

---

# RFID: Kans of bedreiging?

*Een blik op RFID toepassingen en verkenning van de beleidsimplicaties*

---



**Telematica**  
*Instituut*



---

## Colofoon

Title : RFID: Kans of bedreiging?  
Date : 15 januari 2006  
Version : 2.0  
Status : Eindversie  
Editor : Bob Hulsebosch  
Company : Telematica Instituut  
Author(s) : Bob Hulsebosch, Patrick Strating, Wouter Teeuw, Hans Schaffers

### Synopsis:

*Dit document beschrijft een verkenning van RFID toepassingen en de te verwachten ontwikkelingen, en de beleidsimplicaties daarvan voor de overheid. Aan de hand van illustratieve voorbeelden wordt aangegeven op wat voor manieren RFID wordt of zou kunnen worden toegepast, en wat de maatschappelijke impact daarvan is. Naast de uitwerking van beleidsimplicaties is er ook aandacht voor de drivers en barrières voor implementatie van RFID in Nederland, en voor de wijze waarop in de internationale context door overheden met RFID stimulering omgegaan wordt (benchmark).*



# Samenvatting

Een RFID tag is een kleine chip met een antenne die is bevestigd aan een object. Een RFID tag bevat in ieder geval een uniek identificatienummer, dat het individuele exemplaar van het product kenmerkt. Dit nummer wordt met radiogolven door een reader gelezen, vandaar de term RFID: Radio Frequency Identification. Het belang van de toepassing van radiogolven ligt in het kunnen vaststellen van de aanwezigheid van het exemplaar, zonder dat de code direct in het zicht hoeft te zijn (zoals met een streepjescode). De tag maakt zichzelf, en daarmee het object waar het op of in zit, bekend en geeft vervolgens ook nog een unieke identificatie in de vorm van een identifier. Deze identifier is een nummer dat verwijst naar meer gedetailleerde informatie over het object die is opgeslagen in een of meerdere databases. Door het koppelen van zulke databases kunnen diverse gebeurtenissen die het object zijn "overkomen" (b.v. de gang van productie tot verkoop), nagegaan worden. Dit kan bijvoorbeeld van nut zijn bij het bepalen van de echtheid van het object. Afhankelijk van de capaciteiten van de tag is het mogelijk om een deel van die informatie ook op de tag zelf op te slaan, zodat deze altijd, ook zonder netwerktoegang, direct beschikbaar is.

RFID zal in de toekomst veel van de huidige bar- of streepjescode vervangen of complementeren. RFID technologie heeft ten opzichte van de barcode of een aantal voordelen. De Electronic Product Code (EPC) opgeslagen op de RFID tag kan langer zijn dan de UPC code en kan hergeprogrammeerd worden. De EPC is een exemplaarnummer terwijl de barcode een artikelcode betreft: meerdere exemplaren van een zelfde artikel hebben dezelfde artikelcode maar een verschillende exemplaarcode. Tags kunnen automatisch gelezen worden, zodra zij in de buurt van een lezer komen; het object hoeft niet meer op een bepaalde manier voor een lezer gehouden te worden, zoals met een barcode: met radiogolven "werkt het ook om een hoekje" of "ergens door heen", in tegenstelling tot optische technieken. Dit maakt het mogelijk om de tags te verpakken in het product waardoor de RFID tag, in tegenstelling tot de barcode, minder vatbaar is voor fysieke beschadigingen en daardoor beter uit te lezen is. Nadelen van RFID tags zijn dat ze in het hogere frequentiegebied slecht werken in vochtige omgevingen en op metaal. Absorptie van de radiofrequentie-energie en reflecties liggen hieraan ten grondslag.

RFID wordt momenteel vooral gebruikt voor identificatie (bijvoorbeeld toegangscontrole), het voorkomen van winkeldiefstal en voor tracking & tracing doeleinden. Maar de mogelijkheden van RFID gaan verder. Een breed scala van toepassingen is mogelijk door de combinatie van RFID tags met sensoren (temperatuur, locatie, etc.), communicatienetwerken (Personal Area Networks, WiFi, etc.) en draagbare computers (pda's, laptop, wearables etc.), zoals toepassingen rond persoonlijke identificatie/authenticatie, gezondheid, veiligheid en gepersonaliseerde diensten. Sectoren waarvoor RFID relevantie heeft zijn de retail, de maakindustrie, de financiële sector, logistiek en transport, de luchtvaartsector de gezondheidszorg en de sociale veiligheid. Vooral de retail en logistieke sectoren hebben al enige ervaring met het gebruik van RFID. In de andere sectoren is het gebruik ervan veelal nog onontgonnen gebied. Hier liggen voor Nederland ook de meest kansrijke toepassingen. Met de aanwezigheid van enkele internationaal sterke financiële instellingen, een gerenommeerde luchtvaartmaatschappij, een zorgsysteem van hoog niveau als potentiële RFID gebruikers en de aanwezigheid van

Philips en Nedap als belangrijke RFID technologieleveranciers zijn de ingrediënten voorhanden voor succesvolle nieuwe RFID toepassingen. De aanwezigheid van een geavanceerde kennisinfrastructuur kan hierbij helpen. Met de vele aanwezige kleine technostarters is er de mogelijkheid om snel in te spelen op nieuwe, specifieke RFID ontwikkelingen en toepassingen. Ook de Nederlandse overheid kan, net als in veel andere landen het geval is, het gebruik van RFID stimuleren door als launching customer op te treden. Het nieuwe biometrische paspoort (waarvoor Philips de RFID tag levert) is hiervan een goed voorbeeld.

De breedte en veelheid aan potentiële toepassingen van RFID, potentiële belemmeringen die bij de invoering in de praktijk spelen, en de voor een deel onzekere implicaties van het gebruik geven mogelijk aanleiding tot beleidsontwikkeling. Er zijn raakvlakken met maatschappelijke vragen. Thema's inzake mogelijke RFID beleidsimplicaties hebben onder meer te maken met frequentiebeleid (verdeling van frequenties), de veiligheidsproblematiek (het kunnen uitlezen van tags door onbevoegden, klonen en kapotmaken van tags, etc.), het privacybeleid (bijvoorbeeld het volgen van werknemers en goederen, het al of niet verplichten om RFID tags aan te brengen), opslag van gegevens en innovatieve toepassingen (RFID als enabling technologie voor nieuwe diensten en toepassingen in de zorg en het onderwijs). Daarnaast zijn er technische aspecten die voor het DGTP werkerterrein van belang zijn zoals het verdelen van frequentiebanden om interferentie van systemen met RFID tags te voorkomen.

In de voorliggende verkenning is onderzocht of er daadwerkelijk aanleiding tot RFID beleid is en zo ja, hoe dit beleid dan vorm gegeven kan worden. Dit is gebeurd op basis van een inventarisatie van (potentiële) RFID toepassingen en inzichten. Hieruit voortvloeiend worden knelpunten geïnventariseerd, van waaruit mogelijke beleidsrichtingen worden aangestipt. Bij dit alles wordt de internationale context meegenomen.

Uit de verkenning blijkt dat RFID niet meer is weg te denken. RFID is een kleine, eenvoudige technologie met een enorme potentie. Hoewel RFID al langere tijd bestaat, is grote groei te verwachten vanwege de steeds lager wordende productiekosten van de tags en de combinatie met internettechnologie. Veel RFID toepassingen bevinden zich echter nog in een experimenteel stadium. Kenmerkend voor veel toepassingen is dat er een cumulatie is van technische, organisatorische, sociale en economische knelpunten waardoor doorbraken uitblijven. Het selecteren van de juiste RFID technologie in termen van frequenties, tags, antennetypes, readers en databases voor het inrichten van een optimaal en veilig RFID systeem is bijvoorbeeld geen sinecure. Het uitrollen van een RFID infrastructuur voor het verwerken en delen van gegevens is een hele organisatie die vaak bedrijfsoverschrijdend is. Bij veel burgers heerst onduidelijkheid en vrees over de mogelijkheden van RFID met betrekking tot hun privacy. En ook is het voor veel RFID toepassingen moeilijk om een sluitend business model op te voeren. De onderstaande tabel geeft een indicatieve roadmap voor verschillende RFID toepassingen die de pilotfase ontgroeid zijn.

| Heden                            | Over 1-2 jaar   | Over 3-4 jaar           | Over 5 jaar of meer           |
|----------------------------------|---|-------------------------|-------------------------------|
| Toegangscontrole in gebouwen     | Paspoort  | RFID op productniveau   | Sensornetwerken               |
| Identificatie van koeien         | Verscheidende toepassingen met UHF tags in met name de maakindustrie, retail en logistiek | Betalingen              | Near Field Communication tags |
| Logistieke eenheden              |   | Combinaties met sensors | Rekeningrijden                |
| Tegengaan vervalsing van tickets | Post en koeriersdiensten  | Medische toepassingen   |                               |
|                                  |   | Luchtvaartdiensten      |                               |

Een belangrijke conclusie is dat er ontelbaar veel (potentiële) toepassingen zijn van RFID, in een breed toepassingsgebied. Mede door het toenemende gebruik van hoogfrequente UHF RFID tags, soms in combinatie met sensoren voor bijvoorbeeld het meten van de temperatuur luchtvochtigheid, ziet bijna dagelijks een nieuwe innovatieve toepassing het levenslicht. De verkenning van de mogelijkheden van RFID is pas begonnen.

Dit betekent dat er kansen liggen om innovatief en origineel voor de dag te komen en te profiteren van de mogelijkheden. Dit verdient aandacht allereerst omdat innovatie een belangrijk beleidsthema van de Nederlandse overheid is. Aan de andere kant, als RFID teveel wordt geassocieerd met tracking & tracing en retail, kan dat leiden tot een te beperkte blik waardoor kansen onbenut blijven. Zo kan ook het negatief denken voor wat betreft de privacy impact van RFID een belemmerende factor zijn voor het openstaan voor nieuwe kansen.

Behalve deze algemene observaties zijn er nog vele andere concrete knelpunten te benoemen (zie Hoofdstuk 3). De algemene indruk is dat veel van deze concrete knelpunten door technologieontwikkelaars en toepassers gezamenlijk opgepakt zullen worden en dat er weinig directe actie nodig is door middel van concrete *regelgeving*. Vanuit bedrijfskundig perspectief is het voor de meeste partijen ook simpel: als er een sluitende business case is, wordt RFID toegepast (dit is bedrijfskundig jargon voor: 'het kan uit...'). Zo is gebleken uit de praktijkervaringen uitgewisseld op de RFID workshop bij ECP.nl. Wel is het belangrijk dat het aspect "consumentenbescherming" adequaat vertegenwoordigd kan worden door de overheid en zij in het debat over wenselijkheid van bepaalde toepassingen een duidelijke rol kan spelen.

Bovenstaande is echter geen reden voor de overheid om passief te blijven. Al is de noodzaak tot regelgeving beperkt, er zijn voor de overheid rondom RFID volop mogelijkheden om een significante bijdrage te leveren aan duurzaam innovatieve bedrijvigheid. *In plaats van te denken in termen van beleid en regels moeten we veel meer denken in kansen.* Het lijkt zeker een taak van de overheid om voor de juiste randvoorwaarden te zorgen die een succesvolle uitrol van innovatieve RFID toepassingen in Nederland mogelijk maken. Er kan een milieu gecreëerd worden waarin nieuwe toepassingen onderzocht kunnen worden en op een succesvolle en gecontroleerde manier uitgerold kunnen worden.

Concreet kunnen de volgende aanbevelingen geven worden.

- Richt het beleid op het creëren van kansen in plaats van te zoeken naar regelgeving. Regelgeving die zinvol lijkt in het ene toepassingsgebied zal in veel gevallen belemmerend werken in andere toepassingsgebieden. Hierbij is het belangrijk te beseffen dat RFID bij de ene toepassing allang ‘proven technology’ is, maar bij een andere toepassing in een ander sector nog als experimenteel is. Het is daarom raadzaam om terughoudend te zijn met RFID regelgeving.
- Zorg voor goede, feitelijke informatie en zorg voor consumentenbescherming. Dit voorkomt overdreven technologieoptimisme en nodeloze angst bij de burgers. Het creëren van standaard voorlichtingsmateriaal waarmee bedrijven naar de burgers toe kunnen kost weinig moeite en kan hierbij goed helpen.
- Zorg dat harmonisatie in internationale regelgeving nagestreefd wordt op, in het bijzonder, frequentieallocatie en vermogens. Het gaat voor het Nederlandse belang in de breedte niet om de precieze regelgeving, het is vooral van belang dat er geen achterstand ontstaat ten opzichte van andere landen (‘level playing ground’).
- In Nederland, rondom de technische universiteiten en enkele grote bedrijven (bijvoorbeeld Philips), zijn er veel mogelijkheden voor innovatieve technostarters. RFID biedt voldoende mogelijkheden om nog vele jaren innovatieve toepassingen te kunnen genereren. Hiermee kan invulling gegeven worden aan innovatiedoelstellingen van de overheid. Deze kleine technologiebedrijven hebben andere karakteristieken dan het ‘gemiddelde’ MKB. Het verdient aanbeveling uit te zoeken hoe deze technostarters het beste ondersteund zouden kunnen worden.
- Het verdient aanbeveling om de milieu- en gezondheidsaspecten rond RFID vroegtijdig in kaart te brengen. Dit om te zorgen dat er geen verkeerde paden worden ingeslagen die op termijn onhoudbaar zijn en tot desinvesteringen leiden. Denk hierbij bijvoorbeeld aan wegwerp-chips met batterij in verpakkingen of producten. Het benaderen van RFID regelgeving vanuit de milieu- en gezondheidsaspecten leidt waarschijnlijk tot minder discussie en meer consensus dan wanneer de regelgeving vanuit privacyoogpunt wordt bekeken. Hiervoor is aanvullend onderzoek nodig.
- Creëer ondersteunende faciliteiten voor innovatieve bedrijven. Hierbij zijn twee elementen herhaaldelijk genoemd:
  - Creëren van ‘best practices’: veel bedrijven willen RFID wel gebruiken, maar zien door de bomen het bos niet meer. Het creëren of verzamelen van best practices, bijvoorbeeld met betrekking tot welke RFID apparatuur voor welke toepassing, of hoe de privacy te bewaken bij het gebruik van RFID. Dit kan typisch gebeuren in samenwerking met de industrie of overkoepelende organisaties
  - Creëren van een toegankelijke lab-omgeving waarin in het bijzonder kleinere organisaties hun nieuwe producten kunnen uittesten. Internationaal

gezien schieten de RFID kenniscentra uit de grond, bijvoorbeeld als company-lab of samenwerkingsvorm tussen bedrijven en universiteiten.

Enschede, januari 2006.

# Inhoudsopgave

|   |           |
|---|-----------|
| <b>1 Inleiding</b>                            | <b>1</b>  |
| 1.1 De impact van RFID                        | 1         |
| 1.2 Waarom nu?                                | 2         |
| 1.3 Probleemstelling                          | 2         |
| 1.4 Vraagstelling                             | 3         |
| 1.5 Doelstelling en resultaat                 | 3         |
| 1.6 Dankwoord                                 | 3         |
| <b>2 RFID Toepassingen</b>                    | <b>5</b>  |
| 2.1 Introductie                               | 5         |
| 2.2 RFID systemen - De puzzelstukken van RFID | 5         |
| 2.3 Toepassingen van RFID                     | 8         |
| 2.4 Wat gebeurt er in Nederland rond RFID?    | 21        |
| 2.5 Marktpotentieel RFID toepassingen         | 22        |
| 2.6 Samenvatting en conclusies                | 24        |
| <b>3 Knelpunten voor RFID toepassingen</b>    | <b>28</b> |
| 3.1 Introductie                               | 28        |
| 3.2 Technische knelpunten                     | 29        |
| 3.3 Organisatorische knelpunten               | 32        |
| 3.4 Sociale knelpunten                        | 40        |
| 3.5 Economische knelpunten                    | 46        |
| 3.6 Samenvatting                              | 49        |
| <b>4 Internationaal referentiekader</b>       | <b>51</b> |
| 4.1 Introductie                               | 51        |
| 4.2 Verenigde Staten                          | 51        |
| 4.3 Europa                                    | 52        |
| 4.4 China                                     | 54        |
| 4.5 Japan                                     | 55        |
| 4.6 Zuid Korea                                | 55        |
| 4.7 OECD                                      | 55        |
| 4.8 Europese Commissie                        | 57        |
| 4.9 Conclusies                                | 57        |
| <b>5 Van knelpunten naar beleid</b>           | <b>59</b> |
| 5.1 Introductie                               | 59        |
| 5.2 Een blik op de toekomst                   | 59        |
| 5.3 Een actieve taak voor de overheid?        | 60        |
| 5.4 Conclusies en aanbevelingen               | 68        |
| Appendix A - Deelnemers aan de RFID workshop  | 71        |
| Appendix B - RFID standaarden                 | 72        |
| Appendix C - Frequentiebanden                 | 73        |
| Appendix D - Beleidsinstrumenten              | 75        |
| Referenties                                   | 76        |

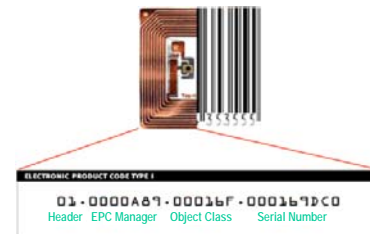
# 1 Inleiding

## 1.1 De impact van RFID

Het Directoraat-Generaal Telecommunicatie en Post (DGTP) van het Ministerie van Economische Zaken heeft behoefte aan tijdige signalering en verkenning van nieuwe ontwikkelingen op haar werkterrein, en aan inzicht in de mogelijke implicaties daarvan voor haar beleidsontwikkeling. Een concreet thema dat op dit moment in de belangstelling staat van DGTP is RFID, ofwel *Radio Frequency Identification*.

Een RFID tag is een kleine chip met een antenne die ergens aangebracht kan worden (aan een persoon, of product) en op afstand uitgelezen kan worden. Een RFID tag bevat informatie over het desbetreffende object. Vaak bestaat deze informatie slechts uit een uniek identificatienummer, ook wel Electronic Product Code (EPC) genoemd, dat verwijst naar meer gedetailleerde informatie over het object die is opgeslagen in databases.

RFID zal in de toekomst veel van de huidige bar- of streepjescode vervangen of complementeren. RFID technologie heeft ten opzichte van de barcode of een aantal voordelen. De Electronic Product Code (EPC) opgeslagen op de RFID tag kan langer zijn dan de UPC code en kan hergeprogrammeerd worden. De EPC is een exemplaarnummer terwijl de barcode een artikelcode betreft: meerdere exemplaren van een zelfde artikel hebben dezelfde artikelcode maar een verschillende exemplaarnummer. Tags kunnen automatisch gelezen worden, zodra zij in de buurt van een lezer komen; je hoeft het object niet op een bepaalde manier voor een lezer te houden, zoals met een barcode: met radiogolven "werkt het ook om een hoekje" of "ergens door heen", in tegenstelling tot optische technieken. Dit maakt het mogelijk om de tags te verpakken in het product waardoor de RFID tag, in tegenstelling tot de barcode, minder vatbaar is voor fysieke beschadigingen en daardoor beter uit te lezen is. Nadelen van RFID tags zijn dat ze in het hogere frequentiegebied slecht werken in vochtige omgevingen en op metaal. Absorptie van de radiofrequentie-energie en reflecties liggen hier respectievelijk aan ten grondslag.



RFID wordt vooral gebruikt voor identificatie (bijvoorbeeld toegangscontrole), het voorkomen van winkeldiefstal en tracking & tracing. Maar de mogelijkheden van RFID gaan verder. Een breed scala van toepassingen is mogelijk door de combinatie van RFID tags met sensoren (temperatuur, locatie, luchtvochtigheid, etc.), communicatienetwerken (Personal Area Networks, WiFi, etc.) en draagbare computers (pda's, laptop, wearables etc.), zoals toepassingen rond persoonlijke identificatie/authenticatie, veiligheid en gepersonaliseerde diensten. Sectoren waarvoor RFID relevantie heeft variëren van de maakindustrie en logistiek en transport tot de gezondheidszorg en sociale veiligheid. RFID is een voorbeeld van een kleine, eenvoudige technologie met enorme potentie.

*Bij RFID wordt doorgaans gedacht aan tracking en tracing, maar een onbeperkt scala van toepassingen is mogelijk door de combinatie van slimme RFID tags met Personal Area Networks, WiFi, en draagbare computers.*

## **1.2 Waaron nu?**

RFID is een technologie die al veel langer bestaat. Meestal wordt gerefereerd aan de eerste toepassingen tijdens de tweede wereldoorlog bij het herkenbaar maken van eigen vliegtuigen ("friendly planes") door middel van op grote afstand herkenbare tags. Met de grote vooruitgang de laatste jaren in de halfgeleiderindustrie en bij de productie van RFID chips kunnen RFID tags nu veel kleiner en goedkoper geproduceerd kunnen worden.

Daarnaast maakt de aanwezigheid van breedband communicatie-infrastructuren (vast en mobiel internet) plotseling veel meer informatieontsluiting mogelijk, en liggen steeds meer toepassingen binnen bereik. Tags maken het mogelijk om de aanwezigheid van objecten op vele plaatsen waar te nemen en vast te leggen. Het Internet, dat als infrastructuur op steeds meer plaatsen beschikbaar is, biedt het platform om die "aanwezigheden" van één object op zijn reis, door bijvoorbeeld een handelsketen te volgen. Vandaar dat gesproken wordt over een "internet of things". Bedenk dat een vijftal jaren geleden elektronisch zakendoen over een veilig en betrouwbaar internet nog als een tour-de-force werd beschouwd. Thans is internet een vast ingrediënt geworden in de zorg, bij de overheid, in het bedrijfsleven en in maatschappelijk verkeer. Hierdoor wordt pas sinds enkele jaren op grote, wereldwijde schaal nagedacht over nieuwe RFID toepassingen.

RFID is een technologie die al veel langer bestaat. Met de grote vooruitgang de laatste jaren in de halfgeleiderindustrie en bij de productie van RFID chips kunnen RFID tags nu veel kleiner en goedkoper geproduceerd kunnen worden. Gecombineerd met de huidige goede beschikbaarheid van breedband communicatie-infrastructuren biedt dit nieuwe mogelijkheden.

## **1.3 Probleemstelling**

De breedte en veelheid aan potentiële toepassingen van RFID, de mogelijke belemmeringen die bij de invoering in de praktijk spelen, en de voor een deel onzekere implicaties van het gebruik geven mogelijk aanleiding tot beleidsontwikkeling. Er zijn raakvlakken met maatschappelijke vragen. Thema's inzake mogelijke RFID beleidsimplicaties hebben onder meer te maken met frequentiebeleid (verdeling van frequenties), de veiligheidsproblematiek (het kunnen uitlezen van tags door onbevoegden), het privacybeleid (bijvoorbeeld het volgen van werknemers en goederen, het al of niet verplichten om RFID tags aan te brengen), opslag van gegevens en innovatieve toepassingen (RFID als enabling technologie voor nieuwe diensten en toepassingen in de zorg en het onderwijs). Daarnaast zijn er technische aspecten die voor het DGTP werkerterrein van belang zijn zoals interferentie van systemen met RFID tags.

## **1.4 Vraagstelling**

In deze verkenning zal ingegaan worden of er daadwerkelijk aanleiding tot RFID beleid is en zo ja, hoe dit beleid dan vorm gegeven kan worden. Bij dit laatste moet gedacht worden aan keuzes rondom internationale afstemming, generieke of specifieke stimulering, het stellen van voorwaarden aan het gebruik van RFID, of aan de overheid als launching customer.

## **1.5 Doelstelling en resultaat**

De doelstelling van dit rapport is het in kaart brengen wat potentiële beleidsimplicaties betreffende het gebruik van RFID in Nederland zijn. Om deze doelstelling te bereiken wordt de volgende aanpak gevolgd.

Als eerste wordt er in Hoofdstuk 2 een overzicht gegeven van de technologie achter RFID en hoe deze techniek bruikbaar ingezet kan worden. Vervolgens geven we een beschrijving van enkele RFID toepassingen in verschillende sectoren. Deze toepassingen zijn bedoeld om de volle breedte van RFID te kunnen bevatten, en bovendien gericht op het kunnen identificeren en analyseren van de mogelijke beleidsimplicaties van deze toepassingen

In Hoofdstuk 3 beschrijven we een aantal knelpunten die voortvloeien uit deze toepassingen zoals o.a. knelpunten rond standaardisatie, beveiliging, privacy, innovatie, en invoeringsvraagstukken (implementatie). Per knelpunt zal worden aangegeven wat de mogelijke oplossingsrichtingen en beleidsimplicaties zijn en welke partijen hierbij op wat voor manier een belangrijke rol kunnen spelen.

Hoofdstuk 4 geeft een internationaal referentiekader. Deze scan van de internationale context betreft met name de argumenten vanuit overheden inzake stimulering van RFID, en de aard van deze stimulering.

Tot slot zal in Hoofdstuk 5 een samenvatting gegeven worden van de belangrijkste beleidsthema's voor de overheid betreffende RFID in Nederland en welke beleidsmiddelen ingezet zouden kunnen worden om dit beleid vorm te geven. Ook zal in dit hoofdstuk een blik op de verre toekomst geworpen worden omdat het beleid hiermee terdege rekening dient te houden.

## **1.6 Dankwoord**

De voorliggende verkenning is mede tot stand gekomen met de hulp en expertise van vele marktpartijen (aanbieders, system integrators, standaardisatieorganen, hardware leveranciers, kennisinstellingen, wetenschappers, en gebruikers) die samen zijn gekomen tijdens een workshop over de beleidsimplicaties van RFID. Onze dank gaat uit naar ECP.nl voor het helpen organiseren van de workshop. Een lijst van deelnemers is te vinden achterin de verkenning (Appendix A - ). Tevens zijn de hoofdresultaten van het ECP.nl onderzoek "Privacyrechtelijke aspecten van RFID" in de verkenning verwerkt. Daarnaast appreciëren wij de input van TNO betreffende privacy- en beveiligingsknelpunten van RFID (sectie 3.4.1).



## 2 RFID Toepassingen

### 2.1 Introductie

In dit hoofdstuk zullen we eerst kort toelichten uit welke elementen een RFID systeem bestaat. Daarna zal het gebruik van RFID aan de hand van verschillende bekende en minder bekende toepassingen in diverse sectoren geïllustreerd worden.

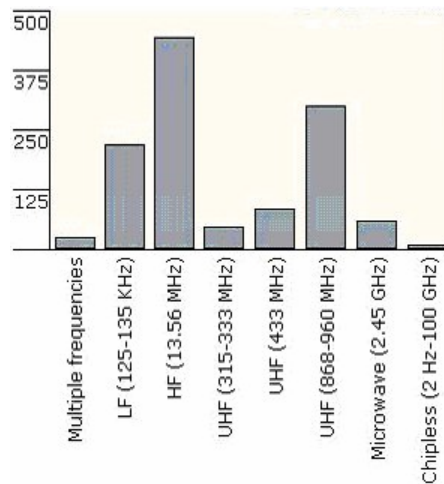
### 2.2 RFID systemen - De puzzelstukken van RFID

In het voorgaande is vooral gesproken over RFID tags. Maar RFID bestaat uit meer dan alleen tags. In deze sectie zullen we de verschillende elementen van een RFID systeem introduceren.

#### 2.2.1 Tags

Ruwweg drie typen RFID tags kunnen onderscheiden worden. Ten eerste de passieve tag, welke zijn energie via zijn antenne uit de radiogolven van de reader haalt. Hierdoor is het bereik beperkt, zijn de kosten laag, is de omvang van de tag relatief klein, en is de levensduur bijna oneindig. Het tweede type tag heeft een eigen batterij welke dient om de RFID tag van energie te voorzien die gebruikt wordt om zwakke radiosignalen op te pikken en voorzien van eigen informatie versterkt weer terug te sturen. Deze tags worden actieve tags genoemd. Actieve tags hebben een groter bereik, zijn duurder, hebben grotere afmetingen (voornamelijk vanwege de voor de batterij benodigde ruimte) en (ook weer vanwege de batterij) een beperkte periode waarin ze gebruikt kunnen worden. Het derde type tag is de semi-passieve tag. Deze tags hebben ook een interne batterij. De energie daarvan wordt echter niet gebruikt voor het versterken van de radiosignalen met het doel om de leesafstand te vergroten maar als energievoorziening voor extra in de RFID chip aanwezige elementen waarmee de intelligentie en geheugenopslagcapaciteit van de tag kunnen worden uitgebreid.

Passieve tags, voornamelijk opererend in het 13.56 MHz en 868-960 MHz gebied, zijn momenteel het meest gebruikt (zie Figuur 1). Desondanks is de populariteit van actieve tags relatief snel aan het toenemen voor bijvoorbeeld geavanceerde militaire- en identificatiesystemen. Actieve tags opereren veelal in het 433 MHz frequentiegebied. Actieve tags worden in tegenstelling tot passieve tags, ook vaak in combinatie met sensoren gebruikt omdat voor het verwerken van de sensordata extra energie nodig is. De in actieve tags aanwezige batterij levert die.



Figuur 1: Gebruik van de verschillende RFID frequentiebanden (uit [1]). LF = Low Frequency, HF = High Frequency, UHF = Ultra-High Frequency. De verticale as geeft het aantal RFID projecten aan. In totaal zijn er 1400 RFID projecten onderzocht.

Door het gecombineerde gebruik van RFID tags en sensoren kunnen specifieke aspecten van de conditie of toestand van het getagde object gemeten en doorgegeven worden aan de leverancier of ontvangende partij. Bijvoorbeeld het Duitse bedrijf Microsensys heeft zo een combinatie ontwikkeld waarbij een RFID tag met een temperatuursensor ingezet kan worden bij het transport van bederfelijke waren als fruit, melk, vlees, diepvriesproducten, bloemen of zelfs bloed. De tag geeft bij het uitlezen het gemeten en opgeslagen temperatuurverloop tijdens transport weer. De sensor heeft een temperatuurbereik van -30 tot +85 graden Celsius. Andere voorbeelden zijn combinaties met sensoren die de geografische locatie bepalen (op basis van GPS bijvoorbeeld), luchtvochtigheid of –druk meten of gevoelig zijn voor bepaalde (chemische) stoffen. Denk bij de laatste ook aan biosensoren.

### 2.2.2 Readers

RFID readers activeren met hun radiogolven de tags en vragen naar informatie. In sommige gevallen kan de reader ook de tag herprogrammeren en zorgen voor het coderen en decoderen van informatie. De communicatie tussen de reader en de computer of het achterliggende systeem gebeurt draadloos of via een kabel. RFID readers opereren typisch in een van de mogelijke frequentiegebieden aangewezen voor RFID en zijn daarom slechts bruikbaar voor bepaalde typen tags. Momenteel is er technisch gezien weinig variatie in de readers. Echter met het toenemende gebruik van RFID tags en de opkomst van een verscheidenheid aan applicaties worden de eisen die gesteld worden aan de readers steeds groter. Te denken valt aan "antibotsing" software om te voorkomen dat een reader meerdere tags tegelijkertijd uitleest, verificatiemogelijkheden om er zeker van te zijn dat alle tags gelezen zijn, software/hardware om interferentie tussen readers onderling te minimaliseren en beveiligingsmaatregelen om ongeautoriseerde toegang tot RFID data tijdens transmissie te voorkomen.

### 2.2.3 Netwerkinfrastructuur / middleware

Nadat de tag door de reader is uitgelezen moet in veel gevallen de data verwerkt worden in het achterliggende systeem (voor het beveiligen van objecten tegen winkeldiefstal is dit niet

per definitie nodig). Typisch zijn hier koppelingen met databases, ERP en CRM systemen met procesalgoritmes voor het verwerken van de ruwe RFID data tot betekenisvolle informatie. Veelal zijn de systemen waaraan gekoppeld moet worden erg heterogeen en is middleware vereist voor efficiënte integratie. De ontwikkeling van deze middleware staat nog in de kinderschoenen (zie ook sectie 3.5.4).

#### 2.2.4 Databases

Databases zijn nodig om de informatie van gelezen tags op te slaan gekoppeld aan een tijd- en locatieparameter. Databases kunnen centraal of gedistribueerd staan. Databases zullen het zwaar krijgen als in de nabije toekomst de enorme hoeveelheden tags veelvuldig gelezen zullen worden door een groot arsenaal aan readers. Niet alleen opslagcapaciteit is hierbij een potentieel knelpunt maar ook de performance van de database.

#### 2.2.5 RFID systemen

Met een *RFID systeem* bedoelen we in dit document een combinatie van tags, readers en IT-componenten die wordt gebruikt met een bepaald doel, in andere woorden voor een bepaalde *toepassing*, bijvoorbeeld het scannen van de inhoud van een pallet of het identificeren van een bloedmonster in een ziekenhuis.

*Met een RFID systeem bedoelen we een combinatie van tags, readers en IT-componenten die wordt gebruikt voor een bepaalde toepassing, bijvoorbeeld het scannen van de inhoud van een pallet of het identificeren van een bloedmonster in een ziekenhuis.*

#### 2.2.6 Kerntoepassingen

Voor toepassingen is het nodig om verbanden en patronen te identificeren in de verzamelde RFID gegevens. Bij toepassingen gaat het dus om het nuttig gebruiken en combineren van de mogelijkheden van RFID. Het plaatsen van een RFID tag op een object komt eigenlijk neer op het geven van een uniek nummer aan dat object. Dit heeft de volgende implicaties:

- RFID maakt het mogelijk dat fysieke objecten zonder enige visuele zichtlijn en in grote hoeveelheden automatisch in ingevoerd worden in informatiesystemen.
- Elk object is een index in een (wereldwijde) gedistribueerde database.
- Elk object heeft een eigen geschiedenis.
- Elk object kan gevolgd worden tijdens zijn levensduur.
- Er kunnen verbanden en patronen gemaakt worden.

Veel RFID toepassingen maken handig gebruik van deze implicaties. Bijvoorbeeld om een object te traceren of om iemand toegang te verlenen nadat hij/zij geïdentificeerd is. De essentie van RFID bestaat uit een aantal kerntoepassingen. Deze kerntoepassingen zijn:

1. Identificatie: De RFID tag geeft aan om welk object het gaat.
2. Authenticatie: De RFID tag toont aan dat het object origineel is, dwz het garandeert de authenticiteit van het object (ervan uitgaande dat er niet met de tag geknoeid kan worden zoals het verwisselen van de tag).
3. Monitoring/Sensing: Via RFID en sensoren wordt informatie verkregen over de context parameters van een object, bijvoorbeeld de temperatuur, locatie, of (bloed)druk.

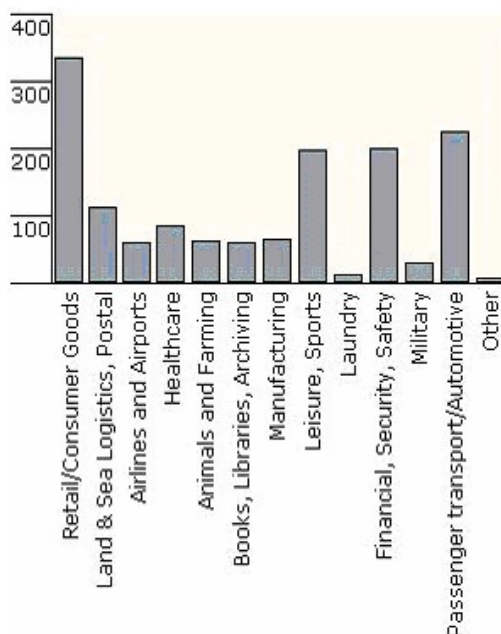
4. Data-opslag: De RFID tag bevat informatie die slaat op het getagde object.

Deze kerntoepassingen lenen zich bij uitstek voor een groot aantal zogenaamde afgeleide toepassingen in verschillende sectoren. Afgeleide toepassingen maken gebruik van een of meerdere kerntoepassingen van RFID om tegemoet te komen aan een bepaalde behoefte. Voorbeelden van afgeleide RFID toepassingen zijn toegangscontrole, betaaldiensten, tracking & tracing, controlesystemen, direct marketing en anti-diefstal en valsemunterij systemen.

## 2.3 Toepassingen van RFID

In deze sectie noemen we een aantal RFID toepassingen. Doel van de opsomming van RFID toepassingen is een beter beeld te krijgen van de impact en reikwijdte van RFID systemen. Uit de opsommingen volgt dat veel knelpunten rondom RFID niet los gezien kunnen worden van het toepassingsgebied.

In deze sectie geven we daarom een overzicht van mogelijke RFID toepassingen in de volle breedte. Om structuur aan te brengen maken we gebruik van een opdeling in sectoren. Figuur 2 geeft aan in welke sectoren RFID gebruikt wordt. De figuur is gebaseerd op een marktonderzoek over 1.400 RFID projecten in 68 landen [1]. Per sector zullen we één of meerdere bekende en minder bekende toepassingen van RFID beschrijven.



Figuur 2: Gebruik van RFID binnen verschillende sectoren (uit [1]). De verticale as geeft het aantal RFID projecten aan. In totaal zijn er 1400 RFID projecten onderzocht.

### 2.3.1 Retail en consumentengoederen

Iedere winkelketen manoeuvreert tussen de nachtmerrie van lege schappen en het debacle van te veel voorraad in de magazijnen. Om in de toekomst zeker te zijn dat de schappen altijd voldoende gevuld zijn terwijl de voorraad minimaal is, wordt RFID door veel retailketens ingevoerd. RFID zorgt voor een betere zichtbaarheid van de toeleveringsketen doordat van een product met een RFID tag altijd met redelijk zekerheid aan te geven is

waar het zich bevindt. Deze zichtbaarheid wordt niet alleen bereikt door een RFID tag op het product te plakken. Maar door een netwerk van readers op te zetten en het product continue te scannen. En daarnaast ook de gegevens over het product te delen. Hierdoor zijn goederen sneller op de eindlocatie, kunnen foutieve leveringen worden vermeden, wordt het beheer en opslag van gegevens makkelijker en er is minder voorraadruimte nodig. RFID leidt zo tot omzetverhoging (op tijd aanvullen van verkochte artikelen), kostenbesparing (doordat producten niet meer bederven of kwijtraken) en inzicht in de voorraden (asset management).

Het taggen gebeurt echter voornamelijk nog op pallet- of kratniveau. Door de nog relatief hoge prijs van de tags en de lage marges op de meeste retailgoederen loont het nog niet om op productniveau te taggen. De tags opereren in het UHF gebied. Ook zien we steeds meer het gebruik van RFID in combinatie met sensoren. Temperatuursensoren worden hierbij het vaakst gebruikt. Enkele aansprekende voorbeelden van RFID in de retail zijn VersSchakel en Wal-Mart (zie hieronder). Als pionierende sector, hebben veel RFID pilots te maken gekregen met consumenten die bezorgd waren om hun privacy. Het koppelen van persoonlijke klantgegevens aan het koopgedrag van de klant kan de privacy schaden. Metro heeft hierdoor zijn klantenkaart, die in eerste instantie voorzien was van een verborgen RFID tag, onder druk van consumenten- en privacyorganisaties moeten intrekken.

De volgende secties zijn gebaseerd op nieuwsberichten en schetsen een beeld van de mogelijkheden en problemen van het gebruik van RFID in de retail- en consumentengoederensector.

### ***VersSchakel [2]***

VersSchakel, waarin Schuitema, Heemskerk, CBL-Versfust, KPN, Wageningen-UR en Capgemini participeren is een van de weinige innovatieve RFID projecten in Nederland. Middels VersSchakel doen de genoemde partijen praktijkervaring op met kratten die zijn voorzien van RFID tags.

Met het project "VersSchakel" zetten de betrokken partijen een nieuwe stap in het sneller, beter en tegen lagere kosten bedienen van de consument door RFID technologie en temperatuurmeting op *fast moving consumer goods* (FMCG) producten te combineren met nieuwe besturingsconcepten om zodoende verse producten in de winkel te hebben staan. De consument staat centraal en er wordt gebruik gemaakt van internationale standaarden.

Aan de hand het temperatuurverloop van RFID getagde goederen wordt de goederenstroom zodanig aangestuurd dat de consument de aangeboden versproducten in een optimale kwaliteit aantreft in de winkel. Getagde goederen die bijvoorbeeld bij een relatief hoge temperatuur getransporteerd zijn zullen bijvoorbeeld eerder het distributiecentrum verlaten dan goederen die voldoende koel zijn gebleven.

Het volgen van de goederenstroom op kratniveau betekent een verdere detaillering van de goederenstroombesturing. Elke CBL-krat kan individueel gevolgd worden in de keten. Doordat het gaat om kratten uit een branchebreed gebruikte pool komen bij een verdere uitrol van het project de kratten met RFID tags voor een groot aantal gebruikers

beschikbaar. Dit kan een belangrijke stimulans betekenen voor het gebruik van RFID in de sector.

Het gebruik van standaard kratten met RFID tags biedt ook nieuwe mogelijkheden voor mechanisatie van de logistieke processen. Voor de beheerder van de krattenpool betekent het gebruik van RFID dat zij op zoek kan gaan naar nieuwe beheermodellen.

Het project 'Verschakel' maakt gebruik van UHF RFID tags volgens de Generation 2 standaard (ook wel *GEN 2* genoemd), een open ISO goedgekeurde standaard voor RFID die is uitgebracht door de internationale non-profit organisatie EPCglobal. Dit zijn de tags die GS1, de stichting die de toepassing van wereldwijde open standaards voor automatische identificatie en elektronische communicatie ten behoeve van bedrijven, consumenten en overheid bevordert, voorschrijft voor het gebruik van de Electronic Product Code. Daarnaast zal KPN een infrastructuur bouwen waarin de projectdeelnemers alle gegevens over de goederenstroombewegingen opslaan en voor elkaar beschikbaar maken. Zo kan men straks gegevens opvragen over de positie en conditie van een bepaalde krat in de keten. Tijdens het project zal men ervaring opdoen met een dergelijke vorm van informatiedelen en gebruiksrichtlijnen opstellen. Het project zal wereldwijd het eerste RFID project met een dergelijke infrastructuur zijn.

### ***Wal-Mart [3]***

Wal-Mart is momenteel een van de koplopers op het gebied van RFID. Een groot aantal producten van deze supergrutter zijn voorzien van RFID tags. Toeleveranciers worden min of meer gedwongen door Wal-Mart om hun producten van tags te voorzien. De POS-gegevens (point-of-sale) uit de 5300 winkels worden per satellietverbinding naar het hoofdkwartier gestuurd, waar de stroom van producten bijna realtime te volgen is. Een belangrijk deel van deze dataverzameling gaat over 'exceptions', een woord dat bij Wal-Mart staat voor te laat geleverde producten, foutieve verpakkingen, teruggebrachte spullen, etc. Er worden specifieke applicaties gemaakt die hierop alert zijn. Andere RFID specifieke applicaties zijn het automatisch versturen van een bestelorder van een product als de winkel daar behoefte aan heeft of het automatisch genereren van lijsten met producten die uit het magazijn naar de schappen moeten.

Ook de toeleveranciers van het concern hebben via een extranet toegang tot een deel van deze gegevens. Vooralsnog hebben ruim honderd leveranciers die aanleveren aan distributiecentra in Texas hier toegang toe. Veel leveranciers zijn niet echt gelukkig met de RFID dwang van Wal-Mart omdat de kosten hoog zijn en er onzekerheid is of deze kosten op lange termijn terugverdiend worden. De angst bestaat ook dat Wal-Mart in de toekomst meer gebruik gaat maken van scan-based trading (SBT), het systeem waarbij de toeleverancier eigenaar van het product blijft tot de detailhandel het verkoopt. Toeleveranciers zien hun geld pas nadat het product verkocht is. Als alle producten voorzien zijn van RFID tags wordt SBT haalbaar. Wal-Mart zou dan alle voorraadrisico's kunnen overhevelen naar de toeleverancier.

Onlangs heeft Wal-Mart enkele voorlopige testresultaten openbaar gemaakt. In een vergelijkend onderzoek tussen 12 winkels uitgerust met RFID en 12 winkels met het traditionele barcode systeem blijkt dat er 16% minder artikelen uitverkocht zijn in de RFID winkels is. De uitverkochte artikelen werden bovendien drie keer sneller aangevuld in de

winkels met RFID. Tevens was er een daling van de totale hoeveelheid producten in het magazijn.

#### ***Metro roept Payback klantenkaart terug [4]***

METRO AG heeft in 2005 geprobeerd om een RFID tag in haar "Payback" klantenkaart te stoppen zonder de klanten hiervan op de hoogte te stellen. Deze klantenkaart zou door de consumenten van de Duitse "Future Store" in Rheinberg gebruikt gaan worden. Na felle kritiek van privacy-activisten van FoeBuD [5], heeft METRO besloten om de kaart te vervangen door een exemplaar zonder RFID tag. METRO Future Store was ook al negatief in het nieuws rond haar (unieke) systeem dat RFID tags deactiveerde bij het verlaten van de winkel, en dat niet bleek te werken.

### **2.3.2 Logistiek en post**

In de logistieke sector valt met tracking en tracing van (zee)containers en poststukken met RFID in potentie veel winst te behalen. Het afhandelen van poststukken kan met RFID veel sneller omdat er tijdens het sorteren en voor het verzenden geen zichtlijn meer nodig is. Of het vanuit bedrijfseconomisch perspectief haalbaar is om alle poststukken met RFID te voorzien is echter nog onduidelijk. Het traceren van zeecontainers wordt al enige tijd gedaan met RFID technologie.

Hieronder volgen enkele "krantenknipsels" van RFID in de logistiek en post.

#### ***Wegwerptags verwerven miljoeneninvestering [6]***

De wegwerp-RFID-tags van het Zweedse bedrijf Cypak ontvangt 30 miljoen Zweedse kronen van het Swedish Industrial Development Fund voor het doorontwikkelen van de tags. Cypak ontwikkelde de tags speciaal voor documenten en ander wegwerpmateriaal. Het doel is om fraudeurs van documenten en producten af te schrikken. De Duitse en Zweedse post hebben al tests gedraaid met de wegwerptags. In de VS heeft verpakkingsbedrijf MeadWestvaco een licentie verworven van Cypak voor medische verpakkingen.

### **2.3.3 Luchtvaart**

Ook in de luchtvaartsector heeft RFID zijn intrede gedaan. Jaarlijks worden miljoenen koffers met bagage ingecheckt op verschillende luchthavens. Het is niet ongewoon dat een klein percentage van deze koffers niet aankomt op de plaats van bestemming. RFID wordt gezien als het middel dit probleem op te lossen. Net als bij de post, is het niet meer nodig om een zichtlijn te hebben met de koffer waardoor deze sneller verwerkt kan worden. Maar de luchtvaart gaat verder. Het bouwen en onderhouden van vliegtuigen is geen sinecure en luistert erg nauw. Met RFID tags kunnen deze processen efficiënter en effectiever uitgevoerd worden waardoor vliegtuigen sneller en in betere toestand het luchtruim weer in kunnen.

De volgende nieuwsitems illustreren de huidige stand van zaken in deze sector.

### ***RFID bouten [7]***

Het Japanse bedrijf KRD is er volgens RFID in Japan in geslaagd tags in ijzeren bouten op te slaan. Dat maakt het mogelijk informatie op te vragen over hoe hard bouten zijn vastgedraaid en of ze wel vast genoeg zitten.

Voor de constructie en het onderhoud van vliegtuigen, waar het essentieel is dat alles goed vast zit, is dit een interessante toepassing.

### ***Boeing verplicht RFID***

Na Wal Mart en het Amerikaanse ministerie van Defensie gaat nu ook vliegtuigbouwer Boeing zijn toeleveranciers het gebruik van RFID opleggen. Niet allemaal trouwens, in eerste instantie alle bedrijven die bij het 787 Dreamliner project zijn betrokken (de nieuwe generatie Boeing-toestellen). Boeing's eis gaat zelfs nog verder dan die van Wal Mart. Boeing wil namelijk gebruik maken van 64 kbyte passieve tags die bestand zijn tegen veranderingen in druk, temperatuur en vochtigheid en die tevens onderhouds- en inspectiedata met zich mee dragen. Probleem is dat deze tags nog niet bestaan....

### ***Schiphol wil chips in bagage invoeren [8]***

Schiphol wil alle koffers uitrusten met een RFID tag. De bagage blijkt zo namelijk veel beter te volgen dan met de huidige manier, waarbij een streepjescode wordt gebruikt. Afgelopen zomer hebben Schiphol en KLM de nieuwe technologie getest. Op het traject Amsterdam – Narita (Japan) kregen alle koffers een radiochip (RFID) mee. De resultaten waren goed; de tags waren, aldus een woordvoerder, erg betrouwbaar. Wat een algehele invoering nog in de weg staat is het feit dat er op dit moment nog geen internationale standaard is. Zo gebruikte Schiphol bij de proef hoge radiofrequenties, terwijl Delta Airlines – dat een soortgelijke proef had draaien – ultrahoge frequenties gebruikte. De IATA (internationale organisatie voor de burgerluchtvaart) heeft inmiddels wel een dergelijke internationale standaard in het leven te roepen.

### ***IATA voert RFID standaard in [9]***

De internationale luchttransport vereniging (IATA) heeft een wereldwijde standaard geïntroduceerd voor bagage RFID-tags. Hiermee wordt gestreefd naar een wijdverspreid gebruik van RFID bij het beheer van de bagageafhandelingen. Ook hoopt IATA dat de fabrikanten van tags zich bewust worden van een nieuw marktsegment en dat daardoor de prijzen van tags naar beneden zullen gaan.

## **2.3.4 Zorgsector en farmaceutische industrie**

In de zorgsector vinden momenteel steeds meer RFID toepassingen hun weg. Met name de grote variëteit in de toepassingen is opmerkelijk. Belangrijke drivers zijn het verbeteren van het welzijn van de patiënt en verkorten van de wachtrijen [10]. Enkele toepassingen van RFID in deze sector zijn:

- Patiënt identificatie en lokalisatie. Betere identificatie van patiënten en baby's in ziekenhuizen verkleint de kans op fouten bij bijvoorbeeld het toedienen van medicijnen of operaties. Er is zelfs geopperd om tags in het lichaam van de patiënt te plaatsen op de plaats waar geopereerd moet worden. Dit om te voorkomen dat bijvoorbeeld het verkeerde been geamputeerd wordt.
- Traceren en lokaliseren van medische apparatuur. Vaak worden medische apparaten door meerdere afdelingen in een ziekenhuis gebruikt. Soms worden ze zelfs uitgeleend aan andere ziekenhuizen. Omdat het hier vaak om relatief dure apparatuur gaat en het zoeken hierna in noodsituaties niet gewenst is, biedt RFID uitkomst. Andere alternatieven voor het lokaliseren van objecten werken niet in gebouwen (zoals GPS) of zijn te duur (zoals WLAN). Interferentie met de medische apparatuur is een regelmatig terugkomend probleem. Echter, enig experimenteren met de locatie van de tag op het apparaat lost dit probleem vaak op.
- Voorkomen van vervalsen van medicijnen / namaakmedicijnen opsporen. Net als in de automobielenindustrie heeft ook de medische sector te kampen met namaakproducten. De gevaren van vervalste medicijnen zijn echter vele malen ernstiger dan bij een vervalste waterpomp. Een RFID tag kan de authenticiteit van een medicijn helpen garanderen. Veel farmaceutische bedrijven, zoals Pfizer en Bayer werken hier daarom hard aan.
- Controleren of tandprotheses en kronen bij de juiste persoon horen door ze te voorzien van RFID tags [11]. Tijdens het productieproces wordt een RFID tag in de prothese gestopt. Vaak is deze prothese in eerste instantie niet goed, moet aangepast of gerepareerd worden. Via de RFID tag weten de tandtechnici precies bij wie een prothese hoort doordat de identifier in de tag gekoppeld is aan de patiënt. Dit werkt efficiënter en resulteert in minder fouten.
- Het monitoren van de temperatuur van gevulde bloedtransfusiezakken. Veel volle bloedtransfusiezakken verdwijnen in de vuilnisbak omdat de temperatuurgeschiedenis ervan onzeker is. RFID in combinatie met een temperatuursensor garandeert de kwaliteit van het transfusiebloed.

Door de gevoeligheid en het belang van medische informatie is het belangrijk dat het RFID gebruik in deze sector aan strikte regels gebonden is. De Food and Drug Administration (FDA) in de Verenigde Staten geeft duidelijk aan op welke manier medicijnen getraceerd dienen te worden [12]. De FDA heeft hierbij een sterke voorkeur voor het gebruik van RFID als de best mogelijke optie (gezien de huidige RFID ontwikkelingen) voor het elektronisch tracken & traceren van medicijnen. Mogelijk zal, bij uitblijven van initiatieven uit de industrie, de FDA in de toekomst een mandaat uitbrengen waar RFID verplicht wordt. Ook de Health Insurance Portability and Accountability Act (HIPAA) 'Privacy and Security Rules' biedt een goede richtlijn voor het ontwikkelen van een 'code of conduct' voor RFID binnen de zorg [13].

De onderstaande nieuwsflitsen geven een beeld van de toepassingen van RFID in de zorgsector en farmaceutische industrie.

### ***RFID tegen het vergeten [14]***

De Finse Alzheimer Vereniging heeft in samenwerking met Pfizer, Nokia, Elisa en Medixine, een telefoon ontwikkeld met een geïntegreerde RFID lezer. Patiënten met de ziekte van Alzheimer kunnen op die manier worden herinnerd aan bijvoorbeeld de medicatie of afspraken.

### ***Eerst een tag in je arm, dan het ziekenhuisbed in [15]***

De Amerikaanse Food en Drug Administration (FDA) heeft voor het eerst een implanteerbare RFID chip goedgekeurd. Het bedrijf VeriChip heeft deze tag, niet groter dan een rijstkorrel, ontwikkeld voor de gezondheidszorg zodat patiënten beter gemonitord kunnen worden. Artsen kunnen nu simpelweg op een website inloggen om de patiëntendata te lezen<sup>1</sup>.

#### **2.3.5 Dieren en Agrarische sector**

In Nederland is de RFID tag massaal in gebruik ter identificatie van grote en kleine (huis)dieren. Miljoenen koeien kregen hiervoor de tag in hun gele oormerk, evenals veel katten en honden die al dan niet tijdelijk verbleven in een asiel.

In de agrosector worden veel veilingkarren al enige tijd getraceerd met behulp van RFID. Zodra deze kostbare karren de veilinghal verlaten worden ze geregistreerd. Daarnaast zijn er nog tal van andere toepassingen van RFID in deze sector denkbaar. Het is bijna onvoorstelbaar welke reis een slachtvarken of -koe soms aflegt alvorens de consument zijn lapje vlees kan eten. Reisschema's via Frankrijk en Italië, om vervolgens weer terug te keren in Nederland zijn geen uitzondering. Dit gegeven in combinatie met de recente uitbraken van varkenspest en de ziekte van Kreutzfeld Jacob ("gekke-koeien-ziekte") hebben ertoe geleid dat vee beter getraceerd moet kunnen worden. RFID kan hiervoor zorgen.

Vanuit de Europese wet- en regelgeving worden steeds hogere eisen geteld aan de traceerbaarheid van artikelen. Per 1 januari 2005 is bijvoorbeeld de *General Food Law* van kracht gegaan. Deze wet schrijft voor dat elke logistieke keten één schakel terug en één schakel vooruit moet kunnen aangeven waar een product vandaan kwam en waar het naar toe is gegaan. Binnen (vooralsnog) vier uur moet bekend zijn wat de oorsprong van een product is. Het wordt als een van de voordelen van RFID gezien dat met (of zelfs dankzij) RFID deze wet kan worden geïmplementeerd. Hiervoor is wel RFID tagging op artikelniveau voor nodig. Ook met (geserialiseerde) barcodes zou dit probleem opgelost kunnen worden.

Hieronder volgen we enkele illustratieve voorbeelden van het gebruik van RFID in deze sectoren.

#### ***Tags moeten gekke koeien tegenhouden [16]***

'Animal Industry Lab' in het Japanse Takayama ontwikkelde een nieuwe gezondheidszorg speciaal voor koeien. De beesten krijgen een speciale RFID tag in hun maag (de tag is groter dan normaal zodat deze niet zomaar uit de maag verdwijnt). En zo wordt elke keer als ze zich in de buurt van een meetpunt begeven, hun lichaamstemperatuur gemeten. Het

---

<sup>1</sup> Meer dan 1000 VeriChips zijn momenteel verkocht waarvan de meeste gebruikt zijn voor klanten van de Baja Beach Club. Voor zover bekend zijn er nog geen medische toepassingen uitgevoerd met de chip.

aantal metingen kan trouwens worden uitgebreid naar ademhalingsritme, hartslag en gegevens over het kalf als de koe zwanger is.

### ***Ruzie over honden en katten [17]***

In de VS is een 'bitter' conflict ontstaan over de vraag welke radiofrequentie nou gebruikt gaat worden voor het traceren van vee en huisdieren. Eigenaren en dierenartsen willen een internationale standaard van frequentie X, terwijl een paar Amerikaanse fabrikanten, die voor hun tags een lagere frequentie gebruiken, blijven protesteren. Een tweede obstakel vormt de vraag of de gegevens versleuteld moeten worden.

### **2.3.6 Boeken, bibliotheken en archieven**

Musea gebruiken RFID voor het indexeren van de stukken. In Nederland worden momenteel naast barcodes ook RFID tags aan bibliotheekboeken toegevoegd [18]. Bibliotheken gebruiken deze tags voor het traceren van boeken en om teruggebrachte boeken weer snel te kunnen terugzetten in de kasten. Op basis hiervan hebben bijvoorbeeld fabrikanten als Nedap boekenkasten ontwikkeld die weten welke boeken ze bevatten [19].

### **2.3.7 Maakindustrie**

Het assembleren van machines is het werk van moderne robots. Met RFID in de assemblagelijnen kunnen robots aan de hand van de informatie die verkregen wordt op basis van de tag begrijpen wat ze moeten doen. Tevens kan in de gaten gehouden worden of, en hoe, alle handelingen uitgevoerd zijn. Zo zou bijvoorbeeld gecontroleerd kunnen worden of een schroef voldoende strak is aangedraaid.

### **2.3.8 Sport en vermaak**

Een bekende RFID toepassing in deze sector is die van de skiliften en pasjes. Met een LF of HF RFID tag in de skipas wordt toegang gekregen tot de skilift. Andere toepassingen zijn het gebruik van RFID bij marathons en autoraces waar de posities van de lopers en auto's geregistreerd worden. Ook Legoland gebruikt RFID voor het traceren van kinderen die hun ouders zijn kwijtgeraakt. Andere themaparken zoals Disneyland hebben plannen om RFID in te zetten voor het reserveren van drukke attracties. Casino's zetten RFID gelabelde fiches in om vervalsing ervan tegen te gaan.

Ter illustratie van de mogelijkheden en knelpunten van RFID volgen hieronder enkele voorbeelden die het nieuws gehaald hebben.

### ***Wereldkampioenschap voetbal 2006 vol met RFID [20]***

Tijdens het wereldkampioenschap voetbal in Duitsland volgend jaar zomer zullen vele nieuwe technieken worden gebruikt. Het gebruik van RFID is ook prominent aanwezig want

95% van de 3,37 miljoen te verkopen kaarten wordt voorzien van RFID tags om vervalsing en illegale wederverkoop te voorkomen<sup>2</sup>.

### ***Nederlands bedrijf levert RFID tijdwaarneming Indy 500 [21]***

Het Nederlandse bedrijf AMB i.t. (identification and timing) leverde het tijdwaarnemingsysteem voor de Indy 500. Elke auto is voorzien van een transponder. Het signaal wordt opgevangen door een detectieloop in het asfalt. AMB levert ook systemen aan de 24 uur van Le Mans en de Olympische Spelen. Bij het bedrijf werken 60 mensen, die samen een omzet van 10 miljoen euro realiseren. AMB is onderdeel van het aan de Euronext genoteerde HAL Trust Holding.

### **2.3.9 Wasserettes**

In grote wasserettes wordt vaak de was van verschillende klanten tegelijkertijd gewassen. Het sorteren van de gewassen kledingstukken was naderhand altijd een monnikenwerk. Met RFID is dit geen probleem meer omdat ieder kledingstuk door middel van een RFID tag en identifieer gekoppeld is aan een klant. De RFID tag kan zelfs aangeven welk wasprogramma gewenst is. Het taggen van kleding kan ook door de retail gebruikt worden voor het geven van mode-adviezen, inruilen van gekochte kleding zonder aankoopbon, indexeren van kledingstukken met veel verschillende maten zoals BH's, en voor het in kaart brengen van het koopgedrag van de consument. Vooral dit laatste heeft voor veel onrust en protest bij consumenten gezorgd en heeft ertoe geleid dat Benetton alle RFID tags uit de kledinglijn heeft gehaald.

### ***Wasmachine leest kledingstukken [22]***

In zijn niet aflatende pogingen om onze huizen volledig van tags en lezers te voorzien heeft het Japanse Dai Nippon Printing nu een wasmachine met RFID lezer ontwikkeld. De machine geeft automatisch aan wat de beste methode is om kledingstukken te wassen. Mits rok, pak of overall voorzien is van een tag natuurlijk. Ook handig: de LG WM-2277HW houdt ook bij hoe vaak een kledingstuk is gewassen, uit welk materiaal het bestaat en stuurt een mail of sms wanneer de was klaar is.

### ***CASPIAN: Geheim plan voor tags in kleding [23]***

Privacyorganisatie CASPIAN beweert dat RFID fabrikant Checkpoint 'spychips'<sup>3</sup> ontwikkelt voor Abercrombie & Fitch, Calvin Klein, en Champion sportkleding. In theorie kunnen mensen die deze kleding dragen door alle Checkpoint tag-lezers getraceerd en geïdentificeerd worden, schrijft CASPIAN. De organisatie meldt verder dat Checkpoint al een systeem van detectiepoorten heeft geïnstalleerd in een reeks winkels. Maar deze theorie kan al praktisch zijn, zegt CASPIAN, want er is geen wettelijke bepaling die retailers

---

<sup>2</sup> Waarom de overige 170.000 kaarten geen tag hebben is onduidelijk.

<sup>3</sup> CASPIAN associeert RFID tags met zogenaamde spychips die alles van je in de gaten houden.

voorschrijft dat consumenten op de hoogte moeten worden gebracht van het gebruik van RFID tags.

### **2.3.10 Financiële- en beveiligingssector**

Banken en andere financiële instellingen zijn al enige tijd bezig om RFID in te zetten voor het betalingsverkeer. Met RFID zou gemakkelijk en veilig betaald kunnen worden. Met name de veiligheid is hier van cruciaal belang.

In Japan zijn al 6 miljoen telefoons met RFID technologie die in principe voor betaling kan worden gebruikt. In Europa loopt de discussie of bankbiljetten van een RFID tag moeten worden voorzien voor het traceren van geld. Voor tolheffingen op autosnelwegen, tunnels en bruggen wordt RFID al ingezet [24]. Elke auto met een RFID tag op de voorruit wordt gescand voor het betalen van de tol.

Zonder er misschien bij stil te staan, is de beveiligingssector een van de grootste gebruikers van RFID. Bijna alle toegangspoortjes naar bedrijfsterreinen en in gebouwen werken met RFID. Het betreft hier vaak LF RFID tags met een betrekkelijk korte scanafstand.

Enkele toepassingsvoorbeelden staan hieronder.

#### ***ABI: Contactloos betalen in aantocht [25]***

Of het nou om RFID of Near Field Communication gaat, volgens het New Yorkse ABI Research betalen we binnenkort allemaal zonder onze pas te gebruiken. Gewoon door langs een poortje te lopen. Ook Philips zet in op NFC én RFID maar afzonderlijke bedrijven zullen slechts één van beide systemen gebruiken.

#### ***VISA lanceert betalen via RFID [26]***

De Amerikaanse tak van credit card imperium VISA lanceerde recentelijk een systeem waarbij klanten door met VISA kaarten voor een terminal te zwaaien, kleine bedragen kunnen overmaken. Het systeem is speciaal bedoeld voor kleinere aankopen zoals fastfood, films etc. MasterCard loopt niet ver achter. De concurrent is bezig met het testen van het PayPass systeem. American Express is bezig met ExpressPay.

#### ***RFID betaalgemak in Japan [27, 28]***

Enkele cijfers rondom het gebruik van RFID voor financiële transacties in Japan:

- Telefoons met RFID chip voor betalen: 6 miljoen
- 20 % van de gebruikers van deze RFID telefoon heeft deze altijd aan staan
- 12,4 miljoen RFID prepaid kaarten uitgegeven tot nu toe. De technologie kan gebruikt worden in 23.000 winkels.
- Het aantal treinkaarten gebaseerd op RFID is 13,5 miljoen, waarvan 8 miljoen inclusief aparte betalingsmogelijkheid (voor de eerlijkheid: maar 1200 winkels accepteren betalingen van deze zogenaamde SUICA-kaarten).

### **2.3.11 Defensie en douane**

Na verschillende de terroristische aanslagen is "homeland security" een hot topic. Strengere grensbewaking en de ontwikkeling van een nieuw biometrisch paspoort met RFID chip zijn hiervan enkele uitvloeiselen. Ook gevangenen en TBS'ers worden met RFID in de gaten gehouden.

#### ***Definitieve richtlijnen ministerie van Defensie [29]***

Het Amerikaanse ministerie van Defensie publiceerde recent de definitieve RFID richtlijnen voor zijn toeleveranciers. In contracten die na 1 oktober 2005 worden gesloten met het ministerie en waarin het gaat om materiaal dat na 1 januari 2006 wordt afgeleverd, worden toeleveranciers verplicht om tags op pallets aan te brengen. Alle containers die naar overzeese bestemmingen worden verscheept, moeten van actieve RFID tags worden voorzien (actief = met een eigen energiebron) waarin de inhoud van de container is vastgelegd door de leverancier. Oplopend naar 1 januari 2007, vallen elk jaar meer goederen onder de RFID richtlijnen van het ministerie. Vanaf 1 januari 2007 betekent dit dat alle pallets met goederen – dus militaire goederen, medische goederen luxe goederen etc. – die waar dan ook naar toe gaan, van tags moeten worden voorzien.

### **2.3.12 Automobielsector en personentransport**

Vervalsingen van onderdelen is een van de grootste problemen in de automobielsector. Omdat de reserve onderdelen business een belangrijke bron van inkomsten is voor veel bedrijven in deze sector is de impact groot. Er wordt geschat dat ongeveer 10 procent van alle auto-onderdelen vals is. Dit komt neer op een inkomstenderving van ongeveer 12 miljard euro per jaar. RFID biedt een unieke gelegenheid om dit soort praktijken tegen te gaan.

Daarnaast hebben terugroepacties in de sector voor grote onkosten gezorgd. Publieke terugroepacties zijn duur en schaden ook het imago van de fabrikant. De terugroepactie van Firestone in Amerika in 2000 kostte ongeveer 14.4 miljoen dollar, waarbij ook autofabrikant Ford een schade van ongeveer 2.6 miljard dollar opliep (Ford maakte gebruik van Firestone banden). Ook hier kan het gebruik van RFID technologie uitkomst bieden om terugroepacties sneller en meer precies te laten verlopen waardoor de schade beperkt blijft.

Wereldwijd zijn de toepassingen van RFID in de automobielsector erg divers. BMW gebruikt RFID voor de identificatie van de auto tijdens het productieproces. Ford, daarentegen, gebruikt het voor identificatie van motoren tijdens de productie en voor container tracking. Volkswagen voor het lokaliseren van gereedgekomen auto's in de fabriek.

Andere toepassingen voor RFID in de automobielsector industrie zijn just-in-time productie, onderdeel-tracking, voorraadbeheer, tegengaan van productimitaties/ervalsingen, distributie en transport, vastleggen reparatiegeschiedenis en volledige automatische assemblage.

Ook voor het vervoer van personen wordt RFID ingezet. In Japan kunnen mensen na een taxirit via hun RFID enabled mobiele telefoon draadloos betalen. LogicaCMG heeft een toepassing ontwikkeld waarbij met RFID in combinatie met een temperatuursensor de

kwaliteit van de wielen van een hogesnelheidstrein in de gaten gehouden kan worden. Een te hoge temperatuur leidt tot een vervorming van het wiel waardoor de reizigers minder comfortabel reizen en het spoor sneller schade ondervindt. Met de toepassing kunnen wielen sneller en effectiever vervangen worden.

Hieronder volgen enkele nieuwsberichten die het gebruik en de mogelijkheden van RFID in de sector illustreren.

### ***RFID cruciaal voor auto-industrie [30]***

Dat beweert een nieuw rapport van onderzoeksbureau Research and Markets. Onderzoek bij 526 RFID leveranciers zou ten grondslag liggen aan de bevindingen. De auto-industrie zou een net-op-tijd-beleid voeren ten aanzien van inventarismanagement bij de dealers. Zelfs bij kleine vergissingen kan dat kostbare gevolgen hebben, stelt het rapport.

### ***Brits kenteken gechipped [31]***

De Britse overheid bereidt een pilot voor waarin nieuwe Britse kentekens worden voorzien van RFID chips. Ook de Amerikaanse overheid heeft plannen met kentekens en RFID en heeft al aangegeven de Britse proef met belangstelling te zullen volgen.

## **2.3.13 Overige sectoren**

Naast de bovenstaande sectoren zie je in algemenere zin dat RFID als technologie opduikt in infrastructuur, zowel infrastructuur in het huis (domoticoepassingen) als in communicatienetwerken.

### **2.3.13.1 RFID in de ICT Infrastructuur**

Veel ouderen zijn vaak aan hun lot overgelaten. Het sociale toezicht is bij velen minimaal. In combinatie met een slechte (fysieke) gezondheid kan dat soms leiden tot nare situaties. Regelmatig wordt er in het nieuws weer melding gemaakt van een bejaarde die al enige tijd dood in haar huis lag. Door slim om te gaan met RFID gegevens van bijvoorbeeld getagde objecten in het huis kan al snel afgeleid worden of er iets verdachts aan de hand is. Het niet opengaan van de koelkast gedurende een lange periode kan resulteren in een seintje naar de zorgverlener om eens een kijkje te gaan nemen bij een bejaarde persoon.

In het bovenstaande voorbeeld is sprake van een zogenaamd "smart home". Het huis weet door middel van een aanwezige RFID infrastructuur wat er allemaal gebeurt. Een ander aansprekend voorbeeld van RFID in een smart home is dat van automatische robotstofzuigers. Deze stofzuigers zuigen het tapijt mooi schoon via RFID tags in het tapijt [32].

De telecomsector is ook al enige tijd aan het kijken wat de meerwaarde van RFID zou kunnen zijn [33]. Enkele toepassingen hier zijn:

- Het ophalen van informatie: een RFID telefoon wordt over een poster of andere objecten gehaald om meer informatie te krijgen [34].
- Geautomatiseerde berichtgeving: het ontvangen van een bericht als je langs een tag loopt (ervan uitgaande dat de mobiele telefoon een geïntegreerde RFID tag lezer heeft).

- Bellen van foto's: plaats een tag achter een foto en je mobiele telefoon gaat bellen nadat deze over de foto is gehaald.
- Integratie van mobiele telefoon met omgeving: de mobiele telefoon 'weet' dat deze in de auto is geplaatst en schakelt automatisch over naar hands-free mode. Deze toepassing kan bijvoorbeeld ook gebruikt worden om de telefoon uit te schakelen op bepaalde locaties (ziekenhuizen, vliegtuigen, conferentieruimtes, etc.).
- Aanwezigheid: detecteren van een mobiele telefoon in een bepaalde ruimte.

Desondanks lijken deze toepassingen maar niet van de grond te komen. Mogelijk heeft dit te maken met het gebrek aan standaardisatie in de gebruikte RFID technologie en diensten. Daar komt bij dat privacy altijd een extra zorg is in deze sector en het onduidelijk is wat precies de impact van RFID op het mobiele netwerk is [35]. Hierbij moet o.a. gedacht worden aan de impact op de capaciteit van de dataverwerking, schaalbaarheid van de netwerk architectuur, integratie van hardware en beveiliging. Schaalgrootte is een andere belangrijke factor voor veel van de hierboven genoemde toepassingen. Een breed aanwezige RFID infrastructuur is hiervoor nodig. Een dergelijke infrastructuur is er momenteel nog niet.

### **2.3.13.2 RFID tags op personen**

In eerdere paragrafen is het taggen van mensen al aangestipt. Het bedrijf Applied Digital Solutions brengt sinds een aantal jaren een RFID tag speciaal voor mensen op de markt: de Verichip [36]. De marketing begon na 2002, met de WTC-aanslagen nog vers in het geheugen. De bedoeling was "terrorisme tegen te gaan". Mensen zouden eigenlijk allemaal een dergelijke chip moeten hebben, aldus Applied Digital. In Zuid-Amerika werkt men o.a. samen met het beveiligingsbedrijf Metro Risk Management dat ontvoeringen oplost voor bedrijven en welgestelden (taggen van kinderen tegen ontvoering). Ook richt het bedrijf zich op medische toepassingen. In de chip kan 128 bits aan informatie tekens worden opgeslagen. De informatie op deze chip verwijst vervolgens naar een dossier, dat bijvoorbeeld op internet is te raadplegen. Het systeem werkt, maar aangezien ambulancepersoneel niet is uitgerust met een RFID scanner is het nut beperkt.

Daarnaast vindt het taggen van mensen plaats vanwege een "publiciteitsstunt". In Nederland is de Rotterdamse Baja Beach Club in het nieuws gekomen met een onderhuidse tag waarmee bezoekers kunnen betalen en dus geen portemonnee op zak behoeven te hebben [37]. Ook gevangenen en TBS'ers lijken een uitgelezen doelgroep, wellicht daarna ook personen met een strafblad. Zowel in Nederland als in het buitenland vinden hier (grootschalige) pilots plaats, zoals in Ohio, USA, met 44.000 gevangenen, overigens met elektronische enkelbanden als een vorm van digitale controle [38].

Naast privacy aspecten (de tag is namelijk niet zomaar uit te zetten) en het punt van lichamelijke integriteit zijn er vanuit religieuze organisaties ook principiële bezwaren tegen deze ontwikkeling (gewetensbezwaren) [39].

#### ***Christenen tegen RFID [40]***

Volgens Freshplaze roepen – enkele – Amerikaanse christenen op tot een boycot van wat zij als het bijbelse 'teken van het beest' zien: de RFID tag. Kon Openbaringen 13:16-18 nog duidelijker zijn: 'Het beest dwong alle mensen, groot en klein, rijk en arm, vrijen en slaven,

op hun rechterhand en op hun voorhoofd een merkteken te dragen. Daardoor kon alleen iemand iets kopen of verkopen als hij dat merkteken droeg, dat wil zeggen: de naam van het beest of het getal dat het symbool van die naam is'.

### ***Slachtoffer identificatie met RFID [41]***

Met behulp van RFID proberen doodgravers in en rond New Orleans het hoofd boven water te houden. De tragische ramp met de orkaan Katrina heeft zoveel slachtoffers veroorzaakt dat het moeilijk wordt het overzicht te bewaren over de talrijke stoffelijke overschotten. De RFID tags worden in de lichamen geïmplantéerd of in de 'bodybag' geschoven.

### ***Robot voor blinden [42]***

Amerikaanse wetenschappers hebben een robot ontwikkeld die navigeert via RFID. Volgens de makers kan de robot blinden helpen om in grote warenhuizen boodschappen te doen. RFID kan dan de items op een boodschappenlijst in de schappen signaleren.

## **2.4 Wat gebeurt er in Nederland rond RFID?**

Nederland heeft op dit moment nog een bescheiden 'track record' als het gaat om RFID. De RFID ontwikkelingen worden met enige terughoudendheid gevolgd. Echte voorbeelden van 'early adaptors' die leidend zijn in hun sector zijn er nauwelijks. Enkele sectoren waarin Nederland actief is met RFID worden hieronder beschreven.

Van oudsher is Nederland sterk in het managen van logistieke processen ('Nederland Distributieland'). Dit is ook terug te zien in de verschillende RFID projecten die in ons land zijn uitgevoerd of worden uitgevoerd. Goed voorbeeld is het VersSchakel project (zie sectie 2.3.1) waar logistieke eenheden met RFID worden gevolgd. Het betreft hier RFID tags in het 433 MHz gebied gecombineerd met een temperatuursensor.

Ook in onze nationale trots, de bloemensector, wordt gebruikt gemaakt van RFID. Al in 2001 voorzag Floraholland (voorheen bloemenvéiling Holland) 100.000 stapelwagens van RFID-tags van Texas Instruments voor het tracken & tracen van deze kostbare eenheden.

Er zijn experimenten op Schiphol bij de bagageafhandeling. Het betreft hier tags die opereren in het UHF gebied.

De Nederlandse Bibliotheek Dienst/Biblión is een van de weinige Nederlandse organisaties die RFID chips al op grote schaal gebruikt. De NBD/Biblión plaatst de chips in alle boeken die ze aan Nederlandse bibliotheken levert, ongeveer 2,7 miljoen per jaar.

Een relatief nieuwe sector waar RFID zijn weg vindt is de zorgsector. Ook hier vinden verschillende experimenten plaats [43]. Doel van de experimenten is de meerwaarde van RFID toepassingen in de zorg aan te tonen. De belangen in deze sector zijn groot. Op dit moment staat een aantal knelpunten in de zorg hoog op de politieke agenda. Denk aan de vergrijzing, de vermindering van het aanbod van zorgverleners, een sterke stijging van de kosten van de zorg en de wachtlijstproblematiek. Het toepassen van RFID innovaties in de zorg geeft mogelijk een deel van het antwoord op deze maatschappelijke knelpunten.

De Rabobank ziet met RFID nieuwe methoden van elektronisch betalen ontstaan. Rabobank wil daarbij zelf ook het initiatief nemen. Volgens Rabobank zal het met RFID op termijn mogelijk zijn om aankopen contactloos af te rekenen, al dan niet door het gebruik van credit/debitcards of mobiele telefoons (iets dat in Japan al mogelijk is).

Philips Semiconductor is een belangrijke chipproducent, en ontwikkelt de chips onder de naam I-code. Philips voorziet bijvoorbeeld de entreekaartjes van het WK voetbal, volgend jaar in Duitsland, van RFID-chips. Op de kaartjes komt alleen een naam te staan, andere gegevens als de locatie van de zitplaatsen komen op de chip te staan. Nedap is een ander Nederlands bedrijf dat al jaren bezig is met RFID technologie in de agrarische sector, in de retail en voor toegangscontrole. Ook de nieuwe Nederlandse paspoorten zullen voorzien worden van Philips chips.




De meest bizarre toepassing is de Baja VIP chip van de Baja Beach Club in Rotterdam. VIP-bezoekers kunnen onderhuids een RFID tag laten plaatsen. De rekening van de drankjes wordt afgeschreven van het saldo op de tag.

In Nederland zullen de eerste grootschalige toepassingen van RFID de OV-chipkaart en het biometrisch paspoort zijn. Met de OV-chipkaart worden al op kleine schaal proeven uitgevoerd. De verwachting is dat het systeem in 2007 overal in Nederland bruikbaar is. De Nederlandse overheid experimenteert in een aantal gemeenten met paspoorten die een RFID tag bevatten met daarop de biometrische gegevens (gelaatsscan en vingerafdruk) van de eigenaar.

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 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.

## **2.5 Marktpotentieel RFID toepassingen**

Bovenstaand zijn verschillende toepassingen geïnterpreteerd. De ene RFID toepassing zal echter realistischer zijn dan de andere. Om het ontwikkelingsstadium en de potentie van RFID toepassingen in kaart te brengen maken we gebruik van de bekende BCG matrix aanpak (Figuur 3). De betekenis van de verschillende vakken hierin voor ons is als volgt:

| BCG-Matrix      |      | relatief marktaandeel   |  |
|-----------------|------|---|--|
|                 |      | hoog  | laag   |
| groeipotentieel | hoog | <br>star     | <br>question mark |
|                 | laag | <br>cash cow | <br>dog            |

Figuur 3: Positionering van toepassingen van RFID.

- Dog: Toepassingen die we weinig zien en waarvan we verwachten dat ze ook geen hoge vlucht zullen nemen.
- Question mark: Toepassingen die nog zeldzaam zijn, maar in gebieden met grote toekomstige potentie.
- Star: Toepassingen die richting volwassenheid gaan.
- Cash cow: Volwassen toepassingen die door bedrijven worden opgepakt.

In het kader van deze studie is het niet mogelijk hier een onderbouwde indeling van de verschillende RFID toepassingen te geven. Op basis van de ontwikkelingen die we zien, zowel in technologie als in toepassingen, kunnen we wel een *expert-oordeel* geven van de trends zoals we die op dit moment waarnemen. Dit is onderstaand weergegeven.

#### *Dogs*

- Onderhuids taggen van mensen. Voorbeelden als het experiment in Baja Beach Club zullen sterk op vrijwilligheid gebaseerd zijn, met altijd alternatieven.

#### *Question Marks*

- Identificatie en lokalisatie van personen. De potentie rond bijvoorbeeld zorg en gedetineerden is groot, maar er zijn ook (privacy) vraagtekens.
- Taggen op individueel object niveau. De potentie is hoog, maar het is nog onduidelijk of het kostentechnisch haalbaar is.

#### *Stars*

- Logistiek. Invoering wordt steeds meer en meer opgepakt, zoals in projecten als Versschakel.
- Paspoort. Hier zijn nog kinderziektes, maar het veiligheidsvraagstuk maakt de (politieke) draagvlak groot.
- Betaalfuncties. Robuustheid van de systemen ten opzichte van alternatieven en de hoge vlucht in Japan geven aan dat hier een veel potentieel in zit. De implementatie-inspanning voor realisatie lijkt echter groot te zijn.
- Counterfeiting. Tickets en medicijnen worden met tags voorzien om het gebruik van vervalsingen tegen te gaan.

#### *Cash Cows*

- Toegangssystemen. RFID voor toegang tot gebouwen en terreinen heeft een bewezen markt.

- Beveiligingssystemen. Het taggen voor antidiefstal vindt reeds lang plaats, met name in de retail sector, maar ook bijvoorbeeld voor kunstcollecties.
- Taggen van dieren. Dit lijkt algemeen geaccepteerd en toegepast.

Cash Cows maakt voornamelijk gebruik van LF en HF RFID tags. Bij de Stars zitten toepassingen die gebaseerd zijn op UHF tags al dan niet gecombineerd met sensoren. Met andere woorden, veel van de commerciële RFID toepassingen maken gebruik van relatief korte scanafstanden (LF en HF), terwijl UHF toepassingen met grotere scanafstanden zich nog voornamelijk in de ontwikkelfase bevinden.

## 2.6 Samenvatting en conclusies

Uit de in dit hoofdstuk beschreven illustratieve voorbeelden blijkt duidelijk dat RFID technologie voor een breed en divers scala aan toepassingen ingezet kan worden. Dit wordt ook bevestigd door recent marktonderzoek. Daaruit blijkt dat RFID steeds belangrijker wordt in *andere* sectoren dan de detailhandelsbranche. Het huidige potentiaal van RFID komt voornamelijk uit relatief traditionele en gevestigde toepassingen als toegangscontrole, autobeveiliging, en het traceren van dieren. In tegenstelling tot een jaar geleden zien de RFID fabrikanten steeds meer activiteit in de logistiek in bredere zin, in de luchtvaart, de gezondheidszorg en de farmaceutische industrie [44]. In deze sectoren is het gebruik van RFID veelal nog onontgonnen gebied. Hier liggen voor Nederland ook de meest kansrijke toepassingen. Hier liggen voor Nederland ook de meest kansrijke toepassingen. Met de aanwezigheid van enkele internationaal sterke financiële instellingen, een gerenommeerde luchtvaartmaatschappij, een zorgsysteem van hoog niveau als potentiële RFID gebruikers en de aanwezigheid van Philips en Nedap als belangrijke RFID technologieleveranciers zijn de ingrediënten voorhanden voor succesvolle nieuwe RFID toepassingen. De aanwezigheid van een geavanceerde kennisinfrastructuur kan hierbij helpen. Met de vele aanwezige kleine technostarters rondom deze bedrijven en kennisinstellingen is er de mogelijkheid om snel in te spelen op nieuwe, specifieke RFID ontwikkelingen en toepassingen.

Met de aanwezigheid van enkele internationaal sterke financiële instellingen, een gerenommeerde luchtvaartmaatschappij, een zorgsysteem van hoog niveau als potentiële RFID gebruikers en de aanwezigheid van Philips en Nedap als belangrijke RFID technologieleveranciers zijn de ingrediënten voorhanden voor succesvolle nieuwe RFID toepassingen.

Ook de Nederlandse overheid kan, net als in veel andere landen het geval is, het gebruik van RFID stimuleren door als launching customer op te treden. Het nieuwe biometrische paspoort (waarvoor Philips de RFID tag levert) is hiervan een goed voorbeeld. Ook de verschillende ministeries verantwoordelijk voor binnenlandse veiligheid, gezondheidszorg en de agrosector zien mogelijkheden voor RFID in de strijd tegen bijvoorbeeld terrorisme, gekke-koeien-ziekte en nationale rampen. Onderzoek toont aan dat het gebruik van RFID in combinatie met een sensor relatief sterk groeit, hoewel het aandeel nog relatief klein is [1]. Het lijkt gerechtvaardigd om te stellen dat RFID niet alleen moet worden beschouwd in het licht van tracking en tracing en handel, maar juist ook in het licht van zorg- en defensietoepassingen, toepassingen voor sociale veiligheid, en toepassingen bij rampenbestrijding. Nationale Besluit Subsidies Investerings Kennisinfrastructuur (BSIK)

onderzoeksprogramma's als Freeband [45] en Smart Surroundings [46] volgen deze visie volledig.

*Het is gerechtvaardigd om te stellen dat RFID niet alleen moet beschouwd in het licht van tracking en tracing en handel, maar juist ook in het licht van zorg- en defensietoepassingen, toepassingen voor sociale veiligheid, en toepassingen bij rampenbestrijding.*

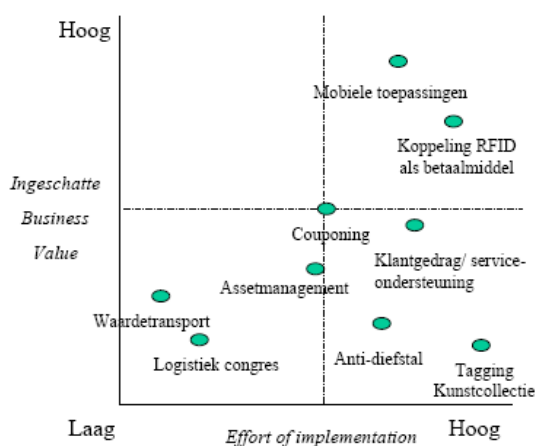
Opvallend is dat de meest innovatieve en interessante toepassingen gebruik maken van RFID tags die opereren in het UHF gebied. Blijkbaar biedt dit meer mogelijkheden voor innovatieve diensten in verband met scanafstand en scansnelheid. Vooral de relatief grote scanafstand en de scansnelheid maken deze tags populair. Voor toepassingen waarbij de kosten van de tags minder relevant zijn, zien we ook een relatief sterke groei in het gebruik van RFID in combinatie met sensoren (zie ook [1]). Deze combinatie resulteert in een enorme verrijking van de gegevens over het getagde object resulterend in een beter inzicht in aspecten van de toestand van het getagde object.

*Opvallend is dat veel innovatieve en interessante RFID toepassingen gebruik maken van UHF tags, al dan niet in combinatie met een sensor.*

Daarnaast valt het ook op dat veel van de genoemde toepassingen van RFID slechts ideeën zijn of in een experimentele of pilot fase zitten. Veel RFID toepassingen zijn nog niet marktrijp. Tijdens de workshop werd de Nederlandse situatie gekarakteriseerd als "gerommel in de marge" met een "zolderkamertje" sfeer.

*Veel RFID toepassingen zijn nog niet marktrijp.*

De potentie van toepassingen wordt bepaald door de zogenaamde "business value" ervan en de inspanning die nodig is om de toepassing uit te rollen. Deze variant van de in sectie 2.5 beschreven BCG matrix is uitermate geschikt om de implementatie-effort van RFID toepassingen aan te geven (zie Figuur 4).



Figuur 4: Toepassingen van RFID [47].

Duidelijk is dat de implementatie-effort van veel interessante UHF RFID toepassingen hoog is. Het is daarom niet verbazingwekkend dat veel van de in dit hoofdstuk gegeven voorbeelden zich nog in een experimenteel stadium bevinden. De technologie is er wel maar de mogelijkheden van RFID worden nu pas ontdekt. En net als bij zoveel andere technologieën, zal het toepassen ervan gepaard gaan met het nemen van de nodige hindernissen. Het selecteren van de juiste RFID technologie in termen van frequenties, tags, antennetypes, readers en databases voor het inrichten van een optimaal RFID systeem is bijvoorbeeld geen sinecure. Die kennis wordt in Nederland langzaam opgebouwd. Enkele schapen zijn al over de dam als we kijken naar marktrijpe UHF RFID toepassingen. Het is daarom slechts een kwestie van tijd voordat de rest volgt. Tabel 1 geeft een indicatieve roadmap voor verschillende RFID toepassingen die de pilotfase ontgroeid zijn.

Tabel 1: Indicatieve roadmap voor marktrijpheid van verschillende RFID toepassingen.

| Heden                            | Over 1-2 jaar   | Over 3-4 jaar                               | Over 5 jaar of meer           |
|----------------------------------|---|---|-------------------------------|
| Toegangscontrole in gebouwen     | Paspoort  | RFID op productniveau                       | Sensornetwerken               |
| Identificatie van koeien         | Verscheidende toepassingen met UHF tags in met name de maakindustrie, retail en logistiek | Betalingen                                  | Near Field Communication tags |
| Logistieke eenheden              |   | Combinaties met sensors                     | Rekeningrijden                |
| Tegengaan vervalsing van tickets | Post en koeriersdiensten<br>OV-chipkaart  | Medische toepassingen<br>Luchtvaartdiensten |                               |

Duidelijk is ook dat RFID kan helpen om maatschappelijke vraagstukken op te lossen (hiermee geven we een antwoord op de vraag die gesteld wordt in het actieprogramma Maatschappelijke Sectoren & ICT van het Nederlandse kabinet [48]). Enkele voorbeelden van nieuwe en bestaande toepassingen in deze context zijn:

- RFID voor het tracken en traceren van gevaarlijke stoffen zodat adequaat kan worden opgetreden bij ongelukken tijdens het vervoer van dergelijke stoffen.
- Het volgen van TBS patiënten op verlosaf volgen middels RFID en GPS.
- Het terugdringen van het wachtrijden (in de zorg, het verkeer of aan de kassa).
- Waarschuwen voor calamiteiten (rampen, vogelgriep).
- Borgen van de voedselveiligheid (BSE, versere producten).
- Het opsporen van gestolen auto's via RFID.
- Het helpen van ouderen en gehandicapten om zich beter staande te houden in de maatschappij. Ouderen kunnen langer en veiliger zelfstandig wonen als ze een armband dragen dat een signaal geeft als ze vallen of bewusteloos raken. Zo'n band kan informatie geven, waardoor een arts beter en sneller kan inschatten wat aan de hand is.

*RFID kan goed ingezet worden om maatschappelijke problemen op te lossen.*

Stuk voor stuk voorbeelden waarbij de maatschappij en de individuele burger profiteren van het toepassen van RFID. Echter, het inzetten van RFID heeft ook een schaduwzijde.

Gegeven de maatschappelijke impact van RFID is het de taak van de overheid om de schaduwzijde ervan goed in beeld te hebben en beleid hierop af te stemmen of om te kunnen anticiperen. Een aantal mogelijk belangrijke beleidsthema's voor de overheid die op dit moment al geïdentificeerd kunnen worden zijn:

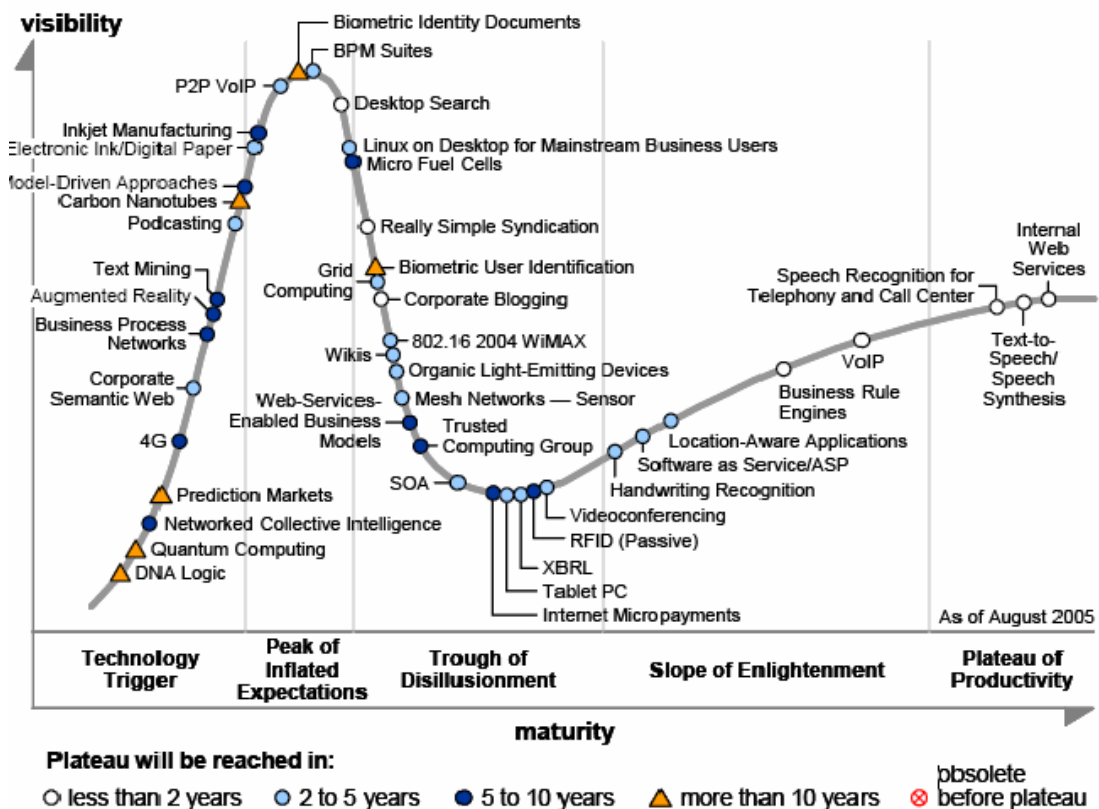
- Beveiliging. Bij het groeiende gebruik van RFID wordt de technologie en de toepassingen ervan steeds belangrijker voor maatschappij en burger. De afhankelijkheid van RFID wordt steeds groter. Hoe zit het met de beveiliging van RFID systemen?
- Privacy. Een ander bekend knelpunt van RFID is de inbreuk ervan op de privacy van de burger. Het tracken en traceren van de burger en zijn gewoontes zijn in theorie mogelijk met RFID. Vooral het taggen van personen zelf stuit op vele morele en ethische bezwaren. Is deze privacy angst gegrond en zijn er voldoende privacybeschermende maatregelen voorhanden?
- Standaardisatie. Gebrek aan standaarden voor RFID leidt tot gebrek aan interoperabiliteit en belemmert het potentieel van RFID.
- Frequenties. Internationale harmonisatie van het gebruik van het frequentiespectrum voor faire handel. Eerlijk gebruik van het frequentiespectrum.
- Invoeringsvraagstukken. Wat komt er allemaal bij kijken als voor het uitrollen van een RFID toepassingen? Wegen de RFID investeringen op tegen de opbrengsten die ermee behaald kunnen worden?

In het volgende hoofdstuk gaan we dieper in op deze knelpunten rond RFID en de beleidsimplicaties ervan.

### 3 Knelpunten voor RFID toepassingen

#### 3.1 Introductie

Ondanks dat RFID al enige tijd bestaat, staat het gebruik ervan voor dit soort toepassingen volgens velen nog in de kinderschoenen. Gartner Research schat in dat RFID momenteel in de “trough of disillusionment” fase van de hype cycle zit (Figuur 5). Om ervoor te zorgen dat RFID een internationaal succes wordt zijn er nog wel obstakels te nemen. Deze obstakels zijn van technische aard zoals de interoperabiliteit van tags en readers en de diversiteit van het internationale frequentiespectrum voor RFID, maar ook, door de vele maatschappelijke raakvlakken, van socio-economische aard zoals de wereldwijde diversiteit aan privacywetgeving en beleving bij de consument.



Figuur 5: Hype Cycle for Emerging Technologies [49].

Aan de hand van de illustratieve RFID voorbeelden uit het vorige hoofdstuk is het mogelijk om een aantal barrières te benoemen die een succesvolle toepassing van RFID in de weg staan. Deze barrières kunnen erg divers van aard zijn, variërend van puur technologische gebreken tot diepe emotionele redenen. Enkele ervan hebben mogelijke beleidsimplicaties voor de overheid.

*Ondanks dat RFID al enige tijd bestaat, staat het gebruik ervan voor dit soort toepassingen volgens velen nog in de kinderschoenen.*

In de volgende secties inventariseren we de knelpunten die we tegen komen bij de verschillende RFID toepassingen uit het vorige hoofdstuk. Kenmerkend voor veel toepassingen is dat er een cumulatie is van technische, organisatorische, sociale en economische knelpunten. Verschillende knelpunten zijn niet altijd los van elkaar te zien. Onderstaand hebben we ze toch op hoofdlijn gegroepeerd naar hun aard. Per knelpunt zal aangegeven worden wat de (mogelijke) oplossingsrichting is en wie hiervoor verantwoordelijk is. De knelpunten zijn in willekeurige volgorde gezet.

*Kenmerkend voor veel RFID toepassingen is dat er een cumulatie is van technische, organisatorische, sociale en economische knelpunten.*

## **3.2 Technische knelpunten**

### **3.2.1 Jammen van reader**

Er is een potentieel risico dat het lezen door de reader wordt verstoord door het bewust zenden van storende signalen. Doordat het systeem op radiogolven werkt zijn er zogenaamde Denial-of-Service (DoS) aanvallen eenvoudig mogelijk m.b.v. een radiozender. Dit middel kan ingezet worden om bijvoorbeeld bedrijfsprocessen te storen. Hoe meer een bedrijf afhankelijk is van RFID tags, hoe groter de schade kan zijn.

Echter, ook de consument kan ter bescherming van zijn privacy een stoorzender bij zich hebben. Hiermee voorkomt hij/zij dat de RFID tags die hij/zij bij zich heeft gescand worden. Het gebruik van dit soort stoorzenders kan een negatief effect hebben op andere, essentiële RFID toepassingen. Te denken valt hierbij aan financiële transacties of medische toepassingen. De vergelijking valt hier te maken met de radarverklippers en desbetreffende stoorzenders die door hard rijdende automobilisten gebruikt worden. Dit soort stoorzenders hinderen de politie bij het uitvoeren van haar taak. Indien het gebruik van RFID stoorzenders een grote vlucht zal nemen dan zal de overheid, net als bij de radarverklippers, hierop in moeten spelen. Er zou bijvoorbeeld een verbod kunnen komen op het gebruik van dit soort RFID jammers, of er zal iets gezegd moeten worden over de maximale reikwijdte van het apparaat om de schadelijke effecten ervan te beperken.

### 3.2.2 Skimming

Skimming is ongeautoriseerde interceptie van RFID transmissies. Met geschikte richtantennes kan over grote afstanden meegeluisterd worden met RFID transmissies<sup>4</sup>. We hebben het dan over afstanden van enkele tientallen tot honderden meters. Het is mogelijk om skimming te voorkomen. Oplossingen zijn het versleutelen van de data, het blokkeren van datatransmissies door jamming, en het toepassen van variërende scanprotocollen door de readers. Andere oplossingen maken gebruik van het 'killen', 'blocken' of 'disablen' van tags. Deze tags hebben de mogelijkheid om zichzelf uit te schakelen of om hun geheugen te wissen of te vullen met zinloze informatie nadat ze gescand zijn. Ook voor dit soort privacybeschermende technieken dient gewaakt te worden dat ze niet doorslaan en het functioneren van RFID onmogelijk maken. Het killen van een tag is bijvoorbeeld een relatief ingrijpende en, vanuit investeringsoogpunt, een dure operatie omdat er dan verder niets meer mee gedaan kan worden.

### 3.2.3 Interferentie

Het lezen door de reader wordt bemoeilijkt doordat interferentie met andere radiosignalen plaatsvindt of dat de radiosignalen worden gereflecteerd of geabsorbeerd.

Het is bekend dat RFID slecht werkt voor metalen objecten vanwege ongewenste reflecties. Vocht absorbeert de energie van de RFID radiogolven. Vochtige ruimte en vloeibare stoffen zoals melkpakken zijn daarom ook probleemgevallen. In veel gevallen worden deze problemen opgelost door te experimenteren met de plaats van de tag op het object. Bedrijven die van RFID gebruik willen maken zullen dit zelf op moeten lossen. Eventueel in overleg met de fabrikanten van de tags. Best practices kunnen helpen voorkomen dat het wiel niet steeds opnieuw wordt uitgevonden. Voorwaarde hiervoor is wel dat deze informatie breed ontsloten wordt. Een RFID testcentrum zou hierbij een rol kunnen spelen.

### 3.2.4 Reader collision

Reader collision is een ander probleem. Reader collision kan voorkomen als twee of meerdere readers in elkaars nabijheid gebruik maken van dezelfde frequentie voor het uitlezen van tags. Tags werken niet als ze door meerdere readers tegelijk gescand worden. Om reader collision te voorkomen zijn de gereserveerde RFID frequentiebanden opgesplitst in aparte bandjes. In Europa is voor UHF RFID een relatief smalle bandbreedte gereserveerd tussen 865.6 en 867.6 MHz welke voor maximaal vermogen gebruikt kan worden. Deze 2 MHz bandbreedte is onderverdeeld in 10 aparte bandjes. Readers kunnen zelf bepalen welk van de bandjes ze gebruiken voor communicatie met de tags. Ze 'luisteren' dan naar kanalen die vrij zijn en hoppen dus van frequentieband tot frequentieband om tags te scannen. Eén frequentieband mag door een reader nooit langer dan 300 milliseconden gebruikt worden. Problemen kunnen zich voor doen als er, in het

---

<sup>4</sup> Het gaat hier om het onderscheppen van RFID communicatie tussen de tag en de reader. Niet om het uitlezen van de tag zelf door een 'kwaadwillige' reader (hier is de afstand slechts 23 meter).

Europese geval, meer dan 10 readers in elkaars nabijheid *continu* aan het scannen zijn. Een elfde reader kan dan problemen krijgen met het scannen van de tags. Gegeven de sterke groei van RFID, en dus ook het aantal readers, is het daarom niet ondenkbaar dat over enkele jaren de UHF RFID band anders ingericht zal moeten worden. Het Europese Telecommunicatie Standaardisatie Instituut (ETSI) zal hierin, samen met de nationale overheden, een wakende rol moeten innemen. Een reader die niet efficiënt omgaat met zijn radiogolven kan het verpesten voor vele andere, wel efficiënt opererende readers in de nabijheid. Er zullen eisen gesteld moeten worden aan de readers. Fabrikanten zullen hieraan moeten voldoen. De eisen kunnen worden opgesteld door certificeringinstanties zoals TNO of NEN maar ook door de overheid.

*Het gebruik van technieken als jamming en slecht afgestelde readers kan een destructief effect hebben op het RFID radiospectrum gebruik. Een wakende rol is hier vereist.*

### **3.2.5 Tag collision**

Tag collision komt voor wanneer een reader meerdere tags tegelijkertijd moet scannen. Dit kan de reader niet verwerken. Er zijn verschillende manieren om tag collision te voorkomen. Een veelgebruikte oplossing is om de tags een uniek, serieel identificatienummer te geven dat gebruikt wordt om collisions te voorkomen. Zo'n collision ID zit diep ingebakken in de tag en heeft niets met de (EPC) identifier te maken waarvan de toepassing gebruikt maakt. Het collision ID wordt alleen gebruikt om de responsetijd van de tag naar de reader toe te bepalen. Omdat elk collision ID uniek is, resulteert dit voor elke tag in een verschillende responsetijd zodat er geen sprake meer is van tag collision.

Het nadeel van het gebruik van deze collision ID's is dat een tag, zelfs als er gebruik gemaakt wordt van versleutelde (ge-encrypte) (EPC) identifiers, uniek geïdentificeerd kan worden. Hierdoor wordt het zelfs mogelijk om het gebruik van het nieuwe paspoort waarin een RFID tag zit te traceren en op die manier de privacy van de eigenaar te schaden (vooral omdat het paspoort voor steeds meer zaken als identificatiemiddel vereist wordt). Om dit te voorkomen zal er gebruikt gemaakt moeten worden van een RFID tag die conform de ISO 14443A specificatie is geproduceerd. In dit soort tags wordt de collision ID op een random manier opnieuw berekend bij elke scan. Het is de taak van de Nederlandse overheid om hier rekening mee te houden en te eisen dat de RFID tags in het Nederlandse paspoort in ieder geval voldoet aan de ISO 14443A specificatie.

### **3.2.6 Bewust kapot maken of verwijderen van tags**

Een andere DoS bedreiging is het deactiveren van tags d.m.v. hoge HF signaalsterktes (waardoor de tags doorbranden) danwel door het versturen van deactiveringscodes naar de tags, die niet altijd goed beveiligd zijn. Winkeliers die gebruik maken van RFID tegen winkeldiefstal doen dit vaak bewust als het product gekocht is door de consument, maar het zou niet toegestaan mogen zijn dat andere mensen dat ook kunnen doen. Dit zou het inzetten van RFID ter voorkoming van winkeldiefstal onbruikbaar maken. Met het steeds goedkoper worden van RFID apparatuur wordt de drempel hiertoe steeds lager. Hier valt niet zo heel veel tegen te doen anders dan het misbruik in de vorm van bewust kapot maken van RFID tags strafbaar maken.

Het verwijderen van tags (om ze eventueel te vervangen door een andere tag) wordt steeds moeilijker doordat producenten ze steeds meer integreren met de verpakking van het object.

*Met het breder beschikbaar komen van RFID apparatuur wordt misbruik ervan waarschijnlijker.*

### **3.2.7 Klonen**

Het is mogelijk om minder goed beveiligde tags te klonen. Een tag die gebruikt wordt ter authenticatie van een object of product wordt dan nagemaakt en op een ander object bevestigd, zodat het een origineel object of product lijkt. Met name in het geval een RFID tag als sleutel (in een toegangspas of in de startonderbreker van een auto) wordt gebruikt kan dit een groot risico zijn. In [50] wordt beschreven hoe via reverse engineering een RFID tag gekloond kan worden om hiermee een auto te stelen of gratis te tanken.

Onderzoekers zijn er al enkele jaren geleden in geslaagd om een SIM kaart te klonen [51]. Gelukkig zijn de meeste telecom operators hierop voorbereid doordat zij regelmatig controleren of een SIM identiteit op hetzelfde tijdstip niet twee keer gekoppeld is aan het mobiele netwerk. SIM kaarten zijn een stuk complexer en beter beveiligd dan de gemiddelde RFID tag. Het klonen van RFID tags zou in de toekomst een probleem kunnen worden. Om klonen te voorkomen zal de beveiliging van de RFID tag beter moeten worden. Tags met voldoende beveiliging zullen een certificaat moeten krijgen zodat gebruikers weten waar ze aan toe zijn als ze op zoek zijn naar een RFID oplossing. Let wel, er zal altijd een afweging gemaakt moeten worden op grond van de waarde van het getagde object en de beveiliging van de tag. Met andere woorden, wanneer loont het voor misbruikers om een tag te klonen?

Standaardisatie-organisaties zoals ISO en overheden kunnen bij het certificeren van (de beveiliging van) tags een rol spelen. Speciale RFID testcentra of instellingen zoals TNO kunnen invullen geven aan deze rol.

## **3.3 Organisatorische knelpunten**

### **3.3.1 RFID technologie standaardisatie**

Goede en gedragen standaarden zijn essentieel voor het succes van RFID. Standaarden voor RFID zijn niet alleen nodig voor de technologie zelf maar spelen ook een rol bij het ontwikkelen en uitrollen van toepassingen. Standaarden zijn niet alleen nodig voor het specificeren van de mogelijkheden van de tags (passief of actief, write/read mogelijkheden) en de eisen met betrekking tot de draadloze interface, maar ook voor de software ondersteuning van de readers en tags, het coderen van de informatie opgeslagen in de tags, het verwerken van de gegenereerde informatie en het borgen van de privacy en beveiliging van de informatie. Een aantal standaarden is aanwezig:

- EPCglobal RFID Standards Activities: EPCglobal is een activiteit van GS1 dat zich bezig houdt met het standaardiseren van RFID frequenties voor logistieke

toepassingen, interfaces, RFID identifiers en de verwerking van de RFID gegevens. Op instigatie van GS1 werkt EPCglobal, samen met gebruikers van de GS1 standaards, leveranciers van hard- en software en universiteiten, aan het definiëren van de benodigde technische specificaties, die vervolgens aan ISO ter ratificering worden aangeboden. EPCglobal heeft onlangs een Generatie 2 RFID specificatie geratificeerd waarin deze aspecten vastgelegd zijn. De EPC technologie kan ook voor andere codesystemen dan dat van GS1 gebruikt worden. Hiermee zorgt EPC voor een belangrijke versnelling in het tot stand komen van wereldwijd bruikbare standaards, die voldoen aan wensen vanuit de toekomstige gebruikers. Het Amerikaanse Department of Defense (DoD) heeft gekozen voor EPC als drager, ook voor de eigen codesystemen (zoals DODAC), ten behoeve van het coderen van goederenstromen met zo'n 40 tot 50 duizend leveranciers. Ook IATA heeft hier zeer recent voor gekozen, voor het identificeren van bagage (met hun al bestaande nummersysteem).

- ISO RFID standaarden: Wereldwijd zijn er momenteel meer dan 120 verschillende protocollen in gebruik voor het uitlezen van tags. De International Standardization Organization (ISO) probeert hier enkele structuur in te brengen. ISO richt zich met name op het standaardiseren van de draadloze interface tussen de tag en de reader voor de verschillende RFID frequenties. Belangrijke ISO standaarden voor RFID zijn voor artikelmanagement (ISO/IEC 18000), gegevensstandaardisatie (ISO/IEC 15418, 15434, 15459, 24721, 15961, 15962), apparaatstandaardisatie (ISO/IEC 18047) en applicatiestandaardisatie (ISO 10374, 18185, 11785, 122/104). Aspecten als data opslag, structuur van de RFID identifiers en fysieke implementatie van tags en readers vallen buiten beschouwing. Appendix B - vergelijkt ISO met EPC en EPC UHF Gen 2.

Ook zijn bepaalde landen zelf bezig met het ontwikkelen van eigen standaarden voor RFID. China, bijvoorbeeld, is momenteel aan het overwegen om voor de interne markt een eigen EPC standaard te ontwikkelen. Drijfveren hierachter zijn dat China haar interne markt wil beschermen door RFID data niet via EPCglobal te laten beheren. Gezien de grootte van de Chinese afzetmarkt en export kan deze afwijkende houding mogelijk een negatieve impact hebben op het internationale gebruik van RFID.

Tenslotte is er een trend dat verschillende industrieën of sectoren momenteel aan het werk zijn aan eigen RFID standaarden. Zo is er EPCglobal voor de retail en wordt er in de luchtvaartsector gewerkt aan een eigen standaard (zie ook mandaat Boeing in sectie 2.3.3). AIM Global is een industrie consortium en autoriteit voor automatische identificatie en mobiliteit. Binnen AIM is een aantal commissies voortdurend bezig met het vastleggen van technische specificaties, keuringsspecificaties en toepassingsmogelijkheden, maar ook met internationale standaardisatie. RFID is een belangrijk onderwerp voor AIM. Onlangs heeft AIM een position statement uitgebracht betreffende RFID standaarden [52]. Met dit statement wil AIM faciliteren in de afstemming tussen de verschillende ISO standaarden en de standaarden die momenteel binnen het bedrijfsleven en industrie (EPCglobal, AIAG, IATA) ontwikkeld worden. Voor wat betreft wetgeving zegt AIM het volgende: "AIM Global favors a worldwide regulatory environment where RFID users in every country can realize robust, high-performance implementations."

Experts tijdens de ITU workshop over Ubiquitous Network Societies [53] in april 2005 hebben benadrukt dat er twee gebieden zijn waar RFID standaarden ontbreken. Het eerste

gebied is dat van identifiers en codering, de tweede is gerelateerd aan dataformaten, frequenties en communicatieprotocollen. Consortia zoals het EPCglobal adresseerden tot voor kort voornamelijk het eerste gebied. Voor het tweede gebied wordt nog veel werk verwacht. Dit is ook onderkend door EPCglobal. Momenteel besteedt EPCglobal veel aandacht en tijd aan het creëren van wereldwijde standaards voor dataformaten, frequenties en communicatieprotocollen. Deze zullen vervolgens worden vastgelegd als ISO standaard. Voor de codering wordt, ten behoeve van bij GS1 aangesloten bedrijven, nadere invulling gegeven aan het toepassen van het GS1 codesysteem; andere gebruikersgroepen kunnen hun eigen codesysteem in de EPC / ISO standaard toepassen (bijvoorbeeld IATA voor de bagage afhandeling).

*Er zijn twee gebieden waar RFID standaarden ontbreken. Het eerste gebied is dat van identifiers en codering, de tweede is gerelateerd aan dataformaten, frequenties en communicatieprotocollen. Consortia zoals het EPCglobal adresseren voornamelijk het eerste gebied. Voor het tweede gebied wordt nog veel werk verwacht.*

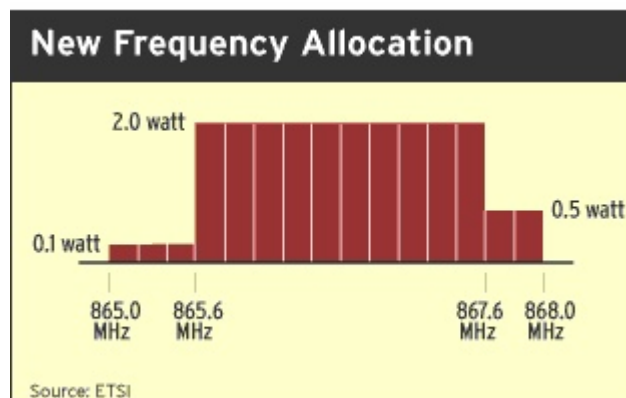
Standaarden ontbreken ook voor de communicatie van de reader met het achterliggende netwerk en voor toegang tot RFID gegevens in dit netwerk. Een partij die hier aan de weg timmert is Reva Systems [54]. Zij hebben onlangs een open architectuur ontwikkeld op basis van standaard interfaces tussen tags, readers en applicatiesoftware. Verder hebben ze een Simple Lightweight RFID Reader Protocol (SLRRP, [55]) voorstel aangedragen binnen EPCglobal en het IETF (Internet Engineering Task Force). SLRRP definieert hoe readers configuratie-, status- en taginformatie moeten oversturen naar het achterliggende IP-netwerk.

### 3.3.2 RFID frequentie- en vermogenstandaardisatie

Zijnde een radiotechnologie, delen RFID tags en readers met andere korte-afstand apparaten zoals telemetrie en alarmen een schaars frequentiespectrum. Het is daarom noodzakelijk dat RFID toegepast wordt conform de regulering van het frequentiespectrum waaronder het toegestane gebruik van gelicenseerde en ongelicenseerde frequentiebanden, elektromagnetische compatibiliteit, interferentie-immuniteit en veiligheid vallen. Appendix C - geeft een overzicht van alle internationaal toegekende frequentiebanden voor RFID. Uit deze tabel blijkt dat het gebruik van RFID in de LF (125 – 134 kHz) en HF (13.56 MHz) banden is, in tegenstelling tot de UHF (860 – 950 MHz) band, duidelijk meer geharmoniseerd over de verschillende regionen. De verschillen in de UHF band komen tot uiting in het toegestane vermogen, de communicatiesnelheid en frequentiebanden. De VS en Canada gebruiken veelal 915 MHz, terwijl Europa 868 MHz gebruikt. Gelukkig kunnen de meeste moderne UHF tags en readers zonder al teveel problemen opereren in beide banden.

Het Europees Telecommunicatie Standaardisatie Instituut (ETSI), de standaardisatieorganisatie voor de telecommunicatie industrie (producenten en operatoren) in Europa, met een wereldwijde invloed, is verantwoordelijk voor het standaardiseren van RFID frequenties binnen Europa. ETSI heeft onder meer de standaarden GSM en TETRA ontwikkeld. De ETSI standaarden relevant voor RFID in het UHF bereik zijn gedefinieerd in

ETSI EN 300-220 [56]. Al snel bleek dat deze standaarden op het gebied van vermogen, bandbreedte en duty cycle onder deden voor de door de Federal Communication Commision (FCC) gespecificeerde UHF banden in de VS. In 2004 kwam daarom een nieuwe standaard uit (EN 302-208) die deze nadelige situatie min of meer gelijk trok. De snelheid van data transfer tussen de tag en de reader, echter, is nog steeds relatief laag. Dit heeft te maken met het feit dat slechts een 3 MHz bandbreedte beschikbaar is (in vergelijking met 26 MHz in de VS). Om zo efficiënt mogelijk om te gaan met de beschikbare bandbreedte is deze opgesplitst in 15 kanalen van elk 200 kHz (zie Figuur 6).

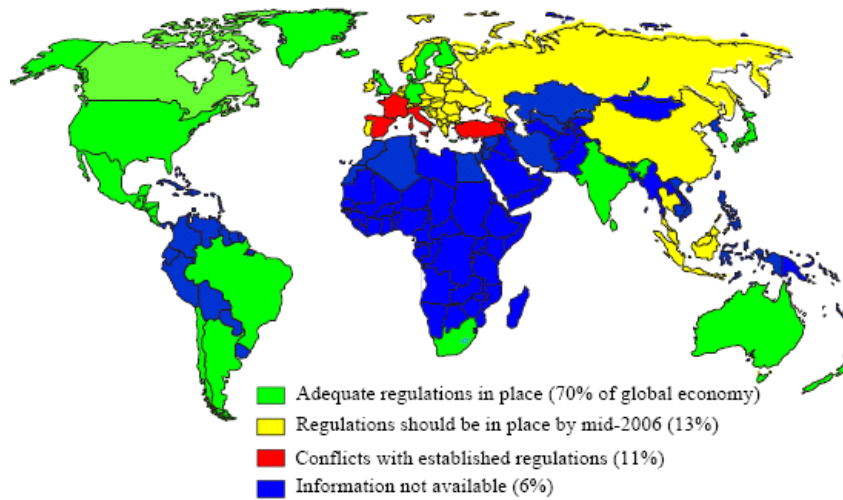


Figuur 6: ETSI's toegekende Europese RFID spectrum en vermogen.

Naast het ETSI speelt het Electronic Communications Committee (ECC) ook een belangrijke rol in de frequentieregulering. Het ECC is verantwoordelijk voor de regulering van de telecommunicatie binnen Europa. De belangrijkste taken van de ECC bestaan uit het opstellen van radiocommunicatie richtlijnen en het coördineren van het toekennen van frequenties in het 9 kHz – 275 GHz bereik.

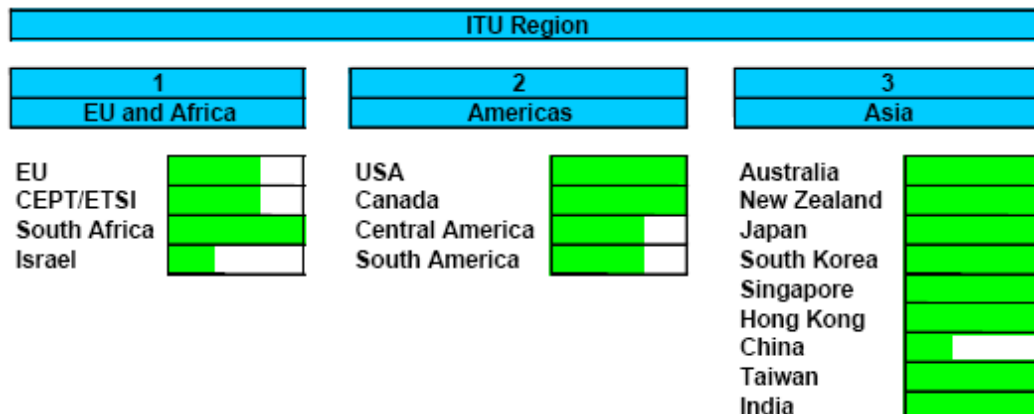
Voor een overzicht van enkele belangrijke andere standaardisatie organisaties zoals ITU, IATA en UPU zie [57].

In september 2004 keurde de Europese Unie de RFID wetgeving voor de UHF band goed (ETSI EN 302 208). Veel Europese landen hebben deze ETSI standaard voor RFID al geïmplementeerd (o.a. Cyprus, Denemarken, Finland, Duitsland, Engeland, IJsland, Litouwen, Slovenië, Zweden en Zwitserland). Toch is er nog een aantal landen waar dit nog niet gebeurd is (o.a. Frankrijk, Spanje, Italië en Turkije). Veelal zijn de betreffende frequenties in die landen al aan andere sectoren en toepassingen toegekend. Mogelijk kan de Europese Commissie hier een rol spelen bij het weghalen van dit knelpunt. Figuur 7 geeft een overzicht van de landen waarbij wetgeving in de UHF band al dan niet geregeld is.



Figuur 7: Wetgeving voor RFID in de UHF band (bron [58]).

Figuur 8 geeft aan in welke mate de huidige wetgeving per land/gebied het gebruik van Gen2 RFID toestaat [58]. Hier is duidelijk te zien Europa achter loopt ten opzichte van de VS, Canada en Azië.



Figuur 8: Mate waarin de huidige wetgeving per land/gebied het gebruik van Gen2 RFID toestaat.

Veel landen in Oost Azië (regio 3) werken nog aan een eigen wetgeving voor RFID. Japan heeft de huidige wetgeving herzien en zal binnenkort de 950 MHz band vrij geven voor ongelicenseerd gebruik van laagvermogen, passieve RFID technologie. Hoogvermogen passieve RFID in deze band zal waarschijnlijk onder licentie vallen en alleen gebruikt mogen worden in industriële gebieden.

Ook is duidelijk dat het gereguleerde radiovermogen per regio verschilt. Deze regulering heeft een directe impact op de afstand waarover tags gescand kunnen worden: hoe hoger het vermogen hoe groter de scanafstand. Als de scanafstand in de VS bij 4 Watt EIRP 10 meter bedraagt, dan zal een ondernemer in Europa, waar een limiet van 3.2 Watt EIRP geldt, slechts tot 6.5 meter kunnen scannen ( $P \sim R^2$ ).

Niet alleen het vermogen, maar ook de beschikbare bandbreedte is gereguleerd. De impact van de bandbreedte op RFID toepassingen is moeilijk in the schatten. Het volgende rekensommetje geeft een indicatie van de impact [59]:

- Stel er moeten 200 tags per seconde gescand worden (een pallet vol met getagde objecten).
- Het uitlezen van een tag kost 100 bits
- Effectief betekent dit dat per seconde 20.000 bits verstuurd moeten worden
- 20 kbs = 40 kHz, baseband requirement (bit '0' = minimale breedte, bit '1' = 2 keer de breedte = in totaal 2x factor voor bits/Hz)
- 40 kHz standaard modulatie (dubbele zijbanden) = 80 kHz fundamentele bandbreedte
- 3<sup>e</sup> harmonische is nodig om het signaal te decoderen = 240 kHz bandbreedte van het communicatiekanaal.

Als we dan bedenken dat in Europa de maximale bandbreedte 200 kHz is dan zien we dat het niet mogelijk is om meer dan 175 producten per seconde te scannen (potentiële 30-40% 'exotische' verbeteringen aan reader en tag design daargelaten). In de VS, waar een 25 MHz bandbreedte is opgedeeld in 50 subbandjes van 500 kHz, zou, in theorie, de 200 tags per seconde zonder problemen gehaald worden. Met andere woorden, Europese regulering van het RFID spectrum benadeelt de Europese ondernemer ten opzichte van de Amerikaanse ondernemer voor wat betreft de scan throughput van producten. Een en ander impliceert ook dat terugdringen van de bandbreedte niet geaccepteerd zal worden door de industrie omdat het een negatief effect op de scansnelheid zal hebben.

In de VS is het gebruik van de 433 MHz band voor actieve RFID tags gereserveerd, onder licentie, voor container tracking. Hiervoor mag meer vermogen gebruikt worden dan is toegestaan voor ongelicenseerde systemen in deze band. Het gebruik van hoog vermogen actieve RFID is alleen toegestaan op industriegebieden zoals scheepswerven en spooreplacements. Zulke systemen staan geregistreerd bij de FCC. In Europa daarentegen is de 433 MHz band een ISM (Industry, Medical, Science) band die speciaal gereserveerd is voor 'short range' apparaten zoals RFID. Merk op dat in de VS, de 433 MHz band niet als een ISM band gezien wordt. In Europa wordt de 915 MHz niet als ISM band gezien, terwijl dit wel weer zo is voor de VS. Verschillen zoals deze vormen een van de uitdagingen in de harmonisatie van RFID frequentiebanden.

Om te voorkomen dat readers een bepaalde frequentie continu in gebruik houden is bepaald dat een reader binnen 300 msec moet hoppen naar een andere frequentieband. Hoe meer banden dus, hoe meer readers tegelijkertijd in elkaars nabijheid kunnen opereren. In Europa zijn hiervoor 10 kanalen gereserveerd, in de VS zijn dit er 50. De gevolgen hiervan zijn besproken in sectie 3.2.3 over interferentie.

*Al met al zitten Nederland en Europa aan de negatieve kant voor wat betreft RFID scansnelheid, scanafstand en capaciteit. Internationale samenwerking en afstemming van RFID frequenties en vermogens is vereist om tot eenduidige uniforme standaarden te komen die een eerlijke handel mogelijk maken.*

### 3.3.3 RFID toepassingsstandaardisatie

Niet elke RFID frequentie is geschikt voor iedere applicatie. Toegangscontrolesystemen gebruiken LF RFID tags; de retail gebruikt UHF tags voor het tracken en traceren van kratten.

Praktische problemen ontstaan wanneer niet duidelijk is welke tag of frequentie voor een toepassing gebruikt moet worden. Wereldwijd worden momenteel 433.92 MHz, 862-892 MHz, 902-928 MHz en 2.45 GHz tags gebruikt voor het traceren van zeecontainers. Hierdoor is het voor de verschillende betrokken partijen moeilijk om op een efficiënte en effectieve manier met elkaar handel te drijven zonder additionele investeringen. Verschillen in telecommunicatiewetgeving en lokaal beleid zijn hier vaak de oorzaak van en zetten standaardisatie onder druk. Standaardisatie per toepassing moet de industrie zelf regelen, de overheden zullen voor een harmonisatie van beleid en wetgeving moeten zorgen.

Een andere oorzaak van deze heterogeniteit in toepassingsstandaardisatie kan zitten in het feit dat er nog veel RFID pilot- en experimenteerlegacy is. Deze nalatenschap zal met de komst van standaarden vanzelf oplossen.

### **3.3.4 Globalisering**

Om te profiteren van de schaalvoordelen van RFID moeten Nederlandse bedrijven de mogelijkheid hebben om met RFID toegang te krijgen tot buitenlandse markten voor het afzetten van hun producten. De Nederlandse overheid kan een belangrijke rol spelen om dit mogelijk te maken door te streven naar internationale harmonisatie van RFID technologie. Transparantie en eerlijkheid van nationale en internationale wetgeving zijn hierbij kritische aspecten.

*De Nederlandse overheid kan een belangrijke rol spelen om dit mogelijk te maken door te streven naar internationale harmonisatie van RFID technologie. Transparantie en eerlijkheid van nationale en internationale wetgeving zijn hierbij kritische aspecten.*

### **3.3.5 Systeemcontrole**

De visie van een open, wereldwijd netwerk voor het opsporen van (informatie over) objecten vereist een speciale netwerkinfrastructuur. Aangezien RFID tags alleen voorzien zijn van een EPC, hebben computers een manier nodig om elke EPC te koppelen aan gedetailleerde informatie over het object dat hoort bij het betreffende EPC. Dit wordt gerealiseerd door de zogenaamde Object Name Service (ONS). Het ONS werkt op een vergelijkbare manier als de Domain Name Service (DNS) van het internet, die computers verwijst naar websites op het World Wide Web. Verisign, dat momenteel manager is van de DNS (Domain Name System) .com en .net roots is door EPCglobal gecontracteerd om de Object Name Service (ONS) te beheren. De vraag rijst of het verstandig en gewenst is om het "Internet of things" door een commercieel bedrijf te laten beheren.

Als er continue gegevens uitgewisseld worden tussen mensen en dingen (soms zonder het zelf te weten) dan rijst de vraag wie uiteindelijk verantwoordelijk is voor deze gegevens. Diefstal van identiteitsgegevens is vandaag de dag aan de orde van de dag. Veelal gebeurt het op het Internet dat mensen hun identiteit kwijt raken met alle gevolgen van dien (je kunt bijvoorbeeld zelfs je huis kwijtraken nadat je identiteit gestolen is [60]). Het is voor veel mensen nu al moeilijk om op een gecontroleerde manier met hun persoonlijke gegevens om te gaan. Met RFID kan dit nog ingewikkelder worden. Als de controle over onze

elektronische identiteitsgegevens niet beter en makkelijker gemaakt wordt dan wordt het voor bepaalde mensen wel heel erg eenvoudig om andere mensen te volgen of zich voor te doen als iemand anders.

Hulpmiddelen en technologieën, zoals privacy enhancing technologies (PETs), voor het managen van persoonlijke gegevens in de digitale wereld ontbreken of schieten tekort in hun bruikbaarheid of functionaliteit. Meer onderzoek op deze gebieden is noodzakelijk<sup>5</sup>.

*RFID vergroot de kans op identity theft. Hulpmiddelen voor het managen van persoonlijke gegevens ontbreken of schieten tekort.*

### **3.3.6 Gezondheid i.v.m. schadelijke straling**

Bij het uitlezen van RFID tags wordt radiosignalen gebruikt, die mogelijk gevaar opleveren voor de gezondheid. Harde bewijzen hierover zijn er (nog) niet [61]. Onderzoek onder 2000 consumenten in Engeland, Nederland, Frankrijk en Duitsland toont aan dat consument zich wel zorgen maakt over zijn gezondheid met de komst van RFID [62].

Echter, net zoals bij GSM en UMTS is het moeilijk om met harde bewijzen te komen die aantonen dat RFID schadelijk is voor de gezondheid. Het voor RFID gebruikte vermogen ligt ver onder de limiet waarbij radiogolven gevaar gaan opleveren voor de gezondheid. Maar wat is de impact van de vele continu aanwezig zijnde tientallen tags en readers waar we in de toekomst mee te maken zullen krijgen? Wegen de bezwaren op tegen de economische belangen? Meer onderzoek naar de impact van RFID straling is nodig. Onderzoekinstellingen en overheidsinstanties kunnen hierbij een rol spelen.

### **3.3.7 Gezondheid i.v.m. per ongeluk consumeren van tags**

RFID tags worden steeds kleiner (ter orde van grootte van een speldenknop). Het is niet denkbeeldig dat tags door personen bewust of per ongeluk geconsumeerd worden, bijvoorbeeld in de vorm van implantaten, of via voedsel of drinken. Het is onbekend welke gezondheidsrisico's hiermee verbonden zijn.

### **3.3.8 Milieuschade i.v.m. productie en verwerking**

Bij de productie van RFID tags wordt het milieu belast, bijvoorbeeld vanwege energiegebruik of etsende chemicaliën. Dit is in het algemeen van tags bekend en een terugkerend issue.

---

<sup>5</sup> De Europese Commissie erkent het belang van privacy enhancing technologies (PETs). Zo is binnen het 5<sup>de</sup> Kaderprogramma van de Europese Commissie is een privacy roadmap uitgezet voor het 6<sup>de</sup> kader (RAPID project). In het 6<sup>de</sup> kader is hierop een vervolg gekomen middels het PRIME project [[www.prime-project.eu.org/](http://www.prime-project.eu.org/)].

Wanneer RFID tags op itemniveau toegepast gaan worden of voor sensornetwerken zal dit een groter issue worden. Alle tags, inclusief hun eventuele batterij, komen uiteindelijk ook weer als afval terug. Onderzoek toont aan dat de consument zich hierover wel zorgen maakt [62].

### **3.3.9 Uitval van tags**

De RFID tag gaat kapot, door slijtage, weersinvloeden of productiefouten. RFID tags gaan meer en meer deel uitmaken van kritische infrastructures. Het kapot gaan van een tag kan dan ernstige gevolgen hebben als hier van tevoren geen rekening mee gehouden is. Ook dit kan vervelende consequenties hebben.

### **3.3.10 Uitval van het totale systeem**

RFID tags maken deel uit van een RFID systeem of RFD toepassing. Niet alleen de tag kan uitvallen, ook andere onderdelen van het systeem zijn gevoelig voor storingen, bijvoorbeeld door 'denial of service' aanvallen van hackers, computer- of netwerkuitval, elektriciteitsuitval, terrorisme, of programmeerfouten. De impact van de uitval hangt af van de toepassing. Voor medische of financiële toepassingen zal de schade groter zijn dan voor het identificeren van een koe of de toegang tot een skilift.

De systeeminfrastructuur van belangrijke en cruciale RFID toepassingen zal moeten voldoen aan speciale voorwaarden. De vergelijking kan in zekere zin gemaakt worden met de telefonie-infrastructuur waar richtlijnen zijn voor de beveiliging en beschikbaarheid van de diensten die erover draaien. Afhankelijk van het doel van de RFID toepassing, dient het een maatschappelijk belang of een bedrijfsbelang, zal de desbetreffende partij zorg moeten dragen voor richtlijnen betreffende de RFID systeeminfrastructuur. Voor maatschappelijke toepassingen zal dit de overheid kunnen zijn.

### **3.3.11 Interoperabiliteit - mismatch tussen tags en readers**

Er kan een mismatch zijn tussen reader en tags, of het systeem achter de reader kan de informatie niet begrijpen, bijvoorbeeld als gevolg van een gebrek aan standaardisatie bij verschillende fabrikanten. Het kan daarbij gaan om hardware mismatches of meer informatietechnische mismatches zoals het ontbreken van een informatieopslagstandaard of semantische interoperabiliteit.

## **3.4 Sociale knelpunten**

### **3.4.1 Privacy**

RFID wordt vaak geassocieerd met het "big brother is watching you" gevoel. Op het internet is het al goed mogelijk om iemands doen en laten te monitoren. Zelfs in de off-line wereld laten veel mensen via creditcards, klantenkaarten en surveillancecamera's al een goed traceerbaar spoor van elektronische gegevens achter. Er wordt door veel mensen en organisaties (zoals CASPIAN) beweerd dat met de komst van RFID het traceren van mensen nog makkelijker zal worden. Veel consumenten zien het verlies van privacy dan

ook als een van de grootste nadelen van RFID [62]. De volgende privacy concerns zijn gerelateerd aan het gebruik van RFID:

1. RFID tags zijn dermate klein dat ze ongemerkt in producten kunnen worden verstopt zonder dat de drager zich ervan bewust is.
2. RFID tags op producten hebben een uniek identificatienummer zodat niet alleen nagegaan kan worden welk product wordt geïdentificeerd, maar eveneens nagegaan kan worden om welk exemplaar het gaat.
3. Omdat RFID identificatienummers uniek zijn is het mogelijk personen te volgen door het nummer van de tag met een persoon te associëren. Door bijvoorbeeld bij de kassa het creditcardnummer te koppelen aan een RFID identificatienummer van een gekocht object weet je met behoorlijke zekerheid wie wat heeft gekocht waardoor gerichte marketing mogelijk is.
4. Op grond van meerdere gescande objecten (in kleding, boodschappentas, en documenten) is het theoretisch al mogelijk om een aardig beeld van iemand op te stellen. In de praktijk is dit soort profilering nog niet zo eenvoudig; het vereist de juiste scanapparatuur en toegang tot de achterliggende informatie over de verschillende gescande objecten. Mogelijk kan het in het ergste geval leiden tot identificatie van de persoon in kwestie of kan in ieder geval resulteren in een toekenning tot een bepaalde doelgroep.
5. Met speciale technieken (groter vermogen, grotere ontvangstantenne) is het mogelijk om RFID tags op afstanden tot bijvoorbeeld 5 meter uit te lezen<sup>6</sup>, hetgeen aanzienlijk verder is dan de normale leesafstand die slechts tientallen centimeters bedraagt. Wanneer de lezers bovendien worden verstopt kan er ongemerkt informatie over personen worden verzameld zonder dat deze personen hiervoor uitdrukkelijk toestemming hebben gegeven (bijvoorbeeld: RFID tag in een klantenkaart en vervolgens verborgen readers op de afdelingen, zodat klanten informatie over de afdelingen waar ze het meest rondlopen krijgen toegestuurd). Deze privacy concern kan ondervangen worden door afscherming (paspoort) of encryptie. Bedrijven zullen zich ook behoeden om de privacy van de klant te schaden; dit kan een slechte naam opleveren en klanten kosten.
6. Veel bedrijven zien in RFID een goede mogelijkheid om goederenstromen in de gaten te houden, ook nadat de goederen gekocht zijn door de consument. De benodigde infrastructuur wordt door grote organisaties geleverd. De informatie in de enorme databases van dit soort organisaties kan potentieel worden gebruikt op een wijze die inbreuk maakt op de privacy van (groepen van) personen.

---

<sup>6</sup> Het 'wereldrecord' passieve tags uitlezen staat op ongeveer 23 meter.

7. Er zijn bedrijven die bij hun klanten een RFID tag laten implanteren. Bijvoorbeeld bij de Baja Beach Club in Rotterdam kan hiermee afgerekend worden. Er zijn in het buitenland ook voorbeelden van bedrijven die medewerkers RFID chips laten implementeren voor de toegangscontrole. Voor zover dit volledig vrijwillig gebeurt, is dit acceptabel. Vooral in het laatste geval (werknemers) kan er twijfel ontstaan over de vrijwilligheid omdat er sprake is van een afhankelijkheidsrelatie.
8. Als de RFID chip persoonlijke informatie bevat, zoals de chip in het paspoort of een chip met daarop alle medische gegevens, dan is de privacy in het geding als deze informatie uit de RFID kan worden gelezen door systemen zonder toestemming van de eigenaar van de informatie.
9. De kosten van RFID tags en readers zijn zo laag dat iedereen de technologie kan gaan gebruiken (voor toepassingen waarvoor ze in eerste instantie niet voor bedoeld zijn). Het toepassen van de technologie zal echter pas van meerwaarde zijn als ook toegang tot de achterliggende netwerken verkregen wordt. Hier ligt immers de informatie die van meerwaarde is voor kwaadwilligen en privacy gevoelig kan zijn.

De belangrijkste privacy zorgen met betrekking tot RFID kunnen als volgt worden samengevat:

- “Tracking me”: RFID gebruiken om je bewegingen te volgen.
- “Know what I buy”: RFID gebruiken meer te weten te komen m.b.t. je aankopen
- “Reading me”: het ongeoorloofd uitlezen van (persoonsgebonden) informatie op een RFID chip.
- Persoonlijke veiligheid: RFID gebruiken om te weten wat ik bij me heb. RFID readers kunnen ingezet worden om te controleren of er geen onbekende RFID ‘spychips’ door kwaadwilligen verstopt zitten in persoonlijke voorwerpen [63]. Stoorzenders kunnen gebruikt worden om te verhinderen dat deze verborgen RFID tags inbreuk plegen op de privacy.

Let wel, sommige van de hierboven genoemde privacybedreigende aspecten zijn niet uniek voor RFID. Ook met andere technologieën kan de privacy ondermijnd worden. Door aan de kassa de afrekening te koppelen aan de klantenkaart (zonder RFID) kan nu ook al het koopgedrag van de consument gevolgd worden.

Recent onderzoek van ECP.nl naar de privacyrechtelijke aspecten van RFID toont aan dat de huidige nationale en Europese wetgeving voldoende handvaten biedt om de privacygevaaren van RFID in te dammen [64]. We zullen hier in sectie 5.3.2 op terug komen.

Toch is de Europese Commissie niet gerust over de impact van RFID op privacy en beveiliging. Daarom heeft ze een Member State Data Protection Authority Werkgroep in het leven geroepen (opgericht onder artikel 29 van de Richtlijn 95/46/EC) met de taak om hier verder naar te kijken. In januari 2005 heeft deze Werkgroep haar eerste inschattingen met

betrekking tot de beveiligingsknelpunten van RFID gegevens openbaar gemaakt [65]. Dit werkdocument beschrijft de mogelijke gevaren en impact van RFID toegepast op productniveau. In het bijzonder als RFID in deze situatie gebruikt wordt voor direct marketing en het traceren van consumenten. Toepassingen van RFID in combinatie met bankrekeningen worden door de werkgroep ook als een risico gezien. In het algemeen maakt de werkgroep zich zorgen “about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights”. Vooral zijn er zorgen over misbruik van RFID technologie door bedrijven en overheden om inbreuk te maken op het privé-leven van individuen. Er wordt daarom ook aanbevolen dat consumenten te allen tijde de mogelijkheid moeten hebben om de informatie opgeslagen in de tags op producten te kunnen verwijderen. Voor pasporten en andere identificatiemechanismen wordt aanbevolen om standaard authenticatieprotocollen te gebruiken (bijv. ISO) om er zeker van te zijn dat alle gegevens versleuteld zijn en ontoegankelijk zonder de juiste autorisatie [66]. Het rapport onderscheidt drie aandachtsgebieden voor beveiliging van RFID gegevens:

- Het gebruik van RFID om informatie te koppelen aan persoonlijke informatie. Een supermarkt kan het koopgedrag van de consument op grond van RFID koppelen aan de persoonsgegevens van deze klant.
- Het gebruik van RFID voor het opslaan van persoonlijke gegevens. Toegang tot openbaar vervoer op grond van een persoonlijk RFID kaart kan resulteren in het volgen van de reiziger. Bij de nieuwe OV chipcard kan de reiziger kiezen tussen een wel en niet anonieme versie.
- Het gebruik van RFID voor het anoniem volgen van consumenten. Het betreft hier het traceren en in kaart brengen van het koopgedrag van anonieme consumenten om hen vervolgens ‘lastig te vallen’ met direct marketing of om de gegevens te verkopen aan derden.

Een extra obstakel voor RFID privacy wetgeving wordt gevormd door de relatief grote verschillen in privacy wetgeving per regio of land. Het is dan ook niet voor niets dat de EU Artikel 29 Member State Data Protection Authority werkgroep onlangs haar zorgen heeft geuit dat RFID mogelijk in strijd is met de eisen zoals gesteld in de Europese Richtlijn voor Gegevensbescherming. In het verlengde hiervan zijn enkele workshops georganiseerd om hierover duidelijkheid te krijgen. Ook het Asia Pacific Economic Cooperation forum (APEC) is momenteel aan het bekijken of RFID valt binnen de onlangs uitgegeven privacy richtlijnen. Met name Zuid-Korea heeft aangestuurd op het ontwikkelen van specifieke RFID gerelateerde privacyrichtlijnen. Japan heeft dit in 2004 al gedaan. Ook in de Verenigde Staten is door de overheid een workshop georganiseerd om de implicaties van RFID voor de consument in kaart te brengen [67]. Tot slot is de OECD werkgroep Informatiebeveiliging en Privacy momenteel bezig om een inventarisatie te maken van de impact van de wereldwijde toepassing van RFID. Daar komt bij dat privacy- en beveiligingsopvattingen verschillen per cultuur: Aziaten zijn over het algemeen minder bezorgd over de gevaren van privacy dan de Amerikanen.

Ook vanuit het bedrijfsleven zijn er verschillende initiatieven voor het (zelf)reguleren van privacy. EPCglobal's “Guidelines on EPC for Consumer Products” is hiervan een goed voorbeeld [68]. Een ander initiatief komt van Simson Garfinkel. In Technology Review heeft Garfinkel de zogenaamde RFID “Bill of Rights” gedefinieerd, een raamwerk met vrijblijvende richtlijnen vanuit het bedrijfsleven voor RFID [69]:

- Het recht om te weten of een product een RFID tag bevat;

- Het recht om RFID tags op dat product te laten verwijderen of vernietigen;
- Het recht om bij RFID toepassingen gebruik te maken van alternatieve diensten zonder RFID tags
- Het recht om toegang te krijgen tot gegevens opgeslagen in een RFID tag;
- Het recht om te weten of, wanneer, waarom en waar tags gelezen worden.

Voor wat meer geavanceerde tags zouden nog wat extra privacy richtlijnen geïdentificeerd kunnen worden:

- Persoonlijke gegevens en persoonsgebonden nummers dienen afdoende beveiligd te zijn tegen ongevoegd uitlezen gezien de impact op de privacy van de betrokkene.
- Persoonlijke data op de chip kan niet uitgelezen worden zonder toestemming van de houder, ook het unieke persoonsgebonden nummer niet.

Een complicatie met actieve RFID tags is dat de meeste actieve tags zijn gebaseerd op bedrijfsspecifieke ("proprietary") protocollen hetgeen een objectieve certificering lastig zoniet onmogelijk maakt.

Ook zullen er voorwaarden aan de lezers gesteld moeten worden:

1. Alle plaatsen waar zich een lezer bevindt moeten duidelijk gemarkeerd zijn.
2. Alleen geautoriseerde lezers hebben toegang tot het achterliggende netwerk.

Het gegevensverwerkende systeem zal moeten voldoen aan de volgende punten:

1. Het dataverwerkende systeem mag geen persoonsgegevens koppelen aan RFID data tenzij daarvoor gegronde redenen zijn of dat door de gebruiker expliciet toestemming gegeven is.
2. Limitatie van de gegevensopslag. Er mag niet meer data opgeslagen worden dan nodig is.
3. Het mag niet mogelijk zijn persoonlijke data naar individuele personen te herleiden. Verzamelde gegevens moeten zoveel mogelijk geaccumuleerd worden.
4. Opslag van via RFID verkregen data dient op veilige manier opgeslagen en verstuurd te worden. Toegang alleen door geautoriseerde personen. Transmissie, databases en toegang tot systemen dienen afdoende beveiligd te zijn.

Door middel van certificering en standaardisatie kunnen deze eisen worden afgedwongen bij leveranciers en systeemintegrators.

*Er zullen eisen gesteld moeten worden aan de RFID tags, readers en het gegevensverwerkend systeem om de privacy van de burger te garanderen en te controleren.*

De bovenstaande richtlijnen zijn sterk vanuit het privacy perspectief opgesteld. In alle gevallen dient een afweging gemaakt te worden tussen de (praktische) werkbaarheid van de RFID toepassing, het belang dat gediend wordt en de privacy van de burger.

### **3.4.2 Bewustzijn – onbekendheid van RFID**

Consumenten beginnen zich steeds meer bewust te worden van de gevolgen van RFID voor hun privacy. Desalniettemin is het aantal mensen dat van RFID gehoord heeft en weet wat het betekent nog relatief laag. Marktonderzoek in de VS heeft uitgewezen dat de bekendheid van RFID onder consumenten is toegenomen het afgelopen jaar (van 28 naar 41%). Interessant genoeg is ondanks de grotere bekendheid van RFID, het aantal mensen dat zich zorgen maakt over de privacy aspecten ervan constant gebleven (65%) [70]. In Europa is de bekendheid gemiddeld slechts 18% (Nederland zit met 12% ruim onder dit gemiddelde) [62].

### **3.4.3 Negatieve sfeer**

Er wordt vaak gerept over een negatieve privacy sfeer rondom veel RFID toepassingen [71]. De vraag is of deze sfeer altijd gebaseerd is op feiten of ook op emoties. Veel verhalen over de mogelijke privacy gevaren van RFID zijn sterk opgeblazen (ze zijn theoretisch mogelijk maar in de praktijk nauwelijks haalbaar) of kunnen nu ook al met andere technologieën gerealiseerd worden. Een eventueel onterechte negatieve sfeer bij de consumenten over de privacygevaar van RFID kan onnodig onrust veroorzaken en/of de groei en het potentieel van RFID in de weg staan.

*Veel verhalen over de privacy gevaren van RFID zijn sterk overtrokken (ze zijn theoretisch mogelijk maar in de praktijk nauwelijks haalbaar) of kunnen nu ook al met andere technologieën gerealiseerd worden.*

Tegen deze achtergrond zou er opgetreden kunnen worden door de overheid om meer maatschappelijk draagvlak te creëren voor RFID. Een onderwijzende en informerende dialoog over de privacy- en veiligheidsaspecten van RFID kan zeker op zijn plaats zijn om de balans te bewaren.

Tegelijkertijd is de vraag of actief beleidsmatig optreden van de overheid nodig is. Vanuit het zelfregulerend vermogen van markt en consumentenbewegingen ontstaat er in ieder geval een veel sterker sociaal krachtenveld om privacyschadelijke effecten van RFID in te dammen (op een veel effectievere manier dan via bijvoorbeeld wetgeving) [72]. Voorbeelden hiervan hebben we al gezien bij de RFID klantenkaart van Metro in sectie 2.3.1: Na protest van burgers is de RFID tag in deze kaart weggehaald.

### **3.4.4 Nieuwe technologie, nieuwe verschillen**

Het is denkbaar dat sommige RFID toepassingen ongewenste sociale effecten met zich meebrengen. Een vaak aangehaald voorbeeld is het volgende. Met een RFID klantenkaart kunnen mensen korting krijgen voor getagde producten. Mensen die weinig geld te besteden hebben zullen eerder zo'n klantenkaart aanschaffen om goedkoop boodschappen

te kunnen doen. Mensen met meer geld kunnen hier onderuit. Ingrijpen door de overheid in dergelijke toepassingen is duidelijk een politieke keuze.

### **3.4.5 Afscherming**

Het lezen door de reader kan niet plaatsvinden doordat het radiosignaal van de reader of tag wordt tegengehouden door afschermingmateriaal (kooi van Faraday effect). Winkeldieven maken bijvoorbeeld gebruik van deze techniek. Getagde artikelen worden dan in een met aluminiumfolie beklede tas gestopt waardoor ze onzichtbaar worden voor de readers bij de deur. Vanuit privacy oogpunt wordt afscherming ook gebruikt. Er zijn al boodschappentassen te krijgen die de artikelen afschermen als men op straat loopt zodat niet zomaar door derden gescand kan worden wat er gekocht is (we gaan hier uit van de situatie dat elke product een RFID heeft, iets wat nu nog niet gebeurt; er wordt binnen de retail momenteel voornamelijk op dozen, pallets en kratten gelabeld). Ook het nieuwe biometrische paspoort maakt gebruik van een metalen afdekplaatje over de tag. Dit om te voorkomen dat de informatie op de tag uitgelezen kan worden.

Afscherming is een goed voorbeeld van een manier die zowel positief als negatief gebruikt kan worden. Het is in dit geval belangrijk om een goede balans tussen veiligheid en privacy te vinden. Informatie over het hoe en waarom van afscherming is hierbij van essentieel belang. Niet alleen de overheid (voor het paspoort) maar ook bijvoorbeeld branche- of overkoepelende organisaties (zoals het Hoofdbedrijfschap Detailhandel of Mitex) kunnen hierbij een rol spelen.

## **3.5 Economische knelpunten**

### **3.5.1 Ongeautoriseerd uitlezen - bedrijfspionage**

Een tag kan worden gelezen door iets of iemand die daartoe niet bevoegd is. Bijvoorbeeld door een crimineel die op zoek is naar informatie over een potentieel slachtoffer. Op grond van de door RFID verkregen informatie kan het slachtoffer bijvoorbeeld lastig gevallen worden met ongewenste reclame of zelfs zijn digitale identiteit verliezen ('identity theft').

Een ander, ook voor de industrie zeer zorgelijk, probleem in deze context is bedrijfspionage. RFID tags kunnen door iedere RFID reader die op de juiste frequentie werkt geactiveerd en zodoende gelezen worden. Met de gelezen informatie kan de spion erachter komen wanneer en waar welk tussenproduct is geproduceerd en voor wie het bedoeld is. Belangrijke gegevens over de bedrijfsorganisatie en -processen kunnen op deze manier bloot gelegd worden.

Bedrijven zullen dit probleem, in samenwerking met leveranciers van RFID technologie, in eerste instantie zelf moeten oplossen.

### **3.5.2 Achterblijven MKB**

Momenteel zijn het vooral de grote bedrijven die actief testen met RFID technologie. Hierdoor zal het productiviteitsverschil tussen deze bedrijven en het MKB alleen maar toenemen.

Daarnaast zullen veel MKB-ers, als toeleverancier of afnemer, vaak min of meer gedwongen worden om te voldoen aan de RFID eisen van deze grote bedrijven. In veel gevallen betekent dit extra kosten voor de MKB-er. Er moeten tags en scanapparatuur aangeschaft worden, tags moeten geplaatst worden en mensen zullen opgeleid moeten worden om goed om te gaan met de apparatuur. Daarnaast ontbreekt het vaak aan voldoende kennis over de technologie en aan informatiesystemen en databases om optimaal van de voordelen van RFID te kunnen profiteren.

Ook kunnen er door RFID nieuwe businessmodellen ontstaan die natuurlijk niet altijd even gunstig uitpakken voor alle partijen, en met name het MKB. Scan-based trading (SBT) is hiervan een voorbeeld omdat in dit model de verantwoordelijkheden en risico's naar de toeleveranciers (het MKB) in de keten worden geschoven (zie Wall-Mart case in sectie 2.3.1). Aan de andere kant ook nieuwe partijen ontstaan. Third party logistics (3PL) dienstverleners zijn hiervan een voorbeeld.

MKB-ers die wel met RFID aan de gang zijn gegaan stuiten vaak op een gebrek aan interesse en enthousiasme bij andere bedrijven en de overheid [73].

Het is vanzelfsprekend dat iedere nieuwe technologie of verandering van context verschuivingen in de bestaande economische verhoudingen met zich meebrengt. Dit is niet per definitie slecht, maar juist een gewenst effect: de beloning van ondernemen en innovatief gedrag. De overheid dient er wel op toe te zien dat alle partijen (inclusief het MKB) een eerlijke kans krijgen om te participeren in deze vooruitgang. Concreet voor RFID betekent dit dat er voldoende kennisbronnen moeten zijn, en mogelijkheden voor experimenteren, ook op kleinere schaal.

*MKB-ers die wel met RFID aan de gang zijn gegaan stuiten vaak op een gebrek aan interesse en enthousiasme bij andere bedrijven en de overheid.*

### 3.5.3 Gegevensverwerking

Als er in de toekomst miljarden voorwerpen met een RFID tag uitgerust zijn dan levert dit een enorme hoeveelheid aan data op die verwerkt moet worden. Het besef van de enorme datahoeveelheden ontbreekt en de impact van RFID op de belasting van het netwerk is onduidelijk [74].

Een simpel rekensommetje leert het volgende: Een grote retailer maakt gebruik van RFID tags op productniveau. Het aantal producten dat een tag draagt is 1 miljard. De hoeveelheid gescande data van deze producten bedraagt dan zo'n 12 Gbytes (1 miljard x 12 bytes per tag). Als de producten om de 10 minuten gescand worden voor tracking en tracing doeleinden, dan wordt per dag zo'n 7200 Gbytes aan data gegenereerd (120 Gbytes x 6 keer per uur x 10 uur op een dag). Stel nu dat er 10 van dit soort retailers zijn, dan verwerken ze met z'n allen zo'n 72000 Gbytes aan data op een dag. Hoewel veel data hiervan dubbel zal zijn en weggegooid zal worden, moet alles toch verwerkt worden (bekijken, weggooien, reageren, etc.).

Er zullen slimme applicaties ontwikkeld moeten worden die op een efficiënte manier omgaan met alle data (weggooien, selectiever bewaren, houdbaarheid, aggregeren, etc.). Hiervoor is meer onderzoek nodig. Bedrijfsleven, kennisinstellingen, infrastructuurleveranciers en software ontwikkelaars zullen elkaar moeten vinden.

*Het besef van de enorme datahoeveelheden ontbreekt en de impact van RFID op de belasting van het netwerk is onduidelijk. Er zullen slimme applicaties ontwikkeld moeten worden die op een efficiënte manier omgaan met alle data.*

#### **3.5.4 Systeemintegratie**

RFID is een onderdeel van een groter geheel - een netwerk en goede applicaties (bijvoorbeeld een voorraadsysteem). De toegevoegde waarde van RFID is met name de "aanwezigheidsmelding", maar die is op zich lang niet voldoende; je moet ook nog wat doen met die melding. Integratie met achterliggende, vaak bestaande systemen is daarom noodzakelijk.

Recent onderzoek toont aan dat de markt voor RFID technologie versnipperd is; er is bijna geen enkele leverancier die per toepassing een volledige oplossing met hardware en software kan leveren [75]. De hardwareproducenten zien een belangrijke rol voor de systeemintegrators bij het ontwikkelen van geïntegreerde, verticale toepassingen. Ondanks enkele uitschieters, worden nog veel RFID toepassingen op "een zolderkamertje ontwikkeld"<sup>7</sup>.

Naadloze integratie met bestaande bedrijfsapplicaties die nu op barcodes draaien, WLAN netwerken, en ERP (Enterprise Resource Planning) en SCM (Supply Chain Management) systemen is nodig, maar ontbreekt nog veelal. Leveranciers en system integrators zijn hiermee hard aan het werk.

#### **3.5.5 Kosten**

Op het moment zijn de kosten van de tags nog te hoog voor bijvoorbeeld het gebruik in kleine verpakkingen en goedkope producten met weinig marge. Gemiddeld kost een tag nu zo'n 20 eurocent. De prijzen dalen echter gestaag door de groeiende vraag naar tags. Een gangbaar criterium is dat taggen op productniveau interessant wordt als de prijs van een tag lager is dan 5 eurocent.

Dit is echter niet meer dan een statistisch weetje. Bij ondernemingen geldt het principe: "als het uit kan, kan het uit...". De deelnemende partijen in de RFID workshop waren unaniem van mening dat prijs van RFID in principe geen beletsel is, "als er maar een sluitende

---

<sup>7</sup> Quote van een van de aanwezigen tijdens de workshop 'Verkenning beleidsimplicaties RFID', 31 oktober 2005, bij ECP.nl te Leidschendam.

business case is". M.a.w. als gevolg van prijsdalingen zal het aantal sluitende business cases toenemen.

Momenteel valt het niet mee om een goede return of investment te berekenen omdat veel RFID systemen nog in de kinderschoenen staan en nog niet optimaal werken. Die hiermee soms gepaarde vertraging laat zich moeilijk vertalen naar kosten.

*"Als er maar een sluitende business case is!"*

### 3.5.6 Ontbreken van best practices

Veel partijen worstelen met basale vragen als "Waar moet ik de tag en reader plaatsen?" en "Welke tag kan ik het beste gebruiken in mijn situatie?" Hierdoor blijven veel RFID toepassingen en projecten in hangen in de pilotsfeer. Het wordt tijd om deze sfeer te doorbreken en echt werk te gaan maken met RFID. De overheid zou hier een stimulerende rol in kunnen spelen door bijvoorbeeld als launching customer op te treden. Hierop wordt verder ingegaan in sectie 5.3.

*De overheid zou hier een stimulerende rol in kunnen spelen door als launching customer op te treden of door te controleren dat voldoende schaalgrootte bereikt wordt bij het uitrollen van RFID toepassingen.*

## 3.6 Samenvatting

In dit hoofdstuk hebben we een groot aantal knelpunten beschreven die in bepaalde mate een belemmering kunnen vormen voor het uitrollen van RFID toepassingen zoals beschreven in hoofdstuk 2. Kenmerkend voor veel toepassingen is dat er een cumulatie is van technische, organisatorische, sociale en economische knelpunten waardoor doorbraken uitblijven. Voor zover mogelijk is reeds een indicatie gegeven wat de mogelijke oplossing van het knelpunt is en wie daarvoor verantwoordelijk is. Een aantal RFID knelpunten met implicaties voor beleid springen eruit. Deze uitdagingen kunnen als volgt samengevat worden:

- Creëren van de situatie waarbinnen de industrie zichzelf kan reguleren op gebieden als veiligheid en privacy.
  - Het aannemen van een pro-actieve (i.p.v. een defensieve) houding om het consumentenvertrouwen te winnen, zowel bij overheid als bedrijfsleven;
  - Overheid en bedrijfsleven dienen alert te zijn op misbruik en nieuwe destructieve technieken als jamming;

- Toepassers van RFID systemen én hun klanten dienen goede eisen te stellen aan de beveiliging van de technologie (tags, readers, en systemen) en de gegevens.
- Randvoorwaarden scheppen voor standaardisatie van RFID technologie, systemen, en toepassingen en zo de invoering stimuleren.
  - Stimuleren van interoperabiliteit van tags en readers (hardware);
  - Harmonisatie van applicatie interfaces en datamodellen om internationale standaardisatie te realiseren;
  - Hulpmiddelen ontwikkelen en invoeren voor het managen en beschermen van persoonlijke gegevens;
  - Best practices voor RFID-toepassing ontwikkelen en demonstreren in RFID testcentra.
- Harmoniseren van het globale RFID frequentiespectrum.
  - Zorg dragen voor gelijke frequenties en vermogens voor eerlijke (internationale) handel.
- Gezondheid en milieu
  - Alertheid op afvalproblemen
  - Alertheid gezondheidsaspecten rondom radiostraling en ‘consumptie’ van RFID-tags.

Opvallend is dat veel van de knelpunten algemeen gelden, d.w.z., er zijn maar weinig RFID knelpunten die specifiek voor Nederland gelden. Dit werd bevestigd in de georganiseerde workshop over de beleidsimplicaties van RFID. Het meest Nederland-specifieke knelpunt zou privacy kunnen zijn: “Nederland is goed in privacy” [76]. Het ECP.nl onderzoek heeft echter uitgewezen dat de huidige privacywetgeving momenteel voldoende houvast biedt om misbruik van RFID tegen te gaan [64]. Veel privacy gevaren met RFID zijn sterk overtrokken; ze zijn theoretisch mogelijk maar in de praktijk moeilijk te realiseren.

In hoofdstuk 5 zullen we, na de internationale beschouwing in het volgende hoofdstuk, de hierboven beschreven uitdagingen verder uitwerken en de implicaties voor beleid aangeven.

## 4 Internationaal referentiekader

### 4.1 Introductie

In dit hoofdstuk geven we de resultaten van een korte scan naar beleidsontwikkelingen rond RFID in enkele landen (VS, Japan, Duitsland, UK), vanuit de Europese Commissie, en vanuit internationale organisaties (OECD). Deze scan is voornamelijk gericht op identificeren van overwegingen vanuit internationale overheden om al dan niet RFID ontwikkelingen te stimuleren, en hun werkwijze daarbij. Daarnaast op het zo mogelijk onderkennen van beleidstrends.

### 4.2 Verenigde Staten

De VS is wereldwijd met grote afstand koploper in RFID toepassing. Het Department of Defense is een grote launching customer vanuit de overheid, met veel invloed op het bedrijfsleven buiten de defensiesector zoals retail en logistiek. Zij heeft ondanks bezwaren op het gebied van privacy (vanuit groeperingen zoals CASPIAN [77]) een beleid ontwikkeld ten aanzien van eisen te stellen aan aanbieders voor het plaatsen van RFID tags. Die eisen zijn vrij strikt en omvattend. Hierdoor is de verwachting dat de RFID technologie een grote impuls zal krijgen.

Daarnaast is het Department of Commerce actief in het scheppen van voorwaarden voor implementatie en onderzoekt de mogelijkheden en uitdagingen van RFID [78]. DoC noemt in een recent artikel (RFID, Opportunities and Challenges in Implementation, 2005) als belangrijkste beleidsthema's het rijper worden van RFID technologie, de harmonisatie van standaarden voor hardware en software en voor gebruik van draadloos spectrum; interoperabiliteit over verschillende RFID toepassingen, bedrijven en landen; privacy en security, en implementatieproblemen (kosten van RFID). Onze indruk is dat DoC vooral informeert en de kaders stelt (open markt, handel, concurrentie) en geen actief RFID bevorderingsbeleid heeft. Zij constateert ten aanzien van de implementatie van RFID door het MKB dat er steeds meer toepassingsmogelijkheden komen in b.v. gezondheidszorg en maakindustrie. De barrières voor adoptie liggen op het vlak van kosten, gebrek aan kennis, en gebrek aan toegang tot nieuwste technologie. Veel verder dan het constateren dat er ook business opportunies voor kleine bedrijven liggen gaat DoC echter niet.

Er is vanuit de overheid (Department of Defense, Department of Commerce, Department of Homeland Security) wel een sterke invloed op het proces van standaardisatie. Met name om er voor te zorgen dat er geen conflicterende standaarden ontstaan die een belasting vormen voor ontwikkelaars. De RFID Intra-Government Council is opgezet als forum om informatie tussen federale instellingen uit te wisselen en afstemming te bereiken over overheidstoepassingen, privacy en security, standaarden en regelgeving.

Daarnaast houden verschillende overheidsinstellingen zich bezig met de privacy problematiek en probeert men consumentenbescherming te realiseren in overheidstoepassingen. Zo is in de e-Government Act (2002) aangegeven dat een "privacy impact assessment" nodig is, zodanig dat privacy overwegingen worden meegenomen door

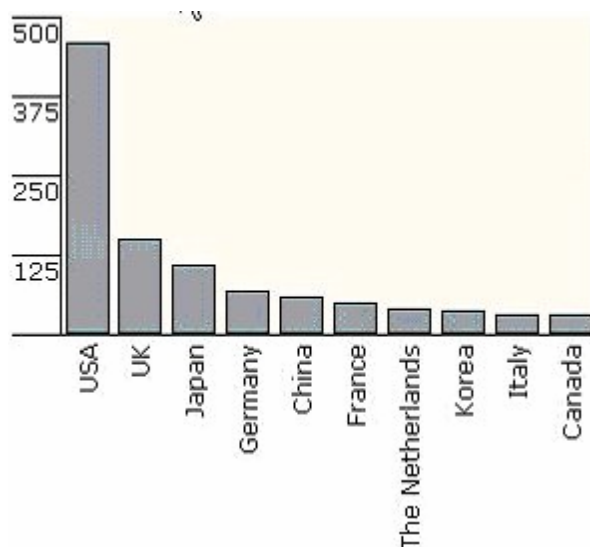
de overheid. Desalniettemin zijn er veel 'bills' ingediend tegen het gebruik van RFID binnen de overheid.

In een recent rapport van het Amerikaanse Government Accountability Office (GAO) staat dat overheidsdiensten nauwelijks aandacht besteden aan de (veiligheids)risico's van RFID [79]. Dertien van de grootste federale diensten gebruiken de technologie al op dit moment, of overwegen deze te gebruiken. Maar slechts één dienst merkte juridische en privacy implicaties van RFID op. Het is niet voor niets dat verschillende staten (zoals Californië en Rhode Island) bezig zijn om via wetgeving meer beperkingen voor het overheidsgebruik van RFID op te leggen [80].

In een poging consumenten, maar vooral het bedrijfsleven gerust te stellen over potentiële problemen met RFID, organiseert de Amerikaanse overheid een aparte workshop over dataverzameling en RFID [81]. Op te merken valt nog dat CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) een belangrijke privacy partij is.

### 4.3 Europa

In Europa zijn Engeland en Duitsland de koplopers van RFID invoering. Nederland loopt ver achter op deze landen. De hoge invoeringskosten en de inpassing in bedrijfsprocessen vormen de belangrijkste struikelblokken [82]. Figuur 9 geeft aan wat de positie van enkele Europese landen is in de globale RFID arena.



Figuur 9: Top 10 landen (uit [1]). De verticale as geeft het aantal RFID projecten aan. In totaal zijn er 1400 RFID projecten onderzocht.

De onderstaande Tabel 2 toont de belangrijkste RFID initiatieven van verschillende Europese landen.

Tabel 2: Belangrijke RFID toepassingen in verschillende Europese landen.

| Engeland                        | Duitsland                     | Frankrijk                 | Nederland                    | Italië                 | Spanje                  |
|---------------------------------|-------------------------------|---------------------------|------------------------------|------------------------|-------------------------|
| "Chipping of Goods" initiatief; | Metro groep initiatief        | Bibliotheken              | Bloemen-veilingen            | Retail                 | Betaal-diensten         |
| Demonstratie-projecten          | Brouwerij industrie           | Retail distributie        | Herbruikbare transport items | Bibliotheek (Vaticaan) | Traceren van dieren     |
| European centre                 | Luchtvaart diensten           | Dagbladen-distributie     | Bibliotheken                 |                        | Retail tagging          |
| Bibliotheken                    | Transport systemen            | Smart Tracing Consortium  | Luchtvaart diensten          |                        | Distributie via pallets |
| Verkeersopstoppingen            | Posterijen                    | L'Echangeur               | Openbaar vervoer             |                        |                         |
| Container transport             | Kaartverkoop sportevenementen | IBM's RFID Testing Centre | Zorg [183]                   |                        |                         |
| Posterijen                      |                               |                           |                              |                        |                         |
| Brouwerij industrie             |                               |                           |                              |                        |                         |
| Kentekenplaten                  |                               |                           |                              |                        |                         |

In de volgende secties zullen we de RFID ontwikkelingen in enkele interessante landen nader beschouwen. We verwijzen naar sectie 2.4 voor de RFID ontwikkelingen binnen Nederland.

#### 4.3.1 UK

De UK is in Europa koploper op het gebied van RFID toepassing. Volgens het Engelse Department of Trade & Industry (DTI) is RFID "the single fastest growing vendor applications sector". DTI is via haar RFID UK initiatief daarom bezig een netwerk van RFID expertcentra op te zetten [84], dat wordt gecoördineerd door AIM UK (bedrijfsleven). Het coördinatiecentrum zit in Yorkshire en wordt gesteund door Yorkshire Forward, de regional development agency. In Bracknell (Londen) is één van de RFID Technology Centres opgezet dat zich Europees profileert. De activiteiten zijn het geven van voorlichting, demonstraties en training. Dit RFID Technology Centre is onafhankelijk en wordt gesponsord door een groep bedrijven (o.a. Intel, Microsoft, Cisco, SAP, Dell) en de overheid (DTI).

Ofcom, de Engelse onafhankelijke autoriteit voor het reguleren van radiofrequenties, heeft onlangs het gebruik van de 865-868 MHz RFID frequentieband versoepeld [85]. De tot voor kort vereiste licentie voor het gebruik van deze band is niet meer nodig. Ofcom wil hiermee het toepassen van RFID in de UK stimuleren en de concurrentiepositie t.o.v. de VS verbeteren.

Onlangs is in de UK een proef gestart met een 'digitaal nummerbord'. Het nummerbord bevat een actieve RFID-tag die uitgelezen kan worden over een afstand van honderd meter.

### **4.3.2 Duitsland**

Duitsland is in Europa na de UK de belangrijkste toepasser van RFID. RFID vervult in het programma "Mikrosystemtechnik" van BMBF (2004-2009) een belangrijke speerpuntrol, met name gericht op de logistiek.

BMBF stimuleert ook het opzetten van innovatiefora in Oostelijke deelstaten om regionale netwerkvorming tussen bedrijven en kenniscentra te stimuleren. Eén van deze fora betreft de toepassing van RFID in de auto-industrie (gecoördineerd door het Institut für Produktion und Logistik, IPL, in Cottbus).

Een aantal ondernemingen heeft een "Verein zur Förderung von RFID" opgericht ([www.info-rfid.de](http://www.info-rfid.de)). Dit Forum wil een platform zijn voor de dialoog tussen bedrijfsleven, overheid, onderzoek en wil de toepassing van RFID stimuleren. Het Forum werkt nauw samen met Fraunhofer IML.

Fraunhofer vervult een belangrijke rol in RFID stimulering, in het bijzonder gericht op de retail, maakindustrie en logistiek. Zo heeft Fraunhofer IML een Open ID Center opgezet in Dortmund, dat als een "neutraal platform voor communicatie, informatie-uitwisseling, en kennistransfer" is bedoeld.

De overheden van Noord-Rijn Westfalen en Nederland hebben op 2 maart 2005 een overeenkomst getekend om op een zestal gebieden intensief samen te werken. Eén van deze gebieden betreft Embedded systems. In dat kader wordt veel aandacht besteed aan de thematiek rond RFID en wireless networks in logistieke systemen.

### **4.3.3 Finland**

In Finland is begin 2005 een publiek-privaat gefinancierd RFID centrum – RFID Lab Finland – geopend, bij Helsinki-Vantaa ([www.rfidlab.fi](http://www.rfidlab.fi)). Een groep ondernemingen waaronder HP en NOKIA steunen dit initiatief, dat deel uitmaakt van het Vantaa High-Tech programma. Het centrum omvat een demonstratie-omgeving van RFID toepassingen. Het Lab wordt gecoördineerd door Vilant Systems.

Daarnaast zijn er RFID testprogramma's, zoals dat in de stad Oulu, uitgevoerd door VTT (Nokia telefoons met RFID lezers uitgerust).

## **4.4 China**

Het is nog onduidelijk welke kant China opgaat met RFID. Waarschijnlijk zal China zich voor de internationale handel conformeren aan de EPCglobal standaard. Voor de interne markt is men aan het overwegen om een eigen RFID standaard te ontwikkelen. Naast privacy- en beveiligingsredenen, vormt de "unieke marktsituatie van China" een belangrijke motivatie voor een eigen standaard.

Naast RFID voor supply chain management, is China van plan om de technologie ook in te zetten in de transportsector, commercie, persoonsidentificatie en medische toepassingen. De Chinese overheid is hierbij de grootste afnemer en gebruiker van RFID tags.

De Chinese RFID markt is ten opzichte van het tweede kwartaal in 2004 meer dan verdubbeld [86]. De Chinese overheid blijkt een belangrijke rol te spelen bij het stimuleren van de markt. Onder meer doordat de overheid veruit de grootste opdrachtgever is.

#### **4.5 Japan**

In de Japanse detailhandel wordt RFID toegepast voor tracking en tracing en voor extra consumentenvoordelen. De overheid heeft bovendien de wetgeving ten aanzien van de zendfrequenties verruimd, zodat het bereik van RFID tags verdubbeld is.

Japan volgt voor RFID in de 135 kHz, 13.56 MHz en 2.45 GHz banden de VS en Europa. Voor passieve UHF RFID zal waarschijnlijk de 950 MHz band gereserveerd worden. De reden voor de keuze van deze relatief hoge frequentie heeft te maken met het feit dat de meeste relevante banden van het frequentiespectrum al toegewezen zijn voor mobiele telecommunicatie, taxi en vrachtwagen communicatiesystemen en een publiek draadloos netwerk voor rampsituaties. Een studiegroep van het Ministerie van Binnenlandse Zaken en Communicatie heeft de overweging om de 433 MHz band toe te kennen voor gebruik door actieve RFID tags uitgesteld. Mogelijke interferentie met amateur radiogebruikers ligt hieraan ten grondslag.

Het Ministerie van Binnenlandse Zaken en Communicatie heeft onlangs in grote lijnen aangegeven hoe zij de rol van RFID ziet in het toekomstige 'u-Japan' als een "ubiquitous network society" [87].

#### **4.6 Zuid Korea**

De Zuid-Korease overheid stimuleert het gebruik van RFID in eigen land om hierdoor een van de grootste exporteurs van RFID technologie te worden. Bedrijven als Samsung en LG investeren veel geld in RFID ontwikkeling en producten. Toch is Zuid Korea, in vergelijking met Japan, de VS en Europa, een nog relatief kleine speler in de RFID arena. Zich bewust hiervan, heeft het ministerie van Binnenlandse Zaken en Telecommunicatie RFID onderdeel gemaakt van haar "839 Strategie" [88]. Deze strategie is bedoeld om nieuwe diensten en moderne communicatie infrastructuren te promoten.

Ook zit de Zuid-Koreaanse industrie niet stil getuige de oprichting van het "Mobile RFID Forum" dat streeft naar integratie van RFID met Korea's geavanceerde mobiele communicatie netwerk.

Het Ministerie van Binnenlandse Zaken en Telecommunicatie heeft in september 2004 aangegeven een technologisch neutrale RFID houding te zullen aannemen waarbij zowel de Europeaanse als Amerikaanse standaarden in acht worden genomen. Vanwege de hoge dichtheid van het Koreaanse frequentiespectrum, geniet de smalle Europeaanse band echter de voorkeur.

#### **4.7 OECD**

De OECD erkent het belang van RFID en is momenteel aan het onderzoeken wat haar rol in de ontwikkeling, stimulering en acceptatie ervan zou kunnen zijn. Hiertoe heeft zij het ICCP

Forum “RFID Applications and Public Policy Considerations” opgezet, dat input verzamelt vanuit de nationale overheden, het bedrijfsleven en onderzoeks- en kennisinstellingen. De OECD ziet haar rol onder meer in het beschikbaar maken van “best practices” voor de implementatie en het gebruik van RFID en in het adresseren van consumentenbelangen.

Tijdens de workshop over “RFID Applications and Public Policy Considerations” in oktober 2005 is vooral het accent gelegd op de aanpak ten aanzien van beleidsthema’s zoals privacy en security, en ten aanzien van invoering in ketens. Daarnaast kwamen mogelijke beleidsinterventies en de internationale samenwerking rond standaarden en interoperabiliteit aan de orde. De status hiervan ligt vooral in het ontwikkelen en afstemmen van ideeën en het voorstellen van initiatieven rond regelgeving (spectrumallocatie), standaardisatie en implementatie. Echte internationale samenwerking en coördinatie moet in Europa van de Europese Commissie worden verwacht.

**Beleidsthema’s vanuit OECD** (bron: ICCP workshop October 2005, [www.oecd.org](http://www.oecd.org) )

- Welke rol spelen best practices op het gebied van invoering en self-regulering, en beleidsinterventies, bij implementatie in de praktijk?
- Welke privacy en security thema’s zijn het belangrijkste, en waar liggen oplossingsrichtingen?
- Wat zijn de meest belangrijke thema’s rond overheidsbeleid en internationale samenwerking inzake interoperabiliteit en standaardisatie?

Enkele voorstellen vanuit de genoemde workshop:

- Opstellen van een “RFID Bill of Rights” waardoor de meest duidelijke vormen van RFID misbruik moeten worden afgedekt (Garfinkel);
- Versnellen van de Europese regelgeving rond RFID (UHF Gen2), vanwege snelle internationale ontwikkelingen rond spectrumallocatie voor Gen2 (zie tabel) (Barthel, EPCglobal)

**Regelgeving RFID UHF Gen2 in Azië vs Europa** (Bron: Barthel, OECD workshop, 2005)

- Japan has formally allocated 952-954 MHz on April 5th 2005
- India has formally allocated 865-867 MHz (4W erp) on May 4th
- China is evaluating the possibility to release a band for RFID within the 917-925 MHz range
- Malaysia is working with the industry. New regulations being considered
- Other Asian countries are expected to adapt their existing regulation
- New European regulations for RFID (ETSI EN 302 208) were approved in September 2004 and have to be translated to national laws; European Commission can speed up or enforce regulations

#### 4.8 Europese Commissie

Vanuit de Europese Commissie is op dit moment met name veel aandacht voor dataprotectie regelgeving gerelateerd aan IPR (DG Justice). Zo is hierover recent een publieke consultatieronde afgerond. Daarnaast behoren thema's zoals R&D (DG INFSO), interoperabiliteit en standaarden (DG Enterprise), diefstal van identiteit, spectrumallocatie, governance van RFID, en IPR en competitie (DG Competition) tot de aandachtsgebieden. Dataprotectie en, in veel mindere mate spectrumallocatie, lijken echter de dominante thema's; er zijn geen initiatieven zichtbaar op het gebied van invoering en gebruik.

De Europese Commissie komt met richtlijnen rond spectrum allocatie. Met deze richtlijnen wil de Commissie bereiken dat er meer ruimte komt in het radiofrequente spectrum voor RFID. Volgens berekeningen zou de RFID industrie hierdoor zo'n 9 miljard euro kunnen groeien. Ook wil de Europese Commissie zo een grotere harmonisatie bereiken voor de standaarden gebaseerd op het succesverhaal van WIFI. De gebruikte strategie voor WIFI zou moeten worden gekopieerd naar die van RFID. Ook wil de Commissie een markt creëren voor de handel in gestandaardiseerde RFID radiofrequenties [89].

#### 4.9 Conclusies

Deze scan berust op een korte desk research en beoogt geen volledigheid. Desalniettemin kunnen een paar voorlopige conclusies getrokken worden over de aard van overheidsbemoeienis in een aantal landen.

- Veel overheden voelen zich met name aangetrokken door de mogelijkheden die RFID technologie biedt om de veiligheid te vergroten en de eigen administratieve processen te versnellen.
- In de Verenigde Staten wordt RFID gezien als een zaak van nationaal belang vanwege belangen op het gebied van handel, defensie en veiligheid. De rol van de overheid is enerzijds die van launching customer, met potentieel grote invloed op economische sectoren, daarnaast beïnvloedt zij de wereldwijde standaardisatie. We hebben geen aanwijzingen voor het opzetten van RFID centra met een publieke functie. Wel worden aan universiteiten met steun van de industrie RFID labs opgezet.
- In Duitsland is RFID speerpunt in het BMBF-programma Microsysteemtechnologie. RFID wordt tevens gestimuleerd door het opzetten van innovatiefora in Oostelijke deelstaten. Er is veel belangstelling voor dialoog tussen overheid, bedrijven en kenniscentra over RFID toepassingen.
- In de UK, koploper in Europa, is via het RFID UK initiatief een netwerk van regionale RFID centra opgezet gericht op communicatie en demonstratie.
- Ook in Finland is een RFID centrum opgezet (Vantaa) met steun van overheid en industrie.
- In China speelt de overheid een belangrijke rol bij het stimuleren van de RFID markt door te functioneren als 'launching customer'.
- De Zuid-Koreaanse overheid stimuleert het gebruik van RFID in eigen land om hierdoor een van de grootste exporteurs van RFID technologie te worden.

Opvallend zijn de RFID centra die als paddestoelen uit de grond schieten. Veelal zijn dit initiatieven van het bedrijfsleven. In sommige gevallen is duidelijk sprake van enige

overheidsbemoeienis. Blijkbaar worden deze centra essentieel bevonden in het stimuleren en uitrollen van nieuwe RFID toepassingen.

*RFID centra schieten overal als paddestoelen uit de grond.*

## 5 Van knelpunten naar beleid

### 5.1 Introductie

Op de website van het Ministerie van Economische Zaken is de missie als volgt verwoord.

Het Ministerie van Economische Zaken bevordert duurzame economische groei in Nederland. Markten waarin ondernemers zich kan ontplooien en waar iedere ondernemer gelijke kansen heeft, er voor consumenten optimale keuzevrijheid is en vitale publieke belangen goed geborgen zijn. Niet alleen gericht op de markt van vandaag maar ook op de markt van morgen. EZ stimuleert vernieuwingszin in alle sectoren van de economie.

*Directoraat-generaal Telecommunicatie en Post (DGTP)* draagt hieraan bij door voorwaarden te scheppen voor goed functionerende netwerken voor elektronische communicatie en post. Het directoraat-generaal heeft bovendien als taak het ICT-beleid van het Rijk te coördineren. Het directoraat-generaal bevordert slim gebruik van communicatienetwerken, creëert stimulansen voor nieuwe ontwikkelingen, zorgt voor stabiliteit en formuleert de spelregels voor consumenten en marktpartijen. Het doel: dynamiek en innovatie, een goede bijdrage aan duurzame economische groei, en veilig en vertrouwd gebruik van telecommunicatie en ICT.

Zeker daar waar het gaat om ontwikkelingen met een grote (strategische) impact, zoals RFID, en daar waar de markt het zelf niet afkan om hiermee goed om te gaan lijkt een rol weggelegd voor DGTP, overigens in samenwerking met marktpartijen, brancheorganisaties en/of kennisinstellingen. Een overzicht van mogelijke beleidsinstrumenten om deze rol in te vullen is gegeven in Appendix D - .

Op basis van bovenstaande is duidelijk dat als het gaat om beleidsimplicaties van RFID, er zeker met bredere blik gekeken moet worden dan alleen naar frequenties en vermogens.

In dit hoofdstuk beschrijven we de belangrijkste aandachtspunten voor de overheid. Allereerst geven we echter nog een stuk toekomstvisie op basis van de toepassingen genoemd in hoofdstuk 2. Het beleid dient rekening te houden met deze ontwikkelingen.

### 5.2 Een blik op de toekomst

Veel te vaak wordt RFID nog gezien als de digitale versie van de streepjescode. Kortom, een elektronische versie van iets dat in de logistiek een belangrijke rol speelt. Dit wordt mede gevoed doordat de meeste RFID tags momenteel read-only zijn en kan gelijk gezien worden als een eerste belangrijke conclusie van deze verkenning.

*Veel te vaak wordt RFID nog gezien als de digitale versie van de streepjescode*

Al eerder is echter genoemd dat ook actieve of semi-actieve varianten bestaan, die in staat zijn zelf te reageren op omgevingsveranderingen (bijvoorbeeld verandering van temperatuur) en vervolgens actief gedrag vertonen via het uitzenden of opslaan van informatie.

Allereerst moet daarom ingecalculeerd worden dat er niet één simpel 'RFID' bestaat, maar dat een *uitgebreid scala aan RFID-chips* ontwikkeld wordt en gaat worden, met allerlei varianten voor gehalten aan informatie, sensorvermogen, interne intelligentie en mobiele communicatiemogelijkheden. Een zeecontainer die zelf meldt dat hij naar de verkeerde haven wordt vervoerd is zeker geen futuristische gedachte. Een dergelijke RFID tag kost vanzelfsprekend meer dan een paar eurocent, maar voor duurdere producten kan een duurdere tags van enkele euro's snel uit.

Aan de andere kant van het spectrum zullen RFID tags steeds goedkoper worden. De voortdurende doorontwikkeling van RFID tags zal leiden tot betere prestaties (minder vermogen nodig, grotere scanafstand, 100% score bij lezen van tags, etc.), meer functionaliteit en dalende kosten. Steeds meer toepassingen zullen daarom technisch en economisch haalbaar worden, waardoor het mogelijk wordt deze overal in te verwerken, maar ook bijvoorbeeld op grote schaal uit te strooien over een groot gebied (sensornetwerken). Bij dergelijke random toepassingen verdwijnt de interesse voor de individuele tag naar de achtergrond, maar staat het totaalbeeld centraal.

Op wat langere termijn is het niet ondenkbaar dat slimme tags in staat zullen zijn met elkaar op ad hoc basis te communiceren en informatie uit te wisselen (bijvoorbeeld in de vorm van 'sensornetwerken'), of dat er twee-weg communicatie ontstaat tussen reader en tag, i.p.v. alleen vanuit de tag naar de reader. De tags worden op dit vlak steeds intelligenter en goedkoper.

Voor wat betreft de readers is de industrie op zoek naar oplossingen om het vermogensverbruik ervan te minimaliseren. Doel hiervan is om RFID readers te incorporeren met populaire draagbare apparaten als mobiele telefoons en PDA's. Ook hierdoor zullen weer tal van nieuwe toepassingen mogelijk worden. B.v. door het 'scannen' van een bushalte krijg je automatisch komende busvertrektijden op je PDA-scherm. Readers zullen, als toegangspoort tot het achterliggende netwerk ook steeds intelligenter worden. Te denken valt aan readers die weten waar gelezen data naar toe moet of die zelf al een stuk datamanagement doen om bijvoorbeeld overbelasting van het netwerk te voorkomen [90].

### **5.3 Een actieve taak voor de overheid?**

Op grond van de genoemde toepassingen en knelpunten en in het licht van de toekomstvisie zien we de volgende hoofdonderwerpen waarvoor activiteiten van de overheid, eventueel in samenwerking met bedrijven, of in interdepartementale samenwerking, denkbaar zijn:

1. Economisch beleid (standaardisatie, innovatie en schaalgrootte);
2. Privacy;
3. Beveiliging;
4. Frequenties;

5. Sociaal beleid;
6. Gezondheid en milieu;
7. Opsporing.

Hieronder geven we per onderwerpgebied de belangrijkste overwegingen die in deze verkenning naar voren zijn gekomen. Deze overwegingen zijn gebaseerd op de in vorige hoofdstukken besproken onderwerpen, namelijk de toepassingen, de knelpunten, en internationale context. Daarbij is ook de praktijkinput van de RFID workshop bij ECP.nl verwerkt.

In niet alle gevallen is aan de overheidskant het Ministerie van Economische Zaken of DGTP de primaire betrokkene. In die gevallen ligt een samenwerking tussen ministeries voor de hand.

### **5.3.1 Economisch beleid**

Als thema van het Ministerie van Economische Zaken is het economische beleid een belangrijk perspectief op RFID. Bij economisch beleid kan het gaan om vele zaken, zoals het stimuleren van innovatief ondernemerschap, het stimuleren van specifieke sectoren, het wegnemen van hindernissen voor innovatie, of het creëren van gelijke kansen voor Nederlandse bedrijven internationaal of voor Nederlandse bedrijven onderling. Aansluitend op de missies van EZ en DGTP gaan we in op een viertal aspecten.

#### **Gelijke kansen internationaal**

Bij gelijke kansen internationaal gaat het er om dat Nederlandse bedrijven geen hinder ondervinden van afwijkende wetgevingen of diversie standaarden in de landen waarmee handel bedreven wordt. Om dit te bereiken is het nodig dat er

- wereldwijde interoperabiliteit komt tussen RFID systemen en een globale harmonisatie van het RFID frequentiespectrum;
- harmonisatie van applicatie interfaces en datamodellen om internationale standaardisatie te realiseren.

In de RFID workshop is van verschillende zijden bevestigd dat het vooral cruciaal is dat er *harmonisatie* plaatsvindt van standaarden en/of wet- en regelgeving. Wat de regelgeving of standaard precies is, is minder van belang.

De overheid kan dit als richtlijn te gebruiken door in alle economisch getinte gremia waarin zij zitting heeft te pleiten voor harmonisatie, d.w.z. te streven naar conformering, in plaats van een specifieke standaard te bepleiten. Hiermee komen Nederlandse bedrijven in ieder geval niet in een ongelijke positie ten opzichte van internationale concurrenten.

#### **Gelijke kansen in Nederland**

Voor de Nederlandse situatie geldt als uitgangspunt dat verschillende bedrijven gelijke kansen moeten hebben om te profiteren van de voordelen van RFID. Hierbij gaat het

natuurlijk niet alleen om het *gebruik* van RFID, maar ook om het ontwikkelen van nieuwe, innovatieve RFID technologie en toepassingen daarvan.

In de RFID workshop kwam naar voren dat de meeste ondernemers aan de gebruikerskant zich mans genoeg vinden zelf keuzes te maken, en dat er in Nederland geen sprake hoeft te zijn van 'achtergestelde' ondernemers. Door sommigen wordt wel de kanttekening gemaakt dat als het praktisch toepassen van RFID nog lang complex blijft (bijvoorbeeld door het voortdurend wijzigen van readers of tags), dat dit waarschijnlijk nadelig is voor kleine bedrijven die weinig R&D (Research & Development) inspanning kunnen opbrengen. Dit is te vergelijken met de situatie rondom EDI (Electronic Data Interchange), de standaard voor elektronische data-uitwisseling, die voor kleine organisaties vaak niet te betalen was/is.

Voor de ontwikkelaars van nieuwe RFID technologie en toepassingen lijkt er wel enige sprake van tweedeling. Veel grote organisaties ontwikkelen of beschikken over interne RFID labs, waarin nieuwe toepassingen kunnen worden uitgetest. Kleine bedrijven (zoals technostarters) kunnen dit niet betalen. Deze bedrijven kunnen gebaat zijn met eenvoudig toegankelijke, publieke RFID labomgevingen.

*Gelijke kansen, in Nederland maar ook internationaal.*

### **Speerpuntenbeleid**

De eerste twee aspecten gaan vooral in op het creëren van gelijke kansen voor ondernemers. Het is echter ook denkbaar dat de overheid ervoor kiest specifieke sectoren of toepassingsgebieden extra te stimuleren. De reden hiervoor kan politiek zijn, bijvoorbeeld het stimuleren van nieuwe zorgontwikkelingen of nieuwe veiligheidstoepassingen, of economisch: het stimuleren van sectoren waar Nederland een duurzame, sterke positie kan verwerven in de internationale economie. Innovatief ondernemerschap is op zich reeds een speerpunt van beleid.

RFID biedt in dit licht vele kansen. RFID is zelf reeds een technologie die geschikt is voor vele innovatieve toepassingen. Daarnaast bezit Nederland over een aantal traditioneel sterke partijen in dit veld (zoals Philips en Nedap). Ook zijn er vele, kleinere technologische partijen actief die RFID technologie verder ontwikkelen of nieuwe diensten ontwikkelen rondom RFID technologie. De aanwezigheid van een drietal sterke technische universiteiten draagt hieraan bij. RFID biedt daarom veel kansen voor het stimuleren van innovatie, en voor het verwerven van een sterke positie in het veld van innovatieve RFID diensten, bijvoorbeeld voor zorgtoepassingen.

De overheid kan hierbij helpen door bij MKB-beleid goed rekening te houden met technologische georiënteerde bedrijven (zoals technostarters). Terwijl voor veel MKB-ers de technologische ontwikkelingen vaak te snel gaan en er een kennisachterstand dreigt, gaat voor technostarters in het algemeen niets snel genoeg! Dit vraagt een adequate benadering. Het is de moeite waard het bestaande instrumentarium op dit punt nader onder de loep te nemen.

*Terwijl men er vaak van uitgaat dat voor MKB'ers een kennisachterstand dreigt, gaat voor technostarters gaat juist niets snel genoeg!*

## **Stimuleren van innovatie in ondernemingen**

RFID biedt naast de mogelijkheden die in speerpunten beleid worden genoemd nog tal van andere mogelijkheden om het innovatief vermogen van Nederland op te schroeven.

In de conceptnota Breedband wordt aangegeven dat Nederland binnen Europa onder de maat presteert als het gaat om elektronische diensten [91]. De grootste knelpunten op het gebied van de ontwikkeling van diensten zijn onder meer het gebrek aan standaarden, schaalgrootte en innovatie. Al deze knelpunten zijn zeker van toepassing op RFID diensten en bieden een unieke gelegenheid om aan te tonen waartoe Nederland in staat is.

Investerings van het bedrijfsleven in informatie en communicatietechnologie hebben aantoonbaar geresulteerd in een wereldwijde groei van de economie. Het is echter nog onduidelijk of en op welke schaal RFID invloed heeft op de nationale en internationale economie. Wel duidelijk is dat bedrijven efficiënter gaan werken met RFID waardoor goederen sneller getransporteerd zullen worden en uiteindelijk goedkoper in de schappen zullen liggen. Tracken en tracen van goederen verloopt sneller en nauwkeuriger. Het scannen van producten verloopt sneller en met minder fouten. Voorraden in winkels kunnen beperkt worden omdat just-in-time levering mogelijk wordt. De echte verbeteringen en economische winst vallen misschien nog wel te halen uit het op een slimme manier analyseren en gebruiken van de grote hoeveelheden RFID data.

De huidige RFID situatie is te vergelijken met een ontdekkingsstocht waar bekeken wordt of en hoe RFID het beste ingezet kan worden. Vaak zijn dit geïsoleerde initiatieven, terwijl veel voordelen van RFID komen uit het netwerkeffect: je hebt er pas wat aan als iedereen het doet. Innovatieve RFID toepassingen zouden daarom volgens velen toch gestimuleerd moeten worden. Drempel bij het subsidiëren nieuwe RFID toepassingen of pilots is dat er vaak niet zozeer sprake is van wetenschappelijk onderzoek of productinnovatie. Daardoor vallen verschillende subsidiëringregelingen af (o.a. BSIK), terwijl de praktijktests voor de betrokkenen vaak toch een sterk experimenteel karakter hebben in de zin dat succes ongewis is. Het verdient aanbeveling iets gedetailleerder na te zoeken of het huidige subsidiëringinstrumentarium voldoende aanknopingspunten biedt voor RFID-innovaties.

Een potentiële rol voor de overheid kan het verzorgen van best practices zijn. De behoefte aan best practices is groot vanuit het bedrijfsleven. Een RFID laboratorium of testcenter dat goed toegankelijk is voor bedrijven zou hierbij kunnen helpen. Het is echter de vraag of de overheid zich hiermee moet bemoeien of dat het bedrijfsleven en bestaande technologiecentra dit zelf zou moeten oppakken. Eventueel met behulp van brancheorganisaties en/of standaardisatieorganen. In ieder geval zien we dat in enkele landen (UK, Finland, ook Duitsland) de bundeling en het toegankelijk maken van RFID kennis erg belangrijk wordt gevonden.

### 5.3.2 Privacy

In het ECP.nl rapport, dat reeds veelvuldig werd geciteerd, is de belangrijkste conclusies dat de bestaande wetgeving voldoet als het gaat om de bescherming van de privacy van de burger. Daarbij zijn wel een aantal overwegingen te plaatsen.

**Enorme datagroei** Mede door het gebruik van RFID systemen zal de hoeveelheid geregistreerde data enorm toenemen. Daarnaast zullen ook softwarepartijen zich inspannen om ook intelligente dingen met al deze data te doen. Daarmee neemt de kans toe dat er verbanden gelegd worden die een inbreuk kunnen zijn op de privacy van mensen, zonder dat daar per sé kwade opzet aan ten grondslag hoeft te liggen. Het is onwaarschijnlijk dat alle database manipulaties afzonderlijk voorgelegd gaan worden en gecontroleerd kunnen worden door overheidsinstanties. In veel gevallen is het immers niet vooraf duidelijk voor de toepasser dat er inbreuk zou kunnen zijn op de privacy. De overheid zal dus mechanismen moeten ontwikkelen om de grootschalige dataverwerkende toepassingen rondom RFID systemen te kunnen controleren, wanneer zij de Wet Bescherming Persoonsgegevens (WBP) wil toepassen. Misbruik van RFID technologie zou dus ook gestraft moeten kunnen worden. Wetgevingstechnisch is dit waarschijnlijk al wel mogelijk, echter of de toezicht-, handhavings- en opsporingsprocessen al zo ver zijn dat dit voldoende aangepakt kan worden is de vraag (zie ook sectie 5.3.7).

**Persoonsgegevens** Hoewel een RFID tag op zich geen persoonsgegeven is, en ook geen persoonsgegevens hoeft te bevatten, is het lezen van tags in de omgeving van een persoon vergelijkbaar met het maken van beelden met videocamera's. Je weet immers nooit welke gegevens gelezen worden en welke verbanden daar mee te maken zijn. De regelgeving rondom beveiligingscamera's geeft daarom interessant vergelijkingsmateriaal. Daarin wordt bijvoorbeeld geregeld dat klanten geattendeerd moeten worden op de aanwezigheid van camera's, er wordt geregeld dat camerabeelden slechts gedurende bepaalde tijd (zeven dagen) bewaard mogen worden, en camerabeelden moeten zodanig zijn beveiligd dat ze niet gemanipuleerd kunnen worden (zie o.a. Vuistregels van College Bescherming Persoonsgegevens [92]).

**Identiteitsdiefstal** Een groeiende zorg op het internet is het misbruik van andermans (digitale) identiteit, ook wel identiteitsdiefstal ("identity theft") genoemd. De oorzaak hiervan is dat veel persoonlijke gegevens min of meer 'rondslingeren' op het internet. Deze gegevens kunnen door kwaadwilligen gebruikt worden om onder een andere naam op het internet te opereren. Met RFID kan identiteitsdiefstal veel erger worden, met name als de tag direct gekoppeld is aan een individu. Denk hierbij bijvoorbeeld aan het RFID paspoort, een tag met daarop het medische dossier of een onderhuidse tag. Mensen krijgen het steeds moeilijker om hun persoonlijke gegevens in de digitale wereld te managen en te controleren. Hulpmiddelen hiervoor ontbreken of schieten tekort.

Aangezien de wetgeving voldoende houvast biedt ligt de verantwoordelijkheid voor zorgvuldigheid met betrekking tot privacy primair bij de bedrijven en organisaties. De overheid kan echter wel *helpen*:

- Door het uitgeven of aanbieden van standaardteksten over WBP en RFID aan consumenten.

- Door het ontwikkelen van do's en don'ts voor bedrijven bij het inrichten van RFID-systemen in relatie tot privacy-aspecten.
- Door het ontwikkelen van standaardteksten voor bedrijven die zij aan hun consumenten kunnen overbrengen (bijvoorbeeld ophangen in een winkel).
- Door het bijdragen aan een positievere privacy sfeer rondom RFID middels het aannemen van een pro-actieve (in plaats van. een defensieve) houding om het consumentenvertrouwen te winnen.

Voordeel van deze maatregelen is dat er geen sprake is van directe overheidssteun aan de bedrijven, maar tegelijk wel degelijk een hoop praktische besommeringen worden weggenomen.

Andere richtlijnen die wel eens voorgesteld worden, verdienen vooralsnog weinig aanbeveling vanuit overheidswege, omdat onduidelijk is in welke mate zij nieuwe toepassingen in de weg staan. Een voorbeeld hiervan is: "Consumenten moeten het recht hebben om te kiezen om een RFID tag te laten verwijderen, vernietigen, of de-activeren na aankoop van een product." Met dit soort marktbeïnvloedende richtlijnen is het beter te wachten tot het nut en belang van de richtlijn onomstotelijk vaststaat.

Samen met de industrie en privacyorganisaties kan de overheid middelen ontwikkelen en inzetten die de consumenten informeren over RFID technologie, wat het voor hun privacy betekent, en welke middelen ze hiervoor tot hun beschikking hebben. Hierdoor kan de negatieve privacy sfeer weggehaald worden en kan er maatschappelijk draagvlak voor RFID technologie gecreëerd worden.

### **5.3.3 Beveiliging**

Het valt te verwachten dat op de lange termijn RFID tags en readers alomtegenwoordig zullen zijn. Het lijkt niet erg plausibel dat in die toekomstige situatie het wordt geaccepteerd (door consumenten én bedrijven) dat iedereen allerlei tags maar zonder enige belemmering van elkaar kan lezen. Met andere woorden, beveiliging/encryptie van tags en readers is een aspect dat weldra cruciaal zal worden voor de verdere verspreiding van RFID technologie.

Het leidt mogelijk tot economische voorsprong dit reeds in een vroeg stadium te onderkennen en innovaties te richten op de duurdere, beveiligde tags. De bal ligt daarvoor in de eerste plaats bij technologieontwikkelaars voor de ontwikkeling van beveiligingstechnologie, en bij de vraagkant om druk uit te oefenen op de ontwikkelaars. Ook de wetenschap kan een bijdrage leveren door het ontwikkelen van efficiënte en effectieve encryptie-algoritmes die passen bij de vaak beperkte mogelijkheden van de RFID tags.

De overheid heeft hierin wellicht een faciliterende rol via voorlichting of het stimuleren van technologie-ontwikkelprogramma's in dit vlak.

De beveiliging van achterliggende RFID-software en de koppeling met ERP (Enterprise resource Planning) en CRM (Customer Relation Management) systemen is zeker een

belangrijke zaak, maar is tegelijk reeds belangrijk aandachtspunt voor de vele software-makers, vanwege de centrale rol die deze systemen tegenwoordig in de bedrijfsvoering spelen. Het valt te verwachten dat dit zowel vanuit de makers als vanuit de vraagkant wel voldoende aandacht krijgt.

#### **5.3.4 Frequenties**

De harmonisatie van het globale RFID frequentiespectrum hebben we al genoemd om eerlijke handel en interoperabiliteit van tags en readers (hardware) mogelijk te maken. Hierbij moet niet alleen gedacht worden aan de harmonisatie van het frequentiespectrum, maar ook het toegestane vermogen en de breedte van de frequentiebanden. Momenteel heeft het verschil in het RFID frequentiebeleid van Europa en de VS een significante impact op scanafstand en -snelheid. Hierdoor bevinden Europese ondernemers zich in een minder sterkere concurrentiepositie.

Organisaties als ETSI en ITU zijn de aangewezen partijen om dit soort zaken als overheid aan te kaarten.

Met de groei van RFID (tags én readers) zal het toegekende frequentiespectrum verstandig gebruikt moeten worden. Vooral de toenemende reader dichtheid kan leiden tot verzadiging van het spectrumgebruik wat kan resulteren in slechte performance van het RFID systeem. Eén slecht (of weinig economisch) opererende reader kan het voor veel andere readers in de nabijheid verpesten. Daarnaast kan het gebruik van stoorzenders, zoals jammers, een negatief effect hebben op andere, essentiële RFID toepassingen. Te denken valt hierbij aan financiële transacties of medische toepassingen. Indien het gebruik van RFID stoorzenders een grote vlucht zal nemen dan zal de overheid hierop in moeten spelen. Voor jammers zal dus iets gezegd moeten worden over de maximale reikwijdte van het apparaat.

#### **5.3.5 Sociaal beleid**

Het toepassen van RFID voor bepaalde doeleinden kan sociale consequenties hebben. Een voorbeeld hiervan is gegeven in sectie 3.4.4 met betrekking tot de klanten-bonuskaart, waar mindervermogenenden zich gedwongen voelen hun privacy gedeeltelijk op te geven voor kortingen. Vandaar dat sommige consumentenbelangenorganisaties richtlijnen voorstellen dat er altijd alternatieve producten zonder RFID aangeboden worden.

Omdat RFID in feite geen echt bijzondere of nieuwe technologie is, lijkt er weinig reden specifieke regels rondom RFID-technologie te ontwikkelen. Wel is het de taak van de overheid om waakzaam te blijven voor dergelijke sociale gevolgen van nieuwe RFID toepassingen, en indien dit nodig is in te grijpen. Zeker gezien het feit dat RFID vanwege de dalende kosten op steeds meer plaatsen zal gaan opduiken. Dergelijke ingrepen zullen waarschijnlijk politiek beargumenteerd moeten worden. Hiermee wordt bedoeld dat het in feite een keuze is die vanuit een visie op de maatschappij wordt gemaakt.

Als er sprake zal zijn van ingrijpen dan is nog steeds een wettelijke one-size-fits-all RFID wetgeving niet verstandig; daarvoor is het toepassingspotentieel van RFID te groot en divers. De industrie neemt zelf ook al initiatief om consumenten gerust te stellen om maar

geen klanten kwijt te raken. Een gedragscode voor bedrijven over hoe om te gaan met RFID lijkt meer op z'n plaats.

### **5.3.6 Gezondheid en milieu**

Er zijn voor RFID geen grote zorgen voor wat betreft milieubelasting en gezondheid. Alertheid is echter zeker gewenst, en met name op de volgende aspecten:

- Bij de productie van RFID: kosten van energie en gebruik van chemicaliën bij productie.
- Verwerking van RFID tags in producten of verpakkingen moet zorgvuldig gebeuren.
- Het breed uitstrooien van tags in de vorm van sensornetwerken vormt een milieubelasting.
- De radiostraling van readers in werkomgevingen.

Het lijkt zeer voor de hand te liggen dat er richtlijnen zullen moeten komen

- voor het verwerken van RFID-tags in producten en verpakkingen waarbij het risico bestaat op consumptie door de consument,
- voor het verwerken van actieve tags (tags met batterij) in producten of verpakkingen die weggegooid worden,
- voor maximale radiostralingsniveaus in werkomgevingen van RFID-readers; en
- voor het breed uitstrooien van tags in de natuur of in agrarische of zeegebieden (toekomst); het terugvinden is immers ondoenlijk.

De milieu- en gezondheidsaspecten verdienen zeker aanvullend onderzoek vanwege hun belang voor de consument en werknemers. Dit is ook zeker een ministerieoverstijgend issue. Het maatschappelijk vraagvlak voor regelgeving zal zonder twijfel veel groter zijn als gezondheid of milieu in het geding is.

Daarnaast is het voor een winkelier of fabrikant een grote onzekerheid wat in de toekomst wel en niet mag wat betreft verwerking van RFID in producten. Te late regelgeving in dit vlak leidt mogelijk tot grote kapitaalvernietiging omdat fabricageprocessen verkeerd zijn ingericht.

### **5.3.7 Opsporing**

Het is meerdere malen aangestipt dat met RFID systemen ook misbruik mogelijk is. Verschillende knelpunten genoemd in sectie 3.2 reppen van mogelijkheden tot bewust misbruik.

Daarbij gaat het om verschillende aspecten, zoals:

- Het bewust schaden of misbruiken van andermans RFID systemen.
- Het overtreden van de WBP met het gebruikte RFID systeem
  - door een slechte beveiliging, of
  - door het leggen van verbanden anders dan waarvoor het systeem bedoeld is (in strijd met Wet bescherming Persoonsgegevens).
- Het gebruik van verborgen, actieve tags die informatie naar de producent zenden.

Het gaat dus enerzijds om misbruik via opzettelijke jamming, afscherming, of ongeoorloofd uitlezen (bedrijfsspionage). Anderzijds gaat het ook om onzorgvuldig gebruik van gegevens (slecht georganiseerde toegangscontrole bijvoorbeeld), of onzorgvuldige ingerichte RFID systemen (niet erg robuust bijvoorbeeld) waardoor inbrekers een kans krijgen.

In dit licht is het van groot belang dat de overheid *leert* over de mogelijkheden van misbruik, en tegelijkertijd *alert is* op dergelijke vormen van misbruik. Dit zal ook samenwerking vereisen tussen verschillende ministeries of departementen. Hieruit volgt dat kennisopbouw zeker een rol zal spelen, maar bovendien moet RFID misbruik een plaats krijgen in de opsporing- en handhavingprocessen.

*In dit licht is het van groot belang dat de overheid leert over de mogelijkheden van misbruik, en tegelijkertijd alert is op dergelijke vormen van misbruik.*

#### **5.4 Conclusies en aanbevelingen**

RFID is niet meer weg te denken. RFID is een kleine technologie met een enorme potentie. Hoewel RFID al langere tijd bestaat, is grote groei te verwachten vanwege de lagere productiekosten en de combinatie met internet-technologie.

Op grond van de toepassingen in hoofdstuk 2 blijkt dat er ontelbaar veel toepassingen zijn van RFID, in een breed toepassingsgebied. Mede door het toenemende gebruik van hoogfrequente UHF RFID tags, eventueel in combinatie met sensoren, ziet bijna dagelijks een nieuwe innovatieve toepassing het levenslicht. De verkenning van de mogelijkheden van RFID is pas begonnen.

Dit betekent dat er kansen liggen om innovatief en origineel voor de dag te komen en te profiteren van de mogelijkheden. Dit gebeurt in Nederland nog te weinig terwijl innovatie een belangrijk beleidsthema is. Dit is mede het gevolg van het feit dat RFID teveel wordt geassocieerd met tracking&tracing en retail. Een algemeen beeld is dat teveel wordt gepraat en “geëxperimenteerd op zolderkamertjes”. Ook het negatief denken voor wat betreft de privacy impact van RFID werkt belemmerend, ondanks het feit dat de wetgeving hiervoor voorlopig toerijkend lijkt te zijn.

Hoewel er vele knelpunten te benoemen zijn (zie hoofdstuk 3), is een algemene indruk dat er weinig directe actie nodig is op het gebied van *regelgeving*. Vele knelpunten zullen door technologieontwikkelaars en toepassers gezamenlijk opgepakt worden. De meeste partijen, softwareontwikkelaars en gebruikerspartijen, vinden zichzelf mans genoeg om de knelpunten op te pakken. Vanuit bedrijfskundig perspectief is het voor de meeste partijen ook simpel: als er een sluitende business case is, wordt RFID toegepast (dit is bedrijfskundig jargon voor: 'het kan uit...'). Zo is gebleken uit de praktijkervaringen uitgewisseld op de RFID workshop bij ECP.nl. Wel is het belangrijk dat het aspect "consumentenbescherming" adequaat vertegenwoordigd kan worden en in het debat over wenselijkheid van bepaalde toepassingen een duidelijke rol kan spelen.

Bovenstaande is echter geen reden voor de overheid of onderzoekspartijen om passief te blijven. Al is de noodzaak tot regelgeving beperkt, er zijn rondom RFID volop mogelijkheden een significante bijdrage te leveren aan duurzaam innovatieve bedrijvigheid. *In plaats van te denken in termen van beleid en regels moeten we veel meer denken in kansen*. Het lijkt zeker een taak van de overheid om voor de juiste randvoorwaarden te zorgen die een succesvolle uitrol van innovatieve RFID toepassingen in Nederland mogelijk maken. Er kan een milieu gecreëerd waarin nieuwe toepassingen op een succesvolle en gecontroleerde manier uitgerold kunnen worden.

Concreet kunnen we de volgende aanbevelingen geven.

- Richt het beleid op het creëren van kansen in plaats van te zoeken naar regelgeving. Regelgeving die zinvol lijkt in het ene toepassingsgebied zal in veel gevallen belemmerend werken in andere toepassingsgebieden. Hierbij is het belangrijk te beseffen dat RFID bij de ene toepassing allang 'proven' technology is, maar bij een andere toepassing in een ander sector nog als experimenteel is. Het is daarom raadzaam om terughoudend te zijn met RFID regelgeving.
- In Nederland, rondom de technische universiteiten en enkele grote bedrijven (bijvoorbeeld Philips), zijn er veel mogelijkheden voor innovatieve technostarters. RFID biedt voldoende mogelijkheden om nog vele jaren innovatieve toepassingen te kunnen genereren. Hiermee kan invulling gegeven worden aan innovatiedoelstellingen van de overheid. Deze kleine technologiebedrijven hebben andere karakteristieken dan het 'gemiddelde' MKB. Het verdient aanbeveling uit te zoeken hoe deze technostarters het beste ondersteund zouden kunnen worden.
- Het verdient aanbeveling om de milieu- en gezondheidsaspecten rond RFID vroegtijdig in kaart te brengen. Dit om te zorgen dat er geen verkeerde paden worden ingeslagen die op termijn onhoudbaar zijn en tot desinvesteringen leiden. Denk hierbij bijvoorbeeld aan wegwerp-chips met batterij in verpakkingen of producten. Het benaderen van RFID regelgeving vanuit de milieu- en gezondheidsaspecten leidt waarschijnlijk tot minder discussie en meer consensus dan wanneer de regelgeving via de privacy-route wordt benaderd. Hiervoor is aanvullend onderzoek nodig.
- Zorg voor goede, feitelijke informatie en zorg voor consumentenbescherming. Dit voorkomt overdreven technologie optimisme en nodeloze angst bij de burgers. Het

creëren van standaard voorlichtingsmateriaal waarmee bedrijven naar de burgers toe kunnen kost weinig moeite en kan hierbij goed helpen.

- Zorg dat harmonisatie in internationale regelgeving nagestreefd wordt op met name frequentieallocatie en vermogens. Het gaat voor het Nederlandse belang in de breedte niet om de precieze regelgeving, het is vooral van belang dat er geen achterstand ontstaat ten opzichte van andere landen ('level playing ground').
- Creëer ondersteunende faciliteiten voor innovatieve bedrijven. Hierbij zijn twee elementen herhaaldelijk genoemd:
  - Creëren van best practices: veel bedrijven willen RFID wel gebruiken, maar zien door de bomen het bos niet meer. Het creëren of verzamelen van best practices, bijvoorbeeld met betrekking tot welke RFID apparatuur voor welke toepassing, of hoe de privacy te bewaken bij het gebruik van RFID. Dit kan typisch gebeuren in samenwerking met de industrie of overkoepelende organisaties
  - Creëren van een toegankelijke lab-omgeving waarin in het bijzonder kleinere organisaties hun nieuwe producten kunnen uittesten. Internationaal gezien schieten de RFID kenniscentra uit de grond, bijvoorbeeld als company-lab of samenwerkingsvorm tussen bedrijven en universiteiten.

Enschede, januari 2006.

## Appendix A - Deelnemers aan de RFID workshop

De lijst van deelnemers die zich aangemeld hebben voor de workshop “Beleidsimplicaties van RFID”, gehouden op 31 oktober 2005 te ECP.nl in Leidschendam.

| Deelnemer           | Organisatie                                    |
|---------------------|--|
| Hek, J. van         | AIDC Consultants BV                            |
| Overheem, J.        | Atos Origin Nederland BV                       |
| Roelofs, B.         | Avery Dennison                                 |
| Roorda, R.          | CBL  |
| Vessies, K.         | DSM Corporate e-Business                       |
| Boerstra, M.        | Federatie Nederlandse Levensmiddelen Industrie |
| Erents, G.C.J.      | GS1 Nederland                                  |
| Gorter de Vries, H. | GS1 Nederland                                  |
| Barmantloo, R.      | Hescon BV                                      |
| Arts, A.            | Hewlett Packard Nederland B.V.                 |
| Serdijn, W.         | Hewlett Packard Nederland B.V.                 |
| Potgieser, P.G.L.   | Interpay Nederland BV                          |
| Brink, J.B.         | Koninklijke KPN NV                             |
| Stam de Jonge, P.   | LogicaCMG Nederland BV                         |
| Bossers, J.B.A.     | Min. van Economische Zaken                     |
| Tijink, D.          | Min. van Economische Zaken                     |
| Akker, G. van den   | Ned. Normalisatie-instituut (NEN)              |
| Schukken, W.        | Ned. Normalisatie-instituut (NEN)              |
| Drunen, L. van      | Nederlands Verpakkingscentrum                  |
| Nieuwesteeg, M.     | Nederlandse Verpakkingscentrum                 |
| Bottemanne, A.      | Oracle Nederland B.V.                          |
| Desertine, M.D.     | Philips Semiconductors BV                      |
| Timmermans, R.      | Pulse Automation Experts bv                    |
| Schermer, B.W.      | RFID Platform Nederland                        |
| Schippers, R.       | SAP Nederland B.V.                             |
| Mierlo, R. van      | Schuitema NV                                   |
| Hulsebosch, B.      | Telematica Instituut                           |
| Strating, P.        | Telematica Instituut                           |
| Teeuw, W.           | Telematica Instituut                           |
| Rieback, M.         | Vrije Universiteit Amsterdam                   |

## Appendix B - RFID standaarden

|              | ISO  | EPC   | ISO   | EPC UHF Gen 2   |
|--------------|--|---|---|---|
| Technologie  | ISO/IEC 18000-x<br>Alle frequenties                | Klasse I-V tags<br>Alleen 13.56 MHz en UHF frequenties  | Technologie standaard voor een zo breed mogelijk set van toepassingen | Beperkt tot '96-bit Write Once' technologie                 |
| Gegevens     | ISO/IEC 15418, 15434, 15459, 15962                 | EPC   | Top-down aanpak   | Bottom-up aanpak  |
| Conformatie  | ISO 18047  | -   | Uitbreidbaar met bijvoorbeeld sensoren en schrijfopties               | Geen uitbreiding mogelijk                                   |
| Applicatie   | Verschilt per industrie (bijv. 18185, 11785, etc.) | -   | Aparte specificatie voor actieve tags                                 | Actieve tags gebruiken hetzelfde spectrum als passieve tags |
| Actieve tags | ISO/IEC 18000 deel 7                               | Niet gespecificeerd   | RAND (reasonable and nondiscriminatory)                               | EPC's IP Policy, royalty free                               |
| Overige      | -  | Reader protocol, object name service, registratiediensten, application level events, informatiediensten | AFIs (Authority and Format Identifier) voor multi-applicatie gebruik  | Geen AFIs   |
|              |  |   | Consistent gebruik van Tag ID, Item ID, Object ID, Chip ID, etc.      | ID-gebruik niet vertrouwt en verwarrend                     |
|              |  |   | EPC + AFI + DSFID (Data Storage Format Identifier) = 128 bits         | 96 bits   |

## Appendix C - Frequentiebanden

| Frequentie          | Regio   | Details   | Eigenschappen   | Toepassingen   |
|---------------------|---|---|---|--|
| 125 – 134 kHz       | VS, Canada, Japan en Europa   | Geen EPC standaard  | Bereik: ~ 10 cm<br>Snelheid: traag  | toegangscontrole<br>Identificatie van dieren<br>Skipassen<br>Anti-diefstalbeveiliging auto   |
| 13.56 MHz           | VS, Canada, Japan en Europa   | Geaccepteerd en veel gebruikt   | Bereik < 1 m<br>Snelheid: traag tot gemiddeld   | Populair voor smartcards   |
| 433.05 – 434.79 MHz | In de meeste Europese landen en in de VS (het gebruik van actieve tags op bepaalde locaties moet geregistreerd worden bij de FCC). In overweging in Japan, China en Zuid-Korea. | ISM-band.<br>In april 2004 verhoogde de FCC het maximale vermogen in deze band onder druk van scheepvaart organisaties  | Bereik: 1 tot 100 m<br>Snelheid: Gemiddeld  | Actief traceren van pallets en kratten<br>Containerbeveiliging<br>Onderhoud en traceren van onderdelen<br>Voertuig tracking<br>Positiebepaling |
| 865 – 868 MHz       | Europa  | Nieuwe ETSI regelgeving staat toe om maximaal 2 Watt ERP tussen 865.6 en 867.6 MHz te gebruiken. Tussen 865.0 en 865.5 maximaal 0.1 Watt ERP en tussen 867.6 en 868.0 maximaal 0.5 Watt ERP | Bereik: 2 tot 10 m <sup>8</sup><br>Snelheid: Gemiddeld tot snel<br>Werkt slecht bij metaal en vocht | Passief traceren van logistieke voorwerpen<br>Banden<br>Tolsystemen<br>Pasportcontrole   |

|                                 |                             |   |                                     |   |
|---------------------------------|-----------------------------|---|-------------------------------------|---|
| 869.4 – 869.65 MHz              | Europa                      | Smalle 250 kHz band met maximaal 0.5 Watt ERP. Oude ETSI RFID band. Nieuwe ETSI RFID band. Listen Before Talk |                                     |   |
| 908.5 – 914.0 MHz               | Zuid-Korea                  |   |                                     |   |
| 902 – 928 MHz                   | VS, Canada                  | Maximaal 4 Watt EIRP  |                                     |   |
| 917 – 922 MHz                   | China                       | Maximaal 2 Watt ERP, tijdelijke toekenning  |                                     |   |
| 918 – 926 MHz                   | Australie                   | Maximaal 1 Watt EIRP  |                                     |   |
| 950-956                         | Japan (voor passieve tags)  | Gereserveerd; wetgeving onderweg  |                                     |   |
| 2.4 – 2.5 and 5.725 – 5.875 GHz | VS, Canada, Europa en Japan | Wordt ook gebruikt voor Bluetooth en Wireless LAN   | Bereik: 1 tot 2 m<br>Snelheid: Snel | Magnetrons<br>Toegangscontrole voertuigen |

EIRP = Effective Isotropic Radiated Power

ERP = Effective Radiated Power (2 Watt ERP is gelijk aan 3.2 Watt EIRP)

## Appendix D - Beleidsinstrumenten

De tabel hieronder geeft een overzicht van middelen die ter beschikking staan bij het omgaan met RFID vraagstukken.

| Beleidsinstrumenten      | Vorm   |
|--------------------------|--|
| Voorlichting             | <ul style="list-style-type: none"> <li>• Het vervaardigen van flyers, brochures of kennisboekjes</li> <li>• Postbus 51 spotjes</li> <li>• Best Practices</li> <li>• Het bezoeken van en geven van presentaties op seminars of congressen</li> <li>• Aan consument, bedrijven of brancheorganisaties</li> </ul>   |
| Wet- en regelgeving      | <ul style="list-style-type: none"> <li>• B.v. conformeren aan internationale standaarden</li> <li>• Het uitvaardigen van richtlijnen voor specifieke toepassingen</li> <li>• het voorschrijven van frequenties en/of vermogens</li> </ul>  |
| Stimulering              | <ul style="list-style-type: none"> <li>• Stimuleren van het geven van voorlichting door bedrijven</li> <li>• Stimuleren van onderzoek</li> <li>• Stimuleren van kennisdeling, b.v. in platforms, rfid platform</li> <li>• Stimuleren van pilots</li> <li>• Stimuleren van specifieke toepassingen of sectoren</li> <li>• Stimuleren van innovatie, b.v. bij kleinere partijen (MKB)</li> <li>• Stimuleren standaardisatie</li> </ul> |
| Scheppen van voorwaarden | <ul style="list-style-type: none"> <li>• Het creëren van RFID kenniscentra aan universiteiten</li> <li>• Het creëren van een RFID lab-omgeving</li> <li>• Het creëren van een DGTP rfid expertise centrum</li> </ul>   |
| Launching customer       | <ul style="list-style-type: none"> <li>• Voorbeeldfunctie</li> <li>• Het gebruik van RFID in overheidsprocessen, b.v. verwerking in paspoorten, gebruik bij toegangscontroles van werknemers in overheidsgebouwen</li> <li>• Creëren kritieke massa voor nieuwe applicaties</li> </ul>   |

## Referenties

- [1] "Trends, facts & Figures from 1.400 RFID case studies", marktonderzoek naar 1400 RFID studies verspreid over 68 landen, 2005, zie <http://www.usingrfid.com/news/read.asp?lc=k15611tx414zw>
- [2] RFID innovatieprijs 2005 juryrapport, zie [http://www.agrologistiek.nl/upl\\_docs/Jury%20rapport%20Schuitema%20.doc](http://www.agrologistiek.nl/upl_docs/Jury%20rapport%20Schuitema%20.doc).
- [3] Gebaseerd op "Wal-Mart kent zijn klant", Computable, 02-09-2005, pagina 24-25.
- [4] [http://www.rfidbuzz.com/news/2004/metro\\_calls\\_back\\_payback\\_with\\_rfid.html](http://www.rfidbuzz.com/news/2004/metro_calls_back_payback_with_rfid.html)  
<http://www.spsychips.com/metro/scandal-deactivation.html>.
- [5] <http://www.foebud.org/>
- [6] <http://rfid.emerce.nl/2004/08/>.
- [7] [http://rfid.emerce.nl/2005/09/rfid\\_bouten.html](http://rfid.emerce.nl/2005/09/rfid_bouten.html).
- [8] 26 augustus 2004 - Door Redactie Computable.
- [9] Emerce RFID, 22 november 2005, zie ook [http://www.morerfid.com/details.php?subdetail=Report&action=details&report\\_id=952&display=RFID](http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=952&display=RFID).
- [10] Healthcare sector survey shows RFID's popularity, UsingRFID.com, zie <http://www.usingrfid.com/news/read.asp?lc=t71121kx585zv&version=printable>.
- [11] RFID Journal, <http://www.rfidjournal.com/article/articleview/1206/1/1/>
- [12] Combating Counterfeit Drugs - A Report of the Food and Drug Administration, februari 2004, zie ook [http://www.fda.gov/oc/initiatives/counterfeit/report02\\_04.html](http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html).
- [13] HIPAA's Privacy and Security rules, 2004, zie <http://www.hhs.gov/ocr/combinedregtext.pdf>.
- [14] [http://rfid.emerce.nl/2005/09/rfid\\_tegen\\_het\\_.html](http://rfid.emerce.nl/2005/09/rfid_tegen_het_.html).
- [15] [http://rfid.emerce.nl/2005/09/eerst\\_een\\_tag\\_i.html](http://rfid.emerce.nl/2005/09/eerst_een_tag_i.html).
- [16] [http://rfid.emerce.nl/2005/05/het\\_is\\_even\\_sli.html](http://rfid.emerce.nl/2005/05/het_is_even_sli.html).
- [17] [http://rfid.emerce.nl/2005/07/ruzie\\_over\\_hond.html](http://rfid.emerce.nl/2005/07/ruzie_over_hond.html).
- [18] <http://www.emerce.nl/nieuws.jsp?id=262738>.
- [19] <http://www.nedaplibrary.com/>.
- [20] [http://rfid.emerce.nl/2005/09/wereldkampioens\\_1.html](http://rfid.emerce.nl/2005/09/wereldkampioens_1.html).
- [21] [http://rfid.emerce.nl/2004/05/nederlands\\_bedr.html](http://rfid.emerce.nl/2004/05/nederlands_bedr.html).
- [22] [http://rfid.emerce.nl/2004/09/wasmachine\\_lees.html](http://rfid.emerce.nl/2004/09/wasmachine_lees.html).
- [23] [http://rfid.emerce.nl/2004/09/caspian\\_geheim.html](http://rfid.emerce.nl/2004/09/caspian_geheim.html).
- [24] Zie [http://rfid.emerce.nl/2004/11/florida\\_gebruik.html](http://rfid.emerce.nl/2004/11/florida_gebruik.html).
- [25] [http://rfid.emerce.nl/2004/10/abi\\_contactloos.html](http://rfid.emerce.nl/2004/10/abi_contactloos.html).
- [26] [http://rfid.emerce.nl/2005/02/visa\\_lanceert\\_b.html](http://rfid.emerce.nl/2005/02/visa_lanceert_b.html).
- [27] [http://rfid.emerce.nl/2005/10/rfid\\_betaalgema.html](http://rfid.emerce.nl/2005/10/rfid_betaalgema.html).
- [28] Klanten van de Japans Luchtvaartmaatschappij JAL kunnen gebruik maken van hun RFID enabled telefoon om sneller en makkelijker te boarden, zie <http://www.jal.com/en/press/0000090/90.html>.
- [29] [http://rfid.emerce.nl/2004/08/definitieve\\_ric.html](http://rfid.emerce.nl/2004/08/definitieve_ric.html).
- [30] <http://rfid.emerce.nl/2005/05/httpwwwitwebcoz.html>.
- [31] [http://rfid.emerce.nl/2005/08/brits\\_kenteken\\_.html](http://rfid.emerce.nl/2005/08/brits_kenteken_.html).
- [32] [http://rfid.emerce.nl/2005/06/british\\_telecom.html](http://rfid.emerce.nl/2005/06/british_telecom.html).
- [33] RFID Opportunities for Mobile Telecommunication Services, ITU-T Lighthouse Technical Paper, Christoph Seidler, Mei 2005.
- [34] Een leuke toepassing hiervan is uitgevoerd in Japan, voor meer informatie zie <http://www.t-engine.org/news/pdf/TEP050202-u01e.pdf>.
- [35] Cisco rapport over "The Impact of RFID on the Network", mart 2005, zie [http://newsroom.cisco.com/dlls/2005/Whitepaper\\_031105.pdf](http://newsroom.cisco.com/dlls/2005/Whitepaper_031105.pdf).
- [36] <http://www.adsx.com/> ; <http://www.verichipcorp.com/>
- [37] [http://www.vnunet.be/computermagazine/detalle.asp?ids=/News/Top\\_Stories/20040429022](http://www.vnunet.be/computermagazine/detalle.asp?ids=/News/Top_Stories/20040429022).
- [38] <http://networks.silicon.com/lans/0,39024663,39122811,00.htm>.
- [39] Tweede Kamer Notitie van de ChristenUnie: RFID-Chips - Kans of gevaar?, 2005, zie [http://www.tweedekamer.christenunie.nl/documenten/tweedekamer/2005-05\\_notitie\\_rfid-chips.doc](http://www.tweedekamer.christenunie.nl/documenten/tweedekamer/2005-05_notitie_rfid-chips.doc).
- [40] [http://rfid.emerce.nl/2005/08/christenen\\_tege.html](http://rfid.emerce.nl/2005/08/christenen_tege.html).
- [41] [http://rfid.emerce.nl/2005/09/slachtoffer\\_ide.html](http://rfid.emerce.nl/2005/09/slachtoffer_ide.html).
- [42] [http://rfid.emerce.nl/2005/05/robot\\_voor\\_blin.html](http://rfid.emerce.nl/2005/05/robot_voor_blin.html).

- [43] Persbericht "Zorgsector start proef met RFID", zie <http://www.rfidnederland.nl/Default2.aspx?tabid=264>.
- [44] Eelco de Jong (Ed.), RFID hardware survey 2005: IS UHF technology ready for European adoption?, LogicaCMG, Amstelveen, 2005.
- [45] [www.freeband.nl](http://www.freeband.nl).
- [46] [www.smart-surroundings.nl](http://www.smart-surroundings.nl).
- [47] Uit "RFID en betaalmogelijkheden - De opmars van RFID, MediaPlaza, Utrecht, 9 september 2004, Harrie Vollaard en Willem de Jager, Rabobank, zie ook [http://www.mediaplaza.nl/uploaded/FILES/\\_seminars/2004/rfid/willem\\_de\\_jager\\_rfid.pdf](http://www.mediaplaza.nl/uploaded/FILES/_seminars/2004/rfid/willem_de_jager_rfid.pdf).
- [48] Het actieprogramma Maatschappelijke Sectoren & ICT, 2005, zie <http://www.maatschappelijkesectorenenict.nl/>.
- [49] Gartner's Hype Cycle Special Report for 2005, zie [http://www.gartner.com/resources/130100/130115/gartners\\_hype\\_c.pdf](http://www.gartner.com/resources/130100/130115/gartners_hype_c.pdf).
- [50] Security Analysis of a Cryptographically-Enabled RFID Device, Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, Michael Szydlo., januari 2005, zie <http://www.rfidanalysis.org/DSTbreak.pdf>.
- [51] Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer, & Stephane Tinguely "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards", 2002 IEEE Symposium on Security and Privacy, Mei 12 - 15, 2002 Berkeley, California, p. 31.
- [52] AIM Global Position Statement on RFID, zie [www.aimglobal.org](http://www.aimglobal.org).
- [53] Zie <http://www.itu.int/osg/spu/ni/ubiquitous/> voor een rapport over de workshop, achtergrondverhalen en presentaties.
- [54] Reva Systems, [www.revasystems.com](http://www.revasystems.com).
- [55] Simple Lightweight RFID Reader Protocol, zie [http://cvs.sourceforge.net/viewcvs.py/\\*checkout\\*/slrrp/slrrp/docs/draft-krishna-slrrp-02.txt](http://cvs.sourceforge.net/viewcvs.py/*checkout*/slrrp/slrrp/docs/draft-krishna-slrrp-02.txt).
- [56] Zie ETSI's website op [http://www.etsi.org/services\\_products/freestandard/home.htm](http://www.etsi.org/services_products/freestandard/home.htm).
- [57] C. Seidler, ITU-T Lighthouse Technical Paper, mei 2005, zie ook <http://www.itu.int/ITU-T/techwatch/docs/rfid.pdf>.
- [58] "EPCglobal – RFID Standards & Regulations" presentatie tijdens de OECD Foresight Forum over "Radio Frequency Identification (RFID) Applications and Public Policy Considerations", Parijs, 5 oktober 2005, zie [http://www.oecd.org/documentprint/0,2744,en\\_2649\\_201185\\_35186234\\_1\\_1\\_1\\_1\\_0.html](http://www.oecd.org/documentprint/0,2744,en_2649_201185_35186234_1_1_1_1_0.html).
- [59] K. Powell, Passive RFID – A Primer for New RF Regulations, Matrics Inc. whitepaper, 2004.
- [60] "This Is Not My Beautiful House! This Is Not My Beautiful Identity!", The Dallas Morning News, augustus 2005, zie <http://www.plastic.com/article.html;sid=05/08/23/19205287;cmt=60>.
- [61] Zie voor meer informatie: "Gezondheidseffecten van blootstelling aan radiofrequente elektromagnetische velden - Probleemanalyse niet-ioniserende straling", J.F.B. Bolte en M.J.M. Pruppers, RIVM Rapport 861020007, 2004, zie ook <http://www.rivm.nl/bibliotheek/rapporten/861020007.pdf>.
- [62] RFID and Consumers, Capgemini, 2005, zie [http://www.capgemini.com/news/2005/Capgemini\\_European\\_RFID\\_report.pdf](http://www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf).
- [63] RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management, Melanie R. Rieback, Bruno Crispo, en Andrew S. Tanenbaum, 2005, zie [http://www.cs.vu.nl/~melanie/rfid\\_guardian/papers/acisp.05.pdf](http://www.cs.vu.nl/~melanie/rfid_guardian/papers/acisp.05.pdf).
- [64] Privacyrechtelijke Aspecten van RFID, ECP.NL, mei 2005, zie <http://www.ecp.nl/publications/RFID.pdf>.
- [65] Artikel 29 Gegevensbescherming Werkgroep, "Working Document on Data Protection Issues Related to RFID technology", WP105, 10107/05/EN, 19 januari 2005. Zie ook <http://www.europa.eu.int/comm/privacy>.
- [66] "The European Union Works Out RFID Privacy Legislation", Information Week, 6 Februari 2005, zie ook <http://www.informationweek.com/showArticle.jhtml?articleID=59301363>.
- [67] Radio Frequency Identification: Applications and Implications for Consumers, a workshop report from the Staff of the Federal Trade Commission, March 2005.
- [68] Guidelines on EPC for Consumer Products, EPCglobal, zie [www.epcglobalinc.org/consumer](http://www.epcglobalinc.org/consumer).

- [69] “An RFID Bill of Rights”, Technology Review, oktober 2002, <http://www.technologyreview.com/articles/02/10/garfinkel1002.asp?p=1>. Zie ook CASPIAN’s “RFID Right to Know Act of 2003”, te vinden op <http://www.nocards.org/rfid/rfidbill.shtml>.
- [70] Zie <http://www.rfidjournal.com/article/articleview/1491/1/1/>.
- [71] VNO/NCW: Privacy hindert doelmatigheid, Automatisering Gids, 11 november 2005.
- [72] Jim Harper, RFID Tags and Privacy: How Bar-Codes-On-Steroids Are Really a 98-Lb. Weakling, Competitive Enterprise Institute, juni 2004.
- [73] Innovatieve mkb’er voelt zich onbegrepen: Overheid en bedrijven tonen weinig enthousiasme voor RFID-chip, Financiële Dagblad, 12-11-2005.
- [74] Cisco rapport over “The Impact of RFID on the Network”, maart 2005, zie [http://newsroom.cisco.com/dlls/2005/Whitepaper\\_031105.pdf](http://newsroom.cisco.com/dlls/2005/Whitepaper_031105.pdf).
- [75] RFID hardware survey 2005 - Is UHF technology ready for European adoption?, LogicaCMG onderzoek.
- [76] InnovationScan “Veiligheid in kennis en toepassing”, SenterNovem, 2005, zie [http://www.senternovem.nl/mmfiles/Innovation%20Scan%20Veiligheid%20definitief\\_tcm24-123958.pdf](http://www.senternovem.nl/mmfiles/Innovation%20Scan%20Veiligheid%20definitief_tcm24-123958.pdf).
- [77] Consumers Against Supermarket Privacy Invasion and Numbering – CASPIAN, website <http://www.nocards.org/>.
- [78] Radio Frequency Identification – Opportunities and Challenges in Implementation, Department of Commerce, Washington DC, April 2005.
- [79] Information Security - Radio Frequency Identification Technology in the Federal Government, Government Accountability Office rapport, mei 2005, zie <http://www.gao.gov/new.items/d05551.pdf>.
- [80] [http://rfid.emerce.nl/2005/06/californi\\_bezig.html](http://rfid.emerce.nl/2005/06/californi_bezig.html).
- [81] [www.technology.gov](http://www.technology.gov).
- [82] Standaard en lage prijs moet RFID helpen, Automatisering Gids, 7 oktober 2005, nr 40, p.5.
- [83] Zorgsector test RFID, Computable, 16 september 2005, p3.
- [84] [www.rfiduk.org/](http://www.rfiduk.org/).
- [85] Ofcom's decision to exempt the use of radio frequency identification equipment in the 865-868 MHz band from Wireless Telegraphy licensing - Statement, 9 november 2005, zie [http://www.ofcom.org.uk/consult/condocs/wireless865\\_868/865\\_868statement/865\\_868.pdf](http://www.ofcom.org.uk/consult/condocs/wireless865_868/865_868statement/865_868.pdf).
- [86] Chinese RFID blijft groeien, Emerce, 29 augustus 2005, zie [http://rfid.emerce.nl/2005/08/chinese\\_rfid\\_ma.html](http://rfid.emerce.nl/2005/08/chinese_rfid_ma.html).
- [87] Ministerie van Binnelandse Zaken en Communicatie website: [http://www.soumu.go.jp/joho\\_tsusin/eng/whitepaper.html](http://www.soumu.go.jp/joho_tsusin/eng/whitepaper.html).
- [88] Zie [http://www.mic.go.kr/eng/res/res\\_pub\\_it839.jsp](http://www.mic.go.kr/eng/res/res_pub_it839.jsp).
- [89] Bron: Infoworld
- [90] The debut of an ‘intelligent’ RFID reader, Industry Weekly, 22 november 2005, zie [www.industryweek.com/PrintArticle.aspx?ArticleID=11047](http://www.industryweek.com/PrintArticle.aspx?ArticleID=11047).
- [91] Zie voor meer informatie <http://www.ez.nl/content.jsp?objectid=11447>.
- [92] Zie Camera’s in het Publieke Domein, College Bescherming Persoonsgegevens, [http://www.cbppweb.nl/documenten/av\\_28\\_cameras.shtml?refer=true&theme=purple](http://www.cbppweb.nl/documenten/av_28_cameras.shtml?refer=true&theme=purple)