

Aan

De Voorzitter van de Tweede Kamer  
der Staten-Generaal  
Binnenhof 4  
2513 AA 's-GRAVENHAGE

Datum	Uw kenmerk	Ons kenmerk	Bijlage(n)
25 september 2006		ET/CSI / 6073683	1

Onderwerp

RFID in Nederland

### *1. Aanleiding*

Radio Frequency IDentification (kortweg RFID) is een technologie die door technologische en prijsontwikkelingen voor steeds meer toepassingen bruikbaar wordt.<sup>1</sup> Internationaal zijn er hooggespannen verwachtingen over de economische mogelijkheden, maar er leven ook zorgen over de mogelijke maatschappelijke nadelen. De heer Slob heeft in een motie (nr. 30 300 XIII, nr. 36) gevraagd om een notitie over RFID met bijzondere aandacht voor privacy. In deze brief en de achterliggende notitie is gepoogd een helder overzicht te schetsen van RFID en de aspecten ervan waar de overheid in beeld komt. Ik vat in deze brief de achterliggende notitie kort samen en ga achtereenvolgens in op:

1. de ontwikkeling van RFID
2. de kansen die RFID biedt
3. de zorgen rond RFID
4. de voorwaarden: frequenties en standaarden
5. de conclusie

### *2. Ontwikkelingen*

De RFID ontwikkeling wordt gekenmerkt door chips die steeds kleiner en goedkoper worden. In de notitie wordt RFID in cards, RFID in apparaten (bv. mobiele telefoon of PDA) en RFID op producten onderscheiden. Hun eigenschappen hebben verschillende

---

<sup>1</sup> RFID staat voor Radio Frequency IDentification en is een technologie waarmee met behulp van radiogolven unieke automatische identificatie van producten op afstand mogelijk wordt gemaakt.

RFID is in de basis vergelijkbaar met de klassieke barcode met als verschil dat een RFID chip niet in het zicht van een scanner gehaald hoeft te worden gelezen maar op beperkte afstand door een 'reader' door objecten heen en met meerdere tegelijkertijd uitgelezen kan worden.

Bezoekadres

Bezuidenhoutseweg 30

Hoofdkantoor

Bezuidenhoutseweg 30

Postbus 20101

2500 EC 's-Gravenhage

Telefoon (070) 379 89 11

Telefax (070) 347 40 81

Email ezpost@minez.nl

Website www.minez.nl

Doorkiesnummer

Behandeld door

**Daniel Tijink**

*Verzoeken bij beantwoording van deze brief ons kenmerk te vermelden*

Telefax

uitwerking op vraagstukken van privacy of innovatie. RFID in cards zijn al langer bekend, in veel toegangspasjes van gebouwen zit bijvoorbeeld een RFID-chip. Nieuwe, grootschalige toepassingen zijn het paspoort en OV-chipcard. Bij RFID in apparaten kan gedacht worden aan telefoons, die een betaalfunctie krijgen of informatie kunnen uitlezen van posters. Deze toepassing bevindt zich nog in het experimenteerstadium.

De meest besproken toepassingen zijn de RFID-tags op producten, die op die manier 'intelligent' worden gemaakt. Een reader kan de tag identificeren en de eventuele informatie uitlezen en naar een database sturen. De tag kan in principe aan allerlei soorten producten worden gekoppeld. De meeste toepassingen bevinden zich echter nog in het experimenteerstadium. Toepassingen die al gebruikt worden bevinden zich vooral in de logistiek en in sectoren als zorg en landbouw. Voorbeelden zijn een bloemenveiling die RFID-chips gebruikt om het logistieke proces van haar containers te verbeteren, Legoland waar verdwaalde kinderen voorzien van een chip sneller kunnen worden teruggevonden, RFID in autobanden als anti-diefstal en voorraadbeheer. Hoewel een RFID-tag vaak vergeleken wordt met een geavanceerde streepjescode zijn er tot op heden nog weinig gevallen waar de klant zelf via artikelen met RFID geconfronteerd wordt.

### *3. Kansen: innovatie*

Wereldwijd wordt de ontwikkeling van RFID gezien als zeer veelbelovend. De omzet van RFID groeit de komende jaren snel. In 2010 wordt hij op 12 miljard euro geschat<sup>2</sup>. De Nederlandse overheid ziet RFID als een interessante, veelbelovende ontwikkeling, waarbij het belangrijk is in deze fase de economische kansen optimaal te benutten, uiteraard binnen randvoorwaarden van privacy en veiligheid. RFID is, net als ICT, een enabling technology: een technologie die ontwikkelingen in andere sectoren mogelijk maakt. RFID kent veel nuttige toepassingen in zeer diverse sectoren: van de logistiek tot de zorg, van het betalingsverkeer tot openbaar vervoer. Bekend voorbeeld is de OV-chipcard, die in Nederland ingevoerd wordt. Een voorbeeld uit de zorgsector is een experiment waarin bloedzakken worden voorzien van temperatuurgevoelige chips waarmee zowel tracering plaatsvindt als dat de temperatuur gecontroleerd kan worden.

Voor de overheid is de vraag of het bestaande innovatie-instrumentarium in Nederland voldoende is voor deze nieuwe ontwikkeling. Innovatie wordt ondersteund via algemene regelingen. In dat kader komt ook RFID aan bod. Zo kunnen (MKB-)ondernemers advies krijgen over invoering van RFID-technologie bij Syntens, ondersteunt SenterNovem innoverende ondernemers met subsidies<sup>3</sup> en heeft RFID een plaats in enkele onderzoeksprojecten<sup>4</sup> daarnaast krijgt RFID mogelijk plaats in grote

---

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

<sup>3</sup> Het aantal toegekende aanvragen aangaande RFID steeg van 51 in 2003, naar 108 in 2004 tot 203 in 2005

<sup>4</sup> Bij TNO of de BSIK-programma's Freeband en Smart Surroundings

innovatieprogramma's, die op dit moment gevormd worden, zoals Fresh on Demand, of Innovatie in de Logistieke keten. Uit de markt komen verschillende signalen dat de bottleneck op dit moment de testfase van toepassingen is en het delen van de opgedane kennis. Er zijn wel voorbeeldopstellingen, maar daarmee kan niet getest worden, omdat er niet ingespeeld kan worden op specifieke omstandigheden van gebruikers.

#### *4. Zorgen rondom RFID: privacy, beveiliging, milieu*

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

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

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

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

De drie genoemde risico's liggen alle drie op het terrein van privacy. Het wettelijke kader dat dit gebruik van data reguleert is geïmplementeerd in de Wet Bescherming persoonsgegevens (WBP). De WBP is technologie-neutraal geformuleerd en geeft dus geen kant-en-klaar antwoord op vragen aangaande RFID en privacy. ECP.NL heeft in haar studie naar privacy geconcludeerd dat het wettelijk kader voor de bescherming van de (informationele) privacy zoals vastgelegd in de WBP volledig van toepassing is op RFID-systemen waarmee persoonsgegevens worden verwerkt. Dit betekent dat RFID-toepassers gebonden zijn aan de regels voor de rechtmatige verwerking van

persoonsgegevens die voortvloeien uit de WBP. Het beschermingsniveau dat hiermee geboden wordt lijkt in het kader van RFID-toepassingen toereikend. Het lijkt dus voorsnog niet noodzakelijk om RFID specifieke aanvullingen te maken op de WBP. Voorsnog wordt aangesloten bij deze conclusie. Het College Bescherming Persoonsgegevens (CBP) is overigens voornemens na de zomer van 2006 met een notitie over RFID te komen, waarin zowel de toepasbaarheid van de wetgeving als de mogelijkheden van toezicht aan de orde zullen komen.

In het algemeen is voor het voorkomen van zorgen over privacy transparantie een sleutelbegrip. Het gebruik van RFID en met name de verwerking en het bewaren van gegevens die RFID genereert, moet voor iedereen op een begrijpelijke manier inzichtelijk kunnen worden gemaakt. Dit adagium geldt zowel voor bedrijven als voor overheden. Daarnaast kan de producerende industrie zelf veel bijdragen aan de vermindering van privacyrisico's door 'privacy by design': wegwerp chips, aan-uit knopjes, goede versleuteling etc.

Voor de *technische veiligheid* van RFID moet naar het hele systeem gekeken worden. De tag, de reader en de database kunnen op verschillende manieren onveilig zijn. De meest genoemde mogelijke verstoringen, zoals verzenden van versturende radiogolven of af luisteren van RFID-systemen zijn strafbaar volgens de Nederlandse wet. Overigens hebben niet alle toepassingen een even hoog niveau van beveiliging nodig. De verantwoordelijkheid voor de beveiliging van toepassingen ligt primair bij de partijen die een RFID toepassing implementeren.

Op het gebied van *milieu en gezondheid* is de lijn duidelijk. RFID valt onder de categorie elektrische en elektronische apparatuur en daarmee binnen twee richtlijnen van de Europese Commissie op het gebied van schadelijke stoffen en recycling van producten. De huidige regelgeving is afdoende om de nadelige effecten van RFID op het milieu te beperken.

RFID maakt gebruik van elektromagnetische velden, waarbij opgemerkt worden dat die opgewekt worden door de readers en dat een 'tag' geen veld draagt. De limieten voor blootstelling van elektromagnetische straling zijn opgesteld door de ICNIRP<sup>5</sup> en erkend door de WHO (World Health Organization). Op basis van deze limieten zijn er Europese Normen op RFID van toepassing<sup>6</sup>. De door RFID gebruikte elektromagnetische velden vallen qua vermogen en qua intensiteit binnen de normen.

---

<sup>5</sup> ICNIRP. The International Commission on Non-Ionizing Radiation Protection.

<sup>6</sup> EN 50364: 2001 en EN 50357: 2001

### 5. Voorwaarden: frequenties en standaarden

Om tot interessante toepassingen te komen dienen ook basisafspraken op orde te zijn. Voor RFID spreken we dan over standaardisatie en frequentieruimte. Standaardisatie is essentieel voor het functioneren van RFID en primair een verantwoordelijkheid van het bedrijfsleven zelf.

De verantwoordelijkheid voor de door RFID gebruikte frequentieruimte ligt primair bij de overheid. Het Ministerie van Economische Zaken implementeert de vanuit internationale gremia aangegeven richtlijnen en aanbevelingen in het Nationaal FrequentiePlan (NFP). In de afgelopen periode zijn er nieuwe banden bijgekomen voor RFID-gebruik, en in de komende tijd worden dat er nog meer. Op dit moment is het beschikbare spectrum adequaat voor RFID-ontwikkeling. Voor het geval RFID mondiaal gezien plotseling een zeer stormachtige ontwikkeling zou doormaken, kan snel voor verruiming van de beschikbaarheid worden gezorgd. Op dit moment zijn er derhalve qua spectrumbestemming en -beschikbaarheid geen knelpunten of problemen voor de RFID-ontwikkeling.

### 6. Conclusie / Acties

In deze brief zijn de ontwikkelingen op het gebied van RFID en de mogelijke beleidsconsequenties kort uiteengezet. Voor meer aanvullende informatie verwijs ik naar de door de Kamer verzochte notitie (zie bijlage). Samengevat is RFID op dit moment nog volop in ontwikkeling. De verwachtingen over de mogelijkheden en de zorgen lopen breed uiteen. Veel beleidsconsequenties van RFID zijn niet uniek. Zorgen over privacy, het regelen van frequentieruimte en het stimuleren van innovatie zijn onderwerpen die ook verbonden zijn aan andere technologieën. De Nederlandse overheid heeft op deze onderwerpen staand beleid. Uit de notitie komt naar voren dat het staande beleid in veel gevallen voldoet of is aangepast: frequenties, milieu en gezondheid, innovatie(grotendeels). Vanzelfsprekend is het van belang RFID zorgvuldig te monitoren vanuit de verschillende invalshoeken, met name privacy en nieuwe toepassingsmogelijkheden. Daarom wordt er een interdepartementale werkgroep ingesteld, waarvoor de departementen worden uitgenodigd waarvan de beleidsterreinen RFID raken: EZ, JUS, VROM, BZK, V&W. Het Ministerie van Economische Zaken zal vanuit haar coördinerende rol het voorzitterschap op zich nemen, de verantwoordelijkheden blijven uiteraard bij de ministeries. De werkgroep heeft de volgende functies:

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

Op het gebied van privacy lijkt wel specifieke aandacht nodig. Het is een onderwerp dat hoog op de agenda van de werkgroep komt. In de notitie zijn de verschillende risico's en

de evaluatie ervan aan bod gekomen. De kernvraag is of de bestaande wetgeving (en handhaving) op het gebied van de bescherming van persoonsgegevens voldoet bij de komst van RFID. Vooral nog wordt aangesloten bij de conclusie van ECP.NL, dat het beschermingsniveau van de WBP voldoende lijkt in het kader van RFID-toepassingen. Tevens wordt het rapport van het CBP afgewacht, dat verwacht wordt in oktober/november. Het zal ook aansluiten bij de discussie die gevoerd wordt door de Europese privacy toezichthouders, verenigd in de art. 29 werkgroep, over RFID en de interpretatie van het begrip 'persoonsgegevens'. Vooruitlopend hierop is voor het voorkomen van zorgen over privacy transparantie een sleutelbegrip. Het gebruik van RFID en de verwerking en het bewaren van gegevens die RFID genereert, moet voor iedereen op een begrijpelijke manier inzichtelijk gemaakt kunnen worden. Tevens biedt 'privacy by design' (zoals versleuteling, chips die uitgezet kunnen worden etc.) goede mogelijkheden om de privacyrisico's te verkleinen.

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

(w.g.) mr. drs. J.G. Wijn  
Minister van Economische Zaken