TECHN 37

Periodieke publicatie van Smals

Januari 2014

Het ABC van RFID

Ontstaan, Technologieën en Toepassingen

Tania Martin heeft een doctoraat in Ingenieurswetenschappen. Sinds september 2013 werkt ze als consultant bij de sectie Onderzoek van Smals. Ze is gespecialiseerd in cryptologie en bestudeert de mogelijkheid om nieuwe bruikbare oplossingen en technologieën te integreren voor de sector van de gezondheidszorg en voor de sociale zekerheid.

Contact: 02 787 56 05
Tania.Martin@smals.be

1. Inleiding

Radiofrequentie-identificatie (RFID[1]) wordt vaak bestempeld als een nieuwe trend. RFID is een contactloze technologie waarmee op afstand en zonder visueel contact transponders, in het algemeen “tags” genoemd, geïdentificeerd en/of geauthenticeerd kunnen worden. De voorziening waarmee tags uitgelezen kunnen worden, heet "lezer", hoewel de naam "interrogator" geschikter zou zijn.

Het is moeilijk om RFID nauwkeurig te definiëren, omdat iedereen zijn eigen visie erop heeft. Twee fundamentele eigenschappen komen echter systematisch terug: elke tag heeft een unieke identificatie en de tags antwoorden op query’s die uitgevoerd worden door lezers, maar ze kunnen niet met elkaar communiceren. In mei 2009 heeft de Europese Commissie de volgende definitie in haar aanbeveling 2009/287/EC [1] gepubliceerd:

“Radiofrequentie-identificatie (RFID) [is] het gebruik van elektromagnetische golven of de koppeling van reactieve velden in de radiofrequentie van het spectrum voor de communicatie naar of van een RFID-tag met behulp van verschillende modulatie- of coderingstechnieken of alleen voor het aflezen van de identificatie van een RFID-tag of andere daarin opgeslagen gegevens.” (Artikel 3.a).

Met dergelijke definitie blijven er echter dubbelzinnigheden bestaan. In het bijzonder de grens tussen RFID en contactloze chipkaarten blijft vaag. De producenten van de chipkaart verkiezen in het algemeen om een onderscheid te maken tussen de twee concepten, omdat de term RFID aan zwakke beveiliging doet denken. Daartegenover staan de producentenvan RFID die contactloze chipkaarten beschouwen als een soort identificatie via radiofrequentie. Tot slot ziet men sinds kort dat NFC[2] zich losmaakt van RFID. Welnu, NFC is op zich slechts een uitbreiding van bepaalde normen van RFID. Deze technologie onderscheidt zich echter door het feit dat elke NFC-voorziening - meestal een gsm - tegelijkertijd kan functioneren als tag en als lezer. Twee gsm’s kunnen dus met elkaar communiceren door NFC te gebruiken om zo behoorlijke hoeveelheden informatie uit te wisselen waarbij fysieke koppeling niet vereist is, in tegenstelling tot bijvoorbeeld Bluetooth.

Dit document zal vooral RFID bespreken, maar ook andere technologievormen gebaseerd op radiofrequentie, zoals NFC of contactloze chipkaarten, komen kort aan bod.

[1] *Radio Frequency IDentification*.

[2] *Near Field Communication*.

De structuur van dit document is de volgende: sectie 2 beschrijft kort het ontstaan van RFID. Sectie 3 leidt de RFID-technologie in, met in het bijzonder de fysieke eigenschappen van tags. Sectie 4 geeft enkele concrete voorbeelden van toepassingen van RFID. Tot slot bevat sectie 5 de conclusie van dit document.

2. Ontstaan van RFID

Hoewel RFID de laatste jaren sterk gegroeid is, begint het verhaal in de helft van de 20ste eeuw. De uitvinding van deze technologie wordt in het algemeen geassocieerd met het ontwerp van het IFF-systeem[3] van de Royal Air Force waarmee de vliegtuigen van de geallieerden tijdens de Tweede Wereldoorlog geïdentificeerd konden worden. Het is onmogelijk om de creatie van RFID toe te schrijven aan een enkele persoon, maar het is wel duidelijk dat Charles A. Walton een grote bijdrage leverde met de publicatie van verschillende octrooien, in het bijzonder het octrooi dat geregistreerd werd in 1973 voor een passieve transponder [2].

Vandaag de dag is RFID met echte rekenkracht het resultaat van de bundeling van kennis in de domeinen van elektronische chips en van radiofrequentie-identificatie. De jaren 80 waren een beslissend keerpunt in de geschiedenis van contactloze technologie met de eerste commerciële toepassingen zoals de identificatie van vee en tolhuizen op autosnelwegen.

RFID kende pas echt een groei in de jaren 90, voornamelijk met de massale verkoop van de tag Mifare Classic[4] [3] ontwikkeld door Mikron (gekocht door Philips Semiconductors, dat vandaag NXP Semiconductors heet) waar honderden miljoenen kopies werden verkocht sinds zijn introductie op de markt. Het grote publiek werd zich pas bewust van de grootte van het RFID-fenomeen met de uitrol van applicaties die nu dagelijks gebruikt worden, zoals de kaarten voor openbaar vervoer, dieridentificatie of zelfs elektronische paspoorten.

3. De RFID-technologie

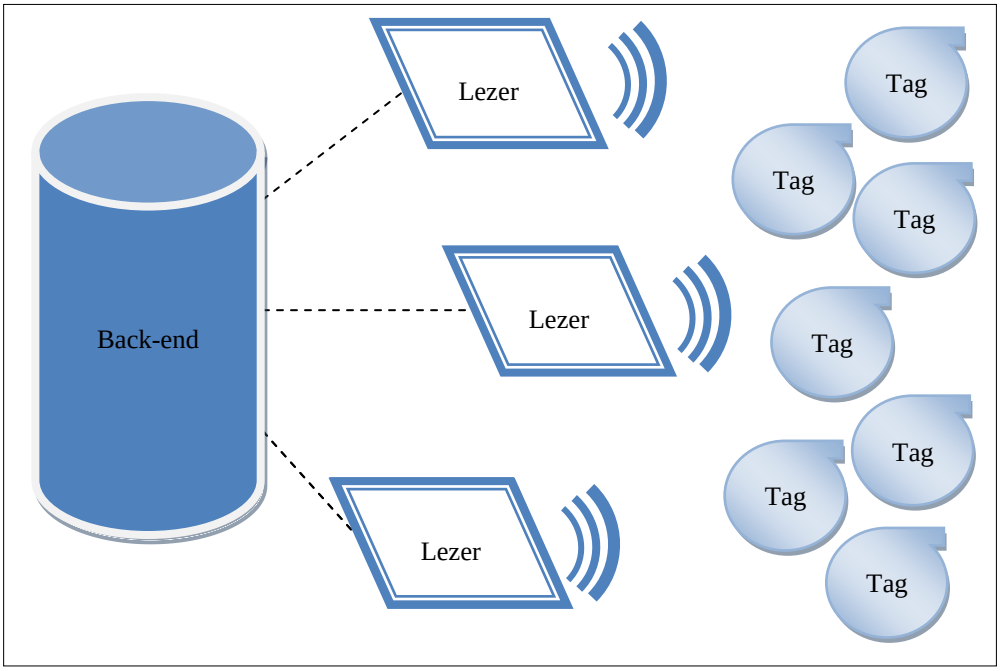
Deze sectie stelt een overzicht voor van de RFID-technologie, gaande van de basisarchitectuur van de systemen die gebaseerd zijn op RFID tot de eigenschappen van bestaande tags en standaarden.

3.1. Architectuur van een RFID-systeem

Zoals voorgesteld in figuur 1 bestaat een RFID-systeem in het algemeen uit drie soorten voorzieningen: tags, lezers en een centrale server die op de achtergrond draait, genaamd *back-end*. Deze entiteiten interageren samen via communicatieprotocols - waar berichten uitgewisseld worden - met de bedoeling om een gegeven doelstelling te bereiken (bv. de tags van het systeem identificeren of authenticeren).

[3] *Identify Friend or Foe*.

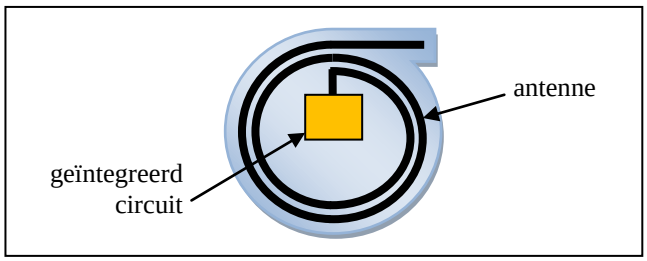
[4] De tag Mifare Classic werd op de markt gebracht in 1995 en was het eerste RFID-product dat voor weinig geld kon opgenomen worden in een contactloze chipkaart waardoor de massaproductie van deze tag mogelijk werd en dit bijdroeg tot zijn succes. Om een voorbeeld te geven: de tag Mifare Classic was aanwezig in meer dan 80 % van de oplossingen op de markt voor contactloze biljettiek in 2012.



Figuur 1: Een typische RFID-architectuur

RFID-tag

Een tag is een transponder, dit wil zeggen een geïntegreerd circuit gekoppeld aan een antenne zoals voorgesteld in figuur 2, ingebouwd in een object op afstand. Er kunnen verschillende voedingsbronnen zijn: ofwel de voedingsbron van de tag zelf, ofwel die van een RFID-lezer. Zijn geheugen kan variëren van enkele honderden bits (zoals voor de EPC-tags[5] [4]) tot enkele kilobytes (zoals de contactloze chipkaarten [5] [6]).

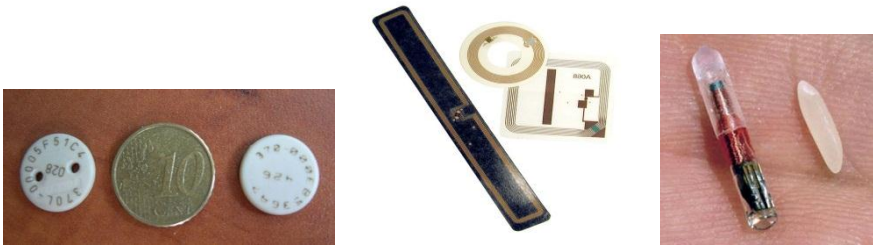


Figuur 2: Vereenvoudigde voorstelling van een RFID-tag

Er kunnen verschillende niveaus bestaan voor de rekenkracht. Bepaalde tags kunnen enkel logische handelingen uitvoeren, terwijl andere symmetrische cryptografie, hashing-functies of zelfs asymmetrische cryptografie kunnen uitvoeren.

[5] *Electronic Product Code*.

Van een tag wordt algemeen gezegd dat hij “violable” of “falsifiable” is; een aanvaller kan gemakkelijk gegevens bemachtigen die opgeslagen liggen in het geheugen van de tag. De communicatieafstand ligt tot slot tussen enkele centimeters en enkele decimeters. De verschillende eigenschappen van RFID-tags worden in de volgende sectie verder uitgelegd.



Figuur 3: Verschillende soorten RFID-tags (bron: Sancho, Grika, LightWarrior/WikimediaCommons)

RFID-lezer

Een lezer is een transceiver. Hij kan communiceren met een tag wanneer deze laatste zich in zijn elektromagnetisch veld bevindt. Hij kan ook communiceren met andere lezers of met de back-end via andere kanalen (bv. Ethernet of Wi-Fi).

Een lezer is krachtiger dan een tag. Zijn rekenkracht komt in de buurt van die van een kleine computer. Hij kan vast (bv. aan de ingang van een gebouw) of mobiel (bv. een smartphone) zijn en wordt algemeen beschouwd als “inviolable”.

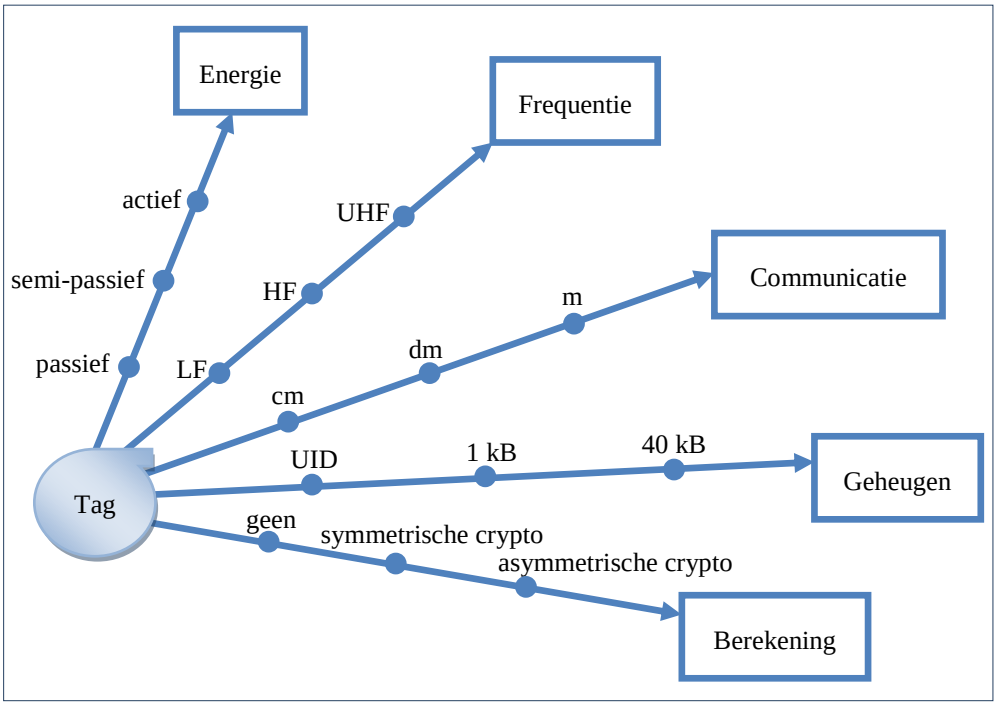
Back-end

De back-end bevat gewoonlijk een database die informatie bijhoudt in verband met elke tag en elke lezer van het systeem (bv. de identificaties van de tags). De back-end kan echter ook een soort switch zijn die enkel de communicaties tussen de lezers doorstuurt. Hij communiceert in ieder geval enkel met de lezers.

Opmerking: Een back-end is niet altijd vereist in een RFID-systeem. Bijvoorbeeld: wanneer een systeem slechts bestaat uit een enkele autonome lezer, dan kan deze voorziening ook de rol van back-end spelen. In andere systemen zijn de back-end en de lezers allemaal samen verbonden via een beveiligd kanaal en kunnen ze dus gezien worden als een enkele entiteit, eenvoudigweg "lezer" genoemd.

3.2. Eigenschappen van de RFID-tags

Een volledige rangschikking van de RFID-technologie opmaken is moeilijk gezien het aantal eigenschappen dat moet beschouwd worden om een tag te definiëren. Alleen tijdens het ontwerp van een RFID-applicatie is het mogelijk om de technologische behoeften te definiëren en later het meest geschikte type tag te identificeren. De voornaamste eigenschappen van RFID-tags worden voorgesteld in figuur 4 en worden hieronder beschreven.



Figuur 4: Hoofdeigenschappen van een RFID-tag

Energiebron

Men onderscheidt twee belangrijke klassen tags naargelang de beschouwde energiebron. De tags die voor hun interne berekeningen en hun communicaties met de lezers gevoed worden door hun eigen batterij worden "actief" genoemd. De tags gevoed door het elektromagnetisch veld van de lezers worden “passief” genoemd. Tot slot zijn er de "semi-passieve" tags die hun eigen batterij voor de berekeningen en ook de energie van de lezer voor de communicaties gebruiken. Dit laatste type tags is in veel mindere mate aanwezig op de markt dan de andere.

Opmerking: De terminologie actief/passief/semi-passief heeft niets te maken met de rekenkracht of de communicatiecapaciteit van een tag, maar enkel met de manier waarop hij gevoed wordt.

De meeste tags die vandaag gebruikt worden, zijn passief en de eenvoudige term "RFID" wordt in het algemeen gebruikt om ze aan te duiden. Bijvoorbeeld: de tags voor de dierentattoo, om de barcodes te vervangen, voor de paspoorten of tickets voor openbaar vervoer zijn passief, terwijl de tags voor het openen van autodeuren of de tolhuizen op snelwegen actief zijn. Verder in dit document zal de term “RFID-tag(s)" verwijzen naar passieve tags.

Frequentie

De RFID-technologie functioneert voornamelijk in vijf frequentiebanden die bepaald zijn door de standaard ISO/IEC 18000 [7]. Deze frequenties worden hieronder opgelijst, samen met de meest representatieve toepassingsdomeinen.

- 124 – 135 kHz (LF[6]): dieridentificatie.
- 13,56 MHz (HF[7]): betaling, toegangscontrole, biljettiek.
- 433 MHz (UHF[8]): toegangscontrole voor parkings.
- 860 – 960 MHz (UHF): logistieke keten.
- 2,45 GHz (UHF): tolhuizen op autosnelwegen, identificatie van containers.

Drie van de vijf frequenties zijn duidelijk de meest gebruikte voor de uitgerolde RFID-applicaties. De eerste is de frequentie 124 – 135 kHz (LF), omdat deze goed kan doordringen in metaal of vloeibare omgevingen. De tweede is de frequentie 13,56 MHz (HF), omdat ze voldoende energie aan de tag geeft om cryptografische bewerkingen uit te voeren. De laatste is de frequentie 860 – 960 MHz (UHF), omdat ze betere communicatieafstanden biedt in het geval van passieve tags.

Natuurlijk is de keuze van frequentie ingewikkelder dan wat hier voorgesteld wordt en hangt veel af van andere parameters zoals de grootte van de antenne, de regulaties op de frequentiebanden per land waar de RFID-applicatie uitgerold wordt, en ook van de productiekosten.

Communicatieafstand

Meerdere parameters beïnvloeden de communicatieafstand tussen tag en lezer, zoals de frequentie, het zendvermogen, de omgeving, de antenne, etc. Voor de passieve tags zijn de drie volgende communicatieafstanden mogelijk naargelang de frequentiebanden:

- Lage Frequentie (LF): enkele centimeters.
- Hoge Frequentie (HF): enkele centimers tot enkele decimeters.
- Ultra-Hoge Frequentie (UHF): enkele meters.

Opmerking: Deze afstanden worden gegeven naargelang de standaarden en specificaties van de fabrikanten. Nochtans hebben meerdere studies aangetoond dat deze afstanden aanzienlijk vergroot kunnen worden met een geschikte lezer [8] [9].

Geheugen

Zoals voor de andere parameters hangt de hoeveelheid beschikbaar geheugen op een tag af van de behoeften van de RFID-applicatie. Men moet minimum enkele tientallen bits hebben om de UID[9] van de tag te kunnen stockeren. Deze identificatie wordt in principe vastgelegd door de fabrikant en kan achteraf niet meer gewijzigd worden. Naast deze UID beschikt de tag in het algemeen over het aanvullend EEPROM-geheugen[10], normaal gezien van een of twee kilobytes. Dit geheugen kan in uitzonderlijke gevallen veel groter zijn, bijvoorbeeld 30 à 70 kilobytes voor een elektronisch paspoort.

[6] *Low Frequency*.

[7] *High Frequency*.

[8] *Ultra-High Frequency*.

[9] *Unique IDentifier*.

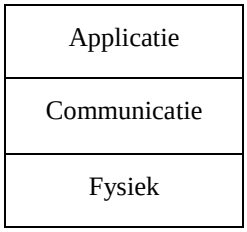
[10] *Electrically Erasable Programmable Read-Only Memory*.

Rekenkracht

De tags zijn duidelijk zeer beperkt op het vlak van berekeningen. Sommige kunnen enkel eenvoudige logische bewerkingen uitvoeren (bv. een ontvangen en een opgeslagen wachtwoord met elkaar vergelijken). Ondanks alles waren de jaren 90 getuige van de opkomst van passieve tags met crypografische capaciteiten, vaak een algoritme voor stroomvercijfering[11]. Vandaag de dag zijn algoritmes voor blokvercijfering[12] zoals 3DES[13] of AES[14] op de passieve tags meer dan courant. Hoewel nog steeds duur op de markt, zijn sommige passieve tags in staat tot asymmetrische cryptografie, bijvoorbeeld voor elektronische paspoorten. Er bestaat dus een brede waaier aan tags met een verschillende rekenkracht die de integrators proberen te minimaliseren voor een gegeven applicatie.

3.3. Standaarden

Momenteel bestaan er verscheidene standaarden verbonden aan RFID, zowel voor de fysieke laag en de communicatielaag als voor de applicatielaag, voorgesteld in figuur 5. Deze sectie stelt de belangrijkste standaarden voor in verband met contactloze technologie.



Figuur 5: Vereenvoudigd lagenmodel voor RFID

ISO/IEC 14443 [10] en ISO/IEC 15693 [11]

Deze standaarden dekken de fysieke laag en de communicatielaag van de frequentieband 13,56 MHz en vormen het draagpunt van de meeste applicaties die niet steunen op eigen normen.

De standaard ISO/IEC 14443 wordt gebruikt voor de tags van het type *proximity* (communicatieafstand van ongeveer 10 centimeter), terwijl de standaard ISO/IEC 15693 bedoeld is voor tags van het type *vicinity* (communicatieafstand van ongeveer 80 centimeter). Bijvoorbeeld: elektronische paspoorten gestandaardiseerd door de ICAO[15] [12] zijn gebaseerd op de standaard ISO/IEC 14443.

[11] Soort symmetrische vercijfering (d.i. dezelfde sleutel wordt gebruikt om een bericht te vercijferen en ontcijferen) waarbij de te vercijferen tekst bit per bit opgeteld wordt bij een zogenaamde vercijferde reeks. Deze laatste wordt zelf afgeleid van de sleutel.

[12] Soort symmetrische vercijfering waarbij de te vercijferen tekst opgesplitst wordt in blokken van een vaste afmeting (bv. 128 bits), en waarbij elk blok vercijferd wordt met de sleutel.

[13] *Triple Data Encryption Standard*.

[14] *Advanced Encryption Standard*.

[15] *International Civil Aviation Organization*.

EPC Class 1 Gen 2 [4]

De uitrol van tags aan zeer lage kostprijs werd aangedreven door het Auto-ID Center, een consortium dat in 1999 opgericht werd in de Verenigde Staten. Deze organisatie, momenteel bestaande uit EPC Global Network en uit verschillende Auto-ID Labs, heeft als doel om RFID in logistieke ketens te standaardiseren en te promoten. De standaard EPC Class 1 Gen 2 gepubliceerd door het EPC Global Network wordt momenteel uitgebreid uitgerold en gevolgd door vele producenten. Het dekt de drie lagen (fysiek, communicatie en applicatie).

NFC

NFC is een draadloze communicatietechnologie die functioneert op de frequentieband 13,56 MHz. Deze technologie is ontworpen door een consortium[16] dat in 2004 opgericht werd door Sony, Philips en Nokia. Momenteel telt het meer dan 150 leden.

Deze technologie is compatibel met RFID – in het bijzonder met de standaard ISO/IEC 14443 – en zorgt voor het lezen en emuleren van tags. Bijgevolg kunnen twee NFC-apparaten, vaak gsm's, communiceren met behulp van de RFID-technologie. Dit laat veel sneller communicaties met een zwak debiet en op korte afstand toe dan Bluetooth- of Wi-Fi-communicaties.

De standaard ISO/IEC 18092 [13] definieert de belangrijkste eigenschappen van NFC en stelt een precies formaat (NDEF[17]) voor om gegevens te stockeren en uit te wisselen. Hij heeft als doel de interoperabiliteit van NFC-apparaten te versterken.

Hoewel men de neiging heeft om een onderscheid te maken tussen NFC en RFID, moet men toegeven dat NFC simpelweg een uitbreiding is van bepaalde standaarden van RFID. De veiligheidsproblemen van NFC zijn dus te vergelijken met die van RFID. De oplossingen voor deze problemen kunnen nochtans verschillen, bijvoorbeeld door de capaciteiten van een gsm te benutten.

Opmerking: Het is mogelijk om een applicatie te ontwikkelen die compatibel is met de NFC-technologie zonder noodzakelijkerwijs gsm's te gebruiken door in een lezer-tag-model te blijven zoals hierboven beschreven.

4. Voorbeelden van toepassingen

Er bestaan veel industriële toepassingen die RFID gebruiken en ze zijn ook uiteenlopend. Ze kunnen in drie categorieën geplaatst worden: (i) toegangscontrole, (ii) opsporing en opvolging van productie en (iii) beveiligde applicatie. Deze sectie stelt elk domein voor en illustreert ze met concrete voorbeelden uit het dagelijks leven.

4.1. Toegangscontrole

Al verschillende decennia lang werden chipkaarten gebruikt voor toegangscontrole. De komst van contactloze technologie op de markt heeft echter voor een tot dan toe ongekend gebruiksgemak gezorgd. De toegangscontrole werd immers eerst uitgevoerd met infrarood passen, later met magneetbandkaarten en uiteindelijk met contactchipkaarten. Het grootste nadeel van deze laatste toepassing is dat de gebruiker zijn kaart in de lezer moet steken, wat een significant tijdverlies inhoudt, voornamelijk bij de toegangscontrole op grote schaal. Het

[16] http://www.nfc-forum.org/

[17] *NFC Data Exchange Format*.

onderhoud van lezers kan daarenboven moeilijk blijken, aangezien de lezers direct toegankelijk zijn en vaak beschadigd worden. De RFID-technologie biedt de mogelijkheid om deze problemen te beperken en om de toegangscontrole te vergemakkelijken door de tag te integreren in een kaart, een sleutel of een armband. Zo moeten de gebruikers enkel het object voor de RFID-lezer houden die de toegangscontrole beheert.

Skipas

De toegangscontrole in skistations heeft in grote mate baat gehad bij de RFID-technologie. In het algemeen wordt de standaard ISO/IEC 15693 gevolgd die een iets langere communicatieafstand toelaat dan de standaard ISO/IEC 14443. RFID vergemakkelijkt het leven van de skiër: hij moet zijn skipas niet meer tussen zijn spullen zoeken; hij steekt gewoon zijn pas (waarschijnlijk in zijn zak) op de plaats van de lezer. De introductie van RFID is ook een troef voor bedrijven die mechanische skiliften maken, omdat deze technologie de stroom skiërs versnelt terwijl een systematische controle behouden blijft.

Figuur 6: Mechanische skiliften gebaseerd op RFID (bron: Baileypalblue/WikimediaCommons)

Automobielsector

Sinds het begin van de jaren 90 heeft de automobielindustrie eveneens RFID geïntegreerd om de veiligheid van toegangscontrole te verhogen. Met een RFID-tag geïntegreerd in een autosleutel kan allereerst een auto automatisch geopend worden zodra de bestuurder zijn voertuig nadert. In deze systemen kan RFID eveneens gebruikt worden als oplossing om de auto te starten: wanneer de bestuurder zijn sleutel in de startcilinder steekt, zal het voertuig controleren of de RFID-tag aanwezig is. Als dit niet het geval is, dan zal de auto niet starten. Deze antistart-systemen zijn in het algemeen gebaseerd op de LF-frequentiebanden die tussen 100 en 135 kHz liggen.

Tolhuizen op autosnelwegen

Het gebruik van RFID in tolhuizen op autosnelwegen is relatief oud. Zoals bij skistations is het doel ook hier om het leven van de bestuurders en van het bedrijf te vergemakkelijken. De bestuurder moet niet volledig stoppen aan de hefboom van het tolhuis. Bepaalde systemen laten zelfs toe dat de bestuurder op volle snelheid het tolhuis voorbij rijdt. Het bedrijf wint hier ook aan efficiëntie en kan zijn kosten drukken. RFID automatiseert de controles waardoor het bedrijf minder personeel moet voorzien in het tolhuis. Aangezien de vereiste leesafstand relatief groot is (ongeveer 5 meter) kan het gebruik van actieve UHF-tags een geschikte oplossing zijn.

Openbaar vervoer

In dit type toepassing biedt RFID ook een voordeel aan de reiziger en aan het vervoersbedrijf. Voor de reiziger is het eenvoudiger omdat hij zijn ticket gewoon voor de lezer moet houden in plaats van het erin te steken. Als het vervoersbedrijf daarenboven zijn tarieven baseert op de afgelegde afstanden, dan moet de reiziger zich niet langer zorgen maken om het aantal zones dat hij doorkruist: hij moet enkel zijn ticket valideren in het begin en aan het einde van zijn reis.

Het vervoersbedrijf kan zijn statistieken over het gebruik van haar infrastructuur veel preciezer bijhouden dan door simpelweg het aantal afgelegde reizen te tellen. De RFID-technologie laat ook aan het bedrijf toe om de namaak van tickets te beperken, omdat het moeilijker is om valse RFID-tags te maken dan valse papieren tickets.

Een groot aantal steden heeft momenteel gekozen voor een systeem voor openbaar vervoer dat gebaseerd is op RFID, zoals Brussel, Parijs, Londen, Amsterdam, Berlijn, New York en Hong Kong. In Brussel lanceerde het openbaarvervoersbedrijf MIVB in 2008 zijn RFID-systeem voor biljettiek, genaamd “MOBIB”, dat het oude systeem zou moeten vervangen dat gebaseerd is op magneetbandkaarten. MOBIB steunt op de standaard Calypso [14] die al in meer dan 20 landen toegepast werd.

Figuur 7: RFID-klapdeur in een metrostation (bron: ProtoplasmaKid/WikimediaCommons)

4.2. Opsporing en opvolging productie

In het logistieke domein is RFID een nieuw alternatief voor barcodes dat twee grote voordelen biedt. Het eerste voordeel is de leesafstand. Barcodes kunnen immers slechts op een zeer korte afstand gelezen worden, terwijl RFID de mogelijkheid biedt om een tag vanop meerdere meters te lezen zonder visueel contact. Deze eigenschap van RFID verhoogt de efficiëntie van het bedrijf aanzienlijk: een pas volstaat om alle paletten in een container te scannen en de status van stocks kan in real time gecontroleerd worden. Het tweede voordeel van RFID is de betere weerstand tegen externe elementen en beschadigingen. Het is duidelijk dat wanneer een barcode geplooid of gescheurd is of vol stof hangt dat het lezen ervan onmogelijk wordt. De leesomstandigheden spelen ook een belangrijke rol. Zo kan een barcode niet gelezen worden als er te veel licht is.

Dieridentificatie

De introductie van RFID voor dieridentificatie gaat terug tot de jaren 80. De technologie wordt gebruikt voor de inventarisering, de productiecontrole en de automatisering van dierenvoeding. De tags worden vastgemaakt aan de oren van de dieren of geïntegreerd in ringen of kettingen, afhankelijk van het soort en de grootte van het dier. RFID kan helpen om de oorsprong van een dier te traceren om kwaliteits- of gezondheidscontroles uit te voeren, bijvoorbeeld om uitbreiding van epidemieën tegen te gaan – de bekendste is de gekkekoeienziekte, of recenter de varkensgriep. Dergelijk gebruik van RFID vereist een volledige interoperabiliteit tussen de verschillende productiebedrijven. Daarom werden bepaalde standaarden gecreëerd, in het bijzonder ISO/IEC 11748 [15] en ISO/IEC 11785 [16] die steunen op de LF-frequentieband 134,2 kHz.

Deze tags kunnen in verschillende vormen voorkomen. Sommige hebben de grootte van een rijstkorrel en worden onderhuids aangebracht met de hulp van een spuit. Andere hebben de grootte van een chocoladereep en worden ingeslikt door de dieren.

Voor huisdieren heeft België de BVIRH[18] aangeduid als het organisme dat verantwoordelijk is voor de identificatie en registratie van honden. Volgens de reglementeringen die van kracht zijn in de Schengen-ruimte kan deze identificatie van honden via een RFID-tag die onderhuids bij het dier wordt ingebracht. Deze tag bevat eenvoudigweg een uniek identificatienummer van 15 cijfers dat gecommuniceerd wordt door de tag wanneer deze gelezen wordt. De BVIRH onderhoudt een database van alle hondenidentificatienummers, alsook de specifieke gegevens van elk dier (bv. leeftijd, ras) en de persoonlijke gegevens van elke eigenaar (bv. naam, adres, telefoonnummer).

Figuur 8: Dier dat een RFID-tag draagt aan zijn oor (bron: Haslam/WikimediaCommons)

Bibliotheek

RFID vergemakkelijkt het uitlenen van boeken en het beheer van de voorraad in bibliotheken. Het automatiseert de uitleen/indienprocedures van boeken en gaat na of een boek verkeerd gerangschikt werd in de boekenrekken. Met de installatie van poortjes aan de uitgangen van de bibliotheek kan daarenboven elk boek dat niet als "uitgeleend" geregistreerd werd een alarm doen afgaan. Bibliotheken gebruiken normaal de RFID-technologie met de HF-frequentieband 13,56 MHz gebaseerd op de standaard ISO/IEC 15693.

[18] Belgische Vereniging voor Identificatie en Registratie van Honden.

Figuur 9: RFID-systeem voor een bibliotheek (bron: LIU/WikimediaCommons)

Opvolging in een logistieke keten

De Amerikaanse reus in supermarktketens Walmart was een van de eerste die RFID gebruikte voor het beheer van zijn logistieke keten. Dit project begon in 2003 toen Walmart zijn grootste leveranciers had opgelegd om hun producten te voorzien van RFID-tags voor eind 2005. De kostprijs was echter veel te hoog voor de leveranciers, waarop Walmart gas terugnam en vroeg om enkel de paletten uit te rusten met RFID-tags. De tags gebruikt door Walmart zijn EPC's Class 1 Gen 2 waarmee de paletten vanop een afstand van ongeveer twee meter gelezen kunnen worden.

4.3. Beveiligde applicatie

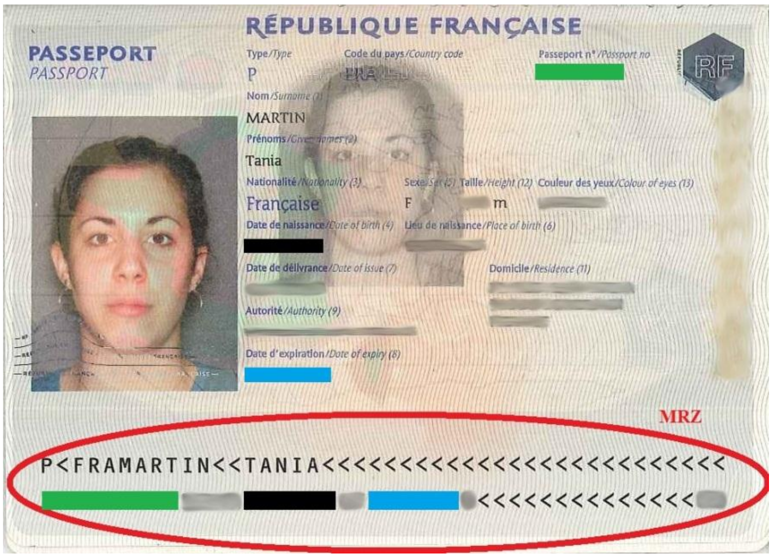
Elektronische paspoorten

De ICAO is de organisatie die elektronische paspoorten heeft ingevoerd. De tags die geïntegreerd zijn in de kaft van de paspoorten voldoen aan de standaard DOC 9303 [12] van de ICAO voor de applicatielaag en aan de standaard ISO/IEC 14443 voor de onderliggende lagen.

De gegevens van de houder van het paspoort liggen opgeslagen in datagroepen, genaamd "DG's[19]". DG1 bevat meer bepaald alle gegevens die geschreven staan in de zone van het paspoort die bedoeld is voor de automatische lezer, genaamd "MRZ[20]". Een voorbeeld van MRZ wordt gegeven in figuur 10 met het paspoort van de auteur van dit document. In figuur 11 wordt de MRZ uitgelegd. We vinden er onder andere de naam en de geboortedatum van de auteur alsook de vervaldatum van het paspoort. DG2 bevat de foto van de houder van het paspoort, en DG3 - voornamelijk gebruikt in Europa - slaat zijn vingerafdrukken op.

[19] *Data Group*.

[20] *Machine Readable Zone*.



Figuur 10: MRZ van een Frans paspoort

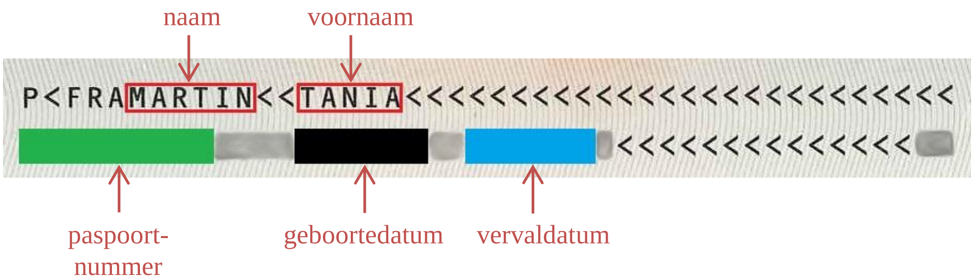


Figure 11: Detail van een MRZ

De integriteit en geldigheid van gegevens opgeslagen op de tag worden beveiligd met behulp van meerdere mechanismes[21]. Het lezen van gegevens wordt ook beschermd door een authenticatieprotocol[22], genaamd "BAC[23]". Zonder BAC in detail uit te leggen, moet men wel onthouden dat de volledige uitvoering van het protocol kennis vereist van de tweede regel van de MRZ van het paspoort. Dit impliceert dat het verplicht is om het paspoort open te houden om toegang te krijgen tot de inhoud van de tag. De paspoorten die vingerafdrukken opslaan gebruiken eveneens een versterkt authenticatiemechanisme, genaamd "EAC[24]" dat enkel de toegang tot de vingerafdrukken toestaat aan overheden die bevoegd zijn voor controles.

[21] De beschrijving van deze mechanismen ligt buiten het kader van dit document. Wie geïnteresseerd is kan [17] raadplegen voor meer details.

[22] In het kader van RFID is een authenticatieprotocol een procedure waarmee een RFID-lezer overtuigd wordt van de identiteit van de RFID-tag waarmee hij communiceert.

[23] *Basic Access Control*.

[24] *Extended Access Control*.

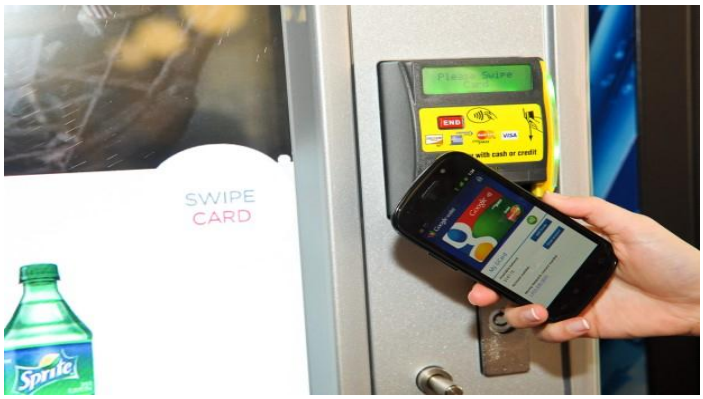
Contactloos betalen

Een recente toepassing gebaseerd op RFID is het contactloos betalen. Ze werd al bestudeerd door meerdere producenten. Het gebruik ervan is op dit ogenblik beperkt tot kleine bedragen. Een van de meest bekende voorbeelden is de Speedpass, ingevoerd in 1997, waarmee Amerikaanse bestuurders hun brandstof kunnen betalen via contactloze betaling in stations van Exxon, Mobil en Esso. De RFID-tags worden in deze systemen geïntegreerd in sleutelhangers en dienen als LF-frequentiebanden van 125 kHz.

Figuur 12: RFID-tag geïntegreerd in de Speedpass-sleutelhanger (bron: Atkinson/WikimediaCommons)

De belangrijkste bankgroepen MasterCard, American Express en Visa hebben eveneens geïnvesteerd in dergelijke toepassingen. Sinds het begin van de jaren 2000 ontwikkelt ieder zijn eigen contactloos betalingssysteem dat, in tegenstelling tot de Speedpass, functioneert via de HF-frequentiestrook van 13,56 MHz met de standaard ISO/IEC 14443.

Contactloze betaling is ook een domein dat in volle groei is voor NFC, in het bijzonder voor openbaar vervoer. Veel landen zoals Frankrijk, Japan of de Verenigde Staten testen NFC-oplossingen om alle kaarten van gebruikers op hun gsm te centraliseren. Volgens de bedrijven zal dit het leven van de gebruikers erg vergemakkelijken. De gsm zal dan tegelijkertijd een kredietkaart, een abonnement voor openbaar vervoer, een ziekteverzekeringskaart en eventueel een identiteitskaart zijn. De gebruiker zal zo goed als geen nood meer hebben aan zijn portefeuille, maar zal enkel zijn gsm nodig hebben.



Figuur 13: Betaling aan een drankautomaat via NFC (bron: Alecrim/WikimediaCommons)

5. Conclusie

RFID is vandaag gekend als de nieuwe tendens op het vlak van identificatie en authenticatie van objecten en personen. Ze steunt op vele verschillende technologieën, met verscheidene standaarden en fysieke eigenschappen. RFID bevindt zich in verschillende toepassingen op de vrije markt die we dagelijks gebruiken.

Met deze uitrol op grote schaal is het dus moeilijk voor de gebruiker om RFID te vermijden. Deze invasie in het dagelijks leven roept bij gebruikers en overheden grote vraagtekens op en brengt angst teweeg wat betreft privacy. Dit is meer bepaald te wijten aan het feit dat de tags geïntegreerd zijn in de objecten gedragen door mensen. Kunnen RFID-tags gegevens onthullen die de privacy van de drager zou kunnen schenden? Kan RFID bedrijven helpen om gegevens van gebruikers te verzamelen? Kan RFID dienen om gebruikers en hun gewoontes te traceren of zelfs op te sporen? Bestaan er genoeg veiligheidsmechanismen die gebruikt worden in de RFID-systemen? Zo ja, zijn deze dan wel efficiënt genoeg? Een volgende Techno zou deze problematiek in verband met het respecteren van privacy in RFID-systemen kunnen aanhalen.

6. Bibliografie

[1] Europese Commissie (Viviane Reding), “Commission recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification," *Official Journal of the European Union,* vol. L(122), pp. 47--51, May 2009.

[2] C. A. Walton, "Electronic Identification and Recognition System". U.S. Patent 3,753,960, 14 August 1973.

[3] NXP Semiconductors, "Mifare Smartcards ICs," [Online]. Available: http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/.

[4] EPC Global Inc., "Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.2.0," October 2008. [Online]. Available: http://www.epcglobalinc.org/standards/.

[5] Infineon, "Contactless SLE 66 Family," [Online]. Available: http://www.infineon.com/.

[6] NXP Semiconductors, "DESFire Tags," [Online]. Available: http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_desfire/.

[7] International Organization for Standardization, "ISO/IEC 18000: Information technology - Radio frequency identification for item management," ISO, 2008.

[8] G. Hancke, "Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens," *Journal of Computer Security*, vol. 19(2), pp. 259--288, March 2011.

[9] P.-H. Thevenon, «Sécurisation de la Couche Physique des Communications Sans Contact de Type RFID et NFC,» 2012.

[10] International Organization for Standardization, "ISO/IEC 14443: Identification cards - Contactless integrated circuit cards - Proximity cards," ISO, 2001--2008.

[11] Internation Organization for Standardization, "ISO/IEC 15693: Identification cards - Contactless integrated circuit(s) cards - Vicinity cards," ISO, 2000-2009.

[12] International Civil Aviation Organization, "Machine Readable Travel Documents, Doc 9303, Part 1, Machine Readable Passports, Fifth Edition," ICAO, 2003.

[13] International Organization for Standardization, "ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol," ISO, 2004.

[14] Innovatron, "Calypso Electronic Ticketing Standard," 1993.

[15] International Organization for Standardization, "ISO/IEC 11784: Radio frequency identification of animals - Code structure," ISO, 1996.

[16] International Organization for Standardization, "ISO/IEC 11785: Radio frequency identification of animals - Technical concept," ISO, 1996.

[17] G. Avoine and J.-J. Quisquater, "Passport Security," in *Encyclopedia of Cryptography and Security (2nd Ed.)*, Springer, 2011, pp. 913--916.