

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

Datum	Uw kenmerk	Ons kenmerk	Bijlage(n)
10 december 2007		ET/IT 7114108	1

Onderwerp
Radio Frequency Identification (RFID)

Naar aanleiding van mijn brief van 27 april inzake Radio Frequency IDentification (RFID) en privacy (30800 XIII, nr 49) stelden de leden van de fracties van CDA, SP, VVD, ChristenUnie op 27 juni jl. nadere vragen. Hierbij ontvangt u, mede namens de Ministers van Binnenlandse Zaken en Koninkrijkrelaties, van Justitie, van Verkeer en Waterstaat en van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer, mijn antwoorden.

Toepassing

De leden van de fractie van het CDA vragen om een overzicht – met een toekomstbeeld – van de daadwerkelijke toepassing van RFID, uitgesplitst naar overheid en particuliere sector.

RFID is een basistechnologie, die tot vele toepassingen kan leiden. Vaak wordt in relatie tot RFID de term 'ubiquitous computing' als toekomstvisie gebruikt; het idee dat alle "getagde" objecten (objecten voorzien van een chip) met elkaar kunnen communiceren. In een rapport van het EU-programma BRIDGE wordt de groei van het aantal passieve tags in de EU geschat: van 144 miljoen tags in 2007 naar 3,2 miljard tags in 2012, tot 86 miljard tags in 2022.¹ Naast de logistieke sector zijn er steeds meer andere sectoren waarin RFID-toepassingen opkomen, zoals consumentengoederen, openbaar vervoer, zorg, ticketing, e-betalen, veiligheid en recycling. Bijgevoegde tabel geeft een – niet uitputtend - overzicht van toepassingen van RFID in Nederland. De schaalgrootte van de toepassingen verschilt.

¹ European passive RFID Market Sizing 2007-2022, BRIDGE, feb 2007

Bezoekadres	Doorkiesnummer	Telefax
Prinses Beatrixlaan 5-7	8130	8270

Hoofdkantoor	Telefoon 070-379 6106	Behandeld door
Bezuidenhoutseweg 30	Telefax 070-379 6154	M. Andriessen
Postbus 20101	Email f.heemskerck@minez.nl	
2500 EC 's-Gravenhage	Website www.minez.nl	Verzoek bij beantwoording van deze brief ons kenmerk te vermelden

Privacy en veiligheid

De leden van de CDA-fractie vragen op welke wijze de Staatssecretaris de ontwikkelingen op het gebied van RFID en privacy zal monitoren, zodat tijdig ingegrepen kan worden, indien nieuwe ontwikkelingen wél inbreuk zouden maken op de bescherming van de privacy. De leden van de SP-fractie vragen op welke wijze de Staatssecretaris wil bevorderen dat data veilig opgeborgen zijn en niet toegankelijk voor mensen van buitenaf, maar wel voor het eigen bedrijf. De leden van de Christenunie vragen op welke wijze toezicht is op de plicht van gebruikers om RFID-gebruik zichtbaar en kenbaar te maken.

Zoals beschreven in de notitie RFID in Nederland (30800 XIII, nr. 5) ligt de verantwoordelijkheid voor de beveiliging van toepassingen in het private domein primair bij de private partijen die een RFID-toepassing implementeren. Het is in het belang van het bedrijfsleven dat de technologie robuust is. Het College Bescherming Persoonsgegevens (CBP) houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Het CBP beziet of zich nieuwe ontwikkelingen aandienen die wel inbreuk maken op privacy. Er is geen wettelijke verplichting voor toepassers van RFID-systemen om zichtbaar en kenbaar te maken dat RFID wordt ingezet. In de praktijk doen zij dit vaak wel. Toepassers van de EPC-standaard (passieve tags) en van NFC (een aan RFID-verwante technologie die met name wordt toegepast voor mobiel betalen) zijn verplicht zich te houden aan richtlijnen die door de ontwikkelaars van de EPC-standaard en de NFC-technologie zijn vastgesteld. Deze verplichten dat gebruik van RFID en NFC kenbaar is voor de gebruiker. Indien persoonsgegevens worden verwerkt zijn toepassers van RFID krachtens de Wet Bescherming Persoonsgegevens (Wbp) wél verplicht betrokkenen hiervan vooraf op de hoogte te stellen.

De leden van de ChristenUnie vragen of het belang van vertrouwen van burgers in overheid en technologie voorop staat, en niet de ontwikkeling van de technologie?

Technologie is een hulpmiddel in dienst van de economie en de maatschappij, geen doel op zich. Vertrouwen van burgers in een technologie is een voorwaarde voor de acceptatie en toepassing – en daarmee het succes - van die technologie.

De leden van de fractie van de ChristenUnie vragen om een reactie op opmerkingen van de heer Terstegge die wordt aangehaald in de nota «Eerste fase evaluatie Wet bescherming persoonsgegevens» (Kamerstuk 31 051, nr. 1) over de onhoudbaarheid van de begrippen in de Wbp als gevolg van technologische ontwikkelingen. Deze leden vragen tevens hoe de Staatssecretaris er op toeziet dat het CBP invulling geeft aan verdere normontwikkeling en of dit een onderwerp is waar de «denktank privacy en nieuwe technologieën» zich mee bezig gaat houden. De leden van de SP-fractie vragen of de Staatssecretaris bereid is er bij collega's op aan te dringen dat RFID-toepassingen expliciet meegenomen worden in de evaluatie van de Wbp en of de consequenties van anonieme sporen ook opgenomen dienen te worden in de Wbp.

De heer Terstegge heeft in het kader van de RFID-discussie in Europa onder meer vraagtekens geplaatst bij het begrip “persoonsgegeven” zoals dat momenteel in de WBP is gedefinieerd, waarbij hij zich af heeft gevraagd of dit begrip nog wel houdbaar is in het

licht van nieuwe informatie- en communicatie technologieën zoals RFID. Hij vroeg zich af of het niet beter zou zijn om in een digitale samenleving “digitale voetsporen” in het algemeen tegen misbruik te beschermen ongeacht of die voetsporen herleidbaar zijn tot een individu of niet. Voorts heeft hij vraagtekens geplaatst bij de wijze waarop de huidige privacywetgeving in Europa in een wereld van “ubiquitous computing” nog op een efficiënte en doelmatige wijze invulling kan geven aan een aantal beginselen van privacybescherming, waarbij hij met name heeft gewezen op het risico dat normerende gebruiksregels zoals de WBP op den duur als obstakel kunnen gaan fungeren voor technologische innovatie en de ontwikkeling van maatschappelijk zinvolle toepassingen van informatie- en communicatie technologie. Met name vanwege het formele karakter van de WBP is hij geen voorstander van het verder oprekken van het begrippenkader om ook het gebruik van dit soort nieuwe technologieën te ondervangen, maar pleit hij voor een fundamentele herbezinning op de wijze waarop privacybescherming in de informatiesamenleving gestalte moet worden gegeven. “Privacy by design” en het tegengaan van misbruik van digitale voetsporen zouden volgens hem daarin een leidende rol moeten spelen.

Het zijn dit soort vraagtekens bij de technologie-onafhankelijkheid van de Wbp als gevolg van technologische ontwikkelingen die voor mijn ambtsvoorganger aanleiding zijn geweest om in samenwerking met ECP.nl een denktank van experts en belanghebbenden op het gebied van privacy en nieuwe technologieën samen te stellen. Deze denktank beschouwt momenteel het juridisch kader voor de bescherming van de privacy van de consument en beoordeelt in hoeverre dit juridisch kader is toegesneden op de introductie van technologieën als RFID. In het onderzoek van de denktank wordt ook gezien of verdere normontwikkeling noodzakelijk is en zo ja op welke wijze deze kan worden vormgegeven. Ik stel uw Kamer eind 2007 van de resultaten van het onderzoek van deze denktank op de hoogte. Vanzelfsprekend zal ook het CBP op de hoogte worden gesteld van de uitkomsten van dit onderzoek en om een opinie worden gevraagd.

De evaluatie van de Wet bescherming persoonsgegevens is op dit ogenblik gaande. De evaluatie is opgesplitst in twee fasen. De uitkomst van de eerste fase die onlangs aan de Kamer is gezonden, behelst een knelpuntenanalyse op basis van bestaande literatuur en een empirisch (veld)onderzoek (“Eerste fase evaluatie Wbp. Literatuuronderzoek en knelpuntenanalyse”, Kamerstukken II, vergaderjaar 2006-2007, 31 051, nr. 1). In de tweede fase van de evaluatie zal uitvoerig aandacht worden besteed aan alle in de knelpuntenanalyse geconstateerde knelpunten, zoals vragen die samenhangen met (onvoorziene) technologische ontwikkelingen die zich rondom de toepassing van RFID zouden kunnen voordoen. Ook de resultaten van het onderzoek van de denktank privacy en nieuwe technologie zullen bij de evaluatie worden betrokken.

De leden van de fractie van de ChristenUnie vragen hoe er op de ontwikkeling van privacy by design wordt toegezien, of ontwikkelaars per nieuwe toepassing moeten aangeven wat de mogelijkheden van het product zijn en op wat voor manier privacy by design is toegepast en wat de rol van de Nederlandse regering is bij de ontwikkeling van Europese “applicatie-specifieke richtlijnen”.

Ik onderschrijf het belang van ‘privacy by design’. Ontwikkelaars en toepassers van nieuwe technologieën zoals RFID en Ambient Intelligence kunnen zelf veel bijdragen aan

de vermindering van privacyrisico's door rekening te houden met privacy-aspecten bij de ontwikkeling van toepassingen en het ontwerp van hun systemen en applicaties. Veel ontwikkelaars brengen zulks momenteel ook in de praktijk. Privacy en security vormen een belangrijk onderdeel van het deelprogramma ICT van het 7e Kaderprogramma van de Europese Commissie. Daarnaast streeft de Europese Commissie in dit verband naar de ontwikkeling en verspreiding van 'good practices'. Ik steun de Europese Commissie in dit streven.

De leden van de VVD-fractie vragen wat de zin is van de interdepartementale werkgroep? Waarom kan Economische Zaken niet de belangen van overheid behartigen mede namens vier andere ministeries? Welk gezamenlijk (afgestemd) internationaal optreden bewaakt de interdepartementale werkgroep en op welke manier? Wat is de zin van een denktank m.b.t. de privacy naast eerder genoemd overleg? Waarom wordt privacy los besproken in plaats van tezamen met de andere aspecten?

Het Ministerie van Economische Zaken is het eerste aanspreekpunt voor het (georganiseerde) bedrijfsleven, consumentenorganisaties, Europese instanties en de OESO aangaande RFID. Zoals ik in mijn brief van 27 april heb uiteengezet coördineert mijn departement als voorzitter van de interdepartementale werkgroep tevens de uiteenlopende beleidsmatige aspecten op het gebied van RFID, waaronder aspecten van privacy. De denktank van experts en belanghebbenden op het gebied van privacy en nieuwe technologieën beschouwt momenteel een deelaspect, namelijk het juridisch kader voor de bescherming van de privacy van de consument en beoordeelt in hoeverre dit juridisch kader is toegesneden op de introductie van nieuwe technologieën zoals embedded systemen en RFID.

RFID stakeholdergroep

De leden van de VVD-fractie vragen welke vertegenwoordigers uit industrie, consumentenorganisaties en overheid namens Nederland plaatsnemen in de door de Europese Commissie opgerichte RFID Stakeholdergroep? Worden deelnemers aangewezen door de Europese Commissie of door de Nederlandse overheid of op een andere manier? Vindt de Staatssecretaris dat de aangewezen deelnemers een juiste afspiegeling van alle betrokkenen en behartiging van alle belangen in voldoende mate garanderen?

The RFID Stakeholders Group bestaat uit vertegenwoordigers van 17 organisaties en bedrijven die daartoe door de Europese Commissie zijn uitgenodigd. Het betreft met name organisaties die actief zijn geweest in de RFID-consultatieronde die de Europese Commissie in 2006 heeft gehouden. De groep vertegenwoordigt zowel de verschillende belangen bij dit onderwerp als een groot aantal landen en economische sectoren. NXP Semiconductors neemt als enig Nederlandse bedrijf deel in deze groep. Consumentenbelangen worden vertegenwoordigd door de Europese consumentenorganisaties BEUC, ANEC en European Digital Rights. De Nederlandse overheid is niet rechtstreeks vertegenwoordigd in de RFID Stakeholders Group. Wel nemen namens de Raad vertegenwoordigers van het Voorzitterschap deel aan de sessies van de Stakeholders Group, echter alleen als waarnemer. De Stakeholders Group vormt naar mijn mening een evenwichtige afspiegeling van alle betrokkenen.

Standaardisatie en interoperabiliteit

De leden van de VVD-fractie vragen of er inmiddels duidelijkheid is over de Europese Commissie en haar streven naar wereldwijde interoperabiliteit? Is hierbij sprake van betrokkenheid van het bedrijfsleven? Wat is het ambitieniveau van de Nederlandse overheid op het gebied van internationale interoperabiliteit (standaardisatie) buiten Europa, zo vragen de leden van de VVD-fractie? Kan de Staatssecretaris naast vragen om verduidelijking ook eigen wensen en ideeën hierover doorgeven aan de Europese Commissie? Kan de Staatssecretaris dit aan zijn actielijstje voor de komende maanden toevoegen?

Standaardisatie is essentieel voor het functioneren van RFID, maar primair een taak voor het bedrijfsleven. De Nederlandse overheid en de Europese Commissie steunen het streven van het bedrijfsleven naar wereldwijde interoperabiliteit van RFID-systemen. De Europese Commissie heeft aangegeven op Europees niveau actie te zullen ondernemen indien op termijn blijkt dat wereldwijde interoperabiliteit van RFID-systemen onhaalbaar blijkt. Ik steun de Commissie hierin.

Verplicht gebruik van RFID en onklaar maken van chips

De leden van de fractie van de ChristenUnie vragen of er oog is voor de problemen van mensen die grote bezwaren hebben tegen het gebruik van RFID en of er mogelijkheden zijn, ook in de toekomst, voor gewetensbezwaarden om zich aan deze technologie te onttrekken. Tevens vragen deze leden een reactie op de aanbeveling van het CBP, dat betrokkenen zich moeten kunnen weren tegen RFID-gebruik, ook in relatie tot het paspoort met RFID of de chipkaart van de NS.

Ik deel de opvatting van het CBP dat burgers waar redelijk over mogelijkheden moeten kunnen beschikken om al dan niet betrokken te worden bij RFID-systemen. Hierbij valt te denken aan het kunnen kiezen voor een alternatief waarbij geen RFID wordt gebruikt of aan het op vrijwillige basis kunnen verwijderen van aangeschafte producten die zijn voorzien van tags.

Wettelijk gezien kan Nederlandse ingezetenen echter niet de mogelijkheid worden geboden een *reisdocument* zonder RFID-chip aan te vragen. Op grond van de Europese Verordening betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten ((EG) nr 2252/2004 van 13 december 2004) is Nederland verplicht om een chip in het reisdocument op te nemen die een gezichtsopname bevat en gegevens over de houder van het document.

Het paspoort en de Nederlandse identiteitskaart zijn reisdocumenten in de zin van de Paspoortwet. De Paspoortwet is een rijkswet die het grondwettelijke recht het land te verlaten faciliteert en waarin o.a. de mogelijkheden om een internationaal geaccepteerd reisdocument aan te vragen zijn geregeld. Omdat bij de aanvraag, verstrekking en uitreiking van reisdocumenten persoonsgegevens worden verwerkt, legt de wet bepalingen vast omtrent het beschermen van de persoonlijke levenssfeer. Ook in de uitvoeringsregelingen, bestemd voor de paspoortuitgevende instanties

(gemeenten, buitenlandse posten, de Koninklijke Marechaussee en op de Nederlandse Antillen en Aruba) zijn zeer stringente regels vastgelegd omtrent de bescherming van persoonsgegevens die in het kader van het aanvraag- en uitreikingsproces worden verwerkt.

Bij de toevoeging van een extra persoonsgegeven (in dit geval een biometrisch kenmerk) worden deze maatregelen opnieuw beoordeeld en waar nodig aangepast. Het spreekt voor zich dat daarbij altijd in ogenschouw wordt genomen de bepalingen van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM), artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (BUPO), de Europese privacywetgeving en de Nederlandse Wet bescherming persoonsgegevens (Wbp), een uitvloeisel van artikel 10 van de Grondwet. Het afnemen van een biometrisch kenmerk betreft het verwerken van persoonsgegevens en moet derhalve voldoen aan de eisen van de Wbp. Het verwerken van persoonsgegevens is te rechtvaardigen onder voorwaarde dat dit op een zorgvuldige wijze geschiedt, en plaatsvindt met het oog op welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De Paspoortwet- en regelgeving voldoet aan die eisen door de paspoortuitgevende instanties hieromtrent regels op te leggen.

Voor wat betreft gewetensbezwaren die een betrokkene heeft bij de aanvraag van een reisdocument met biometrie, kan het volgende worden gemeld. De Grondwet en de internationale regelgeving verplichten de wetgever tot het rekening houden met dergelijke bezwaren. Zij kunnen echter niet zover strekken, dat daardoor het vervaardigen van een degelijk en bruikbaar identiteitsdocument, zoals een reisdocument, geheel onmogelijk wordt. Er bestaat een dringend maatschappelijk belang bij het voeren van een doelmatig veiligheidsbeleid, waarvan controle op personen bij het binnenkomen en het verlaten van ons land belangrijk deel uitmaken.

Naarmate dreigingen zoals die van terrorisme groter worden, zijn beperkingen van grondrechten van sommige burgers eerder te rechtvaardigen, juist ook ter bescherming van de democratie en grondrechten van anderen. Het gerechtvaardigd doel (doelmatig veiligheidsbeleid ter voorkoming en opsporing van strafbare handelingen, alsmede het voorkomen van fraude en misbruik van reisdocumenten) blijkt enkel te kunnen worden bereikt met stringente maatregelen. De ingeslagen weg met biometrische kenmerken op de reisdocumenten, blijkt een goed middel om dergelijke dreigingen te voorkomen en op te sporen. Aan het vereiste van proportionaliteit tussen het na te streven doel van de Paspoortwet (voorkomen van fraude met reisdocumenten en het vervaardigen van een bruikbaar reisdocument) en de gekozen middelen (het gebruik van biometrische kenmerken) wordt met andere woorden voldaan. Daarbij gelden strenge eisen voor de beveiliging van deze gegevens tegen ongeoorloofde kennisneming of andere vormen van misbruik.

Elke *OV-chipkaart*, anoniem of persoonsgebonden, heeft RFID omdat dit noodzakelijk is om de kaart contactloos te laten functioneren bij toegang tot het OV. Er is geen alternatief. De RFID chip bevat evenwel geen persoonsgegevens. De RFID op de OV-chipkaart draagt informatie over een geldsaldo, een abonnementsvorm, bijvoorbeeld trajectkaart, of mogelijk een betaalvoorziening. Ook is er een geboortedatum in verwerkt ten behoeve van het reizen met korting voor ouderen. Deze datum is niet gekoppeld aan

de persoonsgegevens van de kaarthouder. De informatie op de OV-chipkaart kan bestaan uit reisproposities of -rechten. Dit is bijvoorbeeld een abonnementstvorm (maandkaart) of voordeelurenrecht (korting na 9.00u) bij een bepaalde vervoerder. De informatie kan ook bestaan uit een saldo dat op de e-purse staat. Ook kan het een autoreloadfunctie bevatten van TLS (Trans Link Systems) – de elektronische geldinstantie voor de OV-chipkaart als betaalmiddel – waarmee automatisch geld op de kaart wordt geladen als het onder een bepaald bedrag komt. De vervoerder staat hier buiten. Ook bevat de chip een uniek (versleuteld en onzichtbaar) nummer. Dit is een ander nummer dan het eveneens unieke nummer dat zichtbaar op de kaart staat vermeld. Het chipnummer kan in geval van een persoonsgebonden kaart worden gekoppeld aan de gegevens van de klant - houder van de kaart. Deze gegevens liggen bij een vervoerder of TLS die gegevens voor hen noodzakelijke doelen (kunnen) gebruiken. Ten aanzien van TLS geldt dat zij haar systeem zodanig heeft ingericht dat de gegevens altijd gescheiden worden verwerkt. Alleen op verzoek van de klant (bijv. vervanging van zijn kaart) kan TLS het chipnummer koppelen aan de persoonsgegevens van de reiziger. Het gescheiden bewaren van klantgegevens en transactiegegevens met de chipkaart wordt ook voor vervoerders gehanteerd. Zij koppelen gegevens van een reiziger alleen bij noodzaak, zoals klantverzoeken, geld-terug-bij-vertraging en controle geldigheid vervoerbewijs.

De burger wordt op verschillende manieren geïnformeerd over het gebruik en de werking van de OV-chipkaart als elektronisch vervoerbewijs en betaalmiddel. Ik verwacht dat de kennis van de reiziger over de contactloze gegevensverwerking van de OV-chipkaart straks gemeengoed zal zijn.

De leden van de VVD-fractie vragen of de regering wetgeving overweegt die de verplichting oplegt aan leveranciers of verkopers om de RFID-chip onklaar te maken na de verkooptransactie?

Uit bijgevoegd recent onderzoek van ECP.nl, de Consumentenbond en het Rathenau-instituut blijkt dat de meeste consumenten willen weten of in een winkel RFID-chips in of op producten zitten en of deze worden gelezen. Verder blijkt dat veel consumenten zelf willen beslissen of een chip na de aankoop van een product uitleesbaar blijft als daar goede argumenten voor zijn van producent of aanbieder. Ik overweeg geen wetgeving die een verplichting aan leveranciers of verkopers oplegt om de RFID-chip onklaar te maken na de verkooptransactie. Bedrijfsleven noch consument is bij voorbaat gebaat bij automatische uitschakeling van RFID-chips bij de kassa. Consumenten geven dat ook aan. De functionaliteit van de RFID-chip kan ook na de aanschaf van een product voor consumenten immers reden zijn de chip niet uit te schakelen, bijvoorbeeld als de chip informatie bevat die de moeite waard is thuis uit te lezen. Ik zie meer in het bevorderen van transparantie en keuzevrijheid voor de consument om RFID-chips uit te schakelen na aanschaf. Overigens bevatten RFID-chips die voldoen aan de EPC-standaard wel over de technische mogelijkheid om de chip uit te schakelen. Deze vorm van RFID wordt met name gebruikt in logistieke processen zoals transport en retail, maar ook als middel voor het tegengaan van namaakproducten.

Voorlichting

De leden van de SP-fractie vragen op welke wijze de Staatssecretaris wil bevorderen dat bedrijven en overheid bij de invoering van RFID op de hoogte zijn van de geldende regels op het gebied van privacy en deze ook toetsen aan de plannen voor invoering van RFID-toepassingen?

Het CBP geeft voorlichting over de privacyregelgeving aan toepassers van RFID (binnen en buiten de overheid) en ontwikkelaars van RFID-systemen. Daarnaast is in 2006 op initiatief van het Platform Detailhandel Nederland en het Ministerie van Economische Zaken door ECP.NL en het RFID Platform Nederland een – breed verspreide - publicatie samengesteld waarin ondernemers worden voorgelicht over de geldende regels op het gebied van privacy.

De leden van de ChristenUnie-fractie vragen wat de Staatssecretaris doet met de aanbeveling van het CBP dat het vergroten van publieke kennis over de (on)mogelijkheden van RFID-toepassingen kan bijdragen aan het vertrouwen in verantwoorde toepassingen en tegelijkertijd aan het tijdig treffen van maatregelen ter voorkoming van nadelige effecten. Worden er publiekscampagnes ingezet? Weten burgers wat RFID is en waar en hoe het wordt toegepast? De leden van de SP-fractie vragen wat het bereik is van bewustwording- en voorlichtingscampagnes via ECP.nl, RFID-platform Nederland en Mediaplaza? Is de Staatssecretaris van mening dat hiermee ook de mensen bereikt worden die de RFID-toepassingen nog niet kennen? De leden van de SP-fractie vragen tevens of de Staatssecretaris bereid is om Nederlanders breed te informeren door ook andere media en organisaties te betrekken bij de informatie en voorlichting. De leden van de VVD-fractie vragen hoe ver de plannen voor bewustwordings en voorlichtingscampagnes zijn gevorderd, welk budget hiervoor is uitgetrokken en welke begrotingsposten worden hiervoor aangesproken? Is hier niet sprake van een informatieplicht van de leverancier van producten en diensten die RFID gebruikt, zo vragen deze leden?

Het Ministerie van Economische Zaken steunt en voert bewustwordings- en voorlichtingsactiviteiten richting bedrijfsleven en consumenten via ondermeer ECP.nl, RFIDplatform Nederland, Syntens en Mediaplaza; organisaties met een uitstekend bereik onder de doelgroep. Het betreft hier subsidiering van RFID-activiteiten in het kader van het programma Nederland Digitaal in Verbinding en projectsubsidie aan ECP.nl inzake het genoemde en bijgevoegde onderzoek van de Consumentenbond, ECP.nl en het Rathenau-instituut naar de bekendheid van RFID en RFID-toepassingen onder consumenten. In oktober 2007 organiseerde debatcentrum De Balie een tweedaagse publieksbijeenkomst over RFID. EZ sponsorde deze bijeenkomst. De overheidsbijdrage in deze lopende activiteiten bedraagt in 2007 in totaal €100.000,-. Leveranciers en gebruikers van RFID-systemen communiceren via RFID-Nederland ook zelf over de verschillende aspecten van RFID. De Nederlandse overheid communiceert over privacyaspecten van RFID en in het kader van het bevorderen van awareness bij het MKB en consument.

De met het bijgevoegde onderzoek verworven kennis over het 'RFID-bewustzijn' onder consumenten is voor mij aanleiding om te laten onderzoeken op welke wijze, met

medewerking van de RFID-industrie en de gebruikers van de RFID-technologie een etiketteringsysteem kan worden gelanceerd en om zo spoedig mogelijk een aanvang te nemen met de implementatie van een dergelijk systeem. Ik geef de voorkeur aan een systeem van zelfregulering, waarover ik met de RFID-industrie en de gebruikers van de RFID-technologie in overleg zal treden.

De leden van de ChristenUnie vragen wat de Staatssecretaris vindt van de suggestie van het CBP om een informatiepunt in de trant van Postbus 51 én een klachtenregeling voor mogelijk misbruik of oneigenlijk gebruik van RFID (een klachtenloket) in te richten? In dit verband wijzen de leden van de ChristenUnie-fractie de Staatssecretaris op een publicatie van het Rathenau Instituut over RFID, waar treffend een dag uit een gemiddeld Nederlands gezin wordt geportretteerd, waaruit blijkt hoe RFID al met het dagelijks leven is verweven. Mogelijk kan de Staatssecretaris hier zijn voordeel mee doen?

Ik heb kennis genomen van de publicatie van het Rathenau-instituut en deel de analyse dat RFID reeds met het dagelijks leven van mensen verweven is geraakt. De wetgever heeft het CBP een loketfunctie gegeven voor de behandeling van klachten van burgers over de omgang met persoonsgegevens; ook wat betreft klachten over RFID en privacy. Het centrale loket van de Rijksoverheid - Postbus 51 - ontving tot op heden geen vragen of klachten over RFID in zijn algemeenheid. De website van het RFID-platform Nederland werd deels door het Ministerie van Economische Zaken gefinancierd en voorziet reeds in een informatiebehoefte. Het inrichten naast bestaande loketten en informatiepunten van een aparte informatiepunt en klachtenloket voor misbruik of oneigenlijk gebruik van RFID acht ik niet nodig en niet efficiënt.

(w.g.) drs. F. Heemskerk

Bijlage

Selectie van RFID-toepassingen (smart labels, contactloze smartcards en NFC-toepassingen) in Nederland	
Transport en Logistiek	<ul style="list-style-type: none"> • Containermanagement, bv Rotterdamse haven • Track en trace van (verse) goederen, bv Schuitema, FloraHolland, Container Centralen (standaardcontainer in sierteeltsector), Hoogvliet • Bagagetransport Schiphol
Detailhandel	<ul style="list-style-type: none"> • Item-level tagging van producten in de winkel tbv voorraadbeheer en service klanten, bv Selexyz boekhandels • Betalen met mobiele telefoon, pilot C1000/Rabobank en pilot met 30 winkels in Rotterdam (NFC)
Veiligheid	<ul style="list-style-type: none"> • Diefstalpreventie • Toegangscontrole in gebouwen (smartcards) • Track en trace werknemers en gasten in gebouwen • Gevangenis Lelystad • Biometrisch paspoort
Zorg	<ul style="list-style-type: none"> • Track en trace apparatuur en bloedzakken, bv AMC • Tegengaan vervalsing medicijnen
Entertainment en sport	<ul style="list-style-type: none"> • Tijdcontrole bij atletiekwedstrijden • Track en trace bezoekers in pretparken (tbv monitoring bezoekersflow of aanbieden extra diensten), bv Dutch Water Dreams • Toegangscontrole en betalen met geïmplanteerde RFID-chip als service voor VIP-gasten, Baja Beachclub • Ticketing en betalen bij stadions en evenementen, bv Roda JC, Amsterdam ArenA (NFC)
Vervoersmiddelen	<ul style="list-style-type: none"> • Identificeren en lokaliseren van voertuigen, bv Broekman automotive (Rotterdamse haven) • RFID in autosleutels • OV Chipkaart • Tolssystemen: Westerscheldetunnel, Kiltunnel
Veeteelt en huisdieren	<ul style="list-style-type: none"> • Proef met identificatie en registratie schapen, geiten, runderen en varkens (LNV) • Identificatie en registratie paarden • Identificatie en registratie van huisdieren
Musea	<ul style="list-style-type: none"> • Museumtour met RFID, bv Beeld en Geluid • Beveiliging van collectie, bv Boijmans van Beuningen
Openbare Bibliotheken	<ul style="list-style-type: none"> • Voorraadbeheer, self-servicebalies en beveiliging boeken, NDB/Biblion en Vereniging Openbare Bibliotheken