Het merkteken van het beest

Maatregelen bij het gebruik van RFID

Erica Zaaiman
mei 2006

Inhoud

Samenvatting

RFID (radio frequency identification) wordt steeds meer en breder toegepast en de verwachting is dat dit in de komende jaren zo zal doorgaan. Minder aandacht is er voor de risico's van RFID. Zodoende is de hoofdvraag van deze scriptie:

"Hoe kan RFID door het gebruik van technische en beheersmatige maatregelen op een veilige wijze toegepast worden?"

Veilig is hierbij gedefinieerd als de kwaliteitsaspecten continuïteit, exclusiviteit en integriteit. De definities van deze kwaliteitsaspecten zijn:

- continuïteit is de mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben;
- exclusiviteit is de mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruik maken van IT-processen;
- integriteit is de mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.

Hierbij zal onderscheid worden gemaakt tussen de verschillende manieren waarop RFID toegepast kan worden, namelijk als:

a. middel om producten te identificeren;
b. extern middel om individuen te identificeren;
c. intern middel om individuen te identificeren.

Om deze hoofdvraag te beantwoorden is ingegaan op de technische specificaties van RFID en de wetten met betrekking tot RFID. Vanuit voornoemde entiteiten zijn de risico's bij het gebruik van RFID geïdentificeerd, waarna vervolgens te implementeren maatregelen opgesteld zijn voor de drie genoemde toepassingen van RFID.

Voor alle drie de genoemde toepassingen van RFID gelden de volgende maatregelen:

- de communicatie tussen de tag en de reader dient op geen enkele wijze verstoord of geblokkeerd te kunnen worden;
- de reader dient altijd de verkregen gegevens (van de tags) vast te leggen/bewaren;
- de tag dient zodanig bevestigd te zijn op het object dat het verwijderen ervan onmogelijk is;
- een risicoanalyse dient uitgevoerd te worden voor de back-end systemen en de communicatie en voor deze risico's dienen maatregelen getroffen te worden;
- gegevens op de tag dienen niet gewijzigd te kunnen worden door ongeautoriseerden;
- het deactiveren van de tag door onbevoegden dient onmogelijk gemaakt te worden.

Daarnaast geldt voor RFID als middel om producten te identificeren dat een risicoanalyse uitgevoerd dient te worden om te bepalen of de volgende maatregelen van belang zijn:

- de communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden;
- de communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden;
- de tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is;
- de tag en reader dienen zich te authenticeren ten opzichte van elkaar.

Voor de andere twee toepassingen van RFID, namelijk als extern of intern middel om individuen te identificeren gelden tevens de volgende maatregelen:

- de tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is;
- een RFID-systeem welke (bijzondere) persoonsgegevens verwerkt dient te voldoen aan de Wet Bescherming Persoonsgegevens.

Tevens dienen nog drie maatregelen ingevuld te worden aan de hand van de risicoklasse van de persoonsgegevens, welke conform de Wbp bepaald dient te worden. Dit betreft de maatregelen:

- de communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden;
- de communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden;
- de tag en reader dienen zich te authenticeren ten opzichte van elkaar.

In de praktijk zal het lastig dan wel onmogelijk zijn om alle genoemde maatregelen na te leven. Bijvoorbeeld het verstoren of blokkeren van de communicatie tussen reader en tag is slecht te voorkomen. Daarnaast zal het bijvoorbeeld bij bepaald gebruik van tags niet praktisch zijn om een tag tijdelijk te deactiveren indien deze tijdelijk niet gebruikt wordt. Hierdoor is de individu met de tag continue te volgen. Bij een voldoende spreiding van readers ontstaat dan een Big Brother scenario.

Van tags uit class 0 en sommige WORM-tags is momenteel vastgesteld dat deze niet veilig zijn. In de toekomst kan van andere type tags ook vastgesteld worden dat deze niet veilig zijn. Zodoende moet bij de implementatie van een RFID-systeem altijd beoordeeld worden of de te gebruiken tags veilig zijn en of deze voldoen aan de genoemde beveiligingsmaatregelen.
Tijdelijke deactivatie van tags geïmplanteerd in individuen is niet mogelijk, waardoor het de vraag blijft of het wenselijk is deze als intern middel om individuen te identificeren te gebruiken.
Indien de gegevens in risicoklassen II en III van de Wbp vallen is het niet mogelijk om deze te verwerken in combinatie met RFID, behalve als de gegevens alleen op het back-end systeem opgeslagen worden (en deze afdoende beveiligd wordt conform de daarvoor geldende richtlijnen vanuit de Wbp).

Bij de implementatie van een RFID-systeem is het altijd noodzakelijk om een risicoanalyse uit te voeren met betrekking tot de werking van het systeem. De opzet van het RFID-systeem bepaalt namelijk welke risico's aanwezig zijn.

1 Inleiding

1.1 Aanleiding

> ***"En het maakt dat allen, kleinen en groten, rijken en armen, vrijen en slaven, een merkteken ontvangen op hun rechterhand of op hun voorhoofd; en niemand kan kopen of verkopen, als hij dat teken, de naam van het beest of het getal van zijn naam, niet draagt. Nu komt het aan op scherpzinnigheid! Wie doorzicht heeft, kan het getal van het beest berekenen. Het duidt een mens aan, en het getal van die mens is 666."***
>
> Openbaring 13:16-18

Het getal 666 wordt door velen geassocieerd met streepjescodes. Alle strepen uit een streepjescode zijn verbonden met een getal onder de streepjescodes met uitzondering van zes strepen (links, midden en rechts). Deze strepen zijn allen een zes (zie figuur 1).

Figuur 1: 666 in streepjescodes

RFID wordt, als opvolger van de streepjescode, gezien als het merkteken (en daarmee als een gevaar voor de samenleving). Vanuit de samenleving bestaat ondertussen veel meer interesse voor RFID. Dit heeft er onder andere mee te maken dat het formaat van de RFID-chips steeds kleiner wordt en de prijs lager. Een aantal toepassingen waarvoor RFID al in gebruik is, is:

- toegangspas bij Baja Beach Club (geïmplanteerd in het lichaam)[1],
- supply chain management in bijvoorbeeld een boekenwinkel[2],
- medische toepassingen zoals het identificeren van (de medische geschiedenis van) patiënten en verificatie van geneesmiddelen[3], en,
- bewaking van gevangenen[4].

De verwachting is dat vanaf 2005 in vijf jaar tijd de productie van RFID-chips 25 maal groter zal worden (2005: 1,3 miljard RFID-chips[5]).

---

[1] Meer informatie is beschikbaar op: http://www.emerce.nl/nieuws.jsp?id=277589

[2] Meer informatie is beschikbaar op: http://www.webwereld.nl/ref/newsletter/39825

[3] Meer informatie is beschikbaar op: http://www.rfidjournal.com/article/articleview/2075/1/1/

[4] Meer informatie is beschikbaar op: http://www.zdnet.be/news.cfm?id=53006&mxp=109

[5] Meer informatie is beschikbaar op: http://www.informationweek.com/news/showArticle.jhtml?articleID=177101563

RFID geïmplementeerd in een product, polsbandje of individu maakt het mogelijk te traceren welke producten een individu bij zich heeft, te bepalen tot welke groep(en) een individu behoort ("brandmerken") of iemands handel en wandel te traceren. Omdat uit de nieuwsberichten blijkt dat RFID-chips meestal niet of niet adequaat beveiligd zijn, betreft dit publieke informatie.

1.2 Doelstelling

Aan het gebruik van RFID zijn diverse risico's verbonden. Om te bepalen welke risico's dit zijn en hoe deze weggenomen kunnen worden zal in de conclusie de volgende hoofdvraag beantwoord worden:

"Hoe kan RFID door het gebruik van technische en beheersmatige maatregelen op een veilige wijze toegepast worden?"

Veilig is hierbij gedefinieerd als de kwaliteitsaspecten continuïteit, exclusiviteit en integriteit. De definities van deze kwaliteitsaspecten zijn overgenomen uit NOREA geschrift 1 "IT-auditing aangeduid":

- continuïteit is de mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben;
- exclusiviteit is de mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruik maken van IT-processen;
- integriteit is de mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.

Hierbij zal onderscheid worden gemaakt tussen de verschillende manieren waarop RFID toegepast kan worden, namelijk als:

a. middel om producten te identificeren;
b. extern middel om individuen te identificeren;
c. intern middel om individuen te identificeren.

Deze hoofdvraag is verdeeld in de volgende vier deelvragen:

1. Wat zijn de technische specificaties van RFID?
2. Welke wetten met betrekking tot RFID zijn er?
3. Welke risico's zijn er bij het gebruik van RFID?
4. Welke maatregelen dienen gehanteerd te worden bij het gebruik van RFID?

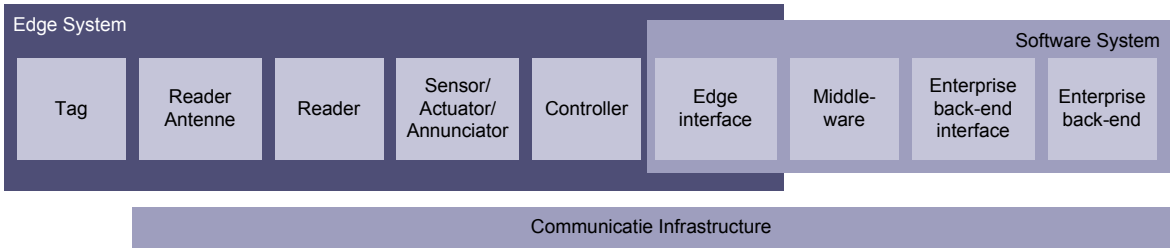
Bij deelvraag 2 zal onderscheid gemaakt worden tussen specifieke wetgeving met betrekking tot RFID en algemene wetgeving op bijvoorbeeld het gebied van privacy. Deelvraag 4 zal resulteren in basismaatregelen, welke vervolgens uitgewerkt zullen worden voor de genoemde toepassingen van RFID.

1.3 Werkwijze

Het onderzoek is uitgevoerd in maart 2006. De deelvragen 1 en 2 zijn uitgevoerd door middel van literatuuronderzoek. Vervolgens heeft een analyse geresulteerd in de antwoorden op de deelvragen 3 en 4.
In de volgende hoofdstukken worden opeenvolgend de genoemde deelvragen behandeld. In hoofdstuk 6, de conclusie, zal vervolgens de hoofdvraag beantwoordt worden. De maatregelen voor het gebruik van RFID zijn in bijlage C opgenomen. In bijlage A is een woordenlijst opgenomen.

2 Techniek en standaarden

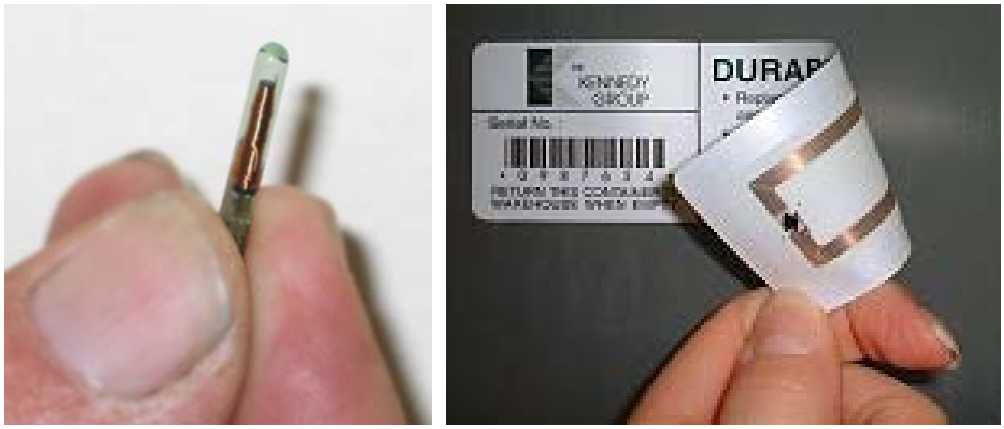
In dit hoofdstuk zal de eerste deelvraag beantwoord worden. Deze vraag is: “Wat zijn de technische specificaties van RFID?”. Een RFID-systeem (radio frequency identification) bestaat uit een aantal componenten zoals opgenomen in figuur 2.



Figuur 2: Schematische end-to-end weergave van een RFID-systeem

De componenten in figuur 2 zijn:

- tag (zie figuur 3);
- reader (zie figuur 4);
- reader antenne (eventueel ingebouwd bij de reader);
- sensor, actuator en annunciator (optioneel; voor externe in- en output met het systeem);
- host en software system;
- communicatie infrastructure.



Figuur 3: Voorbeelden van een RFID-chip

Figuur 4: Voorbeelden van een reader

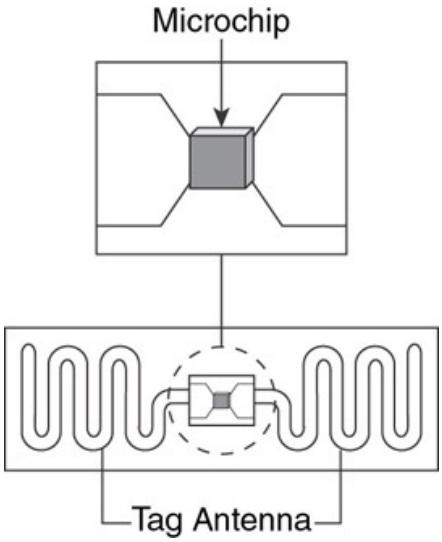
Theoretisch is het mogelijk om een RFID-systeem zonder host en software system op te zetten, maar dan is het niet mogelijk om achterliggende informatie te koppelen met de RFID-chips. Onderstaand (2.1 tot en met 2.6) zal ingegaan worden op de verschillende componenten van een RFID-systeem. In 2.7 worden de standaarden voor RFID besproken.

2.1 Tag

Een RFID-tag kan gegevens opslaan en verzenden aan een reader door middel van radiogolven. Tags kunnen geclassificeerd worden op twee verschillende manieren, namelijk op de mogelijkheden van de tag (passief, actief, semi-actief/semi-passief) en op de mogelijkheid om gegevens te herschrijven (RO (read-only), WORM (write once, read many) en RW (read-write)). Deze twee classificaties zijn onafhankelijk van elkaar. In 2.1.1 tot en met 2.1.3 zal ingegaan worden op de mogelijkheden van de tag, terwijl de mogelijkheid om gegevens te herschrijven toegelicht zal worden in 2.1.4 tot en met 2.1.6.

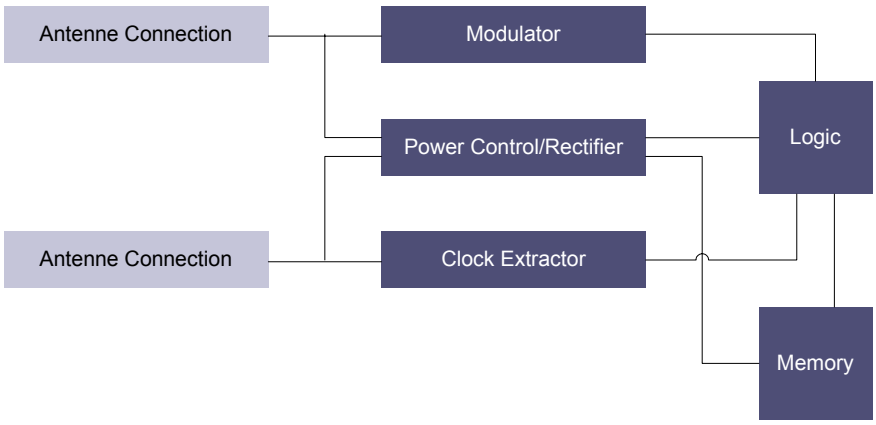
2.1.1 Passieve tags

Een passieve tag heeft geen eigen energiebron (zoals een batterij), maar is hiervoor afhankelijk van de reader. De radiogolf van de reader wordt gebruikt als energiebron voor de tag. Zodoende kan een passieve tag alleen zijn informatie versturen indien een verzoek gedaan wordt door een reader (en met het verzoek dus van energie voorzien wordt). Een passieve tag is opgebouwd uit twee componenten, namelijk een microchip en een antenne (zie figuur 5).



Figuur 5: De opbouw van een passieve tag

In figuur 6 is de opbouw van een microchip weergegeven.



Figuur 6: De opbouw van een microchip

De componenten van een microchip hebben de volgende functionaliteit:

- power control/rectifier: het converteren van de energie van de antenne van de reader naar energie voor de andere componenten van de microchip;
- clock extractor: het extraheren van het kloksignaal van het signaal van de reader antenne;
- modulator: het moduleren van het ontvangen signaal van de reader;
- logic: het implementeren van het communicatie protocol tussen de tag en de reader;
- memory: het bewaren van de gegevens. Meestal is een memory gesegmenteerd (in diverse velden of blokken) zodat verschillende data types (zoals bijvoorbeeld een checksum) opgeslagen kunnen worden.

De microchip wordt steeds kleiner door technologische ontwikkelingen. De afmetingen van een tag worden echter niet bepaald door de microchip, maar door de antenne.

De antenne van een tag wordt gebruikt om energie uit het signaal van de reader te halen voor de tag en voor het zenden en ontvangen van gegevens naar de reader. Bij het ontwerpen van een antenne zijn de volgende factoren van belang:

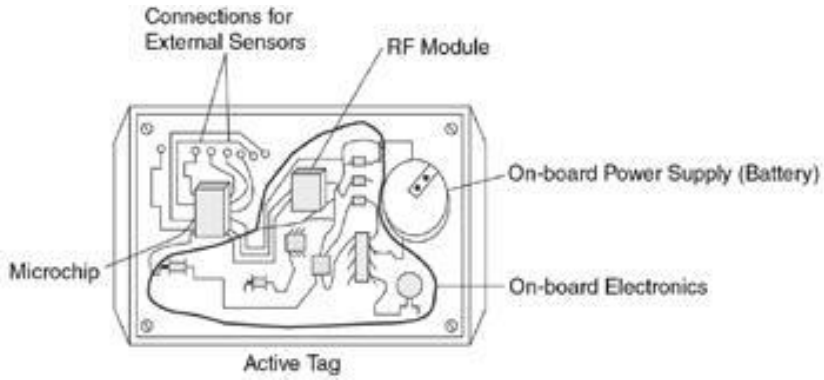
- leesafstand tussen de tag en de reader,
- de oriëntatie van de tag ten opzichte van de reader,
- specifieke producttypes,
- de snelheid van het object met de tag ten opzichte van de reader,
- specifieke omgevingscondities, en,
- de polarisatie van de antenne van de reader.

Tags worden door bovenstaande factoren speciaal ontwikkeld voor een bepaalde taak en een andere taak is vaak niet mogelijk met dezelfde tag. Het zwakste punt van een tag is de connectie tussen de microchip en de antenne van de tag. Schade hieraan kan de tag deels of geheel onbruikbaar maken.

2.1.2 Actieve tags

Actieve tags hebben in tegenstelling tot passieve tags een eigen energiebron en elektronica om een specifieke taak uit te voeren. De eigen energiebron wordt gebruikt om gegevens te transporteren naar de reader, waardoor de energie van de reader niet benodigd is. De elektronica op de tag, welke energie verkrijgen van de eigen energiebron, kan bestaan uit microprocessors, sensors en input/output poorten. Met deze elektronica kan bijvoorbeeld de omgevingstemperatuur gemeten worden, waardoor bepaald kan worden hoe lang een product houdbaar is (en deze informatie wordt vervolgens weggeschreven in het memory).
Actieve tags kunnen ingedeeld worden in twee categorieën met betrekking tot de wijze voor communicatie met de reader:

- transmitter: deze tag laat altijd zijn aanwezigheid blijken door zijn gegevens te broadcasten. Communicatie tussen deze tag en de reader zal altijd door de transmitter begonnen worden;
- transponder (transmitter/receiver): deze tag broadcast zijn gegevens niet, maar wacht hiervoor op een speciaal commando van een reader. Tijdens het wachten bevindt hij zich in een slaaptoestand, waardoor energie van de energiebron gespaard blijft.



Figuur 7: De opbouw van een actieve tag

Een actieve tag is opgebouwd uit de volgende componenten (zie figuur 7):

- microchip: de afmetingen en capaciteiten zijn meestal groter dan die van microchips in passieve tags (zie 2.1.1);
- antenne: dit is een RF module welke de signalen van de tag verzendt en de signalen van de reader ontvangt (zie 2.1.1);
- energiebron;
- elektronica.

De energiebron van een tag (bijvoorbeeld een batterij of gebaseerd op zonne-energie) levert energie aan de elektronica. Tevens wordt energie van deze energiebron gebruikt voor het verzenden van gegevens. De bruikbare tijd van een actieve tag is afhankelijk van de batterij. De levensduur van een batterij wordt bepaald door de interval van het verzenden van gegevens (hoe langer de interval, hoe langer de levensduur van de batterij) en de aanwezige elektronica (zoals sensors en processors).
Indien de batterij van een actieve tag leeg is kan de tag geen gegevens meer versturen. Voor een reader is het niet mogelijk om vast te stellen of een tag niet uitgelezen kan worden, omdat deze zich niet meer in de leeszone bevindt of omdat deze een lege batterij heeft (en dus geen gegevens meer kan versturen). Indien de tag de status van de batterij aan de reader meldt, kan de reader vaststellen dat het wellicht aan de batterij ligt.

De elektronica op een tag maken het mogelijk om te reageren als een transmitter, maar bijvoorbeeld ook om gespecialiseerde taken uit te voeren (zoals waarden weergeven van dynamische parameters of als een sensor reageren). De mogelijkheden waarvoor de elektronica gebruikt kunnen worden zijn eindeloos. Indien de functionaliteiten en daarmee de fysieke afmetingen van de elektronica toenemen, zal dit consequenties hebben voor de afmetingen van de tag.

2.1.3 Semi-actieve (semi-passieve) tags

Een semi-actieve tag bestaat uit dezelfde componenten als een actieve tag (zie 2.1.2). De energiebron van een semi-actieve tag wordt alleen gebruikt voor het leveren van energie aan de elektronica en niet voor het verzenden van gegevens. Een semi-actieve tag maakt voor het verzenden van gegevens gebruik van de energie van de reader. De communicatie tussen een reader en een tag wordt bij een semi-actieve tag dus opgestart door de reader.
Het voordeel van een semi-actieve tag boven een passieve tag is dat de energie van de reader niet gebruikt wordt om zichzelf te bekrachtigen, waardoor een semi-actieve tag op een grotere afstand of met een hogere snelheid uitgelezen kan worden dan een passieve tag. Tevens kan een semi-actieve tag beter uitgelezen worden ondanks de aanwezigheid van RF-afdekkende of RF-absorberende materialen.

2.1.4 RO (read-only)

Een RO tag kan slechts éénmaal geprogrammeerd worden. Dit programmeren (schrijven) vindt plaats in de fabriek tijdens de productie van de tag. De fabrikant van de tag bepaalt de gegevens op de tag en de gebruikers van de tag hebben hierover geen zeggenschap.

2.1.5 WORM (write once, read many)

Een WORM tag kan slechts éénmaal geprogrammeerd (beschreven) worden. Dit wordt gedaan door de gebruiker van de tag. Sommige types van WORM tags kunnen echter meerdere malen overschreven worden door de slechte implementatie.

2.1.6 RW (read-write)

Een RW tag kan meerdere malen (meestal tussen de 10.000 en 100.000 maal) geprogrammeerd (beschreven) worden. Het beschrijven kan plaatsvinden door de reader, maar ook door een actieve tag zelf. Een RW tag bevat een Flash memory of FRAM (Ferroelectric Random Access Memory; vergelijkbaar met EEPROM (Electrically Erasable Programmable Read Only Memory)) om de gegevens op te slaan.

2.2 Reader

De reader kan gegevens lezen van en schrijven naar compatibel RFID tags. Een reader kan een vaste reader zijn of een handheld. Een handheld reader is een reader welke mobiel is. Meestal heeft een handheld ingebouwde antennes. Handhelds zijn duurder dan vaste readers. Een vaste reader is vastgemaakt aan een object. Dit kan bijvoorbeeld een muur zijn, maar het kan ook een bewegend object zijn zoals een vorkheftruck. In tegenstelling tot tags kunnen readers niet goed tegen extreme omgevingsfactoren. Een vaste reader heeft meestal externe antennes nodig om tags te kunnen lezen. Een vaste reader kan opereren in twee verschillenden modussen, namelijk autonoom en interactief.

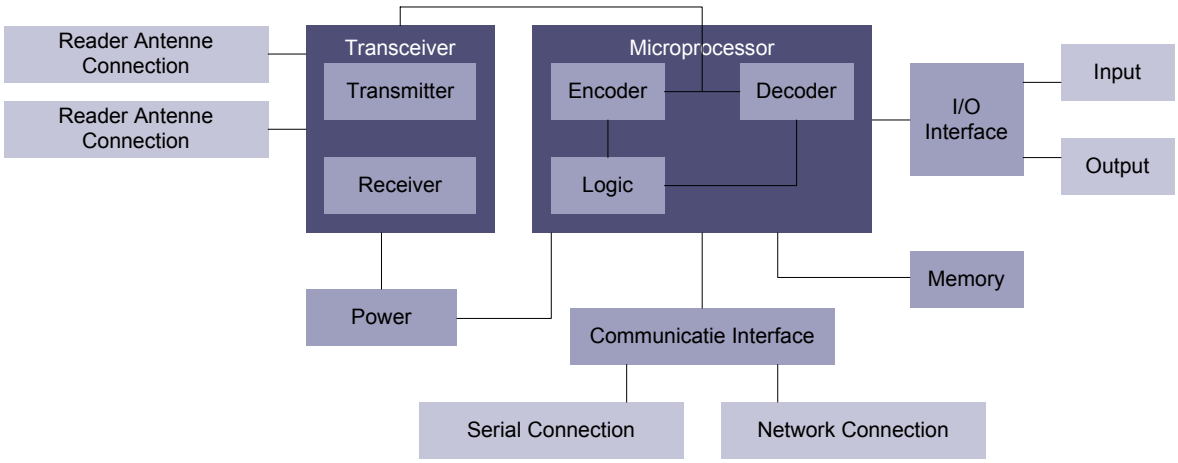
Een reader leest in de autonome modus alle compatible tags welke zich in de leeszone bevinden. Elke keer dat een tag gelezen wordt, wordt deze opgenomen in de lijst van gelezen tags. Een item op deze lijst heeft een zogenaamde permanente tijd. Indien een tag binnen dit tijdsbestek niet opnieuw gelezen wordt, wordt hij verwijderd van de lijst. Op de lijst wordt bijvoorbeeld de volgende informatie bijgehouden:

- het unieke ID van de tag;
- het tijdstip van lezen;
- hoe vaak een tag gelezen is sinds deze voor de eerste maal gelezen is;
- het ID van de antenne welke de tag gelezen heeft (in verband met het uitfilteren van duplicaten (zie 2.5.1));
- de naam van de reader.

Een applicatie op de host machine kan deze lijst periodiek ontvangen. De reader is hierbij verantwoordelijk voor het versturen van de lijst.
Een interactieve reader ontvangt commando's van een applicatie op de host (automatisch) of van een gebruiker door middel van een cliënt (handmatig) en voert deze vervolgens uit. Nadat een commando uitgevoerd is, wordt gewacht op het volgende commando.

Een reader bestaat uit de volgende componenten (zie ook figuur 8):

- transceiver (2.2.1);
- microprocessor (2.2.2);
- memory (2.2.3);
- input/output channels voor sensors, actuators en annunciators (optioneel, maar commercieel een standaard onderdeel) (2.2.4);
- controller (eventueel extern) (2.2.5);
- communicatie interface (2.2.6);
- power (2.2.7).



Figuur 8: De opbouw van een reader

2.2.1 Transceiver

De transceiver is verantwoordelijk voor het zenden en ontvangen van gegevens aan tags. De poorten voor de antennes zijn verbonden met de transceiver. De transceiver bestaat uit de receiver en transmitter.

De analoge signalen van de tag worden via de antenne van de reader aan de receiver doorgestuurd. Deze signalen worden doorgestuurd naar de microprocessor van de reader, welke de analoge signalen omzet naar digitale signalen.

De transmitter wordt gebruikt om energie en het kloksignaal via de antenne te zenden aan de tags in de leeszone. Afhankelijk van het gebruikte type tag (passief, actief, semi-actief) is de communicatie tussen de reader en tag van het volgende type:

- modulated backscatter,
- transmitter type, en,
- transponder type.

Bij modulated backscatter communicatie wordt gebruik gemaakt van passieve en semi-actieve tags. De reader zendt hierbij een continue RF-signaal, welke bestaat uit energie en een kloksignaal. De microchip gebruikt de verkregen energie om een signaal terug te sturen naar de reader.

Transmitter type communicatie wordt alleen gebruikt door actieve tags. De tag broadcast hierbij zijn eigen bericht met regelmatige intervallen naar de omgeving, onafhankelijk van het feit of zich hierin een reader bevindt of niet.
Transponder type communicatie wordt gebruikt door de transponder. Tijdens de slaaptoestand van de tag, zendt deze tag periodiek een bericht om te controleren of een reader luistert. Indien een reader het bericht ontvangt, kan deze de tag instrueren om de slaaptoestand te beëindigen. Als zo'n bericht ontvangen wordt van een reader door een tag, zal deze zich gaan gedragen als een transmitter.

2.2.2 Microprocessor

De microprocessor is verantwoordelijk voor het reader protocol. Het analoge signaal van de receiver wordt gedecodeerd en gecontroleerd op fouten (error check). Tevens kan de microprocessor logic bevatten voor het filteren en verwerken van de verkregen gegevens.

2.2.3 Memory

In het memory worden gegevens opgeslagen zoals de configuratie parameters van de reader en een lijst van gelezen tags. Als er tijdelijk geen verbinding is tussen de reader en het software system, zullen hierdoor in eerste instantie geen gegevens verloren gaan. Het memory heeft echter een limiet, waardoor het geheugen overschreven kan worden. In zo'n geval wordt het geheugen overschreven conform het FIFO-principe.

2.2.4 Input/output channels voor sensors, actuators en annunciators

Met deze componenten (zie 2.4) is het mogelijk om een reader aan en uit te schakelen aan de hand van externe factoren.

2.2.5 Controller

Een controller maakt het mogelijk om te communiceren met de reader en de externe componenten van de reader (zie 2.2.4) door een individu of een computer programma. Meestal wordt de controller geïntegreerd in de reader (bijvoorbeeld firmware), maar het is ook mogelijk om de controller als een apart hardware/software component op te nemen.

2.2.6 Communicatie interface

De communicatie interface bevindt zich tussen de reader en de controller (welke communiceert met externe entiteiten). Via de communicatie interface worden opgeslagen gegevens verstuurd naar de controller. Tevens kan de controller commando's versturen naar de reader, welke hierop kan reageren. De communicatie interface is meestal onderdeel van de controller of bevindt zich tussen de controller en de externe entiteiten. De communicatie interface kan zowel een seriële interface als een netwerk interface hebben.

Een seriële reader gebruikt een seriële interface om te communiceren met een applicatie. De reader is dan fysiek verbonden met een seriële poort van de computer. Het voordeel van een seriële interface ten opzichte van een netwerk interface is de hogere betrouwbaarheid van de communicatie tussen de reader en de computer. De nadelen zijn:

- de maximale lengte van de kabel tussen de reader en de computer;
- de beperking van het aantal readers per computer, omdat de computer onvoldoende seriële poorten heeft;
- het onderhoud van de firmware van elke reader moet apart plaatsvinden;
- de snelheid van seriële transmissie is meestal lager dan netwerk transmissie.

Een netwerk reader kan door middel van een fysiek of draadloos netwerk verbonden worden met een computer. De voordelen en nadelen van een netwerk interface zijn tegengesteld aan de voordelen en nadelen van een seriële interface.

2.2.7 Power

De onderdelen van de reader ontvangen energie van dit component. Meestal ontvangt dit component zijn energie door middel van een standaard elektriciteitsvoorziening (wandcontactdoos).

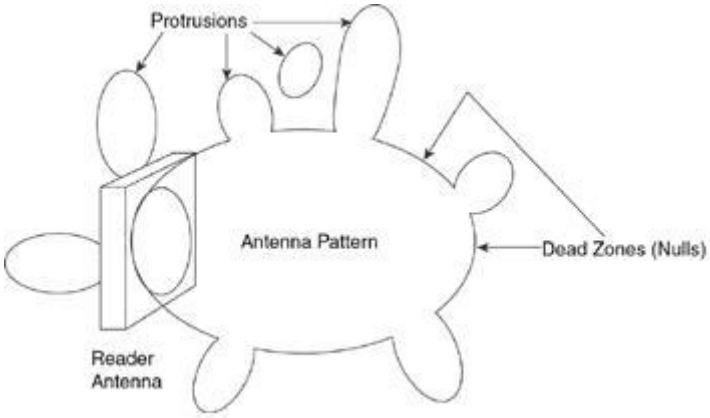
2.3 Reader antenne

De communicatie van de reader met een tag verloopt via de reader antenne. Dit is een afzonderlijk component, welke fysiek aan de reader is aangesloten op één van de momenteel maximaal vier poorten. De antenne broadcast het RF-signaal van de reader en ontvangt namens de reader antwoorden van de tags hierop. De positionering van de reader antenne bepaalt de leesnauwkeurigheid. De volgende aspecten van de antenne worden besproken:

- antenne footprint (2.3.1);
- antenne polarisatie (2.3.2);
- antenne energie (2.3.3).

2.3.1 Antenne footprint

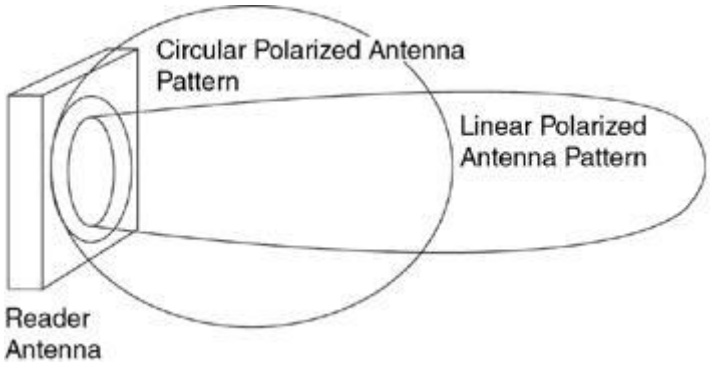
De footprint van een antenne bepaalt zijn leeszone. Generiek is een antenne footprint een drie dimensionale regio welke de vorm heeft van een ellipsoïde of een ballon. In de praktijk blijkt een antenne footprint nooit uniform gevormd te zijn, maar altijd vergroeiingen en uitsteeksels te hebben (zie protrusions in figuur 9). Elk uitsteeksel wordt omgeven door zogenaamde dode gebieden. Hierdoor zal een tag niet altijd gelezen worden aan de randen van een antenne footprint. Binnen de ellipsoïde is het lezen van een tag geen probleem. De antenne footprint is afhankelijk van de omgeving, dus zal bepaald moeten worden door middel van signaal analyse.



Figuur 9: Een voorbeeld van een antenne footprint met vergroeiingen en uitsteeksels

2.3.2 Antenne polarisatie

De trilling van de RF-golven wordt de polarisatie van de antenne genoemd. Deze polarisatie heeft gezamenlijk met de hoek van de tag bij de reader invloed op de leesbaarheid van een tag. De antenne types in UHF (ultra high frequency) zijn lineair en circulair gepolariseerd.
Een lineair gepolariseerde antenne heeft een langer, maar smaller gebied waarin tags gelezen worden ten opzichte van een circulaire gepolariseerde antenne (zie figuur 10). De oriëntatie van de tag is bij deze polarisatie heel belangrijk.



Figuur 10: De antenne footprint bij een lineaire en circulaire gepolariseerde antenne.

2.3.3 Antenne energie

De energie van een antenne wordt in Europa gemeten in ERP (effective radiator power). De maximaal mogelijke energiewaarde voor een antenne wordt bepaald door nationale en internationale regelgeving. De energiewaarde van een antenne kan verminderd worden door het gebruik van een attenuator. Indien dit gedaan wordt, wordt het bereik van de antenne verminderd.

2.4 Sensor, actuator en annunciator

Indien niet gewenst is dat een reader continue aanstaat, kan deze automatisch gestart en gestopt worden door bijvoorbeeld een sensor. Als de sensor een bepaalde externe gebeurtenis waarneemt, zal deze de reader starten. Een annunciator is een elektrisch signaal (bijvoorbeeld een alarm of een lichtsignaal). Een actuator is een mechanisch instrument om objecten te controleren of te bewegen (bijvoorbeeld een robotarm of een mechanisch gestuurd draaihekje).

2.5 Host en software system

Met het host en software system wordt alle hardware en software bedoeld welke gescheiden zijn van de RFID hardware (reader, tag en antenne). Dit systeem bestaat uit de volgende vier componenten:

- edge interface/system (2.5.1),
- middleware (2.5.2),
- enterprise back-end interface (2.5.3), en,
- enterprise back-end (2.5.4).

2.5.1 Edge interface/system

De edge interface/system integreert het complete host en software system met de RFID hardware (reader, tag en antenne). Deze integratie vindt plaats door communicatie tussen het overige deel van het host en software system en een reader van een bepaalde producent. Het overige deel van het host en software system is dan ook niet afhankelijk van de gekozen reader (producent/versie). De edge interface/system kan ook nog de volgende taken uitvoeren:

- het uitfilteren van duplicaten van verschillende readers;
- het zetten van event-based triggers om automatisch een annunciator of actuator te activeren;
- het samenvoegen en selectief verzenden van gegevens aan het host en software system;
- het remote managen van readers;
- het remote managen van zichzelf (indien deze component uit meerdere onderdelen bestaat).

Dit component kan bijvoorbeeld geplaatst worden op gespecialiseerde hardware als onderdeel van een embedded system. De andere delen van het host en software system kunnen dan met dit component communiceren over een netwerk.

2.5.2 Middleware

De middleware is alles tussen de edge interface en de enterprise back-end interface. Vanuit het perspectief van software is dit het belangrijkste gedeelte van het RFID-systeem, welke de belangrijkste functionaliteiten verzorgt, namelijk:

- het delen van gegevens binnen en buiten de enterprise;
- het efficiënt beheren van gegevens welke geproduceerd worden door het RFID-systeem;
- het verzorgen van generieke componenten welke gebruikt kunnen worden bij de implementatie van filtering en aggregatie;
- het mogelijk maken van een ongehinderde koppeling tussen de edge interface en de enterprise back-end interface (waardoor wijzigingen in één van beiden de ander niet beïnvloeden).

De middleware is gebaseerd op een open standaard, zodat het compatible is met verscheidene back-end systemen (zie 2.5.3).

2.5.3 Enterprise back-end interface

Dit is de interface tussen de middleware en de enterprise back-end. Hier vindt de integratie plaats met het bedrijfsproces. Deze interface moet aangepast worden op de middleware en de enterprise back-end.

2.5.4 Enterprise back-end

De enterprise back-end is de verzameling van applicaties en IT-systemen van een bedrijf. Hier vinden de bedrijfsprocessen plaats en worden de gegevens verzameld in een database.

2.6 Communicatie infrastructure

De communicatie tussen de verschillende elementen van RFID vindt plaats door middel van radiogolven (tussen tag en reader (antenne)) of de standaard fysieke of draadloze netwerken (overige connecties). De werkwijze van de standaard fysieke of draadloze netwerken zal hier niet behandeld worden, omdat dit niet afwijkend is voor RFID.
De communicatie tussen de tag en de reader vindt plaats op de RFID frequenties:

- LF (low frequency);
- HF (high frequency);
- VHF (very high frequency);
- UHF (ultra high frequency);
- Microwave frequency.

In tabel 1 zijn deze opgenomen inclusief de gebruikte frequentie en tag (in Europa).

Naam	Frequentie	Tag
LF	125-134 KHz	Passief
HF	13,56 MHz	Passief
VHF	30-300 MHz	Niet van toepassing, wordt niet gebruikt
UHF	865-865,5 MHz, 0,1 watts ERP 865,6-867,6 MHz, 2 watts ERP 867,6-868 MHz, 0,5 watts ERP	Actief en passief
Microwave	2,45 GHz	Semi-actief en passief

Tabel 1: RFID frequenties in Europa

Belangrijke aspecten voor de communicatie tussen de tag en de reader zijn naast de frequentie:

- tag collision (2.6.1),
- reader collision (2.6.2),
- tag readability (2.6.3), en,
- read robustness (2.6.4).

2.6.1 Tag collision

Een reader kan slechts tegelijkertijd met één tag communiceren. Als meer dan één tag tegelijkertijd met een reader probeert te communiceren, ontstaat een tag collision. In zo'n geval moet gebruik gemaakt worden van een singulation protocol welke gebaseerd is op een anti-collision algoritme. Voorbeelden van anti-collision algoritmes zijn ALOHA (HF) en Tree Walking (UHF).

2.6.2 Reader collision

De footprints van twee antennes van een of meerdere readers kunnen overlappen. In het geval dat het antennes betreffen van twee verschillende readers levert dit problemen op. Dit kan alleen opgelost worden door de antennes fysiek voldoende van elkaar te verwijderen of door het gebruik van een attenuator om de footprint van een antenne te verkleinen.
Indien twee antennes van één reader overlappen geeft dit meestal geen probleem, omdat de antennes op andere momenten energie krijgen van de reader. Hierdoor is slechts één antenne tegelijkertijd actief.
Een oplossing is ook het gebruik van de techniek TDMA (time division multiple access). In zo'n geval worden readers geïnstrueerd om op verschillende tijdstippen te lezen. Hierdoor is slechts één antenne van een reader actief op hetzelfde moment. Hierdoor kan één tag meerdere malen gelezen worden in het overlappende gedeelte van de footprint. Zodoende is een filtermechanisme noodzakelijk bij het edge system/interface (2.5.1).

2.6.3 Tag readability

Dit is de eigenschap om de gegevens van een specifieke tag succesvol te lezen. Deze eigenschap wordt bepaald door een aantal factoren (zie 2.1.1). Een belangrijk aspect in het ontwerp van een RFID-systeem is daardoor dat een tag meerdere malen gelezen kan worden, zodat een grotere kans bestaat dat in ieder geval één leesactie succesvol verloopt (zie 2.6.4).

2.6.4 Read robustness

Read robustness wordt ook read redundancy genoemd en staat voor het aantal keren dat een specifieke tag succesvol gelezen kan worden binnen de leeszone. De snelheid van een tag en de hoeveelheid aanwezige tags in een leeszone hebben een negatieve invloed op de read robustness.

2.7 Standaarden

Voor RFID zijn verschillende standaarden beschikbaar, bijvoorbeeld van de volgende organisaties:

- ANSI (American National Standards Institute)
- AIAG (Automotive Industry Action Group)
- EAN.UCC (European Article Numbering Association International, Uniform Code Council)
- EPCglobal
- ISO (International Organization for Standardization)
- CEN (Comité Européen Normalisation)
- ETSI (European Telecommunications Standards Institute)
- ERO (European Radiocommunications Office)
- UPU (Universal Postal Union)
- ASTM (American Society for Testing and Materials)

EPCglobal heeft standaarden ontwikkeld voor RFID welke de grootste kans hebben om wereldwijd geadopteerd te worden. Daarnaast zijn deze standaarden niet specifiek voor een bepaalde toepassing. Zodoende zal in het kader van deze scriptie alleen op deze standaard ingegaan worden. Het EPCglobal Network bestaat uit de volgende vijf componenten[6]:

- Electronic Product Code (EPC) (2.7.1);
- ID System (2.7.2);
- EPCglobal middleware (2.7.3);
- Discovery Services (DS) (2.7.4);
- EPC Information Services (EPCIS) (2.7.5).

2.7.1 Electronic Product Code (EPC)

De Electronic Product Code (EPC) wordt gebruikt om een product uniek te identificeren, maar bevat geen informatie hierover. Een EPC bestaat uit vier onderdelen:

- een header welke de gebruikte EPC versie aangeeft;
- een manager number, welke de bedrijfsnaam of het domein aangeeft;
- een object class, welke het classtype van het object aangeeft;
- een serial number, welke een nummer aan het object meegeeft.

EPCglobal heeft object classes gespecificeerd, waarvan de specificaties in tabel 2 zijn opgenomen.

[6] De verwijzingen naar de specificaties van EPC zijn opgenomen in 2.7.1. Voor alle andere componenten zijn de specificaties beschikbaar op: http://www.epcglobalinc.org/standards_technology/Final-epcglobal-arch-20050701.pdf

Class	Soort tag	Bits	Frequency
0[7]	Passief Class 0: RO Class 0+: WORM	64 bits EPC	UHF (900 MHz)
1[8]	Passief Class 1: WORM Gen 2: RW	Class 1: 96 bits EPC Gen 2: 96 bits EPC 32 bits foutcorrectie en kill commando	Class 1: UHF (860-930 MHz) HF (13,56 MHz) Gen 2: UHF (860-930 MHz)
2	Passief RW	In ieder geval 224 bits gebruikersdata	
3	Actief RW	Nog niet gespecificeerde hoeveelheid gebruikersdata Inclusief microprocessor en I/O-interface	
4	Actief RW	Nog niet gespecificeerde hoeveelheid gebruikersdata Inclusief microprocessor, I/O-interface en batterij	

Tabel 2: Specificaties object classes EPCglobal

Een kill commando houdt in dat de tag de gegevens in zijn geheugen verwijderd of zichzelf zodanig opnieuw configureerd, dat communicatie met een reader niet meer mogelijk is.

De tags van class 0 en 1 zijn niet uitwisselbaar. Daarnaast zullen deze tags vervangen gaan worden door de class 1 UHF Generation 2 tag (ook wel EPC Gen 2 of Gen 2 tag genoemd). De classes 2, 3 en 4 bevinden zich momenteel nog in de prototype fase.

Het toewijzen van één of meerdere blokken EPC aan fysieke objecten en andere entiteiten vindt plaats door de EPC manager (onderdeel van het RFID-systeem bij de organisatie welke RFID gebruikt). Deze rechten heeft de EPC Manager ontvangen van de Issuing Agency (instantie van EPCglobal). De EPC Manager heeft twee unieke verantwoordelijkheden:

- het uitgeven van een EPC aan een fysiek object of een andere identiteit, waarbij de uniekheid van EPC's behouden moet blijven;
- het bijhouden van de Object Name Service (ONS) informatie over het blok of de blokken EPC's, welke door de EPC Manager onderhouden worden (indien EPC's alleen bij een EPC Manager gebruikt worden is dit niet noodzakelijk).

[7] Complete specificatie beschikbaar op: http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

[8] Complete specificaties beschikbaar op: http://www.epcglobalinc.org/standards_technology/Secure/v1.0/HF-Class1.pdf, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf en http://www.epcglobalinc.org/standards_technology/EPCglobal%20Class-1%20Generation-2%20UHF%20RFID%20Conformance%20V1%200%202.pdf

2.7.2 ID System

Voor EPC tags en interface protocols zijn specificaties beschikbaar, zodat readers en tags van verschillende leveranciers interoperabel zijn.

2.7.3 EPCglobal middleware

De middleware is verantwoordelijk voor het efficiënt behandelen van de gegevens. Dit bestaat zowel uit het sorteren, filteren als het verwerken van gegevens. Het zorgt er dus voor dat alleen relevante informatie door de EPCIS naar de back-end systemen van het bedrijf gestuurd wordt.

2.7.4 Discovery Services (DS)

DS geeft toegang tot de EPC gegevens. Een component van de Discovery Services is de Object Name Service (ONS). De ONS kan vergeleken worden met een DNS. Als de ONS als input een EPC ontvangt, produceert hij als output een adres, waar deze EPC gevonden kan worden.

2.7.5 EPC Information Services (EPCIS)

De EPC Information Services (EPCIS) is bedoeld voor het uitwisselen van gegevens tussen de ontvangers van EPCglobal. EPCIS betreft zowel interfaces voor het uitwisselen van gegevens als specificaties van de gegevens zelf.

3 Wetgeving

In dit hoofdstuk zal de deelvraag “Welke wetten met betrekking tot RFID zijn er?” beantwoord worden. Hiervoor zal ingegaan worden op de specifieke RFID wetgeving in 3.1. Tevens zal de algemene wetgeving met betrekking tot privacy behandeld worden in 3.2.

3.1 RFID wetgeving

Nederland heeft nog geen wetgeving met betrekking tot RFID. De ChristenUnie-fractie van de Tweede Kamer heeft in mei 2005 een notitie[9] geschreven over RFID naar aanleiding van de berichten in de media over de steeds bredere toepassingsmogelijkheden van RFID. In de notitie worden door de ChristenUnie enkele maatregelen voorgesteld met betrekking tot RFID, namelijk:

- het vastleggen in de Wet dat het implanteren van RFID-tags bij mensen nooit verplicht kan worden gesteld;
- het aanpassen van de Wet Bescherming Persoonsgegevens, zodat ingespeeld kan worden op de nieuwe technologie;
- het onderzoeken van de gevolgen van grootschalige invoering van RFID-tags voor de maatschappij door de overheid;
- het beveiligen van informatie op RFID-tags:
  - het coderen van informatie op tags zodat deze niet leesbaar zijn door andere readers;
  - het toevoegen van extra informatie aan RFID-tags dient voorkomen te worden (actieve tags hebben memory waarin informatie toegevoegd kan worden);
  - het gebruiken van “Active Authentication” tegen het kopiëren en vervalsen van de inhoud van een RFID-tag;
  - het verbieden van het ongeoorloofd en ongemerkt uitlezen van RFID-tags;
  - het verbieden van het afluisteren en aftappen bij het uitlezen van RFID-tags;
- het verplichten van winkeliers dat RFID-tags bij de kassa gedeactiveerd worden, het onmogelijk maken om gedeactiveerde RFID-tags opnieuw te activeren en het wettelijk verbieden van het volgen van klanten door middel van RFID (ook in een winkel);
- het stimuleren door de overheid van het ontwikkelen en gebruiken van een tag-blokkeerder (deze houdt de informatie welke de RFID-tag uitzendt tegen);
- het voorlichten van consumenten wanneer gebruik gemaakt wordt van RFID-tags op of in producten;
- het informeren van de burgers over de mogelijkheden en onmogelijkheden van RFID door de overheid.

De technologiecommissie van de Tweede Kamer organiseerde op 5 april 2006 een themabijeenkomst over RFID-technologie in samenwerking met het RFID Platform Nederland en ECP.NL. Tijdens de bijeenkomst werden twee debatten gevoerd over respectievelijk de kansen en mogelijke risico’s bij het gebruik van RFID-technologie in Nederland.
Het debat over de kansen en mogelijkheden van RFID voor Nederland ging voornamelijk over de rolverdeling tussen overheid en bedrijfsleven bij het stimuleren van de ontwikkeling van RFID. De rol van de overheid werd vooral gezien in het stimuleren van de toepassing van RFID, voorlichting en bewustwording rondom RFID en het stimuleren van het standaardisatiewerk.

[9] Notitie beschikbaar op: http://www.christenunie.nl/l/library/download/19705

Het debat over de mogelijke risico's van RFID voor Nederland maakte duidelijk dat de consument de grootst mogelijke keuzevrijheid moet hebben bij de acceptatie van RFID en dat de huidige wetgeving niet gewijzigd hoeft te worden in het kader van RFID, maar wel verduidelijkt. Concluderend werd gesteld dat de invoering van RFID op een verantwoorde wijze plaats dient te vinden, waarbij het een gezamenlijke taak van de overheid, aanbieders, gebruikers en maatschappelijke organisaties is om dit voorspoedig te laten verlopen.

Ook de Europese Commissie is begonnen met een debat over de kansen en bedreigingen van RFID voor de overheid, bedrijven en de maatschappij. Dit debat is begonnen door middel van een paneldiscussie tijdens CeBIT 2006. Dit zal opgevolgd worden door vijf workshops (maart tot en met juni 2006). Op basis van de workshops zal een rapport opgesteld worden, waarover on-line gediscussieerd kan worden. Dit zal resulteren in een definitieve versie van dit rapport.

3.2 Wet Bescherming Persoonsgegevens

De Wet Bescherming Persoonsgegevens (Wbp)[10] is gebaseerd op de Europese Directive EC 95/46. De Wbp is gebaseerd op negen principes, namelijk:

1. voornemen en melden,
2. transparantie,
3. doelbinding,
4. rechtmatige grondslag,
5. kwaliteit,
6. rechten van de betrokkenen,
7. beveiliging,
8. verwerking door een bewerker, en,
9. gegevensverkeer met landen buiten de EU.

Deze principes zijn in tabel 3 verder uitgewerkt.

De Wbp is alleen van toepassing voor persoonsgegevens en bijzondere persoonsgegevens. Persoonsgegevens zijn in de Wbp als volgt gedefinieerd: "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon" (artikel 1). Bijzondere persoonsgegevens zijn (artikel 16):

- godsdienst of levensovertuiging,
- ras,
- politieke gezindheid,
- gezondheid,
- seksuele leven,
- lidmaatschap van een vakvereniging,
- strafrechtelijke persoonsgegevens, en,
- persoonsgegevens over onrechtmatig of hinderlijk handelen waarvoor een verbod is opgelegd.

[10] Wet is beschikbaar op: http://www.cbpweb.nl/downloads_wetten/WBP.PDF

Bijzondere persoonsgegevens mogen niet verwerkt worden conform de Wbp met uitzondering van de doelen zoals genoemd in de artikelen 17 tot en met 24. Dit houdt in dat bijzondere persoonsgegevens verwerkt mogen worden door organisaties voor welke dit van belang is (bijvoorbeeld kerk bij godsdienst en lidmaatschap van een vakvereniging bij een vakvereniging) of indien hiervoor een duidelijke wettelijke basis is. Tevens is het mogelijk om bijzondere persoonsgegevens te verwerken indien de betrokkene hiervoor expliciet toestemming geeft.

Principe	Toelichting
Verwerkers moeten de volgende principes naleven:	
Voornemen en melden	Het melden van de verwerking door de verwerker bij de daarvoor aangewezen instantie (in Nederland het College Bescherming Persoonsgegevens (Cbp)).
Transparantie	Het informeren van de betrokkene over de verwerking van persoonsgegevens.
Doelbinding	De persoonsgegevens alleen verwerken voor gespecificeerde, expliciete en wettige doeleinden.
Rechtmatige grondslag	Een rechtmatige grondslag is aanwezig voor het verwerken van de persoonsgegevens.
Kwaliteit	De verwerkte persoonsgegevens dienen toereikend, ter zake dienend, juist, nauwkeurig en niet bovenmatig te zijn.
Rechten van de betrokkenen	De verwerker dient de rechten van de betrokkene te respecteren. Dit betreft bijvoorbeeld het inzagerecht, correctierecht etc..
Beveiliging	De persoonsgegevens moeten beveiligd worden met technische en organisatorische maatregelen welke een passend beveiligingsniveau garanderen.
Verwerkers dienen indien van toepassing de volgende principes na te leven:	
Verwerking door een bewerker	De bewerker dient zich aan dezelfde eisen te houden als de verwerker. Persoonsgegevens mogen alleen bewerkt worden in opdracht van de verantwoordelijke (verwerker).
Gegevensverkeer met landen buiten de EU	De verwerker dient zich ervan te verzekeren dat een afdoende beveiligingsniveau van toepassing is bij het verzenden van persoonsgegevens naar landen buiten de EU.

Tabel 3: Principes van de Wbp

In de Wbp wordt bedoeld met de verwerking van persoonsgegevens: “elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens” (artikel 1). Dit houdt voor RFID in dat als persoonsgegevens op enige manier in het RFID-systeem gebruikt worden de Wbp van toepassing is op het RFID-systeem.

Tevens is sprake van een verwerker en een bewerker. De verwerker wordt in de Wbp de verantwoordelijke genoemd en als volgt gedefinieerd: “de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt” (artikel 1). De bewerker is: “degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen” (artikel 1). Voor RFID betekent dit dat de eigenaar van het RFID-systeem verwerker is en dat als enig onderdeel van de verwerking van de persoonsgegevens uitbesteed is aan een andere organisatie dit een bewerker is.

Het principe beveiliging is door het Cbp verder uitgewerkt in Achtergrondstudies en Verkenningen 23 ‘Beveiliging van Persoonsgegevens’. De beveiliging kent drie kwaliteitsaspecten, te weten exclusiviteit, integriteit en continuïteit. De definitie van het Cbp van de kwaliteitsaspecten is opgenomen in tabel 4. Ter vergelijking zijn ook de definities uit het NOREA geschrift 1 “IT-auditing aangeduid” opgenomen.

Kwaliteitsaspect	Definitie Cbp	Definitie NOREA
Exclusiviteit	Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.	De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruik maken van IT-processen.
Integriteit	De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.	De mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.
Continuïteit	De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften. Continuïteit wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.	De mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.

Tabel 4: De definities van de kwaliteitsaspecten van het Cbp en de NOREA

Uit een vergelijking van de definities van het Cbp met de definities van de NOREA blijkt dat de definities voor continuïteit en integriteit van het Cbp enger zijn dan die van de NOREA, terwijl de definitie van de exclusiviteit van de NOREA enger is dan die van het Cbp. Het Cbp heeft de kwaliteitsaspecten daarnaast specifiek van toepassing gemaakt op persoonsgegevens. De verschillen zijn in tabel 4 onderstreept.

Om te bepalen welke technische en organisatorische maatregelen getroffen dienen te worden, maakt het Cbp gebruik van vier risicoklassen, namelijk:

- risicoklasse 0: publiek niveau;
- risicoklasse I: basis niveau;
- risicoklasse II: verhoogd risico;
- risicoklasse III: hoog risico.

Voor risicoklasse 0 hoeven geen beveiligingsmaatregelen getroffen te worden.
Bij risicoklasse I houden de maatregelen onder andere in dat er een beveiligingsbeleid geïmplementeerd is, dat de administratie organisatie beschreven is, dat zowel de juistheid van het curriculum vitae als de identiteit van nieuwe medewerkers gecontroleerd wordt, dat datamodellen beschreven zijn, dat bevoegdheidsprofielen opgesteld zijn, dat wachtwoorden dienen te voldoen aan de genoemde eisen en dat de persoonsgegevens geback-upt worden.
Aanvullend moet er bij risicoklasse II onder andere een beveiligingsfunctionaris zijn, moet de opslag op mobiele apparatuur versleuteld zijn, moet toegang tot persoonsgegevens door derden beperkt zijn en moet een nauwkeurige identificatie uitgevoerd worden bij het gebruik van persoonsgegevens via een computernetwerk.
Bij risicoklasse III zijn de aanvullende maatregelen onder andere screening van personeel, het tekenen van een geheimhoudingsverklaring door personeelsleden, het gebruik van alleen goedgekeurde apparatuur, het voorzien van gegevensdragers met persoonsgegevens van een markering waaruit de risicoklasse blijkt en het niet toestaan van overdragen van bevoegdheden.
Een compleet overzicht van de maatregelen per risicoklasse is opgenomen in Achtergrondstudies en Verkenningen 23 ‘Beveiliging van Persoonsgegevens’[11].
De bepaling in welke risicoklasse persoonsgegevens vallen dient te worden uitgevoerd conform tabel 5.

Hoeveelheid persoons-gegevens (aard en omvang)	Aard van de verwerking	Persoons-gegevens	Bijzondere persoons-gegevens	Financieel en/of economische persoons-gegevens
Weinig persoonsgegevens	Lage complexiteit van de verwerking	Risicoklasse 0	Risicoklasse II	Risicoklasse II
Veel persoonsgegevens	Hoge complexiteit van de verwerking	Risicoklasse I	Risicoklasse III	

Tabel 5: Model van het Cbp voor het bepalen van de risicoklasse van persoonsgegevens

[11] Complete tekst beschikbaar op: http://www.cbpweb.nl/downloads_av/AV23.pdf

4 Risicoanalyse

Om te bepalen welke risico's toepassing van RFID met zich meebrengt (deelvraag 3: "Welke risico's zijn er bij het gebruik van RFID?") zal een risicoanalyse uitgevoerd moeten worden. Deze risicoanalyse zal uitgevoerd worden voor de twee delen waaruit een RFID-systeem bestaat, namelijk de front-end en de back-end. De front-end bestaat uit de tag, de reader en de communicatie daartussen, terwijl de back-end bestaat uit de reader, de back-end systemen en de communicatie tussen deze componenten. Deze risicoanalyses zijn opgenomen in 4.1 (front-end) en 4.2 (back-end).

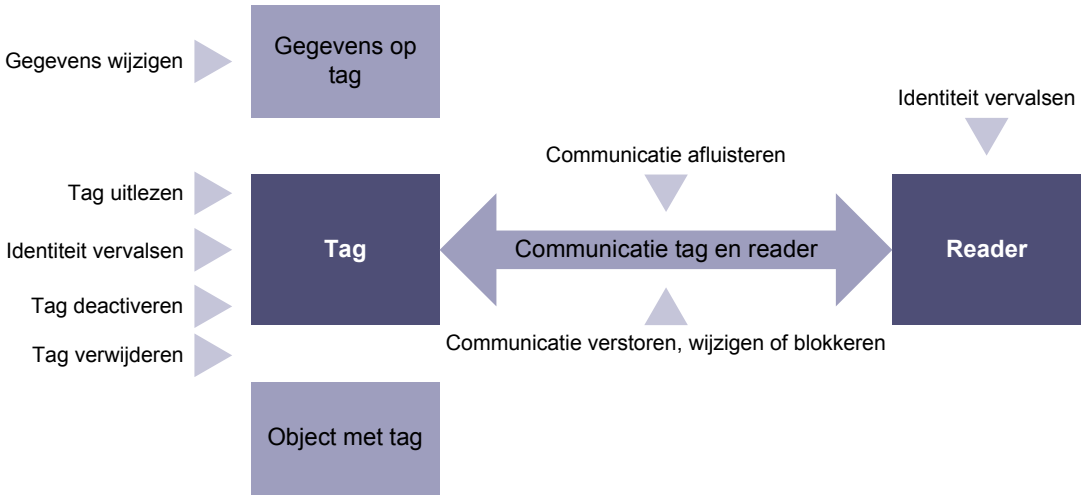
De risicoanalyses zullen zich richten op de kwaliteitsaspecten continuïteit, exclusiviteit en integriteit. De definities van deze kwaliteitsaspecten zijn overgenomen uit NOREA geschrift 1 "IT-auditing aangeduid":

- continuïteit is de mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben;
- exclusiviteit is de mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruik maken van IT-processen;
- integriteit is de mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.

In 4.3 zullen vervolgens de risico's vanuit de Wbp geanalyseerd worden.

4.1 Risicoanalyse front-end

De front-end bestaat uit de tag, de reader en de communicatie daartussen. De front-end is inclusief de risico's opgenomen in figuur 11.



Figuur 11: Risico's voor de tag, reader en de communicatie tussen tag en reader

Hieronder zullen de risico's toegelicht worden:

- gegevens op tag wijzigen: gegevens welke zich op de tag bevinden kunnen gewijzigd worden, zodat verkeerde informatie naar de reader toegezonden wordt;
- tag uitlezen: elke reader kan een compatible tag uitlezen (ook als voor de gebruiker onbekend is dat een reader en/of tag aanwezig is). Hierdoor is het mogelijk om tags te volgen en op elke willekeurige locatie uit te lezen. Het is bijvoorbeeld ook mogelijk om bij de eerste generatie RFID-chips de sleutel te achterhalen, omdat deze niet goed beveiligd zijn[12];
- identiteit tag vervalsen: door de EPC en de beveiligingsinformatie van een tag te gebruiken, kan de betreffende tag gekloond of nagebootst worden;
- tag deactiveren: het is mogelijk een tag te deactiveren door deze mechanisch (bijvoorbeeld een kill-commando of een batterij van een actieve tag ontladen door deze veel te bevragen) of chemisch (bijvoorbeeld straling van een magnetron) stuk te maken;
- tag verwijderen: het is mogelijk om een tag te verwijderen van het object waarop deze zich bevindt;
- communicatie tag en reader afluisteren: door het afluisteren van de communicatie tussen de tag en de reader is bekend welke tags zich waar bevinden, welke informatie een reader opgevraagt en welke informatie een tag geeft;
- communicatie tag en reader verstoren, wijzigen of blokkeren: door bijvoorbeeld veel tags te simuleren, een stoorzender te plaatsen, de gebruikte frequentie te verstoren of tags te verpakken in metaal (kooi van Faraday) is het mogelijk om de communicatie tussen tag en reader te verstoren of te blokkeren. Daarnaast is het mogelijk om de communicatie tussen de tag en reader op te vangen en zelf nieuwe te versturen (man-in-the-middle attack (MITM));
- identiteit reader vervalsen: in bepaalde systemen dient de reader zich te autoriseren aan de tags. Door de identiteit van de reader te vervalsen kan vervolgens alsnog informatie van de tags verkregen worden.

In tabel 6 zijn alle risico's opgenomen inclusief een aanduiding van welke kwaliteitsaspecten bedreigd worden.

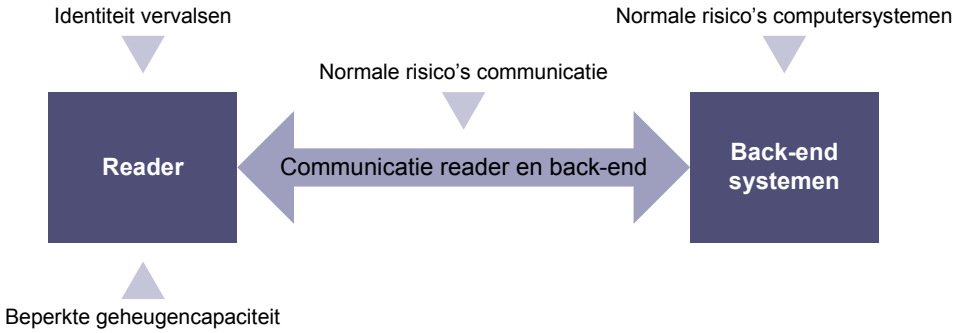
Risico	C	E	I
Gegevens op tag wijzigen			X
Tag uitlezen		X	
Identiteit tag vervalsen		X	X
Tag deactiveren	X		
Tag verwijderen	X		
Communicatie tag en reader afluisteren		X	
Communicatie tag en reader verstoren, wijzigen of blokkeren	X		X
Identiteit reader vervalsen		X	X

Tabel 6: Risicoanalyse met betrekking tot de tag, reader en de communicatie tussen tag en reader (C(ontinuïteit), E(xclusiviteit) en I(ntegriteit))

[12] Zie artikel op: http://tweakers.net/nieuws/41183

4.2 Risicoanalyse back-end

De back-end bestaat uit de reader, de back-end systemen en de communicatie tussen deze componenten. De back-end is inclusief de risico's opgenomen in figuur 12. De risico's voor de communicatie tussen de reader en de back-end systemen zijn ook risico's voor de communicatie tussen de diverse back-end systemen. Risico's welke voor de back-end systemen gelden, gelden ook voor de reader.



Figuur 12: Risico's voor de reader, de back-end systemen en de communicatie tussen deze componenten

De back-end systemen zijn normale computersystemen, waarvoor de risico's gelden welke ook voor normale systemen van toepassing zijn. Dit geldt ook voor de communicatie. Naast deze normale risico's gelden de volgende risico's:

- identiteit reader vervalsen: door de identiteit van de reader te vervalsen kan informatie verkregen worden van de back-end systemen, maar kan ook informatie verstuurd worden naar de back-end systemen;
- beperkte geheugencapaciteit reader: de reader heeft een beperkte capaciteit om gegevens op te slaan indien geen communicatie met de back-end systemen mogelijk is. Indien deze capaciteit vol is, zal het geheugen overschreven worden conform het FIFO-principe, wat gelijk staat aan verlies van informatie.

In tabel 7 zijn alle risico's opgenomen inclusief een aanduiding van welke kwaliteitsaspecten bedreigd worden.

Risico	C	E	I
Identiteit reader vervalsen		X	X
Beperkte geheugencapaciteit reader	X		X
Normale risico's communicatie	X	X	X
Normale risico's computersystemen	X	X	X

Tabel 7: Risicoanalyse met betrekking tot de reader, de back-end systemen en de communicatie tussen deze componenten (C(ontinuïteit), E(xclusiviteit) en I(ntegriteit))

4.3 Risicoanalyse Wbp

Een RFID-systeem hoeft niet altijd te voldoen aan de Wbp. Deze verplichting geldt alleen indien de gegevens in een RFID-systeem identificeerbaar zijn tot een individu. Indien dit het geval is, zal voldaan moeten worden aan Wbp. Hiervoor zullen de risico's gelden welke bij elke verwerking van persoonsgegevens gelden. Specifieke risico's voor een RFID-systeem met betrekking tot de Wbp zijn:

- het RFID-systeem verwerkt wel persoonsgegevens, terwijl de verwerker dit niet erkend heeft: hierdoor denkt de verwerker dat niet voldaan hoeft te worden aan de eisen van de Wbp, terwijl dit wel noodzakelijk is;
- het RFID-systeem is zodanig opgesteld dat het niet zichtbaar is (tag en reader zijn beiden onzichtbaar) en de individuen worden hiervan niet op de hoogte gesteld: de individu is hierdoor niet bekend met het feit dat zijn persoonsgegevens vastgelegd worden, terwijl dit wel duidelijk aan de individu gemeld dient te worden door de verwerker;
- het koppelen van meerdere informatiesystemen (zowel verschillende RFID-systemen als andere informatiesystemen): hierdoor is het mogelijk om gegevens ook voor andere doeleinden te gebruiken, waarvan de gebruiker niet op de hoogte is en/of waarvoor de gebruiker geen toestemming heeft gegeven;
- bijzondere persoonsgegevens worden verzameld: bijzondere persoonsgegevens kunnen vastgelegd worden, terwijl hierbij niet een afdoend beveiligingsniveau nagestreefd wordt. Hierbij kan bijvoorbeeld gedacht worden aan een geïmplanteerde RFID-chip met medische informatie in een individu.

In tabel 8 zijn alle risico's opgenomen inclusief een aanduiding van welke kwaliteitsaspecten bedreigd worden.

Risico	C	E	I
Verwerking van persoonsgegevens		X	
Geen (expliciete) melding van RFID-systeem		X	
Koppelen van informatiesystemen		X	
Het verwerken van bijzondere persoonsgegevens		X	

Tabel 8: Risicoanalyse met betrekking tot de Wbp (C(ontinuïteit), E(xclusiviteit) en I(ntegriteit))

5 Maatregelen

In dit hoofdstuk zal de volgende deelvraag beantwoordt worden: “Welke maatregelen dienen gehanteerd te worden bij het gebruik van RFID?”. Hiervoor zijn eerst basismaatregelen opgesteld, welke toegelicht worden in 5.1. Vervolgens zullen deze maatregelen verder uitgewerkt worden per toepassing van RFID, namelijk als:

- middel om producten te identificeren (5.2);
- extern middel om individuen te identificeren (5.3);
- intern middel om individuen te identificeren (5.4).

5.1 Basismaatregelen

In tabel 9 is een overzicht opgenomen van de risico’s, welke geïdentificeerd zijn in hoofdstuk 4, en de bijbehorende basismaatregelen waaraan een RFID-systeem zodoende moet voldoen. Onderstaand zullen de maatregelen toegelicht worden.

1. De communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden

Het afluisteren van de communicatie tussen tag en reader kan voorkomen worden door deze communicatie te versleutelen. Hierbij kan gekozen worden voor een sterke of zwakke sleutel. De gekozen sleutel dient periodiek heroverwogen te worden, omdat sterke sleutels na verloop van tijd zwakke sleutels kunnen worden.

2. De communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden

Het wijzigen van communicatie kan slecht voorkomen worden, maar kan bijvoorbeeld gesignaleerd worden door het gebruik van een checksum. Hierbij kan gekozen worden voor een zwak of sterk logaritme voor de checksum.

3. De communicatie tussen de tag en de reader dient op geen enkele wijze verstoord of geblokkeerd te kunnen worden

Het verstoren of blokkeren van deze communicatie kan grotendeels voorkomen worden door verstorende objecten te verwijderen uit of niet te plaatsen in de omgeving van de tag en de reader. Deze omgeving kan echter nooit geheel geconditioneerd worden, dus het storen of blokkeren van de communicatie kan nooit in zijn geheel voorkomen worden.

4. De reader dient altijd de verkregen gegevens (van de tags) vast te leggen/bewaren

Om te voorkomen dat een reader de verkregen gegevens niet meer vast kan leggen in verband met te weinig geheugencapaciteit dienen de verkregen gegevens altijd ergens vastgelegd te kunnen worden. Dit kan zowel op de reader zelf zijn als op de achterliggende systemen. Indien de informatie op de reader opgeslagen wordt, dient het geheugen van de reader groot genoeg te zijn. Indien de keuze wordt gemaakt voor de achterliggende systemen dient zorg gedragen te worden voor een hoge beschikbaarheid van de achterliggende systemen en communicatie infrastructuur. Dit kan bijvoorbeeld onder andere bereikt worden door middel van het redundant uitvoeren van deze systemen en infrastructuur.

5. De tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is

Indien de tag niet langer gebruikt wordt zal deze gedeactiveerd moeten worden door bijvoorbeeld het gebruik van een kill-commando of het plaatsen van een tag in een kooi van Faraday. Een kooi van Faraday kan door de consument zelf geplaatst worden om een tag. Op deze manier heeft de consument een grotere vrijheid om zelf te bepalen of een tag gedeactiveerd is.
Een andere optie is het gebruik van een transponder, omdat deze alleen reageert op een informatieverzoek van de reader. Tussendoor bevindt deze zich in een slaaptoestand en verstuurt geen informatie. Hierbij moet wel opgemerkt worden dat deze een batterij heeft en daardoor een beperkte levensduur.
Bij het gebruik van authenticatiemethoden levert het uitlezen van compatible tags geen bruikbare informatie op voor niet-geauthenticeerde readers. Deze kunnen dan hooguit vaststellen dat een tag aanwezig is, maar het is niet mogelijk om vast te stellen welke tag het is.

6. De tag dient zodanig bevestigd te zijn op het object dat het verwijderen ervan onmogelijk is

Het verwijderen van een tag van een object is nooit in zijn geheel te voorkomen, maar door de tag zodanig te bevestigen dat het verwijderen hiervan heel veel moeite kost, kan er voor gezorgd worden dat geen moeite gedaan zal worden om de tag te verwijderen, omdat de winst hiervan te klein is. Dit zal dus afhankelijk zijn van het object, waar de tag zich op bevindt en de houding ten opzichte van RFID van een individu. Een kosten/baten-analyse dient uitgevoerd te worden om te bepalen welke maatregelen genomen moeten worden om het zo goed als onmogelijk te maken om de tag te verwijderen.

7. De tag en reader dienen zich te authenticeren ten opzichte van elkaar

Het authenticeren van de reader en tag ten opzichte van elkaar kan gedaan worden met de beschikbare authenticatiemethoden welke verschillen van het gebruik van wachtwoorden tot en met een challenge-response systeem. Wachtwoorden zijn over het algemeen een zwakke methode (replay-attack), terwijl een challenge-response systeem bij een goede implementatie een sterke methode is.

8. Een RFID-systeem welke (bijzondere) persoonsgegevens verwerkt dient te voldoen aan de Wet Bescherming Persoonsgegevens

Indien een RFID-systeem (bijzondere) persoonsgegevens verwerkt dient voldaan te worden aan de Wet Bescherming Persoonsgegevens (zie 3.2). Belangrijke aspecten hierbij zijn bijzondere persoonsgegevens (vereisen meer beveiligingsmaatregelen) en het koppelen van informatiesystemen (mag alleen met uitdrukkelijke toestemming van de individu van wie persoonsgegevens verwerkt worden).

9. Een risicoanalyse dient uitgevoerd te worden voor de back-end systemen en de communicatie en voor deze risico's dienen maatregelen getroffen te worden.

Voor de back-end systemen en de communicatie tussen deze systemen dient een risicoanalyse uitgevoerd te worden aan de hand waarvan bepaald wordt welke risico's van toepassing zijn. Indien het RFID-systeem (bijzondere) persoonsgegevens verwerkt dient voor de te treffen maatregelen tevens aangesloten te worden bij de Wbp (zie 3.2).

10. Gegevens op de tag dienen niet gewijzigd te kunnen worden door ongeautoriseerden

De gegevens op een tag dienen beveiligd te worden, zodat alleen geautoriseerde reader(s) de gegevens kunnen wijzigen. Dit is mogelijk door het gebruik van authenticatiemethoden waarbij de tag en reader zich ten opzichte van elkaar authenticeren.

11. Het deactiveren van de tag door onbevoegden dient onmogelijk gemaakt te worden

Het deactiveren van een tag door onbevoegden is zo goed als niet te voorkomen, omdat daarover geen zeggenschap bestaat. Een uitzondering hierop is het kill-commando. Als de reader en tag zich ten opzichte van elkaar moeten authenticeren, is het alleen voor een geauthenticeerde reader mogelijk om dit commando te gebruiken. Alle andere vormen van deactiveren kunnen grotendeels alleen voorkomen worden door een goede voorlichting, zodat het bekend is waarom RFID gebruikt wordt en wat het nut is, en het respecteren van de individuele vrijheid door het naleven van de normen en waarden.

Nr.	Maatregel	Risico
1	De communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden.	Communicatie tag en reader afluisteren
2	De communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden.	Communicatie tag en reader verstoren, wijzigen of blokkeren
3	De communicatie tussen de tag en de reader dient op geen enkele wijze verstoord of geblokkeerd te kunnen worden.	
4	De reader dient altijd de verkregen gegevens (van de tags) vast te leggen/bewaren.	Beperkte geheugencapaciteit reader
5	De tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is.	Tag uitlezen
6	De tag dient zodanig bevestigd te zijn op het object dat het verwijderen ervan onmogelijk is.	Tag verwijderen
7	De tag en reader dienen zich te authenticeren ten opzichte van elkaar.	Identiteit reader vervalsen
		Identiteit tag vervalsen
8	Een RFID-systeem welke (bijzondere) persoonsgegevens verwerkt dient te voldoen aan de Wet Bescherming Persoonsgegevens.	Geen (expliciete) melding van RFID-systeem
		Het verwerken van bijzondere persoonsgegevens
		Koppelen van informatiesystemen
		Verwerking van persoonsgegevens
9	Een risicoanalyse dient uitgevoerd te worden voor de back-end systemen en de communicatie en voor deze risico's dienen maatregelen getroffen te worden.	Normale risico's communicatie en computersystemen
10	Gegevens op de tag dienen niet gewijzigd te kunnen worden door ongeautoriseerden.	Gegevens op tag wijzigen
11	Het deactiveren van de tag door onbevoegden dient onmogelijk gemaakt te worden.	Tag deactiveren

Tabel 9: Risico's met de bijbehorende basismaatregelen

Van deze basismaatregelen zijn de nummers 3, 4, 6, 9, 10 en 11 van toepassing voor alle genoemde toepassingen van RFID. De maatregelen 1, 2, 5, 7 en 8 zijn afhankelijk van de Wbp. Als de Wbp niet van toepassing is, dient bepaald te worden of deze maatregelen noodzakelijk zijn in verband met eventuele andere risico's welke gelopen worden.
Indien de Wbp wel van toepassing is zijn de maatregelen 5 en 8 altijd van toepassing. De maatregelen 1, 2 en 7 zijn van toepassing aan de hand van de risicoklassen van de Wbp. Dit dient bepaalt te worden aan de hand van tabel 5. In tabel 10 is opgenomen hoe de maatregelen 1, 2 en 7 vertaald moeten worden naar de risicoklassen van de Wbp. Risicoklasse 0 is niet opgenomen, omdat hiervoor geen aanvullende maatregelen vereist zijn.

Nr.	Maatregel	Risicoklasse I	Risicoklasse II	Risicoklasse III
1	De communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden.	Geen aanvullende maatregelen.	Versleutelen van de communicatie met een algemeen geaccepteerde cryptografiemethode, welke het risico van onbevoegde ontsleuteling uitsluit.	Geen aanvullende maatregelen ten opzichte van risicoklasse II.
2	De communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden.	Geen aanvullende maatregelen.	Geen aanvullende maatregelen.	Het gebruik van een checksum om de integriteit van de gegevens te waarborgen.
6	De tag en reader dienen zich te authenticeren ten opzichte van elkaar.	Logische toegangsbeveiliging, dus een zwakke authenticatie-methode moet in ieder geval gebruikt worden.	Authenticatie gebruiken welke niet onderschept kan worden door onbevoegden (bijvoorbeeld een challenge-response systeem).	Geen aanvullende maatregelen ten opzichte van risicoklasse II.

Tabel 10: Privacymaatregelen voor basismaatregelen 1, 2 en 7 in relatie tot risicoklasse

5.2 Maatregelen bij RFID als middel voor identificatie van producten

Een voorbeeld van RFID om producten te identificeren is het gebruik in een supermarkt. De tags bevinden zich hierbij in de producten (non-food) of op de verpakkingen van de producten (food en non-food). Hierdoor wordt het mogelijk om bij de kassa een boodschappenwagentje in één keer door een poortje te rijden, welke vervolgens alle producten scant. In dit geval wordt RFID niet gebruikt om een individu te identificeren, behalve als deze informatie gekoppeld wordt aan bijvoorbeeld een klantenkaart. Indien de tags op een later moment gescand worden door andere readers, kunnen deze readers alleen informatie verzamelen over welke producten een individu bij zich heeft, maar deze informatie niet linken aan een individu. Wel is het mogelijk om in zo'n geval te scannen wat een individu bij een eerdere winkel gekocht heeft en deze informatie ook vast te leggen. Ondanks dat dit geen persoonsgegevens zijn (behalve als ze gelinkt worden aan een individu) bestaat zo wel de mogelijkheid om veel (niet-identificeerbare) informatie over individuen vast te leggen.

De basismaatregelen uit tabel 9 zijn in tabel 11 uitgewerkt voor RFID als middel om producten te identificeren. Hierbij wordt er vanuit gegaan dat de Wbp niet van toepassing is op het RFID-systeem (en er dus geen persoonsgegevens vastgelegd worden). Indien dit wel het geval is dient voor de maatregelen 1, 2, 5, 7 en 8 aangesloten te worden bij de maatregelen in 5.3.

Nr.	Maatregel	Van toepassing
1	De communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden.	Afhankelijk van risicoanalyse
2	De communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden.	Afhankelijk van risicoanalyse
3	De communicatie tussen de tag en de reader dient op geen enkele wijze verstoord of geblokkeerd te kunnen worden.	Ja
4	De reader dient altijd de verkregen gegevens (van de tags) vast te leggen/bewaren.	Ja
5	De tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is.	Afhankelijk van risicoanalyse
6	De tag dient zodanig bevestigd te zijn op het object dat het verwijderen ervan onmogelijk is.	Ja
7	De tag en reader dienen zich te authenticeren ten opzichte van elkaar.	Afhankelijk van risicoanalyse
8	Een RFID-systeem welke (bijzondere) persoonsgegevens verwerkt dient te voldoen aan de Wet Bescherming Persoonsgegevens.	Nee
9	Een risicoanalyse dient uitgevoerd te worden voor de back-end systemen en de communicatie en voor deze risico's dienen maatregelen getroffen te worden.	Ja
10	Gegevens op de tag dienen niet gewijzigd te kunnen worden door ongeautoriseerden.	Ja
11	Het deactiveren van de tag door onbevoegden dient onmogelijk gemaakt te worden.	Ja

Tabel 11: Maatregelen bij RFID als middel voor identificatie van producten

5.3 Maatregelen bij RFID als extern middel voor identificatie van individuen

Indien RFID gebruikt wordt als extern middel om individuen te identificeren, zal de tag zich bevinden in een object welke door individuen meegenomen wordt. Dit betreft bijvoorbeeld passen (toegangspassen, bankpassen etc.), maar bijvoorbeeld ook het nieuwe paspoort. RFID wordt hier gebruikt als middel om een individu te identificeren of informatie over een individu te verstrekken. In beide gevallen is hier sprake van (bijzondere) persoonsgegevens.
De basismaatregelen uit tabel 9 zijn in tabel 12 uitgewerkt voor RFID als extern middel om individuen te identificeren.

Nr.	Maatregel	Van toepassing
1	De communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden.	Afhankelijk van risicoklasse (tabel 10)
2	De communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden.	Afhankelijk van risicoklasse (tabel 10)
3	De communicatie tussen de tag en de reader dient op geen enkele wijze verstoord of geblokkeerd te kunnen worden.	Ja
4	De reader dient altijd de verkregen gegevens (van de tags) vast te leggen/bewaren.	Ja
5	De tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is.	Ja
6	De tag dient zodanig bevestigd te zijn op het object dat het verwijderen ervan onmogelijk is.	Ja
7	De tag en reader dienen zich te authenticeren ten opzichte van elkaar.	Afhankelijk van risicoklasse (tabel 10)
8	Een RFID-systeem welke (bijzondere) persoonsgegevens verwerkt dient te voldoen aan de Wet Bescherming Persoonsgegevens.	Ja
9	Een risicoanalyse dient uitgevoerd te worden voor de back-end systemen en de communicatie en voor deze risico's dienen maatregelen getroffen te worden.	Ja
10	Gegevens op de tag dienen niet gewijzigd te kunnen worden door ongeautoriseerden.	Ja
11	Het deactiveren van de tag door onbevoegden dient onmogelijk gemaakt te worden.	Ja

Tabel 12: Maatregelen bij RFID als extern en intern middel voor identificatie van individuen

5.4 Maatregelen bij RFID als intern middel voor identificatie van individuen

Als RFID gebruikt wordt als intern middel om individuen te identificeren, is de tag geïmplanteerd in het lichaam van de mens. Dit houdt in dat de individu de tag altijd bij zich heeft. Het betreft altijd persoonsgegevens en afhankelijk van het gebruik van het RFID-systeem ook bijzondere persoonsgegevens.
Hiervoor gelden dezelfde maatregelen als voor RFID als extern middel om individuen te identificeren (zie tabel 12).

6 Conclusie

De conclusie bestaat uit twee onderdelen, namelijk de beantwoording van de hoofdvraag in conclusie en aanbevelingen (6.1) en een persoonlijke reflectie op het onderzoek en de resultaten daarvan (6.2).

6.1 Conclusie en aanbevelingen

De hoofdvraag is:

> ***"Hoe kan RFID door het gebruik van technische en beheersmatige maatregelen op een veilige wijze toegepast worden?"***

Veilig is hierbij gedefinieerd als de kwaliteitsaspecten continuïteit, exclusiviteit en integriteit. De definities van deze kwaliteitsaspecten zijn:

- continuïteit is de mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben;
- exclusiviteit is de mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruik maken van IT-processen;
- integriteit is de mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.

Hierbij zal onderscheid worden gemaakt tussen de verschillende manieren waarop RFID toegepast kan worden, namelijk als:

a. middel om producten te identificeren;
b. extern middel om individuen te identificeren;
c. intern middel om individuen te identificeren.

Om deze hoofdvraag te beantwoorden zijn de maatregelen opgenomen in bijlage C, waarbij onderscheid gemaakt wordt tussen de genoemde toepassingen van RFID.

Voor RFID als middel om producten te identificeren gelden de volgende maatregelen:

- de communicatie tussen de tag en de reader dient op geen enkele wijze verstoord of geblokkeerd te kunnen worden;
- de reader dient altijd de verkregen gegevens (van de tags) vast te leggen/bewaren;
- de tag dient zodanig bevestigd te zijn op het object dat het verwijderen ervan onmogelijk is;
- een risicoanalyse dient uitgevoerd te worden voor de back-end systemen en de communicatie en voor deze risico's dienen maatregelen getroffen te worden;
- gegevens op de tag dienen niet gewijzigd te kunnen worden door ongeautoriseerden;
- het deactiveren van de tag door onbevoegden dient onmogelijk gemaakt te worden.

Daarnaast dient een risicoanalyse uitgevoerd te worden om te bepalen of de volgende maatregelen van belang zijn:

- de communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden;
- de communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden;
- de tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is;
- de tag en reader dienen zich te authenticeren ten opzichte van elkaar.

De verplichte maatregelen voor RFID als middel om producten te identificeren gelden ook voor RFID als intern of extern middel om individuen te identificeren. Tevens zijn hierop de volgende maatregelen van toepassing:

- de tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is;
- een RFID-systeem welke (bijzondere) persoonsgegevens verwerkt dient te voldoen aan de Wet Bescherming Persoonsgegevens.

Daarnaast dienen nog twee maatregelen ingevuld te worden aan de hand van de risicoklasse van de persoonsgegevens, welke conform de Wbp bepaald dient te worden. Dit betreft de maatregelen:

- de communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden;
- de communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden;
- de tag en reader dienen zich te authenticeren ten opzichte van elkaar.

In de praktijk zal het lastig dan wel onmogelijk zijn om alle genoemde maatregelen na te leven. Voorbeelden hiervan zijn:

- de communicatie tussen de tag en de reader dient op geen enkele wijze verstoord of geblokkeerd te kunnen worden: het verstoren of blokkeren van communicatie is niet in zijn geheel te voorkomen, omdat het bijvoorbeeld mogelijk is om een kooi van Faraday te gebruiken;
- de tag dient zodanig bevestigd te zijn op het object dat het verwijderen ervan onmogelijk is: deze maatregel staat tegenover het deactiveren van de tag indien deze niet meer noodzakelijk is. Het deactiveren van een tag kan namelijk ook plaats vinden door deze te verwijderen en dan is het noodzaak dat dit verwijderen eenvoudig plaats kan vinden. Hiervan zal een afweging gemaakt moeten worden (kosten/baten-analyse) of er kan bijvoorbeeld gekozen worden voor mitigerende maatregelen zoals het controleren van alle producten op een tag bij de kassa;
- de tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is: bij bepaalde wijzen van gebruik zal het niet praktisch zijn om een tag tijdelijk te deactiveren indien deze tijdelijk niet gebruikt wordt. Het nadeel hiervan is dat een individu welke de tag bij zich draagt te volgen is. Bij een voldoende spreiding van readers ontstaat dan een Big Brother scenario.

Door de noodzakelijke beveiligingsmaatregelen dient het type van de te gebruiken tag beoordeeld te worden, voordat deze toegepast wordt binnen een RFID-systeem. Hierbij dienen de genoemde maatregelen meegenomen worden, maar ook de relevante beveiligingsinformatie over de tags. Momenteel zijn de tags uit class 0 niet veilig en sommige WORM-tags zijn overschrijfbaar. Tijdelijke deactivatie van tags geïmplanteerd in individuen is niet mogelijk, waardoor het de vraag blijft of het wenselijk is deze als intern middel om individuen te identificeren te gebruiken.
Voor gegevens welke in de risicoklassen II en III van de Wbp vallen geldt zelfs dat het nog niet mogelijk is deze te verwerken in combinatie met RFID, behalve als deze gegevens uitsluitend op het back-end systeem opgeslagen worden. Dit back-end systeem dient dan natuurlijk te voldoen aan alle relevante beveiligingseisen vanuit de Wbp.

Naast bovenstaande maatregelen dient bij de invoering van een RFID-systeem altijd een risicoanalyse gemaakt te worden met betrekking tot de werking van het systeem. Afhankelijk van de opzet van het RFID-systeem zijn bepaalde risico's aanwezig, welke bijvoorbeeld door het gebruik van bepaalde protocollen opgelost kunnen worden. Voorbeelden van risico's zijn een reader collision of een tag collision.

Belangrijke aandachtspunten met betrekking tot RFID zijn:

- de voorlichting over RFID: individuen kunnen keuzes maken over het gebruik van RFID als zij op de hoogte zijn van de mogelijkheden, maar ook de risico's. Goede onafhankelijke voorlichting is noodzakelijk om individuen hiervan op de hoogte te brengen;
- de onmogelijkheid om te controleren of RFID veilig is: individuen kunnen niet vaststellen of een bepaald RFID-systeem voldoet aan de beveiligingseisen, welke hieraan dienen te worden. Zodoende is het aan te raden om een certificaat te ontwikkelen waarmee aangegeven wordt of een RFID-systeem voldoet aan de beveiligingseisen. Vanzelfsprekend dient dit een onafhankelijk certificaat te zijn, welke door onafhankelijke deskundigen toegekend wordt;
- standaardisatie van RFID: met betrekking tot de werking van RFID zijn er verschillende standaarden. Hierdoor is het als organisatie niet makkelijk om te bepalen welke standaard gebruikt gaat worden en hoe in de toekomst zorg kan worden gedragen voor dezelfde standaarden. Zodoende zou het praktisch zijn om wereldwijd één standaard te hebben, welke door alle leveranciers van RFID-apparatuur gebruikt wordt.

6.2 Reflectie

Voordat ik begon aan dit onderzoek was ik niet bekend met de mogelijke beveiliging van RFID-tags en het gebruik ervan. Wel waren de privacy risico's bekend door de grote nadruk daarvoor in de algemene media. Tijdens de voorbereiding, het onderzoek en het schrijven van de scriptie kwamen er steeds meer nieuwsberichten over tags en de beveiliging van tags. Enerzijds kwam dit waarschijnlijk omdat ik er sensitiever voor was, maar anderzijds komt er steeds meer aandacht voor RFID. De nieuwsberichten waren niet alleen afkomstig van ICT-informatiebronnen, maar ook van algemene nieuwssites. RFID begint dus steeds meer te leven.
Aan het einde van het onderzoek en het schrijfproces denk ik redelijk op de hoogte te zijn van RFID en de risico's. Ik zie daarbij mogelijkheden om RFID toe te passen, zoals bovenstaand verwoord in het eerste deel van de conclusie (6.1), maar tegelijkertijd zie ik een groot risico:

Moeten wij wel willen dat RFID-tags geïmplanteerd worden in een mens?

Deze vraag wordt ook opgeroepen in Openbaring 13:16-18, welke opgenomen is in de inleiding. Het antwoord van de Bijbel hierop is duidelijk, omdat het beest gezien wordt als satan of antichrist. Persoonlijk denk ik dat het inderdaad (momenteel) niet wenselijk is om RFID-tags te implanteren in mensen, omdat hiermee de persoonlijke integriteit en privacy van mensen ernstig geschonden wordt.

Twee andere aspecten met betrekking tot het gebruik van RFID zijn de keuzevrijheid en het delen van een RFID-tag.

Keuzevrijheid
Tijdens het debat van de technologiecommissie van de Tweede Kamer (zie 3.1) is naar voren gekomen dat consumenten de grootst mogelijke keuzevrijheid moeten hebben met betrekking tot de acceptatie van RFID. Dit is een goed idee, maar dan moet er een breed draagvlak gecreëerd worden door middel van voorlichting. Een andere optie is om RFID voor sommige toepassingen verplicht te stellen en dan door een onafhankelijke deskundige (bijvoorbeeld RE) vast laten stellen dat de toepassing veilig is en voldoet aan alle relevante wetgeving.

Het delen van een RFID-tag
Als de toepassingen van RFID toenemen, kan het gebeuren dat één individu meerdere RFID-tags bij zich heeft (zowel geïmplanteerd als niet geïmplanteerd). De vraag is of het dan de voorkeur heeft om meerdere toepassingen te combineren op één RFID. Dit is technisch gezien mogelijk, maar daarvoor moeten extra veiligheidsmaatregelen getroffen worden, zodat organisaties niet elkaars gegevens kunnen gebruiken. Hiermee neemt het risico van volgbaarheid natuurlijk wel toe.

Literatuur

Boeken

Lahiri, S., *RFID Sourcebook*. International Business Machines Corporation, 2006.

NOREA, *IT-auditing aangeduid. NOREA geschrift No 1*. NOREA, 1998.

Schultz, R.A., *Contemporary Issues in Ethics and Information Technology*. IRM Press, 2006.

Wireless Communication ReferencePoint Suite. SkillSoft Corporation, 2002.

Websites

2005 Privacy Legislation Related to Radio Frequency Identification (RFID). National Conference of State Legislatures, 2006. Available from: <http://www.ncsl.org/programs/lis/privacy/rfid05.htm> [Accessed 1 april 2006].

2006 Privacy Legislation Related to Radio Frequency Identification (RFID). National Conference of State Legislatures, 2006. Available from: <http://www.ncsl.org/programs/lis/privacy/rfid06.htm> [Accessed 1 april 2006].

AB 1489 Assembly Bill – CHAPTERED. Legislative Counsel of California, 2005. Available from: <http://www.leginfo.ca.gov/pub/bill/asm/ab_1451-1500/ab_1489_bill_20050718_chaptered.html> [Accessed 1 april 2006].

AD.nl – 24 uur per dag actueel nieuws /. AD.nl, 2006. Available from: <http://www.ad.nl/fun/bizar/article153182.ece> [Accessed 19 februari 2006].

Beveiliging eerste generatie RFID-chips laat te wensen over. Tweakers.net, 2006. Available from: <http://tweakers.net/nieuws/41183> [Accessed 9 april 2006].

Bill Tracking – 2004 session. Virginia General Assembly, 2004. Available from: <http://leg1.state.va.us/cgi-bin/legp504.exe?041+ful+CHAP0783> [Accessed 1 april 2006].

Bill Tracking – 2004 session. Virginia General Assembly, 2004. Available from: <http://leg1.state.va.us/cgi-bin/legp504.exe?041+ful+CHAP0660> [Accessed 1 april 2006].

Bill Tracking – 2004 session. Virginia General Assembly, 2004. Available from: <http://leg1.state.va.us/cgi-bin/legp504.exe?041+ful+CHAP0665> [Accessed 1 april 2006].

Blarkom, G.W. van, en drs. J.J. Borking, *Beveiliging van persoonsgegevens. Achtergrondstudies en Verkenningen 23*. Registratiekamer, 2001. Available from: <http://www.cbpweb.nl/downloads_av/AV23.pdf> [Accessed 17 april 2006].

Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag. Auto-ID Center, 2003. Available from: <http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf> [Accessed 1 april 2006].

Emerce – Technologie nieuws: VIP-chips in Rotterdamse Baja Beach Club. Emerce, 2004. Available from: <http://www.emerce.nl/nieuws.jsp?id=277589> [Accessed 10 februari 2006].

EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Conformance Requirements Version 1.0.2. EPCglobal Inc™, 2004. Available from: <http://www.epcglobalinc.org/standards_technology/EPCglobal%20Class-1%20Generation-2%20UHF%20RFID%20Conformance%20V1%200%202.pdf> [Accessed 1 april 2006].

H5929. State of Rhode Island General Assembly, 2005. Available from: <http://www.rilin.state.ri.us/BillText/BillText05/HouseText05/H5929.htm> [Accessed 1 april 2006].

http://legisweb.state.wy.us/2005/enroll/hb0258.pdf. Wyoming State Legislature, 2005. Available from: <http://legisweb.state.wy.us/2005/enroll/hb0258.pdf> [Accessed 1 april 2006].

InformationWeek | RFID Supply Chain | RFID Production To Increase 25-Fold In Four Years | janua. InformationWeek, 2006. Available from: <http://www.informationweek.com/news/showArticle.jhtml?articleID=177101563> [Accessed 10 februari 2006].

News from the States, Summer 2004. National Conference of State Legislatures, 2006. Available from: <http://www.ncsl.org/programs/lis/CIP/CIPCOMM/summer04.htm#RFID> [Accessed 1 april 2006].

Radio Frequency Identification (RFID) | Europa – Information Society. European Commission, 2006. Available from: <http://europa.eu.int/information_society/policy/rfid/index_en.htm> [Accessed 1 april 2006].

RFID Journal – Pfizer Using RFID to Fight Fake Viagra. RFID Journal, 2006. Available from: <http://www.rfidjournal.com/article/articleview/2075/1/1/> [Accessed 10 februari 2006].

RFID-Chips. Kans of gevaar?. ChristenUnie Tweede Kamer, 2005. Available from: <http://www.christenunie.nl/l/library/download/19705> [Accessed 1 april 2006].

Risiken und Chancen des Einsatzes von RFID-Systemen. Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Bundesamt für Sicherheit in der Informationstechnik, 2004. Available from: < http://www.bsi.de/fachthem/rfid/RIKCHA.pdf > [Accessed 17 april 2006].

TECHNICAL REPORT. 13.56 MHz ISM Band Class 1Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0. Auto-ID Center, 2003. Available from: <http://www.epcglobalinc.org/standards_technology/Secure/v1.0/HF-Class1.pdf> [Accessed 1 april 2006].

TECHNICAL REPORT. 860MHz–930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1. Auto-ID Center, 2002. Available from: <http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf> [Accessed 1 april 2006].

The EPCglobal Architecture Framework. EPCglobal Final Version of 1 July 2005. EPCglobal, 2005. Available from: <http://www.epcglobalinc.org/standards_technology/Final-epcglobal-arch-20050701.pdf> [Accessed 1 april 2006].

Utah Legislature HB0185. Utah State Legislature, 2005. Available from: <http://www.le.state.ut.us/~2005/bills/hbillenr/hb0185.htm> [Accessed 1 april 2006].

Webwereld | Boekhandelsgroep voorziet boeken van rfid-tags. Webwereld, 2006. Available from: <http://www.webwereld.nl/ref/newsletter/39825> [Accessed 19 februari 2006].

Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens). Staatsblad, 2000. Available from: <http://www.cbpweb.nl/downloads_wetten/WBP.PDF> [Accessed 17 april 2006].

ZDNet.be news. ZDNet.be, 2006. Available from: <http://www.zdnet.be/news.cfm?id=53006&mxp=109> [Accessed 10 februari 2006].

A Verklarende woordenlijst

Begrip	Uitleg in hoofdstuk
Actief	2.1.2
Actuator	2.4
ALOHA	2.6.1
Annunciator	2.4
Antenne energie	2.3.3
Antenne footprint	2.3.1
Antenne polarisatie	2.3.2
Anti-collision algoritme	2.6.1
Attenuator	2.3.3
Autonoom	2.2
Betrokkene	3.2
Beveiliging	3.2
Beveiligingsniveau	3.2
Bewerker	3.2
Bijzondere persoonsgegevens	3.2
Beperkte geheugencapaciteit	4.2
Cbp	3.2
Clock extractor	2.1.1
College Bescherming Persoonsgegevens	Zie Cbp
Communicatie infrastructure	2.6
Communicatie interface	2.2.6
Continuïteit	4
Controller	2.2.5
Discovery Services	Zie DS
Doelbinding	3.2
DS	2.7.4
Edge interface	2.5.1
Edge system	Zie edge interface
EEPROM	2.1.6
Effective radiator power	Zie ERP
Electrically Erasable Programmable Read Only Memory	Zie EEPROM
Electronic Product Code	Zie EPC
Energiebron	2.1.2
Enterprise back end	2.5.4
Enterprise back-end interface	2.5.3
EPC	2.7.1
EPC Information Services	Zie EPCIS
EPC Manager	2.7.1
EPCglobal	2.7
EPCglobal middleware	2.7.3

EPCglobal Network	2.7
EPCIS	2.7.5
ERP	2.3.3
Exclusiviteit	4
Ferroelectric Random Access Memory	Zie FRAM
Flash memory	2.1.6
Footprint	Zie antenne footprint
FRAM	2.1.6
Gegevensverkeer met landen buiten de EU	3.2
Gen 2	2.7.1
HF	2.6
High frequency	Zie HF
Host en software system	2.5
ID System	2.7.2
Input/output channels voor sensors, actuators en annunciators	2.2.4
Integriteit	4
Interactief	2.2
Issuing Agency	2.7.1
Kill-commando	2.7.1
Kwaliteit	3.2
LF	2.6
Logic	2.1.1
Low frequency	Zie LF
Man-in-the-middle attack	Zie MITM
Memory (reader)	2.2.3
Memory (tag)	2.1.1
Microchip	2.1.1
Microprocessor	2.2.2
Microwave frequency	2.6
Middleware	2.5.2
MITM	4.1
Modulated backscatter	2.2.1
Modulator	2.1.1
Netwerk interface	2.2.6
Netwerk reader	Zie netwerk interface
Object Name Service	Zie ONS
ONS	2.7.1
Passief	2.1.1
Persoonsgegevens	3.2
Power	2.2.7
Power control	2.1.1
Power rectifier	Zie power control
Processor	Zie microprocessor
Radio frequency identification	Zie RFID

Read redundancy	Zie read robustness
Read robustness	2.6.4
Reader	2.2
Reader antenne	2.3
Reader collision	2.6.2
Read-once	Zie RO
Read-write	Zie RW
Receiver	2.2.1
Rechten van de betrokkenen	3.2
Rechtmatige grondslag	3.2
RFID	2
RO	2.1.4
RW	2.1.6
Semi-actief	2.1.3
Semi-passief	Zie semi-actief
Sensor	2.4
Seriële interface	2.2.6
Seriële reader	Zie seriële interface
Singulation protocol	2.6.1
Tag	2.1
Tag collision	2.6.1
Tag readability	2.6.3
TDMA	2.6.2
Time division multiple access	Zie TDMA
Transceiver	2.2.1
Transmitter (reader)	2.2.1
Transmitter (tag)	2.1.2
Transmitter type	2.2.1
Transparantie	3.2
Transponder	2.1.2
Transponder type	2.2.1
Tree Walking	2.6.1
UHF	2.6
Ultra high frequency	Zie UHF
Verwerker	3.2
Verwerking door een bewerker	3.2
Verwerking van persoonsgegevens	3.2
Very high frequency	Zie VHF
VHF	2.6
Voornemen en melden	3.2
Wbp	3.2
Wet Bescherming Persoonsgegevens	Zie Wbp
WORM	2.1.5
Write once, read many	Zie WORM

B Overzicht van figuren en tabellen

B.1 Figuren

B.2 Tabellen

C Maatregelen voor een RFID-systeem

In tabel 13 zijn de maatregelen opgenomen voor een RFID-systeem. Voor elke maatregel is onderscheid gemaakt naar de manier van het toepassen van een RFID-systeem, namelijk als:

- middel om producten te identificeren;
- extern middel om individuen te identificeren;
- intern middel om individuen te identificeren.

Nr.	Maatregel	Middel identificatie producten	Extern middel identificatie individuen	Intern middel identificatie individuen
1	De communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden.	Afhankelijk van risicoanalyse	Afhankelijk van risicoklasse	Afhankelijk van risicoklasse
2	De communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden.	Afhankelijk van risicoanalyse	Afhankelijk van risicoklasse	Afhankelijk van risicoklasse
3	De communicatie tussen de tag en de reader dient op geen enkele wijze verstoord of geblokkeerd te kunnen worden.	Ja	Ja	Ja
4	De reader dient altijd de verkregen gegevens (van de tags) vast te leggen/bewaren.	Ja	Ja	Ja
5	De tag dient (tijdelijk) gedeactiveerd te worden indien deze (tijdelijk) niet meer noodzakelijk is.	Afhankelijk van risicoanalyse	Ja	Ja
6	De tag dient zodanig bevestigd te zijn op het object dat het verwijderen ervan onmogelijk is.	Ja	Ja	Ja
7	De tag en reader dienen zich te authenticeren ten opzichte van elkaar.	Afhankelijk van risicoanalyse	Afhankelijk van risicoklasse	Afhankelijk van risicoklasse
8	Een RFID-systeem welke (bijzondere) persoonsgegevens verwerkt dient te voldoen aan de Wet Bescherming Persoonsgegevens.	Nee	Ja	Ja
9	Een risicoanalyse dient uitgevoerd te worden voor de back-end systemen en de communicatie en voor deze risico's dienen maatregelen getroffen te worden.	Ja	Ja	Ja
10	Gegevens op de tag dienen niet gewijzigd te kunnen worden door ongeautoriseerden.	Ja	Ja	Ja
11	Het deactiveren van de tag door onbevoegden dient onmogelijk gemaakt te worden.	Ja	Ja	Ja

Tabel 13: Maatregelen voor een RFID-systeem afhankelijk van de manier van toepassen

De maatregelen 1, 2 en 7 voor een RFID-systeem zijn in relatie tot de risicoklassen van de Wbp uitgewerkt in tabel 14.

Nr.	Maatregel	Risicoklasse I	Risicoklasse II	Risicoklasse III
1	De communicatie tussen de tag en de reader dient niet afgeluisterd te kunnen worden.	Geen aanvullende maatregelen.	Versleutelen van de communicatie met een algemeen geaccepteerde cryptografiemethode, welke het risico van onbevoegde ontsleuteling uitsluit.	Geen aanvullende maatregelen ten opzichte van risicoklasse II.
2	De communicatie tussen de tag en de reader dient op geen enkele wijze gewijzigd te kunnen worden.	Geen aanvullende maatregelen.	Geen aanvullende maatregelen.	Het gebruik van een checksum om de integriteit van de gegevens te waarborgen.
6	De tag en reader dienen zich te authenticeren ten opzichte van elkaar.	Logische toegangsbeveiliging, dus een zwakke authenticatie-methode moet in ieder geval gebruikt worden.	Authenticatie gebruiken welke niet onderschept kan worden door onbevoegden (bijvoorbeeld een challenge-response systeem).	Geen aanvullende maatregelen ten opzichte van risicoklasse II.

Tabel 14: Maatregelen 1, 2 en 7 voor een RFID-systeem in relatie tot de risicoklassen Wbp