Rathenau instituut

april 2007

Rathenau special

Naast internet, gsm en gps heeft de digitale ruimte er sinds kort een nieuwe dimensie bij: RFID, oftewel *Radio Frequency IDentification*. De kleine op afstand uitleesbare chips werden tot nu toe vooral toegepast in de logistiek om goederen te identificeren. Nu wordt RFID massaal ingevoerd in het publieke domein om mensen te herkennen: toegangspasjes voor kantoren, clubs en voetbalstadions, de ov-chipkaart, het biometrisch paspoort, volgsystemen in pretparken en lokale betalingssystemen. Gebruikers van deze 'slimme' omgevingen zien het gemak dat RFID biedt bij toegangverlening en transacties, terwijl de beheerders de mogelijkheden ontdekken van RFID voor aanvullende dienstverlening en controle van die omgeving. Wat is nieuw aan RFID ten opzichte van andere technologieën in de digitale publieke ruimte? Wie profiteert het meest van deze onzichtbare digitale revolutie?

RFID: meer keuze, gemak en controle in de digitale publieke ruimte

Het Rathenau Instituut heeft onderzoek verricht naar de praktijk van RFID en met experts gesproken over toekomstige ontwikkelingen. In deze Rathenau Special wordt allereerst een beeld geschetst van RFID in het leven van alledag: op welke plaatsen krijgen mensen vooral te maken met RFID, wat voor gegevens worden verzameld en wat betekent dat voor hen? Vervolgens wordt beschreven hoe RFID zich verder kan ontwikkelen in samenhang met andere technologieën. Daarbij wordt gekeken naar de onderlinge verhoudingen tussen gebruikers en beheerders/eigenaren van RFID-omgevingen en de rol die de overheid speelt, nu en in de nabije toekomst.

Gebruikers hebben momenteel veel vertrouwen in hun elektronische sleutel of portemonnee. Ze denken juridisch goed beschermd te zijn tegen misbruik en verwachten niet te worden gevolgd via hun digitale voetsporen. Dat kan in de nabije toekomst wel eens veranderen, zeker als RFID ook wordt ingezet voor opsporingsdoeleinden. Daarbij gaat het om meer dan alleen privacy. Bovenal gaat het om een juiste verhouding tussen keuzevrijheid, gebruiksgemak en controle.

RFID als groeimarkt

RFID werd al toegepast tijdens de Tweede Wereldoorlog om vliegtuigen te identificeren, maar pas in de laatste jaren kwamen de op afstand uitleesbare chips massaal op de markt. Volgens consultancybedrijf IDTechEx werden er in de voorgaande zestig jaar wereldwijd 2,5 miljard tags *verkocht, waarvan zeshonderd miljoen in 2005. In 2006 waren dat er naar verwachting al maar liefst 1,3 miljard. De voornaamste toepassingen: in vrachtverkeer en op smart cards. Van die laatste zijn de ov-chipkaart en het biometrisch paspoort recentelijk de meest spraakmakende voorbeelden.*

Hoe werkt RFID?

Een RFID-systeem bestaat uit vier elementen: RFID-chips, chiplezers, een netwerk en een database. Die elementen wisselen informatie uit. Als de chip dicht genoeg bij een chiplezer komt, geeft de chip zijn code af. De code gaat via het netwerk naar de database waar hij wordt geïdentificeerd, bijvoorbeeld als een bepaald product of persoon. Aanvullende informatie kan vervolgens worden teruggestuurd naar de plek waar de chip werd uitgelezen, waarna een reactie volgt, zoals het berekenen van een prijs of het openen van een deur. Die handelingen worden dan meestal weer geregistreerd, zodat het netwerk kan bijhouden waar en wanneer welke chip tot welke acties heeft geleid.

Betalen aan de pomp met Shell-Easypay RFID chip.

RFID is meer dan een barcode

RFID-chips kunnen veel meer informatie bevatten, sneller, in grote groepen en onzichtbaar worden uitgelezen en in sommige gevallen kan de informatie op de tag worden aangepast. Bovendien gaan ze veel langer mee.

Om soorten RFID-systemen te classificeren wordt over het algemeen onderscheid gemaakt tussen actieve en passieve RFID-chips, *read-only* en *rewriteable* chips en tussen open en gesloten systemen. Een **passieve chip** heeft geen eigen energiebron, maar gebruikt de energie die het signaal van de RFID-chiplezer opwekt in een spiraalvormige antenne op de chip (inductie). De afstand waarop de chip kan worden gelezen is dan ook niet heel groot: in theorie tot op enkele meters, maar in de praktijk slechts op enkele centimeters. Een **actieve chip** beschikt daarentegen over een batterij en kan daardoor zelf een signaal uitzenden. De leesafstand is dan veel groter, afhankelijk van de sterkte van de energiebron en de radiofrequentie. De meeste chips hebben een vaste code die kan worden uitgelezen, **read-only**, terwijl die code bij andere chips ook kan worden aangepast: **read-write**.

Sommige RFID-systemen zijn **gesloten systemen**. Dat betekent dat de code op de chip alleen betekenis heeft binnen de database van het systeem waarvoor de chip is gemaakt. Steeds meer systemen zijn echter **open systemen**. De communicatie tussen chip en chiplezer verloopt dan via standaarden in soorten codes en frequenties. Daardoor kunnen de achterliggende databases van verschillende omgevingen worden gekoppeld. Het bekendste voorbeeld van een open systeem is de Elektronische Productcode (EPC), de beoogde opvolger van de streepjescode.

"Wat maakt het uit. Met m'n gsm en op internet word ik toch ook overal gevolgd?"

RFID is net als internet en gsm een netwerktechnologie. Maar RFID heeft wel zo zijn eigen logica. RFID-systemen worden door uiteenlopende partijen beheerd en de meeste systemen communiceren niet met elkaar, terwijl via internet en gsm alle terminals in principe met elkaar zijn verbonden. Dat betekent dat het voor de verschillende eigenaren gemakkelijk is inzicht te krijgen in individueel gedrag, maar het lastiger is om met RFID een totaalbeeld te krijgen.

"Wat? Kan iedereen me zomaar ongemerkt overal volgen?"

Dat zou alleen kunnen als er overal chiplezers staan die verbonden zijn in één netwerk, zonder enige beveiliging. De kleine, passieve RFID-chips kunnen in de praktijk slechts op enkele centimeters afstand worden uitgelezen en dat is meestal merkbaar. Actieve RFID-chips kunnen grotere afstanden overbruggen, soms zelfs meer dan een kilometer, maar zijn door hun batterij duidelijk zichtbaar.

RFID in het dagelijks leven

RFID-polsband geeft toegang tot zwembad Het Marnix.

Een elektronische sleutel, portemonnee en meer ...

In de nog jonge geschiedenis van RFID in de publieke ruimte zijn slechts enkele incidenten voorgevallen die de kranten haalden. Zo was er publieke controverse rondom de Duitse winkelketen Metro Future Store die klanten zou volgen middels RFID-chips in boodschappen en winkelwagentjes. In feite ging het slechts om een proefopstelling die Metro nooit werkelijk heeft ingevoerd. Wel zijn supermarktketens massaal bezig hun kratten en vrachtauto's van RFID-chips te voorzien. Dit dient echter alleen logistieke doeleinden en is niet bedoeld om klanten te identificeren. Opvallend genoeg zijn het wel de chips in de boodschappen die de ambtelijke discussies over RFID domineren. Maar is RFID dan nergens anders te vinden in het dagelijks leven? Het Rathenau Instituut ging op zoek naar veelvoorkomende voorbeelden. De uitkomsten van deze casestudies worden hier gepresenteerd, samengebracht in een dag uit het leven van een fictief Nederlands gezin.

Ieder zijn eigen digitale identiteit

Hans en Joke wonen met hun kinderen Chris en Jessica en hond Max in Amsterdam. Het is vrijdagochtend en Joke brengt de kinderen naar school. Max gaat mee. Hij heeft een RFID-chip in zijn nek met een nummer dat de dierenarts vertelt wie Max is, wat zijn afstamming is en welke inentingen hij heeft gehad.

OV-chipkaart

Eigenlijk had het al zover moeten zijn: Nederland dat als eerste land ter wereld een RFID-chipkaart invoert waarmee in al het openbaar vervoer kan worden gereisd. Het bleek echter een te grote opgave. Voormalig minister van Verkeer en Waterstaat Karla Peijs verzette daarom de streefdatum naar 1 januari 2009. Momenteel is wel al begonnen met een grootscheepse publiciteitscampagne om reizigers voor te bereiden. Op verschillende plaatsen in Nederland is de ov-chipkaart bovendien in gebruik naast de bestaande betalingssystemen. In opdracht van het Rathenau Instituut vroeg onderzoeksbureau Media Test de gebruikers naar hun ervaringen. Uit het onderzoek blijkt dat de eerste reacties overwegend positief zijn. Reizigers noemen vooral het gebruiksgemak. Maar die positieve houding zou om kunnen slaan als blijkt dat er meer gebeurt met hun reisgegevens dan ze aanvankelijk dachten. Verschillende organisaties bestrijden bovendien dat de kaart reizigers echt zoveel voordelen biedt. >

Het brede publiek maakt kennis met RIFD middels de OV-chip kaart.

Hans zwaait zijn gezin uit bij de voordeur. Hij moet naar zijn werk. Maar eerst moet hij nog een vuilniszak in de ondergrondse vuilcontainer gooien. Hij haalt een pasje tevoorschijn dat hij van de gemeente heeft gekregen en haalt het langs een kaartlezer bij de klep. De klep opent zich en Hans werpt de vuilniszak naar binnen. Via de kaartlezer houdt de gemeente ook bij of de bak al vol is.

Vervolgens wandelt Hans naar de metro. Op het station haalt hij zijn ov-chipkaart tevoorschijn en haalt die langs de scanner bij het poortje. Het vervoersbedrijf leest de chip in de kaart, controleert of er genoeg geld op staat en registreert dat Hans om kwart over acht is ingestapt. “Reistegoed 16,04 euro. Goede reis!”, meldt het beeldscherm bij de scanner. Het poortje gaat open. Als Hans de metro weer verlaat op het Centraal Station, heeft hij bij de tourniquet opnieuw zijn kaart nodig. Het beeldscherm bedankt Hans nu hartelijk voor de reis. Het vervoersbedrijf registreert dat hij om vijf voor half negen is uitgestapt en haalt 1,60 euro van zijn reistegoed af. Het poortje opent zich. Hans neemt nu de trein naar Rijswijk. Zijn treinabonnement is tevens een ov-chipkaart. Hij kreeg hem zomaar thuisgestuurd van de Nederlandse Spoorwegen (NS), al werkt de kaart nog niet in de trein.

Hans werkt bij automatiseringsbedrijf Alcatel. Zijn werknemerspasje bevat een RFID-chip met een batterijtje en kan daardoor een signaal uitzenden dat sterk genoeg is om door kaartlezers in het plafond te worden opgevangen. Als Hans op kantoor arriveert, gaan de schuifdeuren automatisch voor hem open. Hij hoeft zijn pasje er niet eens voor uit zijn zak te halen. De portier krijgt tegelijkertijd op zijn beeldscherm een foto van Hans te zien. Hij ziet bij welke afdeling Hans

RFID polsband geeft in zwembad Het Marnix ook toegang tot kledingkluis.

OV-chipkaart

> Eén kaart voor al het openbaar vervoer in Nederland

De ov-chipkaart is een betaalsysteem dat straks overal in het openbaar vervoer kan worden gebruikt. Wie bus, metro of trein neemt, checkt in door zijn kaart (met daarop een bepaald reistegoed) bij een van de RFID-lezers te houden die staan aan de ingang van de perrons en bij de deuren in trams en bussen. Eenmaal op zijn bestemming, checkt de reiziger bij het verlaten van het vervoermiddel of het perron weer uit, waarna een bedrag wordt afgetrokken van zijn reistegoed. Deze transactie wordt centraal verwerkt door Translink Systems, speciaal voor dit doel opgericht door de vijf grootste vervoersbedrijven (GVB, HTM, RET, Connexxion en de NS). Er zijn drie soorten chipkaarten: een gepersonaliseerde, een anonieme en een wegwerpkaart. Tot nu toe gebruiken reizigers vooral de gepersonaliseerde kaart.

De kaarten bevatten een passieve RFID-chip. Dat betekent dat de energie die nodig is om informatie uit te wisselen tussen kaart en kaartlezer wordt gegenereerd door een signaal dat de lezer stuurt naar de antenne in de kaart. De chip heeft een vast nummer dat dient als sleutel tot de identiteit van de reiziger. Die identiteit ligt opgeslagen in de centrale database van Translink Systems. Plaats en tijd van instappen en het reistegoed worden daarnaast ook op de kaart zelf bijgehouden, op een herschrijfbaar deel van de chip. Zo kunnen conducteurs de kaart controleren met mobiele kaartlezers, zonder dat ze de centrale database hoeven te raadplegen. Bij de gepersonaliseerde kaart staat als extra controlemiddel ook de geboortedatum van de reiziger op de chip. >

Steeds meer voetbalstadions gaan over op een RFID clubkaart als toegangsysteem.

werkt en dat hij vandaag om 2 minuten over half tien is binnengekomen. Ook in de liften en op de verschillende verdiepingen zijn kaartlezers. Mocht er brand uitbreken, dan kan de brandweer in één oogopslag zien wie zich nog waar in het gebouw bevindt. De laptop van Hans heeft eveneens een actieve RFID-chip. Mocht iemand ermee vandoor gaan, dan zal de sensor bij de uitgang dit melden aan de portier.

In Amsterdam neemt Joke die middag de auto om enkele boodschappen te doen en om de kinderen uit school te halen. Onderweg tankt ze bij Shell en betaalt met haar Shell Easypay-pas. Shells database registreert dat Joke om kwart voor drie voor 25 euro heeft getankt aan de Amsteldijk. Om drie uur staat Joke voor de school. Jessica en Chris komen aangerend. “Mam, kun je me bij het zwembad afzetten? Ik wil nog even trainen”, vraagt Jessica. Geen probleem. Haar moeder stuurt fluks de auto naar sportcentrum Het Marnix aan de Marnixstraat. Daar aangekomen doet Jessica een polsbandje om en loopt naar de ingang. Ze houdt het polsbandje bij een scanner en de tourniquet gaat open. De achterliggende database heeft haar geïdentificeerd als betalende abonnee en stuurt een foto naar de receptionist die zo kan controleren of niet iemand anders met Jessica’s polsbandje gaat zwemmen. In de kleedkamers zijn de muntmechanismen van de kluisjes vervangen door RFID-sloten, die eveneens reageren op het polsbandje. Als Jessica is uitgezwommen, haalt ze haar kluisje weer leeg en gaat ze door de poortjes naar buiten. “Deze abonnementhouder is vandaag van kwart over drie tot tien voor half vijf in het zwembad geweest”, aldus de database van Het Marnix. Als abonnementhouder krijgt Jessica korting op de toegang tot het zwembad.

Hans gaat die avond naar Alkmaar, met collega’s naar een voetbalwedstrijd: AZ tegen Roda JC. Ze hebben geen papieren toegangskaartjes, maar elk een persoonlijke clubpas met RFID chip. Tijdens de rust zwaait vriend Ger genereus met zijn AZ-pas: “Ik haal wel bier.” Hij is namelijk jarig. De database registreert na twee rondjes: “Fan is dit jaar twaalf keer hier geweest en heeft vanavond tien bier gekocht.” Hans heeft nog wel eens de KNVB gebeld om te vragen of er niet één nationale kaart komt. “Da’s gemakkelijk bij uitwedstrijden en dan kun je ook veel beter de hooligans eruit houden”, zei hij nog. Maar volgens de voetbalbond zal die ene kaart er voorlopig niet komen. Elk stadion wil zo zijn eigen systeem.

Afdwalen en andere apenstreken

De volgende dag is zaterdag. Joke en Chris gaan naar dierentuin Apenheul, Hans en Jessica naar opa die in een zorgboerderij zit. Een paar jaar geleden werd bij opa de ziekte van Alzheimer geconstateerd. Eigenlijk moest hij naar een verzorgingstehuis, omdat hij door zijn ziekte nogal eens ging dwalen. Maar voor een man die het

RFID-chip in Apentas volgt bezoekers-stromen.

liefst in zijn moestuin werkte en in de buitenlucht was, was dat geen aantrekkelijk vooruitzicht. Zorgboerderij Erve Knippert in Haaksbergen bood uitkomst. Daar krijgen de ouderen die de dagopvang bezoeken een enkelbandje om met een actieve RFID-chip. Sensoren rondom het erf slaan alarm als een van de bejaarden te ver afdwaalt. Joke vond het aanvankelijk niets: "Die dingen gebruiken ze ook in die Big Brother-bajes in Lelystad. Opa is verdorie toch geen gevangene?!" Hans dacht er anders over: "Zo is hij vrij en veilig." En inderdaad, als ze bij Erve Knippert aankomen, is Hans' vader rustig aardbeien aan het plukken in de tuin.

Joke en Chris zijn inmiddels aangekomen bij de ingang van de Apenheul. Daar krijgt Joke een speciale apentas om de waardevolle spullen in te doen. Anders pakken de rondlopende apen ze. Chris rent meteen het park in en verdwijnt uit het zicht. Afgelopen zomer in Denemarken ging hij er bij een bezoek aan Legoland ook al zo vandoor. Maar toen had hij een polsbandje om met een RFID-chip en kon Hans het Kidspotter-systeem bellen om te zien waar Chris was gebleven. Nu niet. Maar wat Joke niet weet is dat deze keer zijzelf is 'getagd'. De 'aapvrije' tas bevat een actieve RFID-chip om de bezoekersstromen door het park te volgen. Het systeem is niet bedoeld om verdwaalde kinderen op te sporen – de tasdrager blijft anoniem – maar om de routes te optimaliseren. Terwijl Joke druk heen en weer loopt op zoek naar Chris, registreren de sensoren in het park dat iemand een wel zeer vreemde route volgt. En bij analyse van de gegevens zal de afdeling marketing zich ongetwijfeld afvragen of de bewegwijzering wel voor alle bezoekers duidelijk is.

Na twee uur door het park te hebben gehold, vinden Chris en Joke elkaar eindelijk terug. Chris ziet nu pas de apentas en vraagt of hij hem mag dragen. "Graag", zegt Joke. "Maar we moeten nu toch echt weer gaan hoor." Bij de uitgang loopt Chris alweer een aardig eind voorop. Als hij langs de receptie gaat, klinkt opeens een alarm. Een sensor meldt dat iemand er met een apentas vandoor probeert te gaan. Joke en Chris geven de tas terug en rijden naar huis.

Duistere escapades en schimmige transacties

Die avond gaat Joke stappen in Rotterdam. Met haar vrienden Freek en Anita gaat ze naar de Baja Beach Club. Ze vraagt Hans om zijn ov-chipkaart, want die heeft ze zelf nog niet. Ze neemt de metro naar het station en vervolgens de trein naar Rotterdam. Freek en Anita wachten haar op bij het station en samen gaan ze naar de nachtclub. Bij de ingang trekt Joke haar portemonnee om de entree te betalen. Dan zegt Freek: "Laat maar, let op." Hij wordt vriendelijk begroet door een van de portiers, die een scanner tegen Freeks arm houdt. Net als de andere zeventig vips van de club heeft hij een RFID-chip laten implanteren. Op een beeldscherm komt Freeks foto tevoorschijn. Eronder staat zijn naam, dat hij nog 824 euro dranktegoed heeft en dat hij twee introducés mag meenemen.

Anita is diep onder de indruk van Freek zijn cybernetische speeltje. Joke niet. Zij denkt aan

RFID: altijd en overal.

het RFID-implantaat van hun hond Max. Binnen wordt Freek nog paar een keer gescand: als het gezelschap het vipdek betreedt en telkens als Freek een rondje haalt. Ooit was er veel media-aandacht voor dit systeem. Sommige journalisten vonden het implanteren van een RFID-chip te ver gaan. Mensen zijn toch geen runderen, schreven ze dan. Enkele christenen zagen het implantaat zelfs als het teken van de duivel, waarbij ze verwezen naar Bijbelpassages die de komst van satan aankondigen door een merkteken in de hand. Aanvankelijk had eigenaar van de Baja Beach Club Jo van Gaalen de chip willen invoeren als universeel betaalsysteem voor alle nachtclubs. Maar onder alle negatieve aandacht heeft hij daar voorlopig vanaf gezien. Freek heeft er nooit echt over nagedacht. Hij vond het vooral een cool gadget dat zijn status als vip bevestigde. Zijn enige voorwaarde is dat de gegevens binnen de club blijven. Anderen hoeven nu eenmaal niet te weten wat hij er doet en hoeveel hij er uitgeeft.

Na een leuke avond in de nachtclub mist Joke net haar trein. Op het station wacht ze op de volgende. Haar ogen dwalen ondertussen af naar een apparaat in de hal. Het is de oplader voor de ov-chipkaart. Ze legt de kaart in het bakje om te controleren of er nog genoeg op staat. Dan ziet ze dat ze ook de laatste tien ritten kan opvragen. Nieuwsgierig drukt ze op het knopje en er rolt een bonnetje uit. Tijdens de treinreis bestudeert ze de tijden en stations die op het bonnetje staan. Hans is die dag om kwart over acht ingestapt en om vijf voor half negen weer uitgestapt. En hé, deze week is hij een paar keer een half

OV-chipkaart

> Eerste ervaringen met de nieuwe manier van reizen

In het gebruikersonderzoek heeft het Rathenau Instituut aan honderd reizigers gevraagd waarom ze een ov-chipkaart hebben aangeschaft. De eerste reactie was eenduidig: gebruiksgemak. Geen gedoe meer met geld, kaartjesautomaten of strippenkaarten. "Gewoon kaart langs de reader en gaan. Alleen niet vergeten weer uit te checken, want anders betaal je de volle mep", drukte een van de deelnemers het uit. Anderen gaven aan de kaart te hebben gekregen van hun werkgever of van de NS, omdat ze al een abonnement hadden. Ongeveer een derde van de gebruikers noemde ook nadelen van de kaart, zoals problemen bij in- en uitchecken of een hoger reistarief. Slechts negen procent was overwegend negatief over het betaalmiddel. De rest was positief of neutraal. Vrijwel alle geïnterviewden zeiden de ov-chipkaart te zullen blijven gebruiken. Waarbij overigens moet worden aangetekend dat het hier gaat om voorlopers, die nieuwe technologieën gemakkelijk accepteren. >

uurtje in het centrum geweest, halte Nieuwmarkt. Maar dat is de rosse buurt ...

Een uur later in Amsterdam stormt Joke woedend de metro uit. Ze vergeet uit te checken en de database van het vervoersbedrijf registreert dat Hans een kwartier na midder-nacht is ingestapt en nooit meer is uitgestapt. Hij betaalt daarom de hele reis tot aan eindpunt Gein. Thuisgekomen sleurt Joke haar echtgenoot uit bed en duwt hem de ov-chipkaart en het bonnetje onder zijn neus. “Wat doe jij zo iedere keer na je werk in die buurt? Je denkt toch zeker niet dat ik gek ben!” Hans wrijft de slaap uit zijn ogen en kijkt schaapachtig naar het bonnetje. Dan begint hij te lachen. “Ik ben inderdaad op de Wallen geweest. Maar er zitten ook juweliers. Kijk.” Hij haalt een klein doosje uit het nachtkastje en toont Joke een schitterend horloge. “Het was eigenlijk bedoeld voor ons tienjarig huwelijk, maar ik kan het je net zo goed nu alvast geven.” Joke smelt en neemt Hans stevig in haar armen. “Dit horloge bevat overigens ook een RFID-chipje”, zegt Hans. “Om te garanderen dat het geen namaak is.” Joke kijkt verschrikt op. “Je gaat me er niet mee volgen, toch?” “Nee hoor”, lacht Hans. “Technisch is dat niet mogelijk.” En in stilte: “Tenminste ... nu nog niet.”

OV-chipkaart

> OV-chipkaart geeft inzicht in reisgedrag

Het betaalsysteem van de OV-chipkaart is een debetsysteem: de reiziger betaalt vooraf een bedrag waar de reiskosten vervolgens van worden afgetrokken. Het systeem kan daardoor volledig anoniem zijn. Een gepersonaliseerde kaart heeft echter voordelen, zowel voor reiziger als vervoerder. Ten eerste kan de kaart automatisch worden opgeladen via een bankmachtiging. Dit dient het gebruikersgemak. Ten tweede kan de klant, als abonnee of speciale doelgroep, allerlei kortingen krijgen. De vervoersbedrijven gaan vrij ver in personalisatie van de kaart: bij aanschaf wordt zelfs een kopie van het paspoort gevraagd.

Uit het gebruikersonderzoek blijkt dat veel mensen onbewust hebben gekozen voor een persoonlijke kaart: ze kenden de mogelijkheid van de anonieme kaart niet, deze was niet beschikbaar of ze kregen ongevraagd een kaart toegestuurd van vervoerder of werkgever. Bovendien is de anonieme kaart duurder. Het College Bescherming Persoonsgegevens (CBP) is hier fel op tegen, omdat mensen zo worden gedwongen hun persoonsgegevens af te staan. >

De gevolgen van digitale voetsporen in RFID-systemen

Op kantoren worden steeds meer toegang-systemen uitgerust met RFID.

Het voorgaande verhaal laat zien hoe gebruikers van RFID digitale voetsporen achterlaten in uiteenlopende omgevingen. Enkele van de beschreven systemen kunnen oneigenlijk gebruikt worden om mensen ongevraagd te volgen en te controleren. Maar vooralsnog gaat het – zeker gezien de schaal waarop RFID nu in het publieke domein wordt ingevoerd – relatief goed. De mogelijkheden om mensen te volgen zijn in de praktijk bovendien begrensd, omdat de afzonderlijke systemen slechts een beperkt beeld geven van de gebruikers. Dat kan echter veranderen. Veel toegangs- en betaalsystemen zullen straks uitsluitend met RFID werken. RFID-systemen kunnen ook steeds meer aan elkaar en aan andere technologieën worden gekoppeld. Gebruikers worden dan via hun digitale voetsporen steeds transparanter voor de beheerders van die omgevingen. Omgekeerd worden de RFID-omgevingen voor gebruikers juist steeds minder inzichtelijk. De huidige balans tussen keuze, gemak en controle kan dan verstoord raken. Dat heeft ook gevolgen voor de rol van de overheid. Enerzijds zal het lastiger worden de Wet bescherming persoonsgegevens te handhaven. Anderzijds zal de overheid zelf meer gebruik kunnen maken van digitale voetsporen, bijvoorbeeld bij de opsporing van verdachten of getuigen.

Op weg naar een 'internet van dingen'

Uit de interviews die het Rathenau Instituut hield met diverse gebruikers van RFID-systemen blijkt dat de meeste weinig problemen zien in de digitale voetsporen die ze achterlaten in RFID-omgevingen. Wel moet voor gebruikers duidelijk zijn wie de omgeving beheert en er moet iets tegenover staan: gemak, korting of veiligheid. De meeste gebruikers zien vooral in het gemak van RFID een voordeel en ze gaan ervan uit dat RFID niet meer is dan een elektronische portemonnee of sleutel. Die berusting is in zekere zin terecht. Want anders dan bijvoorbeeld internet- en gsm-verkeer, vertellen de digitale sporen van RFID-gebruikers nog niet zo heel veel over hen. De systemen beslaan slechts een beperkt gebied: een enkel reistraject, een kantoorgebouw of een club. Bovendien bestaan er nog vaak alternatieven, zoals strippenkaarten, streepjescodes, magneetkaarten, sleutels of contant geld. Dat beperkt soms het gebruiksgemak, maar geeft wel enige mate van keuzevrijheid, terwijl beheerders beperktere mogelijkheden hebben voor controle. Ze kunnen immers geen totaalbeeld krijgen van alle bewegingen van alle mensen.

Diverse ontwikkelingen wijzen erop dat dit gaat veranderen. Allereerst zal het gebruik van een aantal recentelijk ingevoerde RFID-systemen de komende jaren sterk toenemen. Het biometrisch paspoort en de ov-chipkaart worden nu nog op beperkte schaal gebruikt en geven daarmee slechts een beperkt beeld van de reizigerspopulatie. Maar als over een paar jaar alle oude paspoorten zijn vervangen en de ov-chipkaart de enige betaalwijze in het openbaar vervoer is, bevatten de achterliggende databanken opeens een totaalbeeld van alle gebruikers, inclusief hun bewegingen binnen het systeem.

Ten tweede ligt ook de koppeling van verschillende RFID-systemen voor de hand. Dat dient het gemak van de gebruiker, die meer mogelijkheden krijgt met minder pasjes, en van de beheerder, die zijn dienstverlening kan uitbreiden en meer controle krijgt over de omgeving. Vooral een combinatie van reizen en betalen leent zich hier goed voor, zoals te zien bij de Japanse Suica-kaart. Dit is een OV-chipkaart waarmee ook in winkels betaald kan worden. Ook de Speedpass van oliemaatschappij ExxonMobil is een voorbeeld. Met de pas kan bij de Amerikaanse benzinestations van het concern direct aan de pomp worden afgerekend. De pas kan verder worden gebruikt voor betalingen in de snackbar en de winkel van het tankstation.

Ten derde is er een tendens om RFID-systemen te koppelen aan andere systemen binnen de digitale ruimte, zoals de mobiele telefoon, internet of digitale camera's. In het Britse Madejski-stadion van de voetbalclub Reading bijvoorbeeld worden de RFID-gegevens van de clubkaarten gekoppeld aan die van de beveiligingscamera's om snel de identiteit van eventuele relschoppers te achterhalen. Wereldwijd werken banken en telefoniebedrijven momenteel samen om betaling via *Near Field Communication* (NFC) mogelijk te maken. De mobiele telefoon dient dan als RFID-chip en -lezer tegelijk en kan bovendien via internet allerlei gegevens koppelen. In Frankrijk en Finland zijn in de toeristische sector al verschillende proeven gehouden met NFC, waarbij de mobiele telefoon RFID-chips in reclameposters en wegwijzers uitleest.

Tot slot zal het samengaan van al deze verschillende netwerken een nieuwe impuls krijgen door de invoering van IPv6 (Internet Protocol versie 6). Het huidige IPv4 wordt gebruikt om aan internetcomputers en -servers een IP-adres toe te wijzen. IPv6 bevat zoveel nieuwe adressen, dat het in principe mogelijk is elk object – dus ook elke RFID-chip – en elke persoon op aarde een uniek nummer te geven. Volgens ingewijden zal hiermee een alomvattend 'internet van dingen' ontstaan, waarin vrijwel alle bewegingen en handelingen in de fysieke wereld een evenbeeld krijgen in de virtuele ruimte. RFID wordt daarbij vanwege het gebruiksgemak en de lage kosten gezien als een sleuteltechnologie.

Het zal nog de nodige tijd duren voor het zover is. Maar ondertussen is wel duidelijk dat de huidige RFID-toepassingen nog maar het begin zijn van een veel omvangrijkere ontwikkeling, waarbij de onderlinge verhoudingen tussen gebruikers en beheerders van RFID-omgevingen drastisch kunnen veranderen. Als systemen uitsluitend met RFID gaan werken en onderling worden gekoppeld, krijgen steeds meer beheerders steeds beter inzicht in het gedrag van gebruikers. Omgekeerd wordt het voor gebruikers steeds onduidelijker in welke omgeving welke persoonlijke gegevens worden gebruikt en door wie. Deze overschrijding van de grenzen tussen verschillende omgevingen is dus niet alleen technologisch van aard, maar ook organisatorisch: vervoersbedrijven krijgen inzicht in werktijden, werkgevers nemen de rol van bank over en telefoniebedrijven handelen in treinkaartjes. De gebruiker zal via zijn digitale voetsporen steeds transparanter worden voor zijn omgeving, terwijl die omgeving zelf voor de gebruiker steeds minder transparant wordt.

Toepasbaarheid van de WBP

Gebruikers van RFID-systemen genieten bescherming onder de Wet bescherming persoonsgegevens (WBP). Daarin is vastgelegd onder welke voorwaarden gegevens mogen worden gebruikt die op de een of andere manier verwijzen naar een fysiek persoon (zie kader). Volgens analyses van organisaties als het College Bescherming Persoonsgegevens (CBP), de Nederlandse Vereniging voor Informatietechnologie en Recht (NVvIR) en ECP.nl is de wet *in principe* voldoende om de relatie tussen gebruikers en beheerders van RFID-omgevingen te reguleren. De handhaving in de praktijk zal echter lastig zijn. In de casestudies kwam het Rathenau Instituut de volgende belemmeringen tegen.

Ten eerste is het de vraag of, gezien de massale invoering van RFID door zeer uiteenlopende partijen, alle gebruikers en beheerders op de hoogte zijn van de regels van het CBP en de WBP. In het bovengenoemde geval van automatiseringsbedrijf Alcatel is de invoering van de actieve RFID-toegangspassen besproken met de ondernemingsraad en waren de principes van de WBP leidend. Op een andere werkplek die het Rathenau Instituut bezocht leek dat niet het geval. Nieuwe werknemers kregen een RFID-'toegangssleutel', terwijl verschillende werknemers, waaronder ook een afdelingshoofd zich ongevraagd toegang hadden verschaft tot de database, waar duidelijk uit was op te maken wie wanneer op kantoor kwam. Geen van de betrokkenen was zich er echter van bewust dat de WBP werd overtreden.

Ten tweede kan een beheerder van een RFID-omgeving de gebruiker weliswaar formeel gezien voldoende informeren over de dataverzameling, maar het hem tegelijkertijd zo moeilijk mogelijk maken om werkelijk inzicht te krijgen. Bekend zijn de gebruikersovereenkomsten die bestaan uit ellenlange, onvindbare of ondoorgrondelijke teksten. Zo sturen de Nederlandse Spoorwegen gebruikers van de dalurenkaart een RFID-pas toe en vermelden in de begeleidende brief dat ingebruikname van de pas gezien wordt als instemming met de gebruikersvoorwaarden, die alleen zijn te vinden op een website. Zoals bekend is NS van plan de gegevens ook voor marketingdoeleinden te gebruiken en is het CBP hier fel op tegen. In sommige gevallen kan zelfs in de overeenkomst staan dat de gegevens mogen worden doorgespeeld aan derden en de eigenaar van de RFID-omgeving er dan niet meer verantwoordelijk voor is, zoals bijvoorbeeld bij de Amerikaanse Speedpass van ExxonMobil. De gebruikersovereenkomst bevat in dit geval ook een clausule die het mogelijk maakt de voorwaarden eenzijdig te wijzigen zonder de gebruiker hierover te informeren. Allemaal redenen die een gebruiker misschien doen besluiten om zijn pas links te laten liggen, zou hij hiervan tenminste op de hoogte zijn.

Ten derde kunnen data ook anoniem worden geanalyseerd, zoals het geval is in de Apenheul. De bezoekers worden via de actieve RFID-chip in de apentas door het park gevolgd zonder hun toestemming. De chip is echter niet gekoppeld aan enige persoonlijke informatie over de drager. Er is daarom geen sprake van een persoonsgegeven en de WBP is niet van toepassing. Al zal niet elke bezoeker de chip op prijs stellen, ze ondervinden er ook geen nadeel van. Dat zou echter wel kunnen als een beheerder van een RFID-omgeving zijn prijzen of diensten aanpast op basis van die anonieme data.

Als laatste kan worden opgemerkt dat bij veel RFID-omgevingen pas na ingebruikname blijkt wat er zoal mogelijk is met de verzamelde gegevens. Stapsgewijs kunnen dan nieuwe functies worden getest en toegevoegd. Dit verschijnsel wordt ook wel *function creep* genoemd. Zal de beheerder van de RFID-omgeving dan bij elke stap al zijn klanten vragen om toestemming, en hen inzage bieden in de data, of zal dit in de praktijk ondoenlijk blijken? Willen klanten bovendien hierover wel continu worden geïnformeerd, of vertrouwen zij liever op de beheerder en voert het gebruiksgemak de boventoon?

Deze belemmeringen voor de uitvoering van de WBP zijn al waar te nemen. Maar hoe zal het gaan in de toekomst? Als er steeds meer RFID-systemen komen, zal het praktisch steeds lastiger worden om alle gebruikers overal over te informeren. Systemen die straks uitsluitend met gepersonaliseerde RFID-chipkaarten werken, ontnemen gebruikers de keuze om geen persoonsgegevens af te staan. Als systemen van

OV-chipkaart

> In het reizigersonderzoek zijn vragen gesteld over het gebruik van die gegevens. Hieruit blijkt een oplopende schaal van privacygevoeligheid. In een eerste spontane reactie noemden maar twee ondervraagden als nadeel: "Ik kan gevolgd worden." Vervolgens werd de deelnemers gevraagd of zij denken dat met de kaart ook persoonlijke gegevens worden verzameld. Een kleine meerderheid (56%) dacht van wel. Ze dachten daarbij vooral aan naam, geboortedatum en telefoonnummer. Toen daarop werd gesteld dat de kaart inzicht geeft in het reisgedrag, reageerde menigeen verrast. Een kleine meerderheid zei hiermee geen problemen te hebben, een derde bleek tegen. Toen gevraagd werd of ook de politie inzage mag krijgen in die reisgegevens, hetzij om verdachten te achterhalen of om getuigen te vinden, bleek bijna de helft tegen: respectievelijk 46 en 43 procent. Ook ongevraagde reisadviezen en aanbiedingen op basis van het reisgedrag stuitten op weerstand: 32 en 42 procent was tegen. En dat terwijl aanvankelijk vrijwel niemand bezwaar had tegen de mogelijkheid te kunnen worden gevolgd! Was dit onwetendheid of desinteresse? Uiteindelijk zei 66 procent dat de voordelen van de ov-chipkaart opwegen tegen dit nadeel, 18 procent vond van niet. Al met al zijn er dus toch behoorlijk wat reizigers die moeite hebben met de digitale voetsporen die ze achterlaten, ook al willen ze vrijwel allemaal de kaart blijven gebruiken. <

Volgens de Wet bescherming persoonsgegevens (WBP) moet het gebruik van RFID-data voldoen aan de volgende principes:

1. Doelspecificatie: de beheerder moet een duidelijk omschreven doel aangeven voor de te verzamelen gegevens.
2. Beperking van gegevensverzameling: de beheerder mag niet meer verzamelen dan voor het doel noodzakelijk is.
3. Doelbinding van gegevens: de beheerder mag gegevens niet gebruiken voor andere doelen dan waarvoor ze verzameld zijn.
4. Gegevenskwaliteit: de beheerder moet toezien op de actualiteit, betrouwbaarheid en volledigheid van gegevens.
5. Beveiligingswaarborgen: de beheerder moet zorgen voor een adequate technische en organisatorische beveiliging van de gegevens.
6. Openheid: de gegevensverzameling en de herkomst van de gegevens moeten transparant zijn.
7. Individuele deelname: er moet een regeling zijn voor inzage-, correctie-, verwijderings- en bezwaarrecht.
8. Aansprakelijkheid: de verantwoordelijke voor de gegevens dient gepaste maatregelen te treffen om aan de hierboven genoemde principes te voldoen.

Deze principes zijn een vertaling van Europese wetgeving. De WBP geldt niet als het gaat om de bescherming van de economische of financiële belangen van de staat, of als er sprake is van voorkoming, opsporing of vervolging van strafbare feiten.

verschillende beheerders worden gekoppeld, kan het steeds lastiger worden één enkele beheerder aan te wijzen als verantwoordelijke. Het doel van het systeem dat aan de WBP wordt getoetst, zal vaag blijven als het telkens van tijd tot tijd verandert of wordt uitgebreid.

Bovenal zal door grootschalige invoering van RFID de hele notie veranderen van wat eigenlijk een persoonsgegeven is. Het gaat dan immers niet meer uitsluitend om de informatie die is gekoppeld aan een fysiek persoon, bijvoorbeeld diens naam of bankrekeningnummer, maar ook om allerlei interacties die hij met het systeem heeft, zoals zijn reis- of koopgedrag. Beheerders van systemen kunnen op basis van die informatie hun diensten aanpassen en bijvoorbeeld aantrekkelijke kortingen geven, extra service verlenen of aanbiedingen onder de aandacht brengen. Ze kunnen hierover heel open zijn en beargumenteren dat gebruik van al deze aanvullende informatie belangrijk is voor een gezonde bedrijfsvoering. En eerlijk is eerlijk, gebruikers zullen dikwijls de vruchten plukken van zo'n persoonlijke benadering. Maar met al die aanbiedingen en voordelen kunnen beheerders klanten tegelijkertijd ook sturen in hun gedrag. En ondertussen wordt daarbij volop gebruikgemaakt van gegevens die weliswaar mensen identificeren, maar die niet vallen onder de wettelijke definitie van persoonsgegevens en waarvoor de restricties van de WBP niet gelden.

RFID en opsporing

Tot nog toe is er in Nederland geen geval bekend waarbij RFID een sleutelrol vervulde in het oplossen van een ernstige misdaad. In theorie kan de aanwezigheid van een unieke chip op een bepaalde plaats of een RFID-database met verkeersgegevens aanwijzingen geven of een verdachte op een bepaald moment ergens is geweest of een bepaalde handeling heeft verricht. Gezien het beperkte beeld dat de RFID-data geven van gebruikers is dat vooralsnog niet erg waarschijnlijk. Voorlopig blijven gegevens van gsm-verkeer en internetcommunicatie en bankgegevens daarom interessanter voor de opsporingsdiensten. Naarmate systemen echter vaker exclusief met RFID gaan werken en ze vaker worden gekoppeld – en dus zoals gezegd een totaalbeeld van de gebruikers ontstaat -– zal deze informatie wel aantrekkelijk worden voor opsporingsdoeleinden. Hoe die informatie precies gebruikt gaat worden moet de toekomst uitwijzen. Wel kunnen enkele tendensen in de opsporing worden genoemd die relevant zijn voor het gebruik van RFID. De tendensen staan uitgebreider beschreven in de recent verschenen studie van het Rathenau Instituut *Van privacyparadijs tot controlestaat?*
Volgens de auteurs van de studie zijn in de afgelopen twintig jaar veel maatregelen genomen om middelen en bevoegdheden voor opsporingsonderzoek uit te breiden. Opsporingsdiensten kunnen steeds meer zelfstandig onderzoek doen, hebben steeds meer toegang tot informatie die voor andere doeleinden is verzameld en hebben meer mogelijkheden om derden te dwingen mee te werken aan de gegevensverzameling. Onderzoek is ook steeds vaker verkennend van karakter, waarbij op basis van risicoprofielen potentiële verdachten worden gevolgd. Deze uitbreiding van de bevoegdheden van opsporingsdiensten stamt, anders dan vaak wordt aangenomen, al

van voor de terroristische aanslagen van 11 september 2001 en is voornamelijk ingegeven door de strijd tegen de georganiseerde misdaad in het algemeen en nieuwe technologische mogelijkheden, met name in de ICT.

"Sherlock Holmes kon aan de hand van een voetafdruk allerlei conclusies trekken over de mens boven de voet: wat voor bepakking hij droeg, of hij oud was of jong, hoe rijk hij was, enzovoort. Dankzij RFID hebben we daar geen Sherlock Holmes meer voor nodig."
Uitspraak van Harm Brouwer, Hoofd van het Openbaar Ministerie, tijdens het congres eNederland 2005.

Het regeerakkoord van het kabinet-Balkenende IV lijkt voort te bouwen op deze tendens.
In het hoofdstuk *Veiligheid, stabiliteit en respect* staat te lezen: "Het functioneren van politie en OM wordt versterkt; er wordt optimaal gebruikgemaakt van nieuwe technologie om het opheldergingspercentage te verbeteren. Knelpunten worden weggenomen en er komen geen nieuwe belemmeringen, procedures of beperkingen." (p. 33) Wel wordt gesteld: "Bij alle maatregelen verantwoordt de overheid de gevolgen voor de privacy van de burger." (p. 34)

Gezien de huidige ontwikkelingen ligt het voor de hand dat opsporingsdiensten steeds vaker RFID-databases zullen opvragen in geval van een concrete verdenking. Maar ze kunnen ook verder gaan en de data bij voorbaat vorderen om RFID-sporen te analyseren op basis van risicoprofielen, afzonderlijk en in onderlinge samenhang. De inzet van RFID-data bij opsporing zal effect hebben op de publieke beleving van RFID. Sommige mensen zullen zich veiliger voelen als de staat eenieders digitale voetsporen volgt. Anderen zullen het een te grote aantasting van hun privacy vinden. Een dergelijke ontwikkeling zal ook consequenties hebben voor de beheerders van RFID-omgevingen. Ook van hen zal de een kiezen voor veiligheid, terwijl de ander vreest klanten kwijt te raken als zijn RFID-systeem door de staat kan worden aangewend voor controle. De vraag is daarmee hoe de balans tussen keuzevrijheid, gebruiksgemak en controle zal veranderen. Hierover bestaat vooralsnog veel onduidelijkheid.

Een discussie op zichzelf is het biometrisch paspoort. Hier heeft de burger namelijk straks geen keuze de RFID-toepassing *niet* te gebruiken en gaat het om de gegevens van de hele bevolking. Vooralsnog dient de RFID-chip in het paspoort vooral om het inchecken op luchthavens gemakkelijker te maken en om fraude te voorkomen. Zolang nog niet iedereen een biometrisch paspoort heeft, geven de data slechts een fragmentarisch beeld. Maar omdat uiteindelijk elke burger er straks een moet hebben, zal het voor opsporingsdiensten interessant zijn als de gedigitaliseerde foto's (en later de irisscan en de vingerafdruk) op de chip centraal worden bewaard, zodat ze die gemakkelijk kunnen vergelijken met bijvoorbeeld sporen die gevonden zijn op een plaats van een misdaad. De Europese wetgeving laat de keuze om al dan niet een centrale databank met biometrische gegevens in te richten vooralsnog over aan de afzonderlijke lidstaten. Duitsland en Italië zijn principieel tegen centralisatie, maar in Nederland is de keuze nog niet zo expliciet gemaakt. Als alsnog wordt besloten tot een centrale opslag, dient de vraag zich aan welke instanties toegang krijgen tot de databank, en op welke manier en voor welke doeleinden ze de gegevens mogen gebruiken. Alleen inzage bij concrete verdenkingen, of een dataminingsysteem met risicoprofielen? Ook zal moeten worden besloten wat er naast de biometrische informatie aan RFID-data moet worden bewaard. Moet straks elke douanepassage van elke Nederlander centraal worden geregistreerd?

"Overheden zijn altijd geïnteresseerd in plaatsen waar veel gegevens over personen samenkomen. Die interesse bestaat ook bij veel andere partijen. De overheid echter is in staat om invloed uit te oefenen op de grenzen van het juridisch toelaatbare. De overheid moet er niet op uit zijn middels RFID over steeds meer gegevens te kunnen beschikken. De burger moet vertrouwen hebben in verantwoord RFID-gebruik door de overheid." (CBP: 2006, p. 7).

De opgave:

evenredig profijt van een onzichtbare digitale revolutie

OV-chipkaart

> Gemak voor gebruiker en beheerder

De ov-chipkaart ontmoet veel kritiek bij organisaties die gebruikersbelangen behartigen. Het CBP heeft de NS herhaaldelijk vermaand dat zij de reisgegevens niet mogen gebruiken voor marketingdoeleinden. Een dergelijk gebruik ligt buiten het eigenlijke doel van het systeem en is daarmee strijdig met de Wet bescherming persoonsgegevens (WBP). Zolang de anonieme kaart duurder en moeilijker verkrijgbaar blijft, is ook de keuzevrijheid van de reiziger onderwerp van discussie.

Reizigersorganisatie ROVER stelde op 16 januari 2007 in een manifest: "Van de beloofde zegeningen voor de reiziger is zo goed als niets over." Het nieuwe systeem zou reizen duurder maken en de tarieven minder inzichtelijk. Van het gebruiksgemak zou weinig overblijven. Volgens de reizigersorganisatie is het zelfs onduidelijk of wel kan worden volstaan met één chipkaart voor het hele openbaar vervoer. Zo zou de NS de voordeelurenkorting alleen op zijn eigen kaart willen zetten. ROVER is ook fel gekant tegen het principe van 'kaartje laden', waarbij de reiziger naar een automaat moet om met zijn pinpas een treinkaartje op de chipkaart te zetten.

Het gebruikersgemak lijkt het dus af te leggen tegen de controle- en marketingvoordelen voor vervoerders. Terwijl RFID reizigers allerlei mogelijkheden biedt die vooralsnog onbenut blijven, zoals een Best Pricing-systeem. Reizigers kunnen dan vrij in- en uitstappen en het systeem rekent achteraf het voordeligste reistarief af. De gebruiker krijgt dan een melding dat hij in de afgelopen maand bijvoorbeeld een abonnement of juist een voordeelurenkaart heeft gehad. Voordeel voor de vervoerders is daarbij dat gebruikers zo een duidelijk nut zien om de kaart te personaliseren.

Ook in de Tweede Kamer is de ov-chipkaart al tientallen malen besproken. Telkens weer worden vragen gesteld bij gebruiksgemak, privacy en prijsstelling. Het valt daarom nog maar te bezien of het nieuwe kabinet erin zal slagen om de ambitie van één kaart voor heel Nederland waar te maken. <

De moderne mens leeft in een tijd waarin de fysieke publieke omgeving razendsnel digitaliseert en toegroeit naar een internet van dingen. RFID wordt in die ontwikkeling gezien als een sleuteltechnologie. Vooralsnog maken de kleine op afstand uitleesbare chips vooral veel handelingen in het dagelijks leven gemakkelijker en beheersbaarder. Gebruikers zien RFID-chips vaak als niets meer dan een elektronische sleutel of portemonnee. Slechts weinigen zijn zich bewust van de digitale voetsporen die ze achterlaten. Voor zover ze dit wel beseffen, vertrouwen ze op een correct beheer. Als RFID straks op steeds meer plaatsen aanwezig is en steeds meer systemen worden gekoppeld, geven die sporen een steeds vollediger beeld van die gebruiker. Er moet daarom worden gezocht naar het juiste evenwicht tussen gebruiksgemak, keuzevrijheid en controle.
Het Rathenau Instituut formuleert hiervoor de volgende aanbevelingen:

1. Gebruikers moeten weten wat beheerders kunnen en mogen met RFID

Beheerders en overheid moeten openheid geven over wat zij kunnen en mogen doen met de informatie die via RFID wordt verkregen. Maar transparantie mag niet leiden tot een overdaad aan informatie: gebruikersovereenkomsten moeten kort, duidelijk en beschikbaar zijn. Die overeenkomsten moeten niet alleen worden getoetst aan de WBP, maar ook op gebruiksvriendelijkheid.

2. Geef gebruikers een rol bij het ontwerpen van RFID-omgevingen

Bij het ontwerpen van een RFID-systeem worden belangrijke keuzes gemaakt die gevolgen hebben voor de latere gebruikers. De eigenaar heeft daarbij een voorsprong: hij kent de mogelijkheden van het systeem en kan het systeem bouwen naar zijn eigen wensen. Dit kan er bijvoorbeeld toe leiden dat een systeem werkt met persoonsgegevens, terwijl die voor het functioneren niet noodzakelijk zijn. Ook kan het gebeuren dat een systeem als vanzelfsprekend met RFID wordt uitgebreid, terwijl andere technologieën ook goed werken. Door gebruikers en belangenorganisaties te betrekken bij het ontwerpen van RFID-systemen kunnen ze de opties van anonimiteit en keuzevrijheid bewaken. Dit hoeft innovatie in de dienstverlening niet te belemmeren: juist gebruikers kunnen innovatief zijn in het bedenken van nieuwe toepassingen voor RFID-systemen.

3. Verantwoorde uitbreiding van RFID-omgevingen

De twee voorgaande punten nemen toe in belang als de mogelijkheden van een RFID-omgeving worden uitgebreid door haar te koppelen aan andere omgevingen of andere technologieën, zoals de mobiele telefoon of internet. Zo'n uitbreiding kan nuttig zijn, bijvoorbeeld om het aantal pasjes of handelingen terug te dringen of om de dienstverlening uit te breiden. De beheerder van het systeem krijgt zo wel een completer beeld van zijn gebruikers. De mogelijke gevolgen daarvan moeten zichtbaar zijn voor die gebruikers. Als systemen van verschillende beheerders worden gekoppeld, moet ook helder zijn voor de gebruikers welke beheerder verantwoordelijk is voor welke gegevens. Systemen mogen bovendien niet worden gekoppeld als dit voor gebruikers nauwelijks voordelen oplevert en slechts leidt tot een onevenredige toename in de controlemogelijkheden van beheerders.

4. Bezinning op de WBP en het begrip 'persoonsgegeven'

De uitgangspunten van de WBP zijn goed, maar steeds moeilijker te handhaven in de praktijk. De gebruiker zal zich niet in alle gevallen bewust zijn van de digitale voetsporen die hij achterlaat en wat daarmee gebeurt, zeker als RFID op steeds meer plaatsen wordt toegepast. De rol van belangenorganisaties wordt daarmee belangrijker. Onderzocht moet worden bij welke toepassingen van RFID er formeel geen sprake is van een persoonsgegeven, terwijl interacties met die omgeving wel degelijk consequenties kunnen hebben voor de gebruiker. Vervolgens moet worden gekeken in hoeverre dergelijke consequenties van anonieme sporen ook moeten worden opgenomen in de WBP.

5. Duidelijke keuzes bij RFID als opsporingsmiddel

RFID is interessant voor opsporingsdoeleinden, omdat het inzicht kan bieden in wie, waar, wanneer wat doet. Een verzoek vanuit de opsporingsdiensten tot inzage van de databases van een werk- of reisomgeving zal bij concrete verdenkingen tegen een verdachte op weinig weerstand stuiten. Naarmate RFID-systemen steeds alomvattender worden, kunnen ze echter ook worden gebruikt voor verkennende onderzoeken, zoals analyse op risicoprofielen. Het verdient aanbeveling te onderzoeken of een dergelijke toepassing wenselijk, dan wel effectief is.

Referenties

Capgemini (2005) *RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business.*

Das, R. & Harrop (2006) RFID Forecasts, Players & Opportunities 2006 – 2016 IDTechEx

Garfinkel, S. & B. Rosenberg (eds.) (2006). *RFID: Applications, Security and Privacy*. Addison-Wesley

OECD (2006). *Radio Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations.* DSTI/ICCP(2005)19/FINAL. 27 februari 2006.

Schermer, B. & M. Durinck (2005). *Privacyrechtelijke aspecten van RFID.* ECP.nl.

Schermer, B. & G.J. Zwenne (2005). *Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen.* NvvIR.

Publicaties van het Rathenau Instituut

2007

De publieke perceptie van RFID in Nederland. (werktitel) Den Haag: Rathenau Instituut. Publieksonderzoek in samenwerking met RFID Platform Nederland en de Consumentenbond. Verwacht in oktober.

Krom, A. & B. Walhout (eindred.). *Ambient intelligence: toekomst van de zorg of zorg van de toekomst?* Den Haag: Rathenau Instituut. Verwacht in juni.

Hof, C. van 't. *RFID & identity management in the everyday life of European citizens: balancing convenience, control and choice in a new dimension of the digital public space.* Brussel: Europees Parlement. Eindrapport STOA-project 'RFID & Identity Management'. Verwacht in april.

Hof, C. van 't. *What do RFIDS tell about you? A user perspective on identity management: discussion paper.* - Brussel: Europees Parlement. - 7 p. Discussiestuk STOA-workshop 'RFID in the everyday life of Europeans [...]', 24 januari.

Vedder, A. et al. *Van privacyparadijs tot controlestaat?* Den Haag: Rathenau Instituut. - 90 p. - (Studie ; 49)

2006

Hof, C. van 't & J. Cornelissen. *RFID and identity management in everyday life: case studies on the front-line of developments towards ambient intelligence.* - ETAG. - 94 p. STOA-rapport voor het Europees Parlement.

Hof, C. van 't & M. van Lieshout. *Naar een internet van kleine dingen: politiek-bestuurlijke kwesties bij de invoering van RFID.* - Den Haag: Rathenau Instituut. - 8 p. Notitie voor de Themacommissie Technologiebeleid van de Tweede Kamer.

RFID and identity management : STOA opinion on RFID. Den Haag: Rathenau Instituut. - 2 p.

Deze publicaties zijn digitaal verkrijgbaar op www.rathenau.nl.
Voor meer informatie over RFID kunt u contact opnemen met Christian van 't Hof, e-mail: c.vanthof@rathenau.nl.

Met dank aan

Jessica Cornelissen (onderzoek)
Bart Schermer (RFID Platform Nederland)
Jaap Henk Hoepman (Radboud Universiteit)
Koen Dupon (Consumentenbond)
Denktank RFID & Privacy
(RFID Platform Nederland/Ministerie EZ).

Colofon

Deze Special is een uitgave van het Rathenau Instituut.
Het Rathenau Instituut stimuleert publiek debat en publieke oordeelsvorming over maatschappelijke, ethische en politieke effecten van moderne wetenschap en technologie. Daarnaast onderzoekt het instituut hoe het wetenschapssysteem is georganiseerd en hoe dit reageert op wetenschappelijke, maatschappelijke en economische veranderingen.

Tekst
Christian van 't Hof
Rinie van Est

Eindredactie
Dirk van Harten

Fotografie/beeld
Kelle Schouten
Stang Gubbels, illustratie pag. 7
Hollandse Hoogte, pag. 14

Grafische productie
Herbschleb & Slebos, Monnickendam

Drukwerk
Meboprint, Amsterdam

Redactieadres
Rathenau Instituut
Postbus 95366
2509 CJ Den Haag
telefoon (070) 342 15 42
telefax (070) 363 34 88
info@rathenau.nl
www.rathenau.nl