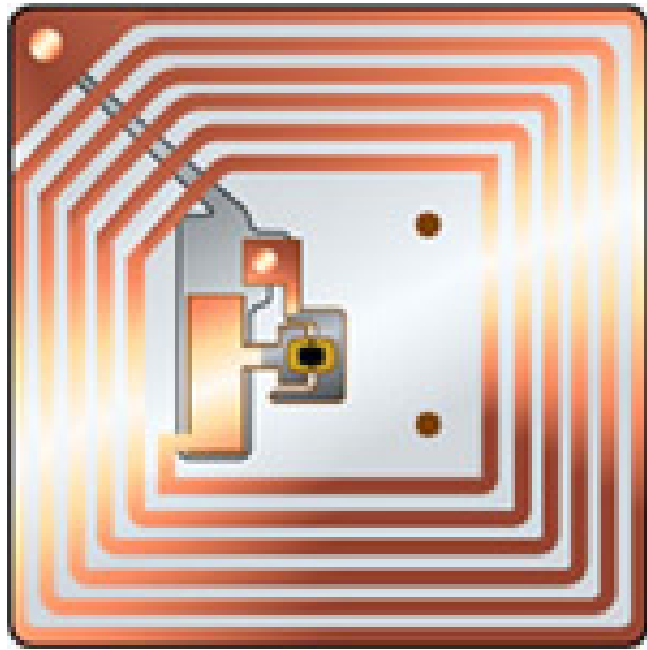


Notitie

“RFID in Nederland”



Ministerie van Economische Zaken

September 2006

Inhoudsopgave.

Inhoudsopgave.....	2
Hoofdstuk 1: Inleiding.....	3
Hoofdstuk 2: Techniek en toepassing.....	5
2.1 Hoe werkt RFID?	5
2.2 Classificatie van de technologie en toepassingen	6
2.2.1 Smart labels	6
2.2.2 Contactloze smartcards	7
2.2.3 NFC	8
2.3 Verwachtingen rondom RFID.....	9
Hoofdstuk 3: Kansen voor RFID ontwikkeling in Nederland.....	10
3.1 Groeimogelijkheden	10
3.2 Innovatie bij de drie soorten RFID.....	11
3.3 Innovatiebeleid in Nederland	12
3.4 Conclusies	14
Hoofdstuk 4: Zorgen rond RFID ontwikkeling in Nederland.....	15
4.1 Privacy.....	15
4.1.1 De risico's	15
4.1.2 Evaluatie van de privacyrisico's	16
4.1.3 Beperken van privacyrisico's	17
4.2 Veiligheidsrisico's.....	19
4.2.1 veiligheidsrisico's per onderdeel.....	19
4.2.2 Beperken van veiligheidsrisico's	20
4.3 Milieu en Gezondheid	21
4.3.1 RFID en elektromagnetische velden	21
4.3.2 Milieu-aspecten	22
4.4 Conclusies	23
Hoofdstuk 5: Standaardisatie en frequentieruimte.....	24
5.1 Standaardisatie	24
5.1.1 Waarom is standaardisatie belangrijk?.....	24
5.2.2 Huidige stand van zaken	24
5.3 Frequentiebanden voor RFID.....	26
5.4 Conclusies	28
Hoofdstuk 6: Conclusies en Acties.....	29
6.1 Conclusies	29
6.2 Acties.....	32

Hoofdstuk 1: Inleiding.

RFID staat voor Radio Frequency IDentification. RFID is een technologie die door technologische en prijsontwikkelingen voor steeds meer toepassingen bruikbaar wordt. Internationaal zijn er hooggespannen verwachtingen over de economische mogelijkheden, maar tevens zorgen over de mogelijke maatschappelijke nadelen. De heer Slob heeft in een motie (nr. 30 300 XIII, nr. 36) gevraagd om een notitie over RFID met bijzondere aandacht voor privacy.

RFID is een automatisch identificatiemiddel. Het gaat om een kleine chip waarvan de informatie op afstand is af te lezen of te beschrijven. RFID is in de basis vergelijkbaar met de klassieke barcode met als verschil dat een RFID chip niet in het zicht van een scanner hoeft te worden gelezen maar op beperkte afstand, door objecten heen en met meerdere tegelijkertijd uitgelezen kan worden. Voorbeelden van gebruik zijn elektronische toegangspasjes in gebouwen, het nieuwe Nederlandse paspoort en de OV-chipcard in het openbaar vervoer

RFID is op zich geen nieuwe techniek. Al in de Tweede Wereldoorlog werd zij, in een andere vorm maar op basis van hetzelfde principe, gebruikt om de eigen vliegtuigen te onderscheiden van de vijandige. Met de grote vooruitgang van de laatste jaren in de halfgeleiderindustrie en bij de productie, kunnen RFID-chips nu steeds kleiner en goedkoper geproduceerd worden. Gecombineerd met de huidige goede beschikbaarheid van breedband communicatie-infrastructuren biedt dit nieuwe mogelijkheden¹. De verwachting is dat het gebruik van RFID een grote vlucht zal gaan nemen in de toekomst². RFID zal een bijdrage kunnen leveren aan economische groei en innovatie. Het is belangrijk te anticiperen op deze snel groeiende technologie en de daar uit voortvloeiende toepassingen die ons dagelijks leven in de nabije toekomst zullen beïnvloeden.

In de afgelopen twee jaar begon het maatschappelijke debat over RFID in Nederland langzaam op gang te komen. De Christen Unie is zeer alert op de ontwikkeling rond RFID en heeft eerder een notitie over RFID³ geschreven en daarnaast een motie ingediend tijdens de begrotingsbehandeling van het Ministerie van Economische Zaken, waarop deze notitie het antwoord is. Daarnaast zijn tal van andere partijen actief op dit vlak. Zo heeft de Consumentenbond in december 2005 in een brief aan het Ministerie van Economische Zaken haar zorgen geuit over de manier waarop RFID in Nederland wordt ingevoerd, heeft het Rathenau Instituut een startnotitie⁴ rond RFID geschreven op verzoek van de parlementaire themacommissie technologie en is er een platform RFID Nederland opgericht.

In deze notitie is gepoogd een helder overzicht te schetsen van RFID en de aspecten ervan waar de overheid in beeld komt. Daarbij wordt nagegaan of het staande beleid voldoet aan de nieuwe ontwikkelingen. In hoofdstuk twee wordt ingegaan op de techniek van RFID en wordt een classificatie gemaakt van drie soorten RFID en de bijbehorende toepassingen. In

¹ Uit "RFID: Kans of bedreiging. Een blik op RFID toepassingen en verkenning van de beleidsimplicaties". Telematica Instituut. 2006

² Consultancyfirma Frost en Sullivan voorspelt dat de omzet in de markt voor RFID technologie in 2010 11,7 miljard zal bedragen.

³ Christen Unie; RFID-Chips Kans of Gevaar?. Mei 2005.

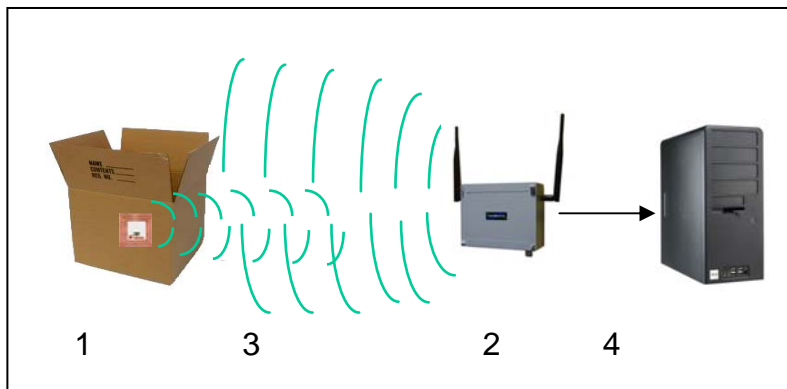
⁴ "Naar een internet van kleine dingen; Politiek-bestuurlijke kwesties bij de invoering van RFID". Rathenau Instituut. 2006

hoofdstuk drie komen de kansen voor RFID ontwikkeling voor de drie voornoemde categorieën behandeld. Dat wordt gematched met het innovatiebeleid in Nederland. De ontwikkeling van RFID biedt niet alleen kansen, maar geeft ook zorgen. In het vierde hoofdstuk komen die aan bod. Naast privacy, dat de grootste zorg is, komen veiligheid en milieu en gezondheid aan bod. Hoofdstuk vijf gaat in op standaardisatie en frequentieruimte, voorwaarden voor een goed functioneren van RFID. In het laatste hoofdstuk staan de conclusies en acties

Hoofdstuk 2: Techniek en toepassing.

2.1 Hoe werkt RFID?

RFID staat voor Radio Frequency Identification en is een technologie waarmee met behulp van *radiogolven* de unieke *automatische identificatie* van producten, dieren en/of personen op afstand mogelijk wordt gemaakt. RFID werkt in het algemeen als volgt: een chip gekoppeld aan een antenne (1) kan radiosignalen opvangen die worden uitgezonden door speciale leesapparaten (2). De chip gebruikt de elektromagnetische energie van het uitgezonden radiosignaal (3) om een eigen radiosignaal op te wekken, waardoor een bericht terug gestuurd wordt aan het leesapparaat. De inhoud van dit bericht is de informatie die opgeslagen ligt in de chip. Meestal zal dit slechts een uniek nummer zijn, maar er kan ook aanvullende informatie in de chip worden opgeslagen zoals productinformatie. Het leesapparaat stuurt deze informatie vervolgens door naar achterliggende informatieverwerkende systemen (4). De combinatie van een RFID-chip met een antenne wordt een 'tag' genoemd



Figuur 1. Schematische weergave van een RFID-systeem

RFID is zoals gezegd geen nieuwe technologie. Het is een technologie die zich in vele toepassingen al vele malen heeft bewezen. De reden dat RFID de laatste jaren zo in de aandacht staat heeft te maken met de verdere ontwikkeling van de technologie. De ontwikkeling van RFID verloopt op een manier zoals die vaak voorkomt bij doorontwikkeling van technologie. De RFID-chips worden zowel steeds kleiner als goedkoper. De steeds kleinere chips maken steeds meer toepassingen mogelijk en vanwege de dalende kosten zijn deze steeds eerder rendabel.

Het succes van RFID en de bijbehorende hoge verwachtingen en zorgen zijn te danken aan een aantal specifieke technische eigenschappen. RFID-tags kunnen draadloos worden uitgelezen met onzichtbare radiogolven. Hierdoor is geen 'line of sight' nodig zoals bij het uitlezen van barcodes. Bovendien kunnen er door een leesapparaat (reader) meerdere RFID-tags tegelijk worden uitgelezen. Het chipje in een gemiddelde RFID-tag is niet veel groter dan een speldenknop en hoewel de antenne nog redelijk wat ruimte in beslag neemt, zijn RFID-tags toch behoorlijk klein. Door de geringe afmeting van RFID-tags kunnen ze onopvallend in producten of verpakkingen worden verwerkt.

2.2 Classificatie van de technologie en toepassingen

RFID is verworden tot een containerbegrip waarin een aantal verschillende categorieën is te onderscheiden. De indeling die hier gebruikt wordt is gebaseerd op technische eigenschappen en verheldert de bespreking van privacyaspecten en de kansen voor innovatie in de komende hoofdstukken. In deze notitie worden drie categorieën onderscheiden: *smart labels*, *smart cards* en *Near Field Communicatie (NFC)*.

2.2.1 Smart labels

De technologie

Wanneer over RFID wordt gesproken, wordt meestal bedoeld op smart-labels. Dat zijn labels met daarin veelal eenvoudige RFID tags, die slechts een unieke code bevatten die niet gewijzigd kan worden. Zo'n label zit op of in de verpakking, maar kan ook in het object zelf worden aangebracht. Hiermee wordt het in principe mogelijk om datgene waaraan de tag gekoppeld is te identificeren en bijbehorende informatie op te zoeken in een achterliggende database.

De maximale afstand waarop een smart label kan worden uitgelezen is ongeveer zeven meter. Het is mogelijk om de maximale leesafstand te beperken tot een paar centimeter dan wel de leesafstand te vergroten door de RFID-tag uit te rusten met een batterij. Er wordt dan wordt gesproken over een actieve tag, die in staat is op eigen initiatief een signaal uit te zenden. De leesafstand kan dan oplopen tot 100 meter. De tag wordt daardoor wel groter en duurder. Ook kan een tag uitgerust worden met een sensor, waardoor naast de identiteit ook andere informatie kan worden meegestuurd, zoals informatie over de temperatuur, de vochtigheidsgraad of de (lucht)druk

De eenvoudige tags zullen meestal aan een object gekoppeld worden, maar kunnen ook aan dieren of mensen gekoppeld worden. Meestal gebeurt dit door middel van een polsbandje, maar ook een implantaat in het lichaam is mogelijk. In de meeste gevallen vervullen deze onderhuidse implantaten dezelfde functie als de hierboven genoemde smart labels: zij vereenvoudigen het proces van identificatie, authenticatie en autorisatie doordat zij een uniek nummer bevatten dat draadloos uitgelezen kan worden. Implantaten kunnen veiliger zijn dan losse smart labels omdat ze moeilijker verloren of gestolen kunnen worden.

De toepassingen

Voor de smart-tags zijn er vele toepassingen te bedenken. Daarop zijn ook de hoge verwachtingen aangaande RFID gebaseerd. Een mogelijk toekomstig scenario is dat producten getagd worden en er een 'Internet of things' ontstaat, waarbij de getagde objecten met elkaar kunnen communiceren. Zo ver is het echter nog lang niet. Op dit moment zien we met name toepassingen in de logistiek maar ook in de agrarische- of de zorgsector. In het boekje *RFID in de praktijk*⁵ worden 35 voorbeelden van toepassingen genoemd. Een greep daaruit om een beeld van de mogelijke toepassingen te geven:

- Internationaal bekend is de supermarktketen WalMart. Zij wil dat de top 100 leveranciers hun producten op pallet en doosniveau voorzien van een RFID-tag. Men wil hiermee het voorraadbeheer verbeteren en de winkelvoorraad verkleinen.
- Een grote gebruiker is FloraHolland, die 150.000 RFID chips gebruikt voor haar logistieke proces van het verplaatsen van bloemen in containers.

⁵ RFID in de praktijk, Capgemini, 2005, p.53-60

- Retailer Hoogvliet maakt gebruik van RFID binnen zijn distributiecentrum in Alphen aan den Rijn om fouten in het logistieke proces te reduceren en de efficiency te bevorderen
- Bij het attractiepark Legoland kunnen kinderen worden voorzien van een RFID-armband waardoor het mogelijk wordt om een verdwaald kind weer snel met zijn ouders te herenigen.
- Het Australische Osborne Park Hospital heeft besloten om RFID in te zetten om de veiligheid op de kraamafdeling te vergroten en baby's te kunnen identificeren.
- Door de integratie van RFID-tags in geldzakken en RFID readers in de ontvangende geldkluizen, hoeft er geen personeel meer aanwezig te zijn bij het ontvangen van de geldtransporten van de Rabobank. Geldleveringen kunnen nu ook plaatsvinden buiten kantooruren.
- De boeken van boekhandel Selexyz vinden dankzij een RFID-tag hun weg van het nationaal distributiecentrum tot op de plank. De klant die het boek bestelde, krijgt automatisch een e-mail of sms-bericht. Personeelskosten zijn sterk verlaagd door vergemakkelijkte inventarisatie en verwerking, de service naar de klant is verhoogd.

2.2.2 Contactloze smartcards

De technologie

Contactloze smartcards zijn toepassingen waarbij een chipcard wordt uitgerust met RFID-technologie. Hierdoor wordt contactloze communicatie mogelijk. Dit in tegenstelling tot de magneetstrip op de huidige bankpassen waarbij fysiek contact moet worden gelegd. Een contactloze smartcard bevat een kleine microprocessor met een beperkt geheugen en een kleine rekeneenheid net als in de huidige bankpassen; het verschil zit in de wijze van communiceren. Omdat de smartcard een kleine microprocessor bevat is het ook mogelijk om de kaart van meer hoogwaardige beveiliging te voorzien, zoals een ingewikkelder versleuteling (encryptie).

De toepassingen

De twee toepassingen van de smart card waarmee bijna elke Nederlander te maken zal krijgen zijn de OV-chipcard en nieuwe Nederlandse reisdocumenten. Te zijner tijd zal de bovengenoemde bankpas/chipknip ongetwijfeld een draadloze variant krijgen, met de noodzakelijke strenge beveiligingseisen.

- *De OV-chipcard*

De OV-chipkaart is een nieuw betaalmiddel voor het openbaar vervoer. De kaart is even groot als een bankpas en bevat een onzichtbare RFID-chip. De kaart kan worden opgeladen met een saldo in euro's, waarmee de reiziger overal kan reizen. De OV-chipkaart is een stuk makkelijker in vergelijking met de huidige vervoerbewijzen. Met één kaart kan door heel Nederland betaald worden voor trein, bus, tram en metro.

- *Het nieuwe paspoort*

De introductie van een nieuwe 'generatie' elektronische Nederlandse reisdocumenten zal plaatsvinden op zaterdag 26 augustus 2006⁶. De reisdocumenten zijn voorzien van een RFID-chip. Er ligt een EU-verordening aan ten grondslag waarin de keuze voor een RFID-chip is gemaakt. Daarin staan de normen voor de veiligheidskenmerken en biometrische gegevens in paspoorten en reisdocumenten.

⁶ Tweede Kamer; 2004-2005, 25764 nr. 26

De chip bevat de weergave van de foto (in kleur), naam, voornamen, geboortedatum, geslacht, documentnummer, sofi-nummer (in de toekomst burgerservicenummer), datum einde geldigheid document. De chip die in de reisdocumenten wordt opgenomen wisselt, bij het uitlezen van de chip, informatie uit met de documentlezer. Zo wordt het moeilijker het document te vervalsen en ook moeilijker om zich te identificeren met een reisdocument van iemand anders. De chip heeft de bijzondere eigenschap – volgens de afgesproken standaard – dat het nummer steeds wisselt als de chip wordt “aangesproken”.

2.2.3 NFC

De technologie

Near Field Communication (NFC) onderscheidt zich van smart labels en smartcards op het punt dat deze meer mogelijkheden voor data-uitwisseling tussen tag en reader ondersteunt. NFC zal meestal deel uitmaken van een bestaand apparaat zoals mobiele telefoons of PDA's. NFC maakt twee-weg communicatie tussen label en reader mogelijk, waardoor er informatie in beide richtingen kan ontstaan. Het initiatief komt daarmee bij de gebruiker te liggen. Hij activeert zijn 'apparaat' om gegevensuitwisseling of transactie tot stand te brengen.

De toepassingen

NFC heeft tal van mogelijke toepassingen, waarvan de meeste overigens nog niet zijn gerealiseerd. De meest veelbelovende toepassingen zijn betalen met je telefoon en mobile ticketing.

- *Mobile ticketing bij Roda JC*

Roda JC draait als eerste in Nederland proef met een nieuw systeem waarbij de mobiele telefoon de functies van de (Seizoen) Club Card overneemt. Vijftig supporters gebruiken hun mobiele telefoon voor toegang tot het Parkstad Limburg Stadion en voor het doen van aankopen bij horecapunten en de fanshop.

In Amsterdam start in de herfst van 2006 een pilot-project voor betalen met de mobiele telefoon. Hierbij wordt gebruik gemaakt van door Philips en Sony ontwikkelde Near Field Communication (NFC) technologie. Tijdens de eerste fase van de pilot krijgen ongeveer honderd Amsterdammers een Nokia met NFC-chip uitgereikt. Bij een aantal winkeliers in en rond het World Trade Center wordt een betaalterminal geplaatst waar vervolgens draadloos betaald kan worden.

- *RFID wegwijzers en posters*

In de Japanse steden Uji en Shiga is onlangs een pilot gestart waarbij toeristen met behulp van RFID informatie over hun omgeving kunnen krijgen. RFID-tags worden op verschillende plekken in de stad aangebracht. Een toerist kan met behulp van een RFID-reader in zijn mobiele telefoon via de RFID-tag aanvullende informatie opvragen over de omgeving zoals de locatie van restaurants, winkels en toeristische trekpleisters.

2.3 Verwachtingen rondom RFID.

Het is belangrijk een onderscheid te maken tussen de verschillende categorieën binnen RFID. Die leiden namelijk niet alleen tot verschillende toepassingen, maar verhelderen ook andere discussies over RFID zoals die over privacy of innovatie welke in de volgende hoofdstukken nog aan de orde komen.

De laatste tijd staat RFID sterk in de belangstelling. Grote conferenties worden vanuit de EU (Europese Unie), ITU (International Telecommunications Union), OECD (Organisation for Economic Co-operation and Development) en vele anderen georganiseerd en er verschijnen talloze publicaties over dit onderwerp. Uit deze belangstelling komt soms een beeld naar voren dat RFID-technologie in een vergevorderd stadium is. Een deel van de experts verwacht dat het toepassen van RFID meer invloed op ons dagelijks leven zal hebben dan de opkomst van het Internet.

RFID is de technologie die een zogenaamd 'Internet of things' mogelijk maakt. Een wereld waarin we met meer objecten kunnen communiceren en waarin die objecten ook onderling kunnen communiceren. Er leven hoge verwachtingen over de economische voordelen die met behulp van RFID kunnen worden behaald. Die verwachtingen moeten nog wel worden waargemaakt. Op dit moment bevinden veel toepassingen zich nog in de pilot-sfeer of zijn nog slechts in de ideeënfase. Ook zijn er in de ontwikkeling op weg naar goed functionerende RFID-systemen nog een aantal hobbels van verschillende orde te nemen. Hierbij moet gedacht worden aan problemen als privacybescherming en milieu, maar ook aan het afspreken van standaarden en het daadwerkelijk op gang brengen van innovatie.

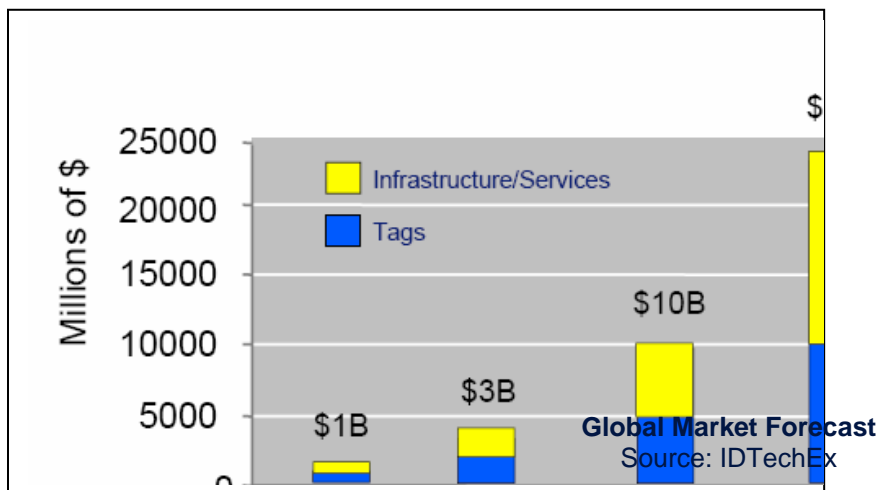
Hoofdstuk 3: Kansen voor RFID ontwikkeling in Nederland.

3.1 Groeimogelijkheden

Voor Nederland is innovatie onontbeerlijk. Daar is iedereen zich in Nederland van bewust. Nederland kan niet concurreren op lage lonen maar wel op innovativiteit. De afgelopen vier jaar heeft de regering het belang van innovatie benadrukt door het inrichten van het InnovatiePlatform.

De innovatie zit niet alleen in verbeteringen in de technologie zelf, die kleiner, slimmer, goedkoper, energiezuiniger wordt. Deze verbeteringen zorgen juist dat veel meer toepassingen binnen bereik komen. Deze nieuwe toepassingen vormen een groot deel van de innovatie die door RFID teweeg wordt gebracht. Anders gezegd: RFID is een ook enabling technology, het is een ‘grondstof’ voor andere innovaties.

De internationale ontwikkelingen voor RFID zijn zeer veelbelovend. De komende jaren wordt een doorgaande groei verwacht. Het is daarom belangrijk voor het Nederlands bedrijfsleven gebruik te maken van de kansen die deze ontwikkelingen biedt. Uiteraard ligt daarvoor de verantwoordelijkheid grotendeels bij het bedrijfsleven zelf. De overheid voert innovatiebeleid om de mogelijkheden te vergoten. In paragraaf 3.2 wordt de innovatie in de drie soorten RFID geschetst, in paragraaf 3.3 volgt een kort overzicht gegeven van het Nederlandse innovatiebeleid, met de relevantie voor RFID en in 3.4 volgen de conclusies.



Figuur 2. Verwachte omzetgroei van de RFID-markt tot 2015.

3.2 Innovatie bij de drie soorten RFID

In dit hoofdstuk wordt de driedeling *smartlabels*, *smartcards* en *NFC* gevolgd eerder die in hoofdstuk 2 is gemaakt.

RFID-tags: grote verwachtingen en concrete toepassingen

Innovatie op het gebied van RFID-tags wordt gedreven door twee perspectieven. Enerzijds het perspectief van de hoge verwachtingen van wat RFID mogelijk zou kunnen maken en anderzijds vanuit het perspectief van de concrete toepassingen in het hier en nu.

De hoge verwachtingen van RFID zijn vaak gekoppeld aan grootschalige toepassingen van RFID-tags. Het idee is dat we naar een wereld gaan waar alles 'getagd' is. Dat er een 'internet of things' ontstaat waar alle 'dingen' met elkaar kunnen 'communiceren'. Deze verwachtingen geven ruimte voor het doen van vernieuwend onderzoek, op zoek naar vernieuwende innovaties, bijvoorbeeld aan universiteiten of in onderzoeksprogramma's. Een voorbeeld hiervan is het onderstaande onderzoek:

TNO stuurde in de eerste maanden van 2006, in het kader van het MarcoPolog project een aantal proefpersonen op pad door Den Haag om een interactief digitaal reisverslag te maken met een UMTS-mobieltje, een zakcomputer, een GPS-ontvanger en een RFID-leespen, die voortdurend met elkaar en de buitenwereld in verbinding stonden. Met behulp van deze apparatuur maakte zij foto's, filmpjes en spraakopnames, en ze kregen achtergrondinformatie over objecten die zij in de musea bekeken. MarcoPolog is gebaseerd op een Personal Network, een technologie die verschillende privé-netwerken van eindgebruikers met elkaar verbindt zelfs als de gebruiker erg mobiel is. MarcoPolog is ontwikkeld door het Freeband-project PNP2008, dat tot doel heeft het concept van Personal Networks verder te ontwikkelen met een aantal realistische demonstrators.

Niet alleen verwachtingen zijn een motor voor innovatie, ook pogingen RFID in de praktijk toe te passen vragen om innovatiekracht. Vaak vindt die toepassing alleen binnen het eigen bedrijf plaats, omdat het gebruik over bedrijfsgrenzen heen complex is. Een interessant voorbeeld, waar dat wel geprobeerd wordt is de pilot Versschakel, de winnaar van de RFID-innovatieprijs 2005. In deze pilot worden kratten 'getagd' waarin verse groente vervoerd worden.

Vers Schakel

Vers Schakel is een project waarin Schuitema, Heemskerk, het Centraal Bureau Levensmiddelenhandel, KPN, Capgemini en Wageningen Universiteit ervaring opdoen met de toepassing van RFID-technologie in het logistieke proces van verse gesneden groenten. Omdat binnen het project RFID in combinatie met temperatuursensoren wordt gebruikt is het niet alleen mogelijk om de groenten door de hele keten te volgen, maar ook om de temperatuur vast te leggen waaraan de groenten hebben blootgestaan. Met deze informatie kan de versheid van de groenten beter gegarandeerd worden.

Smart cards: grote projecten

Met name smart cards voor simpele toepassingen (toegangspasje) zijn al een tijd in gebruik. Meer innovatieve toepassingen van de smart card op het gebied van veiligheid, betalingsverkeer en (openbaar) vervoer komen nu grootschalig binnen bereik. De introductie vindt zowel door private partijen als de overheid plaats. Hoewel de overheid de projecten niet uitvoert met een innovatief oogmerk, zullen grootschalige toepassingen ongetwijfeld innovatiemogelijkheden opleveren.

Near Field Communication: de grote jongens

Voor NFC is de RFID-chip meestal opgenomen in een apparaat, zoals de mobiele telefoon of een PDA. De meeste toepassingen worden dan ook ontwikkeld door bedrijven die zulke apparaten produceren. Zo werken Philips, Nokia en Sony samen om het gebruik van 'touch-based' interactie in consumenten-electronica, mobiele telefoons en PC's, slimme objecten te faciliteren. Een deel van de innovatie gaat over standaardisatie en interoperabiliteit. Philips heeft in de stad Caen een proef lopen, waar mensen met hun mobiele telefoon kunnen betalen, openbaar vervoer informatie kunnen krijgen bij de bushalte of een trailer kunnen downloaden van een film als ze bij de bioscoop een keuze uit het aanbod willen maken.

3.3 Innovatiebeleid in Nederland

Voordat we ingaan op de vraag of het innovatieve klimaat ten aanzien van RFID verder zou moeten worden versterkt, volgen nu eerst enkele algemene noties over het Nederlandse innovatiebeleid. In grote lijnen kunnen er vier vormen van innovatiebeleid waarin de overheid een rol heeft worden onderscheiden:

- Het bevorderen van innovatief onderzoek.
- Het ondersteunen van innovatie in het MKB.
- Het bundelen en versterken van innovatieve sectoren.
- Innovatie op inhoud.

Voor alle vier heeft de overheid verschillende instrumenten om dit te ondersteunen.

1. Innovatief onderzoek

Veel innovatie vindt zijn oorsprong in onderzoek. Op het gebied van RFID varieert dat onderzoek van technisch onderzoek naar de werking van de chip en de antenne, tot het verkrijgen van kennis over praktijktoepassingen. Vanuit de overheid stroomt er onderzoeksgeld naar de universiteiten dat onder andere wordt aangewend voor RFID-onderzoek. Zo vindt er op de drie Technische Universiteiten, de Radboud Universiteit en de Vrije Universiteit onderzoek naar RFID plaats. Ook lopen er subsidieprogramma's voor innovatief onderzoek. Een belangrijk voorbeeld in de afgelopen jaren zijn de BSIK-programma's, zoals Smart-surroundings en Freeband (programma Marcopolog), waar consortia van onderzoeksinstituten en bedrijven samenwerken aan innovatief onderzoek.

Met TNO beschikt Nederland over een onderzoeksinstituut dat toegepast onderzoek doet. Voor RFID is TNO-ICT het meest relevante instituut. Er loopt een groot aantal activiteiten op het gebied van RFID, waaronder RFID voor Schiphol, RFID in de logistiek en RFID in de zorg. Ook is er onderzoek gebundeld in topinstituten, het Telematica Instituut in Twente doet werk op het gebied van RFID.

2. Innovatie in het MKB

Voor de ondersteuning van het MKB zijn er verschillende subsidieregelingen die grotendeels via SenterNovem lopen. Het uitdagingskrediet is bedoeld voor excellente innovatieprojecten in het MKB. De WBSO⁷ is een fiscale stimuleringsregeling waarmee een deel van de loonkosten voor R&D kan worden vergoed. Met de innovatievouchers kan voor een bepaald bedrag kennis worden ingekocht. Deze regelingen zijn niet specifiek gericht op RFID, maar wel op innovatie.

⁷ De WBSO is een fiscale stimuleringsregeling die een deel van de loonkosten voor speur- en ontwikkelingswerk (S&O), vergelijkbaar met Research and Development (R&D), compenseert.

Van 2004 tot en met 2006 hebben zo'n 100 ondernemers gebruik gemaakt van de WBSO met een project waarin RFID een rol speelde, waarbij de grote dienstverleners in de meerderheid waren (check). Bij elkaar ging het om een subsidiebedrag van ongeveer één miljoen op een totaal van 400 miljoen euro.

Syntens is een innovatienetwerk voor MKB-ondernemers. Zij hebben bij verschillende toepassingen van RFID geadviseerd. Er is ook on-line workshop over RFID ontwikkeld⁸. Een voorbeeld van een advies is het volgende:

RFID in de band

In de Verenigde Staten zijn grote bandenfabrikanten al bijna klaar met het testen van RFID-tags in buitenbanden. Naar aanleiding van deze ontwikkelingen heeft Vereniging VACO met behulp van Syntens en PreventNet B.V. een onderzoek laten uitvoeren naar de toepassingsmogelijkheden voor VACO-leden. Het onderzoek is verricht bij bedrijven uit de VACO-sectoren Landbouw en Industrie die banden fabriceren en/of verkopen. Alle bedrijven hebben te maken met omvangrijke en vaak complexe (internationale) logistieke stromen die middels RFID-technologie sterk vereenvoudigd kunnen worden.

Voordelen voor VACO-leden zijn onder andere: snellere en nagenoeg foutloze bandenregistratie bij ingang/uitgang, effectievere voorraadbeheer en antidiefstaltoepassingen. Een belangrijk nadeel is dat er momenteel nog weinig informatiesystemen beschikbaar zijn die 'plug & play' aangesloten kunnen worden op een RFID-systeem.

3. Innovatieprogramma's

Op dit moment wordt het innovatiebeleid binnen EZ herijkt. Centraal staat de gedachte dat focus en massa wordt aangebracht in de activiteiten en subsidies. EZ kiest daarom voor een programmatische aanpak op een aantal belangrijke thema's. Vraagsturing en maatwerk staan daarbij voorop. Bedrijven en samenwerkingsverbanden van bedrijven, kennisinstellingen en lokale overheden kunnen projectvoorstellen indienen. Een aantal van deze thema's is al gekozen (mede op basis van het werk van het InnovatiePlatform). Het gaat om de thema's Food en Flowers, High Tech Systemen & Materialen en Water en waarschijnlijk ook Chemie en Life Sciences & Gezondheid. Gewerkt wordt nog aan verschillende initiatieven, zoals Fresh on Demand, om bederf in de voedselketen terug te dringen, Innovatie in de Logistieke en mogelijk 'Innovatie in de Diensten'. Geen van deze innovatieprogramma's heeft RFID-innovatie als doel, maar bij een aantal zal RFID de meest geschikte technologie zijn om bepaalde innovatieve doelen te bereiken

4. Innovatie op inhoud

Naast deze activiteiten vanuit het innovatiebeleid speelt de overheid soms ook een innovatieve rol vanuit een inhoudelijke behoefte aan verbetering. Eerder kwamen al het paspoort en de OV-chipcard naar voren. Het grootschalig in gebruik nemen daarvan is een doorbraak voor RFID-toepassingen en voor overheid een mogelijkheid om een maatschappelijk probleem op te lossen. Dat is ook de kern van het zojuist gestarte programma Maatschappelijke sectoren & ICT. Hier draait het om de opschaling van ICT-pilots tot daadwerkelijke toepassingen die een bijdrage leveren aan het oplossen van maatschappelijke problemen in de sectoren mobiliteit, zorg, veiligheid en onderwijs. Een interessant voorbeeld van innovatie op inhoud is onderstaande, gestimuleerd door het ministerie van VWS.

⁸ <http://www.syntens.net/workshop/nd/index.html>

RFID in de zorg

Op verzoek van het Ministerie van VWS en met steun van het Ministerie van EZ is Capgemini in 2005 een onderzoek gestart naar de toepassingsmogelijkheden van RFID in de gezondheidszorg. Capgemini doet dit onderzoek samen met het Academisch Medisch Centrum (AMC), Geodan, Intel en Oracle. Het project bestaat onder andere uit drie pilots die de toegevoegde waarde van RFID in de zorgpraktijk moeten aantonen. Zo wordt RFID gebruikt voor personenidentificatie en –lokalisatie rond de operatiekamer (OK) om het zorgproces in kaart te brengen, voor het tracken en traceren van OK-materialen als implantaten en disposables met een hoge kostprijs en omloopsnelheid en tenslotte voor tracken en traceren van bloedproducten met behulp van temperatuurgevoelige RFID-tags.

3.4 Conclusies

We zien dat op het gebied van NFC grote bedrijven voorop lopen met bedrijven als Philips en Nokia in een voortrekkersrol. Bij de smartcard vindt op dit moment grootschalige toepassingen plaats bij het paspoort en de OV-chipkaart. Bij RFID-labels is een onderverdeling gemaakt tussen innovatie op basis van verwachtingen en op basis van concrete toepassingen. Op het vlak van verwachtingen, (fundamenteel) onderzoek lijkt Nederland vrij goed uitgerust (zie ook citaat TI hieronder), hoewel tegenstemmen wijzen op de overtekening van FES-fondsen en de Smartmix.

Op het gebied van toepassingen en pilots lijkt er een leemte te bestaan. De invoering van RFID-toepassingen gaat niet zonder horten of stoten. Er komen signalen (onder andere via RFID-Nederland), dat er behoefte is aan mogelijkheden om nieuwe toepassingen te testen en kennis hierover te delen. Ook één van de aanbevelingen van GSI op het gebied van standaardisatie aan de technologiecommissie van de Tweede Kamer gaat in die richting. Het is daarom verstandig te onderzoeken of er inderdaad behoefte is aan testmogelijkheden voor RFID of dat de bestaande mogelijkheden voldoen. Er zal moeten worden aangesloten bij het innovatiebeleid zoals de Nederlandse overheid dat voorstaat.

“Daarnaast heeft Nederland een zeer goede kennisinfrastructuur waarin in ruime mate financiële middelen voorhanden zijn om innovatief RFID-onderzoek te doen. De mogelijkheden van RFID kunnen verkend worden en oplossingen van knelpunten kunnen uitgebreid worden uitgedacht en getest. In onderzoeksprojecten binnen verschillende BSIK programma's zoals Freeband en Smartsurroundings komt RFID aan de orde als bruikbare technologie voor innovatieve toepassingen. De goede verankering van Nederlandse onderzoeksinstituten en universiteiten in Europese onderzoekskaders kan helpen bij het definiëren van RFID gerelateerde onderzoeksprojecten en opzetten van internationale consortia.”

RFID: Kans of bedreiging, Telematica Instituut, 2005, p.22

“De ontwikkelde en nog te ontwikkelen standaards voor RFID zijn het resultaat van het op elkaar afstemmen van toepassingswensen en technologische ontwikkeling. Het uitvoeren van testen in een operationele omgeving speelt daarbij een belangrijke rol. Steun van de overheid voor het mogelijk maken van testprojecten is daarbij zeer welkom.”

Aanbevelingen GSI Nederland, 18-4-2006

Hoofdstuk 4: Zorgen rond RFID ontwikkeling in Nederland.

4.1 Privacy

4.1.1 De risico's

Bij de toepassing van RFID-technologie is sprake van al dan niet vermeende privacyrisico's. Zo kunnen RFID-tags ongemerkt op afstand worden gelezen. Bovendien worden de RFID-tags steeds kleiner en kunnen ze worden verwerkt in producten of op de verpakking van producten. Daarnaast is het is voor een consument niet altijd duidelijk of een product een RFID-tag bevat. Hierdoor kan het voor de consument onduidelijk zijn of hij RFID-tags bij zich draagt en zo ja of de informatie op deze RFID-tags informatie over hem overdraagt aan hem onbekende personen of instanties. De meest gehoorde privacyrisico's zijn:

Volgen van mensen

RFID-systemen maken het in theorie mogelijk om mensen te volgen. RFID-tags maken het immers mogelijk om een individueel product te volgen. Wanneer een consument een product bij zich draagt waarvan de RFID-tag kan worden uitgelezen ontstaat er een privacyrisico. Op dat moment kan deze persoon namelijk in theorie gevolgd worden aan de hand van het artikel dat hij of zij bij zich draagt.

Categoriseren van mensen

RFID-systemen maken het mogelijk om een grote hoeveelheid informatie te verzamelen. De informatie die deze systemen verzamelen worden opgeslagen in een achterliggende database. Wanneer deze informatie kan worden gekoppeld aan persoonsgegevens kan deze informatie worden gebruikt om bepaalde kenmerken van een individu in kaart te brengen. Een dergelijk profiel kan vervolgens worden aangewend om een beter inzicht te krijgen in het gedrag van individuele personen. Deze informatie kan bijvoorbeeld worden gebruikt om onderscheid te maken tussen verschillende categorieën consumenten.

Dit categoriseren van mensen is bij het uitvoeren van overheidsbeleid of bij marketing van producten overigens een gebruikelijke en bekende methode en ook algemeen aanvaard, mits dit op een deugdelijke grondslag gebeurt. Soms is daar expliciet toestemming voor nodig van de betrokken personen. Bij RFID-technologie is het voor de consument niet duidelijk wie de informatie kan lezen en wat daar vervolgens mee gebeurt.

Persoonsinformatie uitlezen

Een ander risico dat vaak genoemd wordt is de mogelijkheid om met bijvoorbeeld een draagbare reader op afstand in huizen of boodschappentassen van mensen te "kijken". Dit zou het voor kwaadwillenden mogelijk kunnen maken om door middel van de aldus verkregen informatie heel doelgericht in te breken of mensen te beroven.

4.1.2 Evaluatie van de privacyrisico's

Zoals gezegd is RFID een containerbegrip voor meerdere technologieën die ieder meerdere toepassingen kennen. De specifieke toepassing bepaalt in hoeverre de mogelijke privacyrisico's daadwerkelijk tot problemen leiden. De privacyrisico's worden besproken aan de hand van de eerder geïntroduceerde classificatie van de technologie.

Near Field Communication (NFC)

NFC kent de minste privacyrisico's. Dit komt omdat de maximale leesafstand beperkt is tot enkele centimeters. Het is dus niet mogelijk om op grotere afstand ongemerkt contact te leggen. Daarnaast kan bij een apparaat dat is uitgerust met een NFC functie deze functie altijd worden uitgeschakeld. Omdat er toch enig risico bestaat is het ook bij NFC belangrijk dat er een voldoende niveau van beveiliging wordt aangebracht, zodat de op het apparaat opgeslagen persoonsgegevens niet kunnen worden uitgelezen zonder de expliciete toestemming van de eigenaar.

Smartcards

In veel gevallen zal een smartcard persoonsgegevens bevatten. Het nieuwe paspoort is hier een voorbeeld van. Een goede beveiliging is dus essentieel. Er zijn veel technische mogelijkheden om smartcards te beveiligen. De extra kosten die hiermee gemoeid zijn vormen meestal geen belemmering, omdat smartcards op zich al een relatief kostbare toepassing vormen van de RFID-technologie.

Smartlabel

Zoals in hoofdstuk 2 is uiteengezet bevatten smartlabels geen persoonsgegevens, maar alleen een unieke code die het product identificeert. De verwachting is dat in de toekomst smartlabels op grote schaal zullen worden toegepast. Voor de beoordeling van de privacyrisico's van smartlabels is het van belang of de smartlabels wel of niet in de handen van de consument komen. Op dit moment worden in de logistieke sector met name containers of grootverpakkingen van een smartlabel voorzien. Zolang er nog geen smartlabels op individuele producten zitten is er geen sprake van privacyrisico's. Pas als consumenten producten met smartlabels in hun bezit krijgen kunnen bepaalde privacyrisico's realiteit worden. Meer specifiek valt over de onderscheiden privacyrisico's het volgende op te merken:

- *Volgen van mensen*

Om mensen in de openbare ruimte met RFID-tags te kunnen volgen moet aan twee voorwaarden worden voldaan. Ten eerste moet er een zeer dicht netwerk van readers aanwezig zijn. Immers, zoals aangegeven is (de maximale afstand waarop een eenvoudige RFID-tag kan worden uitgelezen is ongeveer 7 meter), of de readers moeten zeer strategisch staan opgesteld. Dergelijke netwerken zijn er op dit moment niet. Als een dergelijk netwerk in de toekomst wel zou ontstaan, moet nog aan een tweede voorwaarde worden voldaan, namelijk dat diegene die iemand wil volgen ook toegang heeft tot de systemen en de achterliggende databases. De RFID-tag zendt immers slechts een unieke code uit, geen persoonsgegevens. Een eventuele koppeling met persoonsgegevens kan alleen door koppeling van verschillende systemen en bestanden tot stand worden gebracht. Het is niet te verwachten dat één persoon of organisatie toegang zal hebben of zelfs kunnen krijgen tot allerlei losse systemen die in bezit en beheer zijn bij andere organisaties. Ter relativering overigens nog het volgende: in vergelijking met de theoretische mogelijkheid om iemand op basis van RFID-tags te volgen, is het op dit moment ook al technisch mogelijk om iemand via zijn of haar mobiele telefoon te volgen.

Het volgen van mensen in een besloten ruimte, bijvoorbeeld medewerkers in een bedrijf door middel van een werknemerspas, is wel mogelijk en soms ook de reden van het gebruik van RFID. Zo weet men bijvoorbeeld waar een arts zich in het ziekenhuis bevindt. Hieraan zitten uiteraard privacy-aspecten die binnen de bedrijfsomgeving besproken kunnen worden.

- *Categoriseren van mensen*

Met het categoriseren van mensen wordt bedoeld dat er op basis van verzamelde data een profiel van een persoon kan worden aangemaakt. Om een interessant profiel op te stellen moet er meer informatie beschikbaar zijn dan alleen een uniek nummer van een product dat een persoon bij zich draagt; men moet dan ook over persoonsgegevens beschikken. Alleen de eigenaar van de database is daartoe in staat. De angst dat bedrijven een profiel van hun klanten maken is overigens niet nieuw. Met de komst van digitale kassa's, klantenkaarten en elektronisch betalen bestaat deze mogelijkheid al geruime tijd. De komst van RFID betekent alleen dat er (nog) meer data beschikbaar komen. Op deze data zijn dezelfde privacy-regels van toepassing als op de klantenkaarten en dergelijke.

- *Persoonsinformatie uitlezen*

Deze risico's, zoals het op afstand kunnen "lezen" welke goederen een persoon bij zich draagt dan wel zich in een huis bevinden, worden pas actueel indien RFID-technologie op grote schaal wordt gebruikt. Op dit moment zijn er bijvoorbeeld nog weinig tot geen consumentengoederen die voorzien zijn van een RFID-tag. De meeste RFID-tags die in omloop zullen komen bevatten alleen een uniek nummer. De verdere gegevens staan in een database die wordt beheerd door diegene die het product gemaakt en/of verkocht heeft. Als deze database voldoende is beveiligd, levert het uitlezen van een RFID-tag dus geen informatie op over het product waar de tag aan is bevestigd.

Concluderend

Concluderend kan worden gesteld dat er privacy-risico's aan RFID-technologie zijn verbonden, maar ook dat deze niet zo gemakkelijk en groot zijn als soms wel wordt beweerd. Het volgen van mensen kan eigenlijk alleen binnen een besloten omgeving. Het maken van een (consumenten)profiel is niet gemakkelijk omdat voor de noodzakelijke verbinding van een RFID-nummer en een persoonsgegeven er toegang moet zijn tot meerdere databases. Het uitlezen van de informatie van een RFID-tag is niet snel naar personen te traceren. Essentieel in alle gevallen is de verbinding aan persoonsgegevens. In de volgende paragraaf wordt gezien hoe de risico's daarvan beperkt kunnen worden.

4.1.3 Beperken van privacyrisico's

De kern van de beschreven privacyrisico's is het onrechtmatig gebruik van persoonsgegevens. Dit onrechtmatige gebruik kan zowel bewust als onbewust plaatsvinden. Er is een aantal mogelijkheden om onrechtmatig gebruik van persoonsgegevens te voorkomen of te beperken. Het kader vormt de privacywetgeving. Zelfregulering, technologie en bewustwording zijn effectieve methoden om de risico's te beperken.

Wetgeving

Het wettelijke kader is de Europese dataprotectie richtlijn die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens (WBP). Het toezicht op de WBP is opgedragen aan het College Bescherming Persoonsgegevens (CBP). De WBP geeft aan wanneer er sprake is van een persoonsgegeven en wat daar vervolgens mee mag gebeuren. De

wet geldt voor de verwerking van gegevens van 'natuurlijke personen'. Het is overigens niet verboden persoonsgegevens te verwerken. In veel gevallen is het verwerken van persoonsgegevens zelfs noodzakelijk, bijvoorbeeld om een transactie te kunnen doen of een product te kunnen leveren. Wel moet er een goede grondslag zijn voor de verwerking van persoonsgegevens. Is een dergelijke grondslag niet aanwezig, of worden de gegevens voor een ander doel gebruikt dan waarvoor zij oorspronkelijk zijn verkregen, dan is de verwerking in strijd met de wet.

De WBP is technologie-neutraal geformuleerd en geeft dus geen kant-en-klaar antwoord op vragen aangaande RFID en privacy. heeft in haar studie naar privacy geconcludeerd dat het Vooralsnog wordt aangesloten bij deze conclusie, waarbij de vraag van het toezicht nog niet is beantwoord. Het CBP is voornemens na de zomer van 2006 met een nota over RFID te komen, waarin zowel de toepasbaarheid van de wetgeving als de mogelijkheden van toezicht aan de orde zullen komen.

De relatie RFID en privacy wordt ook besproken in de artikel 29 werkgroep binnen de EU. De Artikel 29 werkgroep is het onafhankelijke overlegorgaan van alle Europese nationale privacytoezichthouders. Nederland wordt hierin vertegenwoordigd door het CBP. De groep adviseert de Europese Commissie over privacykwesties. Binnen de werkgroep vindt ook afstemming en harmonisatie van nationaal beleid plaats. In januari 2005 heeft de werkgroep een eerste publicatie uitgebracht op het gebied van RFID⁹. In deze publicatie heeft als doel om toepassers en producenten van RFID-technologie te adviseren over de relatie met de data protectie richtlijnen¹⁰ en de richtlijn voor privacy en elektronische communicatie¹¹. De artikel 29 werkgroep ziet dit document als een eerste verkenning van de situatie en zal RFID in de toekomst nauwlettend volgen en verdere adviezen uitbrengen wanneer nodig.

Zelfregulering

Een tweede instrument na wetgeving is zelfregulering door de partijen die gebruik maken van RFID-technologie. Het bedrijfsleven zal immers alleen profiteren van de mogelijkheden van RFID als de consumenten deze technologie accepteren. Het is dus in het belang van het bedrijfsleven dat zij op een zorgvuldige manier omgaan met het invoeren en gebruiken van RFID. Een slordig opgezette pilot met RFID door het Duitse supermarktconcern Metro leidde bijvoorbeeld tot flinke demonstraties voor de pilotwinkel. Bij het bedrijfsleven bestaan initiatieven om te komen tot gemeenschappelijke afspraken. ECP.nl heeft gewerkt aan een gedragscode en GS1, de organisatie achter EPCglobal, publiceert guidelines over hoe RFID op een verantwoorde manier ingezet kan worden. Gezien de diversiteit van de gebruikers is het niet gemakkelijk afspraken te maken waarmee iedereen kan instemmen. Ook functioneren guidelines en gedragscodes op basis van vrijwilligheid. Toch kunnen ze een nuttige (voorbeeld)functie vervullen.

Technologie

Er zijn veel technologische mogelijkheden voor het beveiligen van RFID-technologie. Eerder is al de RFID-tag op het paspoort genoemd, die pas werkt als het paspoort geopend is. De informatie op de chip zelf kan ook beveiligd worden met encryptie. De RFID-tag kan dan wel worden uitgelezen, maar de informatie is onleesbaar. Ook de communicatie tussen de RFID-

⁹ Article 29 Data Protection Working Party; Working Document on data protection issues related to RFID technology. 10108/05/EN

¹⁰ Directive 95/46/EC 24 October 1995

¹¹ Directive 2002/58/EC 12 July 2002

tag en het leesapparaat kan worden versleuteld. Hierdoor is het alleen voor een geautoriseerd leesapparaat mogelijk om de RFID-tag uit te lezen.

Dit type oplossingen worden ook wel privacy-by-design oplossingen genoemd en kunnen in aanvulling op privacy-wetgeving een krachtig instrument vormen. De privacy wetgeving kan immers bewust of onbewust overtreden worden en brengt handhavinglasten met zich mee. Door “privacy by design” wordt de kans op overtredingen aanzienlijk gereduceerd.¹²

Transparantie

Privacyrisico's ontstaan wanneer partijen bewust of onbewust op een onrechtmatige manier met de door hun verzamelde informatie omgaan. In het algemeen is voor het voorkomen van zorgen over privacy transparantie een sleutelbegrip. Het gebruik van RFID en met name de verwerking en het bewaren van gegevens die RFID genereert, moet voor iedereen op een begrijpelijke manier inzichtelijk gemaakt kunnen worden.

4.2 Veiligheidsrisico's

Elke technologie heeft zijn kwetsbaarheden en bij een nieuwe technologie worden die vaak pas geleidelijk aan ontdekt en zo mogelijk hersteld. De technische kwetsbaarheid van RFID systemen kan liggen in de drie verschillende onderdelen van het systeem. Hieronder wordt een kort overzicht gegeven van de verschillende mogelijkheden om een RFID systeem te verstoren.

4.2.1 veiligheidsrisico's per onderdeel

De tag

RFID-tags kunnen bewust door iemand kapot gemaakt of verwijderd worden. Dit kan door het verzenden van hoog frequentie signalen waardoor de tag ‘doorbrandt’ of door het verzenden van deactivateercodes. In theorie is ook het kopiëren of *klonen* van een RFID-tag mogelijk. Een tag die gebruikt wordt voor het vaststellen van de authenticiteit van een object, persoon of product kan op een ander object, persoon of product worden bevestigd zodat het op het origineel lijkt. Tenslotte kan een tag worden afgeschermd van het radiosignaal van de reader. Dit kan zowel positief (bescherming van de privacy van de drager van een paspoort) als negatief (winkeldiefstal) worden toegepast.

De reader

De reader in het RFID-systeem kan theoretisch gezien op verschillende manieren, bewust en onbewust, verstoord worden. Voorbeelden van het bewust verstoren van de communicatie tussen tag en reader zijn: het verzenden van versturende radiogolven (*jammen* van reader), het ongeoorloofd uitlezen van de RFID-tags (*skimming*) en het afluisteren van de verzonden informatie tussen tag en reader (*eavesdropping*)

De database

De data die door een RFID-systeem worden verzameld, worden opgeslagen in een database. Het is mogelijk dat partijen zich op onrechtmatige wijze toegang verschaffen tot deze database. Onlangs kwam uit een onderzoek van de Vrije Universiteit naar voren dat het de onderzoekers was gelukt in een door henzelf gecontroleerde testomgeving een RFID-systeem te besmetten met een virus. In deze testomgeving was het gelukt om de achterliggende database te compromitteren. Omdat RFID een toepassing is binnen een technologische infrastructuur is het voor een goede beveiliging noodzakelijk ook te kijken naar de andere

¹² Jeroen Terstegge, Toepassingen en toekomst van RFID, in: Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen, Zwenne, G.J. en B. Schermer (red)

onderdelen van dit systeem. Databases en logistieke systemen zullen, net als dit nu al het geval is, moeten worden beschermd voor vijandige aanvallen, zoals virussen, hackers, etc. –

De hiervoor genoemde manieren om RFID-systemen te verstoren of te gebruiken voor criminele doeleinden zijn veelal strafbaar volgens de Nederlandse wet. Uitzonderingen zijn het uitlezen van onbeveiligde tags (geen strafbepaling) en het afluisteren van onbeveiligde RFID-signalen. Meestal zullen deze weinig interessante informatie bevatten.

De meest interessante informatie is in principe in de achterliggende databases te vinden. Misbruik zal in veel gevallen op deze databases, die op meerdere plekken beschikbaar kunnen zijn, zijn gericht. In deze gevallen gaat het dus niet zozeer om nieuwe strafbare gedragingen, maar om ‘gewone’ computercriminaliteit.¹³

4.2.2 Beperken van veiligheidsrisico's

Er zijn verschillende mogelijkheden om de werking van een RFID-systeem te verstoren. Naarmate de technologie breder wordt ingezet, worden de risico's daarvan groter. Het bedrijfsleven (fabrikanten en toepassers van RFID technologie) en de overheid moeten samen werken aan een veilige invoering van deze technologie, door te werken aan certificering en universele standaarden en normen, die een hoge mate van beveiliging in de systemen voorschrijven.

Concluderend

De vraag of RFID voldoende is beveiligd kan niet zonder meer met ja of neen worden beantwoord. Het hangt van de specifieke toepassing af of er een hoog niveau van veiligheid nodig is. Niet voor alle toepassingen is een hoog niveau van beveiliging nodig. De verantwoordelijkheid voor de beveiliging van toepassingen in het private domein ligt primair bij de private partijen die een RFID toepassing implementeren. Het is in het belang van het bedrijfsleven zelf dat de technologie robuust is. In het geval van publieke toepassingen is het belangrijk dat deze aan de burger ‘opgelegde’ toepassing ook veilig is en de overheid dient hierop alert te zijn.

Betere beveiliging van de RFID-systemen kan door de overheid gestimuleerd worden door actief te sturen op certificering, standaardisatie en normalisatie, vooral wanneer zij zelf als toepasser van RFID optreedt (zoals dit bij het nieuwe paspoort het geval is) of door dit uit te dragen via gremia als de Europese Commissie en de NEN (CEN).

¹³ Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen. (Nederlandse Vereniging voor Informatietechnologie en Recht NVvIR). Hoofdstuk 7, pag 95.

4.3 Milieu en Gezondheid

De volgende paragrafen zullen ingaan op twee andere zorgen rondom RFID. De eerste paragraaf geeft uitleg over de relatie tussen RFID en elektromagnetische straling. De tweede paragraaf gaat in op de mogelijke milieubelasting van RFID-toepassingen.

4.3.1 RFID en elektromagnetische velden

RFID systemen maken gebruik van elektromagnetische velden (EMV). EMV is, net zoals het zichtbare licht, een vorm van niet-ioniserende straling. Omdat EMV door sommigen wordt geassocieerd met ioniserende straling zoals dat van kernenergie is (die zoals algemeen bekend is wel degelijk gevaarlijk is), wordt ook aan RFID makkelijk een gezondheidsissue verbonden. Een groot verschil is echter dat ioniserende (nucleaire) straling wel de biologische celstructuren kan veranderen. Niet-ioniserende radiofrequente stralingsvormen, die een miljoenste tot een miljardste deel van de energie-inhoud daarvan hebben, kunnen celstructuren beslist niet veranderen.

Radio-toepassingen die frequenties boven 100 kHz gebruiken kunnen opwarming van het lichaam veroorzaken. Teveel opwarming van het lichaam kan schadelijk zijn. RFID creëert over het algemeen echter uiterst zwakke veldsterktes.

Naar emv-gezondheidsgevolgen van specifiek RFID is nog niet veel onderzoek gedaan; dat is ook lastig omdat nog een beperkt aantal voorbeelden van dergelijke producten op de markt is, en men dus ook nog niet weet wat relevant is om precies te onderzoeken (qua toegepaste frequentie, veldsterkte, modulatie, blootstellingsduur, onderzoeks-eindpunten enz). Dat onderzoek en die normstelling¹⁴, parallel aan de RFID-ontwikkeling zelf, is in het internationale speelveld overigens wel snel in opkomst.

Tav blootstelling is het leesapparaat (zie hoofdstuk 2) dat em-velden verspreidt.. De chip (tag) zendt normaliter niet. Het leesapparaat kan de chip/tag activeren die dan op een kort moment een signaal naar het leesapparaat terugstuurt.

Ten aanzien van allerlei toepassingen die EMV emitteren zijn in de afgelopen jaren al duizenden onderzoeken uitgevoerd naar de effecten daarvan op de gezondheid.¹⁵ Daardoor is er al een enorme brede kennis op dit vlak, wat voor een flink deel ook prima toepasbaar is op rfid. Voor de algemene bevolking zijn risico-situaties vooralsnog onwaarschijnlijk; er wordt op uiterst zwakke vermogens gewerkt en de blootstellingstijden zijn kort.

Voor rfid toegepast in werksituaties is waarschijnlijk wat meer beschouwing aangewezen, i.v.m. de mogelijke aanwezigheid van meer en sterkere leesapparaten, en grotere nabijheid aan werkenden daarvan. Werkenden kunnen zich daarnaast langere tijden in dergelijke velden bevinden (logistieks sector en goederen-handling). In 2004 is in Brussel de richtlijn EMV voor werkenden vastgesteld. Deze richtlijn dient in 2008 in Nederland te zijn geïmplementeerd. Overigens is het ook nu al zo dat de werkgever die voor zijn werkenden Risico Inventarisatie- en Evaluaties moet opstellen daarbij ook emv in de beschouwing¹⁶ moet meenemen, en indien aan de orde, maatregelen moet nemen, bijvoorbeeld instructies voor het betrachten van afstand tot een bron.

14 ICNIRP (The International Commission on Non-Ionizing Radiation Protection) Statement; Health Physics, August 2004, volume 87, Number 2

15 Zie de WBLDB-onderzoeksdatabase www.femu.de

¹⁶ Bijvoorbeeld moet dan worden gelet op medewerkers met medische implantaten, zoals pacemakers en metalen pennen in botten, indien zij in de buurt van RFID-lezers werken. Overigens kennen deze implantaten nu reeds een immuniteit tot 10v/m. Heel waarschijnlijk zijn ook hier risico's niet te verwachten.

In algemene zin geldt dat partijen die radio-apparatuur, en dus ook RFID-apparatuur, op de markt brengen volgens de R&TTE-richtlijn¹⁷ verantwoordelijk en aansprakelijk zijn voor de veiligheid/gezondheid daarvan.

4.3.2 Milieu-aspecten

De productie en verwerking van tags in en op producten levert een extra milieubelasting op. Ten eerste bij de productie van de tags, ten tweede bij de verwerking van de tags en de producten waarop of in deze zijn verwerkt.

Op dit moment zijn er twee Europese richtlijnen¹⁸ die specifiek betrekking hebben op elektrische en elektronische apparatuur, te weten:

- WEEE: Waste Electrical and Electronic Equipment¹⁹. Doelstelling van de wet is preventie en reductie van de hoeveelheid afval van elektr(on)ische apparatuur en het stimuleren en bevorderen van hergebruik en recycling van het afval.
- RoHS: Restriction of the use of Hazardous Substances in Electrical and Electronic Equipment²⁰. Op grond van deze wet moeten producenten het gebruik van bepaalde gevaarlijke stoffen als lood en cadmium in elektronische apparatuur uitfaseren.

Deze Europese richtlijnen zijn in Nederland geïmplementeerd vanuit VROM onder de Regeling Beheer Elektrische en Elektronische Apparatuur (REA) en het Besluit Beheer Elektrische en Elektronische Apparatuur (BEA). REA is de Nederlandse uitwerking van WEEE, en BEA is de Nederlandse uitwerking van RoHS.

Het belangrijkste kenmerk van deze regelgeving is dat de producent verantwoordelijk is voor zijn apparatuur van “de tekentafel tot aan het hergebruik”. Producenten en importeurs van ICT apparatuur zijn wettelijk verplicht om producten die in Nederland op de markt gebracht zijn na afdanken terug te nemen en te zorgen voor hergebruik en milieuverantwoorde verwerking van deze producten. Hiervoor kunnen producenten zich verenigen in non-profit organisaties die het hergebruik en afvalverwerking uitvoeren.

Volgens de Europese Commissie²¹ valt RFID onder de definitie van elektrische en elektronische apparatuur en valt het in de derde categorie; “IT and telecommunications equipment”. Dit betekent dat de producenten van RFID tags zijn gebonden aan de RoHS richtlijnen en de daarin genoemde stoffen niet mogen verwerken in de tags. Voor de WEEE richtlijn geldt een andere argumentatie. Wanneer de tags worden geplaatst op de verpakking van producten valt RFID niet onder de richtlijn. Ook als het om elektrische of elektronische apparatuur gaat omdat RFID dan geen deel uitmaakt van deze eerder genoemde apparatuur. Echter wanneer ze in elektrische of elektronische apparatuur zelf wordt verwerkt dan valt RFID wel onder de WEEE richtlijn en is de producent verantwoordelijk voor de recycling van het totale product, inclusief de RFID-tag.

¹⁷ Radio and Telecommunications Terminal Equipment Directive

¹⁸ De richtlijnen zijn in alle lidstaten (nationaal) wettelijk van kracht geworden op 13 augustus 2004.

¹⁹ Directive 2002/96/EC

²⁰ Directive 2002/95/EC

²¹ Uit: Frequently Asked Questions on Directive 2002/96/EC and Directive 2002/95/EC. DG-Environment. February 2006.

4.4 Conclusies

De RFID techniek is als zodanig geen gevaar voor de volksgezondheid ook niet wanneer deze techniek in de toekomst op grote schaal gebruikt zal worden. Voor de kleine groep die beroepsmatig langer aan straling wordt blootgesteld is de richtlijn EMV voor werkenden vastgesteld, deze wordt dient in 20087 in Nederland geïmplementeerd.

RFID valt onder de categorie elektrische en elektronische apparatuur binnen twee richtlijnen van de Europese Commissie op het gebied van schadelijke stoffen en recycling van producten. Dit betekent dat de huidige regelgeving de nadelige milieubelasting van RFID voldoende beperkt.

Hoofdstuk 5: Standaardisatie en frequentieruimte.

Voor een goed gebruik van RFID-toepassingen dienen de randvoorwaarden op orde te zijn. Bij RFID is het belangrijk dat er gedeelde afgesproken standaarden zijn en dat er voldoende ruimte in de ether is gereserveerd. Op beide aspecten wordt in dit hoofdstuk ingegaan.

5.1 Standaardisatie

5.1.1 Waarom is standaardisatie belangrijk?

Wanneer gegevens worden uitgewisseld tussen verschillende partijen is het van groot belang dat de systemen elkaar wederzijds begrijpen. Ook voor RFID speelt standaardisatie een belangrijke rol. In gesloten systemen en toepassingen (toegangscontrole, tolwegen) is standaardisatie vaak geen probleem omdat de eigenaar van het systeem de volledige controle heeft over de technologie die wordt toegepast. Echter zodra er sprake is van open (door meerdere partijen gebruikte) systemen en toepassingen, wordt standaardisatie en normalisatie belangrijk.

Omdat RFID steeds vaker in zulke open (logistieke) systemen wordt toegepast is het al geruime tijd onderwerp van debat in verschillende standaardisatie discussies op internationaal-, nationaal- en industriële niveau. Standaardisatie heeft hierbij betrekking op verschillende onderdelen binnen een systeem zoals de organisatie van de gegevens op de tag (data structuur), de wijze waarop readers en tags communiceren (air interface), de tests die aantonen dat apparaten voldoen aan de standaard (conformiteit) en de technologie die wordt gebruikt bij specifieke toepassingen.

Standaardisatie is dus van belang voor gezamenlijk toepassing van RFID door verschillende bedrijven of organisaties. Wanneer internationale standaarden en interoperabiliteit tussen de verschillende systemen ontbreken, kunnen bijvoorbeeld paspoorten niet internationaal worden herkend, kan een container met Chinese producten niet automatisch herkend worden door de Nederlandse reader in de haven en wordt het logistieke proces vertraagd. Dit alles leidt tot hogere kosten voor alle gebruikers en toepassers van systemen.

5.2.2 Huidige stand van zaken

Standaarden en normen komen in de praktijk op verschillende manieren tot stand. Zo worden er in ISO²² verband normen ontwikkeld voor zowel de RFID-technologie als voor RFID-toepassingen. Daarnaast zijn er de *de facto* standaarden waarbij relatief grote toepassers een voorkeur ontwikkelen voor een bepaalde oplossing. Aan de hand van onderstaand overzicht wordt duidelijk welke partijen voor RFID op dit moment het meest van belang zijn:

²² International Organization for Standardization

- ISO

De ISO-normen voor RFID-technologie richten zich met name op data syntax, tag identificatie en air interface protocollen. Daarnaast wordt er binnen ISO-verband gewerkt aan normen voor diverse toepassingen van RFID, zoals containers, dierenidentificatie, diefstalpreventie, identificatiekaarten en verpakkingen.

Om incompatibiliteit tussen de-facto standaarden en ISO-normen te voorkomen, streeft ISO er actief naar om de-facto standaardisatie organisaties in een zo vroeg mogelijk stadium in het formele normalisatieproces te betrekken. Zo is er bijvoorbeeld een effectieve liaison tussen ISO en IATA²³ die ertoe heeft geleid dat de RFID-standaard van IATA voor bagageafhandeling gebaseerd is op de ISO-18000-6 norm. Organisaties als GS1 en AIM global spelen een actieve rol in het ontwikkelproces van de ISO-normen voor RFID.

In ISO participeren belanghebbenden uit verschillende landen. Nederlandse belanghebbenden kunnen via NEN deelnemen in het normalisatieproces van ISO. De ISO (International Organization for Standardization) werkt aan het definiëren van diverse standaarden. Met name op het gebied van de gesloten RFID-systemen zijn er al veel standaarden door ISO ontwikkeld en deze zijn dan ook al jarenlang actief in toepassingsgebieden als smartcards.

- GS1/ EPCglobal

In de open²⁴ systemen, waar de toepassingen vooral gezocht moeten worden in de logistieke processen, zijn op dit moment nog weinig standaarden definitief vastgesteld. Vanuit de supermarktwereld (o.a. WalMart en Metro), het Amerikaanse ministerie van Defensie, Boeing allen met vele toeleveranciers, is brede steun ontstaan voor de EPC-standaard en de huidige toepassingen zijn dan ook gebaseerd op deze standaard.

EPCglobal is onderdeel van GS1, de organisatie die internationaal de barcodestandaard beheert. Als de initiator van deze RFID-standaard, heeft ze zich als doel gesteld om specificaties voor tags en readers te ontwikkelen die wereldwijd gebruikt kunnen worden. Ook wordt er gewerkt aan standaarden voor de identificerende nummering op de tags en standaards voor het uitwisselen en beschikbaar stellen van gegevens over de producten op een netwerk van databases. Mede door druk van het Amerikaanse ministerie van Defensie, een grote voortrekker van RFID, wordt de EPCglobal class 1 generation 2 standaard ook een ISO standaard.

- CEN/NEN

In Europa heeft CEN (European Committee for Standardization) een belangrijke rol gespeeld in de ontwikkeling van normen op het gebied van automatische identificatie. Deze normen zijn inmiddels bijna allemaal ingebracht in ISO. Ook de ontwikkeling van normen voor RFID vindt nu helemaal plaats binnen ISO. CEN speelt hierin echter nog steeds een rol omdat er onlang een ad hoc groep is opgericht die de aspecten van de Europese wet- en regelgeving bij de ontwikkeling van de ISO-normen voor RFID moet bewaken. Nederlandse belanghebbenden kunnen via NEN deelnemen in het normalisatieproces van CEN.

²³ IATA: International Air Transport Association. Deze zomer wordt bij de bagageafhandeling op Schiphol in samenwerking met KLM gebruik gemaakt van RFID-technologie.

²⁴ Open systemen zijn systemen die kunnen worden gelezen/gebruikt buiten het systeem van een enkel bedrijf.

- Europese Commissie

Ook binnen de Europese Commissie is er nadrukkelijk aandacht voor het vraagstuk rondom standaardisatie. Het jaar 2006 staat in het teken van een brede consultatie op het gebied van RFID, standaardisatie is daarbij een van de belangrijke onderwerpen, die mogelijk leidt tot een aanbeveling of witboek.

Naast bovengenoemde partijen zijn er ook nog verschillende initiatieven vanuit landen als China, Japan en Korea. Al deze landen hebben al aangegeven dat ze hun systemen zullen harmoniseren met de ISO standaarden. Ook andere partijen als de ANSI/INCITS²⁵ zijn actief op het gebied van standaardisatie, maar zijn deze overigens al compatibel met de ISO-standaard.

5.3 Frequentiebanden voor RFID

RFID tags en readers communiceren digitaal met elkaar en daarvoor maken ze gebruik van frequentiespectrum. Zoals bij alle gebruik van frequentiespectrum moet men ook bij RFID-toepassingen werken conform de daarvoor geldende regels, onder andere m.b.t. het toegestane gebruik van gelicenseerde en ongelicenseerde frequentiebanden, elektromagnetische compatibiliteit, interferentie-immuniteit en de veiligheid. Binnen de ordening van het spectrumgebruik maakt RFID gebruik van de bestemming SRD (Short Range Devices).

In het frequentiespectrum is er in globaal drie gebieden bestemming ingeruimd voor SRD (en dus RFID)-toepassingen:

- a) In het laagfrequente gebied zijn de 125kHz-band en de 13 MHz-band hiervoor aangewezen; deze banden zijn geschikt voor toepassingen die met korte leesafstanden (kunnen) werken, d.w.z. 10 cm à 1 meter, en die een niet al te hoge leessnelheid behoeven. Hier valt te denken aan toepassingen met passieve tags, bijvoorbeeld antidiestalsystemen, smartcards, identificatie van vee. Een 'passieve' tag houdt in dat de veld-energie vanaf de reader de tag activeert.
- b) In het UHF-gebied (de 433 MHz band en de 865 MHz band) treft men vooral toepassingen aan met zgn. semi-actieve tags; dit soort tags bevat doorgaans een batterijtje dat een paar jaar werkzaam blijft. Voorbeelden van toepassingen in deze band zijn tracking and tracing van voorwerpen in logistieke systemen. In deze band wordt doorgaans een goed bereik gerealiseerd tussen 2 meter en 10 meter; dit soort tags kan redelijk snel reageren op readers.
- c) In de 2,4 GHz-band treft men toepassingen met zogenoemde actieve tags; dit soort tags bevat bijvoorbeeld verwisselbare batterijtjes. Typisch bereik is tussen 1 en 2 meter en de leessnelheid is zeer hoog. Een voorbeeld van een toepassing is toegangscontrole voor voertuigen.

RFID werkt op zeer zwakke vermogens waardoor op veel plaatsen en door vele partijen deze frequenties tegelijk kunnen worden toegepast. Hierdoor kan RFID op zeer grote schaal worden gebruikt terwijl het toch geen schaarste van frequentieruimte hoeft te ondervinden. Op sommige spectrumdelen moet het LBT-mechanisme worden toegepast (Listen Before Talk); dit betekent dat de reader op zoek gaat naar een vrij/leeg stukje spectrum om te gaan

²⁵ (ANSI) American National Standards Institute en (INCITS) InterNational Committee for Information TechnologyStandards

gebruiken; door dit principe wordt een hoge(re) benutting van het beschikbare spectrum bereikt.

Voor de toepassing en verdere ontwikkeling van RFID is het belangrijk dat er voldoende en tevens adequaat spectrum daarvoor beschikbaar is. Ook is het belangrijk dat de bestemming in verschillende wereldregio's op zodanige wijze is geharmoniseerd en gestandaardiseerd dat interoperabele mondiale toepassing van apparaten goed mogelijk is. In internationale overleggen wordt voortdurend aan verdere harmonisatie en standaardisatie gewerkt; de gremia die zich met name op het frequentiegebied hiermee bezighouden zijn het ECC (Electronic Communications Committee²⁶) en ETSI (Europees Telecommunicatie Standaardisatie Instituut²⁷). In deze gremia worden permanent de marktontwikkelingen gevolgd en wordt afgewogen of er aanleiding is voor herbestemmingen van spectrumdelen die niet of weinig (meer) worden gebruikt, in de richting van met name opkomende toepassingen die extra spectrumruimte nodig hebben; ook de RFID-ontwikkelingen (technologie, markt) worden daar nauw gevolgd.

Het ministerie van Economische Zaken implementeert de vanuit het internationale gremia aangegeven richtlijnen en aanbevelingen in het Nationaal FrequentiePlan (NFP). In de afgelopen periode zijn er nieuwe banden bijgekomen voor RFID-gebruik, en in de komende tijd worden dat er nog meer.

In grote lijnen zijn RFID-frequentiebestemmingen in de verschillende wereldregio's geharmoniseerd. Op enkele punten zijn er wat verschillen, maar in de praktijk heeft dat geen tot weinig consequenties; het kan bijvoorbeeld voorkomen dat het aangewezen spectrum van Europese en Amerikaanse readers iets ten opzichte van elkaar versprongen zit, maar tags uit beide continenten antwoorden op beide soorten readers.

²⁶ <http://www.ero.dk/ecc>

²⁷ <http://www.etsi.org/>

5.4 Conclusies

Diverse organisaties zijn bezig met het vastleggen van RFID-standaarden, ISO 18000 en EPC groeien thans naar elkaar toe. Zo zal de ISO 18000 standaard de EPC standaard integreren in de nieuwe standaarden. Dit biedt voldoende mogelijkheden om op een eenduidige manier diverse handelspartners in een globale open economie met elkaar te laten communiceren. De RFID-standaarden zijn op dit moment voldoende ontwikkeld om te kunnen worden toegepast in bedrijfsprocessen.

Op het gebied van standaardisatie doet de markt zijn werk. Het is echter van belang dat de Nederlandse overheid er voor waakt dat de standaarden die internationaal worden ontwikkeld niet ten koste gaan van de door Nederlandse publieke en private partijen gebruikte standaarden. Door de vertegenwoordiging in gremia als de Europese Commissie en de CEN, waarin het Nederlandse bedrijfsleven wordt vertegenwoordigd door de NEN, wordt een Nederlandse inbreng, voor zover mogelijk, gewaarborgd.

Op dit moment is het beschikbare spectrum adequaat voor RFID-ontwikkeling. Voor het geval RFID mondiaal gezien plotseling een zeer stormachtige ontwikkeling zou doormaken, kan snel voor verruiming van de beschikbaarheid worden gezorgd. Op dit moment zijn er qua spectrumbestemming en -beschikbaarheid geen knelpunten of problemen voor de RFID-ontwikkeling.

Hoofdstuk 6: Conclusies en Acties.

6.1 Conclusies

Veel aandacht voor RFID

De RFID-ontwikkelingen krijgen veel aandacht. Er loopt een consultatie door de Europese Commissie, de ITU en de OESO hebben er conferenties aan gewijd, universiteiten doen onderzoek, Philips heeft hoge verwachtingen, de technologiec commissie van de Tweede Kamer organiseerde een RFID-middag en Nederland heeft een RFID-platform.

Er is ook alle reden voor die aandacht. RFID is een interessante technologie, die door technologische en prijsontwikkelingen voor steeds meer toepassingen bruikbaar wordt. De vraag voor de komende jaren is voor welke (grootschalige) toepassingen RFID benut gaat worden.

RFID is een technologie waarvan vele experts grote mogelijkheden verwachten. Een mogelijk toekomst scenario is dat bijna alle producten uitgerust worden met een RFID-tag en op die manier 'intelligent' kunnen worden gemaakt, zodat er 'communicatie' kan plaatsvinden tussen die tags. Op dit moment zijn we daar ver van verwijderd en de vraag is ook of we ooit in zo'n situatie terecht zullen komen, omdat voor elk RFID-systeem nog een businesscase gevonden moet worden.

Het is daarom belangrijk naar de reële ontwikkelingen te kijken. In de notitie zijn alleen voorbeelden opgenomen die daadwerkelijk plaatsvinden. Er vallen een paar dingen op. Veel voorbeelden bevinden zich allereerst nog in een experimenteel stadium of bij hun eerste toepassing. Daarnaast vinden de meeste toepassingen plaats in het logistieke proces binnen een bedrijf of tussen toeleveranciers, en zijn er nog weinig tot geen voorbeelden waar de klant zelf via artikelen met RFID geconfronteerd wordt.

Aan de andere kant bestaat er ook angst voor het onbekende van RFID. Met name de mogelijke privacyconsequenties van het gebruik van RFID roepen veel vragen op. Ook hier zal de toekomst moeten uitwijzen wat de daadwerkelijke gevaren zijn, hoewel er natuurlijk in bepaalde mate op geanticipeerd kan worden.

Kansen voor RFID

Op dit moment ziet de Nederlandse overheid RFID in eerste instantie als een interessante, veelbelovende ontwikkeling. Het is een techniek die veel nuttige toepassingen kent in zeer diverse sectoren: van de logistiek tot de zorg, van het betalingsverkeer tot het paspoort. Vanuit de overheid wordt innovatie ondersteund via algemene regelingen. Zo kunnen (MKB)ondernemers advies krijgen over invoering van RFID bij Syntens, ondersteunt SenterNovem innoverende ondernemers met subsidies²⁸, heeft RFID een plaats in enkele onderzoeksprojecten²⁹ en krijgen mogelijk plaats in grote innovatieprogramma's, die op dit moment gevormd worden, zoals Fresh on Demand, of Innovatie in de Logistieke keten. Uit de markt komen verschillende signalen dat de bottleneck op dit moment de testfase van toepassingen is en het delen van de opgedane kennis. Er zijn wel voorbeeldopstellingen, vaak

²⁸ Het aantal toegekende aanvragen aangaande RFID steeg van 51 in 2003, naar 108 in 2004 tot 203 in 2005

²⁹ Bij TNO of de BSIK-programma's Freeband en Smart Surroundings

van bedrijven die RFID systemen willen verkopen, maar daarmee kan niet getest worden, omdat er niet ingespeeld kan worden op specifieke omstandigheden van gebruikers.

Zorgen bij RFID ontwikkeling

Naast de kansen die RFID biedt voor de economie, zijn er ook zorgen rondom de ontwikkeling ervan. In de notitie worden drie zorgen rondom RFID behandeld. Privacyrisico's worden gezien als de grootste zorg bij RFID. De ontwikkeling van RFID-technologie en toepassingen is nog in volle gang. Dat betekent ook dat het moeilijk is een reëel beeld te krijgen van de mogelijke risico's. De meeste risico's die genoemd worden zijn nog niet daadwerkelijk opgetreden, maar zouden in de toekomst kunnen voorkomen. In de notitie zijn de veelgenoemde risico's gecategoriseerd.

Ten eerste *het volgen van mensen*. De kans hierop is klein, omdat er een zeer dicht netwerk van readers moet zijn, mensen producten of toepassingen van RFID-chips bij zich moeten dragen en de afgelezen informatie door verschillende databases gekoppeld moeten worden. In kleinere, besloten, ruimte is volgen wel mogelijk en is het vaak ook een bewuste toepassing. In een ziekenhuis kunnen artsen of patiënten gevolgd worden, in een fabrieksterrein medewerkers. Belangrijk is in dat geval dat mensen weten dat ze gevolgd worden en dat het niet voor oneigenlijke doelen gebruikt wordt.

Ten tweede *het onrechtmatig koppelen van data*. Een RFID-chip geeft informatie door (vaak enkel de identiteit van de chip). Afhankelijk van de toepassing wordt die informatie doorgestuurd naar een database. Die data mag niet onrechtmatig gekoppeld worden. Dit is geen nieuw risico, maar wel één waarvan de mogelijkheden zullen toenemen bij meer toepassingen van RFID. Er zullen immers meer data over producten en personen wordt uitgelezen en bewaard.

Het derde risico is het *ongemerkt uitlezen van informatie*. Daarvoor is vaak adequate beveiliging mogelijk, zowel fysiek (bv: aluminiumfolie, afbreekchip) als digitaal via encryptie (bv: versleuteling).

De drie genoemde risico's liggen alle drie op het terrein van privacy. Het wettelijke kader dat dit gebruik van data reguleert is geïmplementeerd in de Wet Bescherming persoonsgegevens (WBP). Het toezicht op de WBP is opgedragen aan het College Bescherming Persoonsgegevens (CBP). De WBP geeft aan wanneer er sprake is van een persoonsgegeven en wat daar vervolgens mee mag gebeuren. Een cruciale vraag voor de overheid op het terrein van privacy is of de huidige wetgeving voor bescherming persoonsgegevens voldoende is voor ontwikkelingen als RFID. Binnenkort komt het College Bescherming Persoonsgegevens hierover met een notitie. In het algemeen is voor het voorkomen van zorgen over privacy transparantie een sleutelbegrip. Het gebruik van RFID en met name de verwerking en het bewaren van gegevens die RFID genereert, moet voor iedereen op een begrijpelijke manier inzichtelijk kunnen worden gemaakt. Dit adagium geldt zowel voor bedrijven als voor overheden. Daarnaast kan de producerende industrie zelf veel bijdragen aan de vermindering van privacyrisico's door 'privacy by design': wegwerp chips, aan-uit knopjes, goede versleuteling etc.

Voor de *technische veiligheid* van RFID moet naar het hele systeem gekeken worden. De tag, de reader en de database kunnen op verschillende manieren onveilig zijn. De meest voorkomende verstoringen, zoals afluisteren, verzenden van verstorende radiogolven of

afluisteren van RFID-systemen zijn strafbaar volgens de Nederlandse wet. Overigens hebben niet alle toepassingen een even hoog niveau van beveiliging nodig. De verantwoordelijkheid voor de beveiliging van toepassingen ligt primair bij de partijen die een RFID toepassing implementeren.

Op het gebied van *milieu en gezondheid* is de lijn duidelijk. RFID valt onder de categorie elektrische en elektronische apparatuur en daarmee binnen twee richtlijnen van de Europese Commissie op het gebied van schadelijke stoffen en recycling van producten. De huidige regelgeving is afdoende om de nadelige effecten van RFID op het milieu te beperken. RFID maakt gebruik van elektromagnetische velden, waarbij opgemerkt worden dat die opgewekt worden door de readers en dat een 'tag' geen veld draagt. De limieten voor blootstelling van elektromagnetische straling zijn opgesteld door de ICNIRP³⁰ en erkend door de WHO (World Health Organization). Op basis van deze limieten zijn er Europese Normen op RFID van toepassing³¹. De door RFID gebruikte elektromagnetische velden vallen qua vermogen en qua intensiteit binnen de normen.

Standaardisatie en frequentieruimte

Voor het komen tot interessante toepassingen dienen ook basisafspraken op orde te zijn. Voor RFID spreken we dan over standaardisatie en frequentieruimte. Standaardisatie is essentieel voor het functioneren van RFID, zeker als de toepassing buiten de grenzen van het eigen bedrijf of het eigen land wordt gebruikt. De standaardisering vindt vooral plaats in internationale gremia als ISO, EPCglobal, CEN en ETSI. Nederland is daarbij betrokken via haar eigen standaardisatieorganisaties (bv. NEN). De overheid heeft een (kleine) rol wanneer er internationale of inter-Europese conflicten ontstaan. De verantwoordelijkheid voor frequentieruimte ligt wel bij de overheid, bij het ministerie van Economische Zaken. Er is op dit moment voldoende ruimte beschikbaar voor RFID in het frequentieplan. Het zijn de frequentiebanden bestemd voor SRD (Short Range Devices). Mocht er (onverwacht) meer ruimte nodig zijn dan zijn er voldoende mogelijkheden om die beschikbaarheid te vergroten.

³⁰ ICNIRP. The International Commission on Non-Ionizing Radiation Protection.

³¹ EN 50364: 2001 en EN 50357: 2001

6.2 Acties

In deze notitie zijn de ontwikkelingen op het gebied van RFID uiteengezet en is gekeken naar mogelijke beleidsconsequenties. Samenvattend kan geconcludeerd worden dat RFID een ontwikkeling is, die zowel kansen biedt als zorgen baart.

De vraag is of de ontwikkelingen op het gebied van RFID aanleiding zijn om specifiek beleid te ontwikkelen voor RFID. In de notitie kwamen twee zaken naar voren. Ten eerste is het veld van de RFID-toepassingen op dit moment nog volop in ontwikkeling. De verwachtingen over de mogelijkheden en de zorgen lopen nog erg uiteen. Ten tweede, zijn veel beleidsconsequenties van RFID niet uniek. Zorgen voor privacy, het regelen van frequentieruimte en het stimuleren van innovatie zijn onderwerpen die ook verbonden zijn aan andere technologieën. De Nederlandse overheid heeft op deze onderwerpen staand beleid. Uit de notitie komt naar voren dat het staande beleid in veel gevallen voldoet of is aangepast: frequenties, milieu en gezondheid, innovatie(grotendeels).

1. Interdepartementale werkgroep

Gezien de ontwikkelingsfase en het bestaande beleid worden er op dit moment geen grote specifieke beleidsmaatregelen voorgesteld. Wel is het belangrijk RFID zorgvuldig te monitoren vanuit de verschillende invalshoeken.

Daarom wordt er een interdepartementale werkgroep ingesteld, waarvoor de departementen worden uitgenodigd, waarvan de beleidsterreinen RFID raken: EZ, JUS, VROM, BZK, V&W. Het ministerie van Economische Zaken zal vanuit haar coördinerende rol het voorzitterschap op zich nemen, de verantwoordelijkheden blijven uiteraard bij de ministeries. De werkgroep heeft de volgende functies:

- Attenderen op (en eventueel adresseren van) ontwikkelingen en risico's rondom RFID.
- Gesprekspartner voor het georganiseerde bedrijfsleven en consumentenorganisaties aangaande RFID.
- Gezamenlijk (afgestemd) internationaal optreden: EU, maar ook bilateraal.
- Coördineren van overheidsactiviteiten op het gebied van RFID.

2. Privacy

Op het gebied van privacy is specifieke aandacht nodig. Het zal een onderwerp zijn dat hoog op de agenda van de werkgroep komt. In de notitie zijn de verschillende risico's en de evaluatie ervan aan bod gekomen. De kernvraag is of de bestaande wetgeving (en handhaving) op het gebied van de bescherming van persoonsgegevens voldoet bij de komst van RFID. Vooralnog wordt aangesloten bij de conclusie van ECP.NL, dat het beschermingsniveau van de WBP voldoende lijkt in het kader van RFID-toepassingen. Tevens wordt het rapport van het CBP afgewacht, dat verwacht wordt in oktober/november 2006. In het algemeen is voor het voorkomen van zorgen over privacy transparantie een sleutelbegrip. Het gebruik van RFID en met name de verwerking en het bewaren van gegevens die RFID genereert, moet voor iedereen op een begrijpelijke manier inzichtelijk gemaakt kunnen worden. Tevens biedt 'privacy by design' (zoals versleuteling, chips die uitgezet kunnen worden etc.) goede mogelijkheden om de privacyrisico's te verkleinen.

3. Innovatie

Tot slot komt uit de notitie naar voren dat op het gebied van innovatie er vraag is naar een testfaciliteit voor RFID. Onderzocht zal worden of er daadwerkelijk behoefte is aan testmogelijkheden voor RFID en hoe die zouden kunnen worden ingevuld. Dit in eerste instantie aansluitend bij bestaande beleidsmogelijkheden.