevoegdheden.

Een verdere ontwikkeling van de chipkaart vereist op een aantal punten maatschappelijke discussie. Die discussie is van belang op het terrein van de biometrie (welke typen biometrie worden wanneer gebruikt, welke vormen van biometrie hebben de voorkeur: persoonsgebonden of niet persoonsgebonden, anonieme of tot op de persoon herleidbare);

De technologie vereist andere vormen van controle dan tot dusverre gebruikelijk waren. Algemeen uitgangspunt is dat het gewenst is de tijd te nemen voor de ontwikkelingen rond de chipkaart voor het nodige maatschappelijke vertrouwen. De dynamiek van de markt is groot. De kans is niet ondenkbeeldig dat er een ‘gevecht’ tussen de marktpartijen gaat ontstaan, waarvan de burger de dupe wordt. Het gaat daarbij niet alleen om geld, maar ook om de vereiste maatschappelijke zorgvuldigheid, zoals de bescherming van de persoonlijke levenssfeer en de betrouwbaarheid rond iemands identiteit. De individu moet opboksen tegen machtige partijen, of het nu om marktpartijen gaat of om de overheid. Veiligheidsvraagstukken moeten primair worden bezien vanuit de gebruiker. Het maatschappelijk vertrouwen komt tot uiting als individuen in volle vrijheid besluiten de chipkaart te gebruiken.

Ook de multi-functionaliteit dient onderwerp van nadere studie en discussie te zijn: hoeveel verschillende functies mogen er op een kaart? Is het verantwoord zorgpas, patiëntenkaart en medische beroepskaart te integreren? Daarbij moet in een vroegtijdig stadium rekening worden gehouden met Europese richtlijnen.

Tenslotte de opsporingsinstanties. Er lijkt op voorhand geen reden aan te nemen dat een verdere uitgroei van de chipkaart tot aanmerkelijke criminele gevolgen zal leiden. Uiteraard zullen die er wel zijn. Voorbeelden: fraude, valse telefoonkaarten. Wel lijkt met name de opsporing negatief te worden beïnvloed (denk aan vooruitbetaalde GSM-kaarten) die het afluisteren bemoeilijken.