Radio Frequency Identification (RFID)

Keywords

Radio Frequency Identification, RFID, RFID security, tag, tag reader, EAS, Electronic Article Surveillance, Uniform Code Council, UCC, EAN.

Abstract

While Radio Frequency Identification (RFID) was first conceived in 1948, it has taken many years for the technology to mature to the point where it is sufficiently affordable and reliable for widespread use. From Electronic Article Surveillance (EAS) for article (mainly clothing) security to more sophisticated uses, RFID is seen by some as the inevitable replacement for bar-codes. With increasing use comes increasing concern on privacy and security. Clearly there is considerable work to be undertaken before RFID becomes as pervasive as bar-codes although the tempo of change is increasing rapidly.

Introduction

RFID is an area of automatic identification that is gaining momentum and is considered by some to emerge as one of the most pervasive computing technologies in history. In its simplest form, RFID is a similar concept to bar coding. It is seen as a means of enhancing data processes and is complementary to existing technologies. It is a proven technology that has been in use since the 1970s.

A more complex description is an electromagnetic proximity identification and data transaction system. Using " RFID tags" on objects or assets, and " readers" to gather the tag information, RFID represents an improvement over bar codes in terms of non-optical proximity communication, information density, and two-way communication ability. Operational RFID systems involve tags and readers interacting with objects (assets) and database systems to provide an information and/or operational function.

RFID is used for a wide variety of applications ranging from the familiar building access control proximity cards to supply chain tracking, toll collection, vehicle parking access control, retail stock management, ski lift access, tracking library books, theft prevention, vehicle immobiliser systems and railway rolling stock identification and movement tracking.

While RFID systems can yield great productivity gains, they also expose new threats to the security and privacy of individuals and organisations.

A Brief History

One of the earliest papers exploring RFID is a landmark paper by Harry Stockman " Communication by Means of Reflected Power" published in 1948. This came on the heels of the radar and radio research undertaken during the Second World War. There are also several technologies related to RFID, such as long range transponder systems of IFF (Identification Friend or Foe) systems for aircraft. It was, however, thirty years before technology caught up with the theory with the development of the integrated circuit, the microprocessor and changing business practices.

In the 1950' s there was a theoretical exploration of RFID techniques with a number of pioneering research and scientific papers being published. In the 1960' s various inventors and researchers developed prototype systems. Some commercial systems (for example,

Sensormatic and Checkpoint) were launched with the electronic article surveillance (EAS) equipment used as an anti-theft device. These systems used 1-bit tags detecting the presence or absence of a tag, were used in retail stores attached to high value items and clothing. These proved an effective anti-theft measure and is arguable the first and most widespread commercial use of RFID.

In the 1970s there was a great deal of interest in RFID from researchers, developers and academic institutions including such organisations as Los Alamos Scientific Laboratory and the Swedish Microwave Institute Foundation. There was much development work in this period and such applications as animal tagging became commercially viable.

In the 1980s RFID applications extended into a number of areas. In Europe animal tracking systems became widespread and toll roads in Italy, France, Spain, Portugal and Norway were RFID equipped.

The 1990s were significant with the widespread adoption of electronic toll collection in the United States. In 1991 an electronic tolling system opened in Oklahoma where vehicles could pass toll collection points at highway speeds, (no toll booths). In Europe there was also considerable interest in RFID applications including toll collections, rail applications and access control.

RFID tolling and rail applications appeared in many countries including Argentina, Australia, Brazil, Canada, China, Hong Kong, Japan, , Malaysia, Mexico, New Zealand, South Korea, South Africa, Singapore and Thailand.

Developments continued in the 1990s with integrated circuit development and size reduction until microwave RFID tags were reduced to a single integrated circuit.

Currently there is considerable work being undertaken in the rationalisation of frequency spectrum allocation between countries, development of standards and the introduction of many commercial applications. There are now over 350 patents registered with the US Patent Office related to RFID and RFID applications.

Table 1: The Decades of RFID[1]

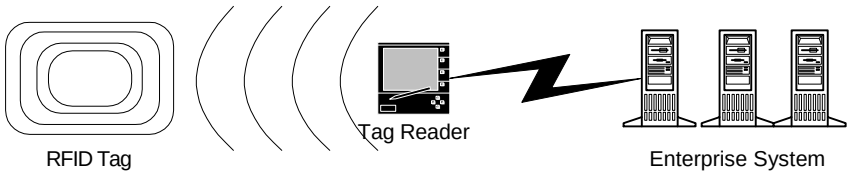
Decade	Event
1940 - 1950	Radar refined and used, major World War II development effort. RFID invented in 1948.
1950 - 1960	Early explorations of RFID technology, laboratory experiments.
1960 - 1970	Development of the theory of RFID. Start of applications field trials.
1970 - 1980	Explosion of RFID development. Tests of RFID accelerate. Very early adopter implementations of RFID.
1980 - 1990	Commercial applications of RFID enter mainstream.
1990 - 2000	Emergence of standards. RFID widely deployed. RFID becomes a part of everyday life.

What is RFID?

Today RFID is a generic term for technologies that use radio waves to automatically identify people or objects[2]. There are several methods of identification, the most common of which is to associate the RFID tag unique identifier with an object or person. An RFID system (Figure 1)will typically comprise:

- An RFID device (tag);
- A tag reader with an antenna and transceiver
- A host system or connection to an enterprise system.

Figure 1



Tags

RFID devices fall into two broad categories, those with a power supply (a battery) and those without. An RFID device that actively transmitted to a reader is known as a transponder (TRANSmitter/resPONDER). Unpowered passive devices are known as " tags" . More recently, common usage has described transponders as " active tags" and unpowered devices as " passive tags" . Active tags are typically also read/write devices while passive tags are generally read only.

Active tags are larger and more expensive that passive tags. The use of a battery places a limit on the life of the device, although with current battery technology this may be as much as ten years.

Passive tags have an unlimited life, are lighter, smaller and cheaper. The trade-off is limited data storage capability, a shorter read range and they require a higher-power reader. Performance is reduced in electromagnetically " noisy" environments.

There are also semi-passive tags where the battery runs the chip' s circuitry but the device communicates by drawing power from the reader.

Tags are available in a wide variety of shapes, sizes and protective housings. Animal tracking tags, which are injected beneath the skin, are approximately 10mm long and 1mm in diameter. Some tags are encapsulated in credit card sized packages, typically building access cards. Others are for use in harsh environments such as container tracking applications and can measure 120x100x50mm. The smallest devices commercially available measure 0.4x0.4mm and are thinner than a sheet of paper.

Tag Data

Tags can incorporate read only memory (ROM), volatile read/write random access memory (RAM) or write once/read many memory (WORM). ROM is used to store security data, a unique device identifier and operating system instructions. RAM is used for data storage during transponder interrogation and response.

Data will comprise a unique identifier and may also include:

- An operating system;
- Data storage (volatile or non-volatile);
- An electronic product code (EPC - the successor to the bar-code).

Tag Operation

Passive tags draw their power from the transmission of the reader through inductive coupling. The passive tags will then respond to the enquiry. Inductive coupling usually requires close proximity.

Active tags usually communicate through propagation coupling and respond to the reader' s transmission drawing on internal power to transmit.

Frequency Ranges

Frequency allocations are generally managed through legislation and regulation by individual governments. Internationally there are differences in frequencies allocated for RFID applications although standardisation through ISO and similar organisations is assisting in compatibility. For example, Europe uses 868 MHz for UHF and the US uses 915 MHz. Currently very few frequencies are consistently available on a global basis for RFID applications. Three frequency ranges are generally used for RFID applications:

Table 2. Frequency Bands and Applications[3]

Frequency Band	**Characteristics**	**Typical Applications**
Low 100-500 kHz	Short to medium read range Inexpensive low reading speed	Access control Animal identification Inventory control Car immobiliser
Intermediate 10-15 MHz	Short to medium read range potentially inexpensive medium reading speed	Access control Smart cards Library control
High 850-950 MHz 2.4-5.8 GHz	Long read range High reading speed Line of sight required Expensive	Railway vehicle monitoring Toll collection systems Pallet & container tracking Vehicle tracking

In general, low-frequency passive tags have an effective range of 30cm, high frequency passive tags around one metre and UHF passive tags from 3 - 5 metres. Where greater range is needed, such as in container tracking and railway applications, active tags can boost the signal to a range of 100 metres.

RFID Usage Categories

RFID devices can be classified into four usage categories:

- EAS (Electronic Article Surveillance);
- Portable Data Capture;
- Networked systems;
- Positioning systems.

EAS

These are typically one-bit systems used to sense the presence or absence of an object. The most common use is in retail stores as an anti-theft device. Tags are attached to clothing or other items and trigger an alarm if the goods leave the store before the tag is deactivated. These have been in widespread use for some years and are found in a variety of retail stores including clothing, small appliances, electrical goods and book stores.

Portable Data Capture

Used in conjunction with portable readers where the data required from the tagged object may vary. Some devices are being combined with sensors to record, for example, temperature, movement (seismic) and radiation.

Networked Systems

Characterised by fixed position readers and used to track the movement of tagged objects. Usually directly connected to an enterprise system. This is a typical inventory application of the technology.

Positioning Systems

Where objects (vehicles, animals or even people) are tagged and the system provides automatic location and can provide navigational support.

Applications

Used mainly in transportation, logistics, manufacturing, processing and security, typical applications include:

- Animal tagging;
- Animal husbandry;
- Toxic and medical waste management;
- Postal tracking;
- Airline baggage management;
- Paper money anti-counterfeiting;
- Anti-counterfeiting in the drug industry;
- Vehicle immobilisers and alarms;
- Road toll collection;
- EAS;
- Access control;
- Time and attendance;
- Manufacturing processes with robotics;
- Monitoring of offenders;
- Passports.

RFID Standards

The lack of standardisation and the lack of harmonisation of frequency allocation is hampering growth in this industry. There is a proliferation of incompatible standards with major RFID vendors offering proprietary systems. ANSI and ISO have been working to develop RFID standards and some have been adopted for such applications as animal tracking (ISO 11784 and 11785), and supply chain goods tracking (ISO 18000-3 and ISO 18000-6).

Advantages

The principal advantages of RFID system are the non-contact, non line-of-sight characteristics of the technology. Tags can be read through a variety of visually and environmentally challenging conditions such as snow, ice, fog, paint, grime, inside containers and vehicles and while in-storage.

With a response time of less than 100 milliseconds, an RFID reader can read many (several hundred) tags virtually instantaneously. Tags coupled with sensors can provide important information on the state of the goods. For example, refrigerated goods can be monitored for temperature, problem areas identified and alarms raised.

Some developments and uses

The US military has used RFID technology since the early 1990's with the first deployment to Bosnia in the mid 1990's. The United Kingdom armed forces adopted RFID in 2003 and negotiations are in progress with NATO partners[4].

The US Department of Defense and Wal-Mart require their major suppliers to implement RFID technology in their supply chains by 1 January 2005[5]. All cartons and pallets must be equipped with RFID tags. This will provide a major impetus for the widespread adoption of the technology in the US.

UK's Tesco supermarket chain has begun work to roll out an RFID network that tracks shipments from its central distribution centre to all 98 Tesco Extra Superstores by Christmas 2004[6]. This is the first stage of a plan to implement RFID across more than 2000 stores and distribution centres in the UK.

In January 2003, Gillette announced an order for 500 million RFID tags to be incorporated into razor and razor blade packaging[7].

In March 2003 Benetton announced similar plans to weave RFID tags into its designer clothes, although this was reversed in the face of an organised consumer boycott.

Mastercard and American Express have been testing RFID cards.

Mobil has been promoting its 'Speedpass" fuel card since 1997.

Most high-end cars are now equipped with an RFID tag in the car keys.

Delta Airlines is testing RFID on some services, tagging 40,000 bags[8]. Many other airlines have tested RFID technology but Delta is the first airline to commit to using RFID technology[9]. Delta currently misplaces 4 out of every 1000 bags costing US$100 million per year to recover, deliver or replace them. British Airways announced recently that they will

also be investing in RFID technology. British Airways currently misplace 18 bags per 1000 costing an average of US$100 per bag. The airline suffered significant difficulties in 2004 when 11,000 bags were lost following strikes[10].

The seaport operators, who account for 70% of the world's port operations have agreed to deploy RFID tags to track the 17,000 containers that arrive at US ports daily.

Star City Casino in Sydney has placed RFID tags in 80,000 employee uniforms in an attempt to curb the theft of the uniforms. The new Wynn Las Vegas casino has incorporated RFID into betting chips to curb the use of fake chips, misuse of credit facilities and late placement of bets[11].

Michelin is planning to build RFID tags into its tyres. The tag will store a unique number for each tyre, associated with the vehicle's identification number (VIN). The tag can also measure tyre wear.

The European Central Bank is planning to embed RFID tags into high-denomination bank notes as an anti-counterfeiting measure, by 2005. The bank notes already incorporate such measures as holograms, foil strips, special threads, microprinting, special inks and watermarks. At present, the US dollar is the world's most counterfeited currency. However, with the growth of the European Union and the growing use of the Euro, this will become the most common currency in the world[12].

The Mexican Government implanted RFID chips into its top judicial officials to provide tracking if the official is kidnapped. It is also used for access control[13].

These are some examples of current usage of RFID tags. There are other applications under consideration. For example, the incorporation of RFID tags into important documents such as birth certificates, driver licences, educational certificates, manuscripts, medical registrations and so on. In fact any document where authenticity and veracity is essential.

Growth in Usage

Radio Frequency Identification systems are emerging as a practical means of Auto-Identification in a wide variety of applications from access control to animal tracking. RFID systems are likely to supersede bar codes in some applications and complement bar codes in others. RFID is expected to help in reducing costs of supply chain management and inventory management in addition to the many other applications outlined above. Cost savings have been estimated to be as high as 8 to 10 percent of inventory associated costs[14].

While RFID usage is limited at present, Evans Data Corporation, an IT market research organisation, is predicting that RFID usage will increase by 450% in 2005 and a further 96% in 2006[15]

The widespread adoption of RFID is a foregone conclusion, according to some industry commentators[16]. A major driving force being the adoption of the technology by such influential organisations as the US Department of Defense, Wal-Mart and Tesco.

More on Standards

The EPC system defines technical protocols and creates a data structure for the stored information. The EPC system was researched and developed at the Auto-ID Center at the Massachusetts Institute of Technology (MIT) and in November 2003

responsibility for the commercialisation and management of the EPC system was transferred to EPCglobal Inc. This organisation is an affiliate of the Uniform Code Council (UCC) and EAN International (EAN); EAN and UCC created and maintain the EAN.UCC System, which covers global e-business communications standards, numbering schemes, uniqueness management, and bar code symbology standards, including the U.P.C. and EAN bar code symbols used on consumer goods around the world[17]. While there are some differences with the ISO standards, these organisations are now working together to rationalise standards.

EPC specifications have defined five tag classes, based on functionality:

Figure 2[18]

Class	Nickname	Memory	Power Source	Features
0	Anti-Shoplift Tags	None	Passive	Article Surveillance
1	EPC	Read-Only	Any	Identification Only
2	EPC	Read-Write	Any	Data Logging
3	Sensor Tags	Read-Write	Semi-Passive or Active	Environmental Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc Networking

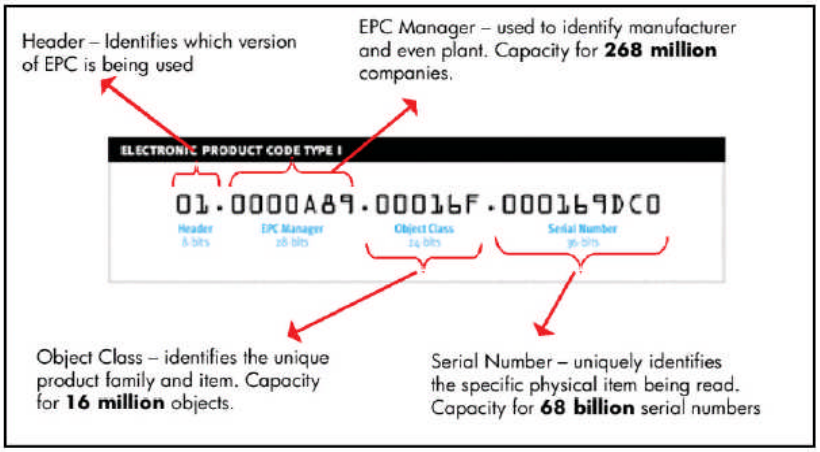
The current version of the Electronic Product Code (EPC) Tag Data Standard specifies the format for encoding and reading data from 64 and 96 bit RFID tags[19]:

Figure 3

EPC TYPE	HEADER SIZE	FIRST BITS	DOMAIN MANAGER	OBJECT CLASS	SERIAL NUMBER	TOTAL
64 bit type I	2	01	21	17	24	64
64 bit type II	2	10	15	13	34	64
64 bit type III	2	11	26	13	23	64
96 bit and more	8	00	28	24	36	96

Figure 4[20]

EPC Class 1 (96 bit) Tag Content



* Global Commerce Initiative/IBM EPC Roadmap, November 2003

Privacy and Security

Simple RFID readers can cost as little as US$20[21] and circuits and articles have been published in electronics and enthusiasts magazines[22] to allow you to build your own readers. There are security and privacy concerns with this technology which fall broadly into the following areas:

- Location privacy;
- Customer information;
- Corporate espionage;
- Insecure operating environments;
- Denial of service;
- Spoofing;
- Technical attacks;
- Compromise of supporting systems.

Location Privacy

Data can be extracted from tags and used to track individuals, thus violating location privacy. This is not unique to RFID systems as other systems including cellphones, many Bluetooth and other wireless enabled devices may be subject to the same privacy issue.

Customer Information

Where a customer has made multiple purchases, information on buying patterns or the identification of high value items can result.

Corporate Espionage

If unprotected RFID tags are used, a retailer' s stock may be monitored or tracked by competitors, marketing organisations, news media, private investigators or information brokers. This can yield sales, marketing, product mix and other valuable commercial information.

Insecure Environments

RFID tags often operate in hostile environments and can be subject to intense electronic or physical attacks. Examples include container tracking, supply chains and manufacturing processes.

Denial of Service

Denial of service may be caused by " flooding" an area with RF energy, thus incapacitating the readers.

Spoofing

Spoofing occurs where tags are replicated from data transmitted by the tag. This is a particular risk with access control systems. It is technically feasible that attackers may alter the contents of a tag to facilitate theft, disguise the identify of the tagged item or to remove items from the premises.

Technical Attacks

Because they are wireless, passive RFID tags may be susceptible to fault induction, timing attacks or power analysis attacks[23]. Again all wireless devices may be susceptible to these types of attack. Lukas Grunwald, a consultant with a German technology organisation, has

created a software tool, RFDump, that reads and can re-programme some RFID tags. This tool is available from the Internet.

Compromise of Supporting Systems

Microsoft is writing code to accommodate RFID for its Axapta, Great Plains and Navision systems and is expected to have the software RFID-ready by the middle of next year. SAP is embracing RFID[24] and Oracle announced recently that its 10g database and application server are able to interface with RFID data streams[25].

The passive (classes 0 and 1) tags we can expect to find in general retail use can store very little information and generally have no writable memory. They do, however, contain unique identifiers which, when linked to a supporting application or system (database), can store additional information on the tagged item and a read history and lifecycle of that item. They also store tag " kill" codes to deactivate tags. Clearly, and in this case, the valuable data is in the database not in the tag.

The rules on protecting the confidentiality of this information do not change when the collection mechanism changes (RFID tags and readers). The question of liability can also arise. This applies whether the information is commercially sensitive or deals with and individual's privacy.

Supporting systems constitute the greatest risk of information compromise, but a risk which is relatively well understood.

Legislation

Several privacy advocate groups have proposed frameworks to manage consumer privacy in relation to the use of RFID. These frameworks emphasise individuals rights to location privacy and have three basic elements:

- RFID must undergo a formal technology assessment, and RFID tags should not be affixed to individual consumer products until such assessment takes place. This may be accompanied by a " seal of approval" to provide a visual guide that the tags in use conform with approved guidelines;

26

- RFID implementation must be guided by existing privacy legislation and good privacy practice. This may include clear notice, consumer education and consumer choice; and
- Certain uses of RFID should be prohibited, for example tracking individuals with RFID tags in consumer purchases.

However, another essential element is an organisation's ability to track products in the supply chain in the most cost-effective and efficient manner without excessive compliance costs. This could be viewed as a fundamental part of doing business.

While there is considerable debate on RFID and privacy concerns, no specific legislation to deal with RFID has yet been passed. In the US, bills have been proposed in California and Massachusetts and legislators from the Virginia General Assembly intend to study RFID as

an " invasive technology" , along with facial recognition, hidden cameras, spyware and Internet wiretaps[27]. The need to legislate or regulate to manage the public policy aspects is gaining momentum.

Costs

A major constraint on the widespread use of RFID technologies is the cost of the tags. The most widely used tags are Electronic Article Surveillance (EAS, class 0) tags which cost between 1 and 6 US cents each. Over 6 billion of them are used annually[28]. These EAS tags are a one-bit tag and contain little or no information, merely indicating presence or absence.

Passive tags (class 1) with some data storage cost between five and ten US cents each in large quantities (several million). High value items, cartons and pallets are being tagged (class 2-4) and here costs may be up to US$100 per tag. At current prices it is not economic to incorporate tags into every retail item. Prices will fall as manufacturing technologies improve and there is a prediction that 10 billion tags will be used annually by 2007[29] with 1 trillion being delivered in 2015. In the last 50 years only one billion RFID passive tags (other than EAS tags) and 500 million active tags have been sold. While the use of RFID technologies is predicted to grow significantly, it may take several years to get to the point where the majority of retail items are tagged.

Countermeasures

RFID tags standards incorporate a 64-bit region that cannot be modified and remains unique to the tag itself. This can be used to authenticate the tag and defends against tag spoofing[30]. Where class 2,3 or 4 RFID tags are used in access cards, a new bitstream (possibly cryptographically signed) can be uploaded each time the card is used. This reduces the opportunity for a spoofed card to be used and significantly increases the risk of discovery as legitimate cards that are not accepted by the system will soon be reported.

Replay attacks can be protected against through the use of a " hidden" authentication bitstream or serial number on the tag and use a challenge/response mechanism using the hidden number to establish the tag' s credentials. The hidden number is never transmitted.

To successfully replace bar-codes, RFID devices must be very low cost. To keep the cost down, these are generally passive devices with limited functionality. Affordable tags cannot yet perform standard cryptographic operations necessary for privacy and security having only 500-5000 gates. By contrast, the Advanced Encryption Standard (AES) requires some 20,000 - 30,000 gates to manage cryptographic security[31]. Security for the current generation of passive RFID tags therefore represents a considerable challenge[32].

Two techniques have been proposed to address eavesdropping of RFID devices. One, proposed by MIT is known as " silent tree walking" . If two or more tags respond to a reader at the same time, a collision occurs. When this happens, the read performs a binary tree walk-though the address space, one bit at a time, until a unique response can be determined.

The other technique, proposed by RSA Laboratories involves the use of pseudonyms with tags having multiple identifiers which are rotated. Legitimate systems will recognise all identifiers associated with a particular tag. So while eavesdroppers will be able to read the tags, they will need to know all identifiers associated with a tag to interpret the data or successfully track a tag.

RSA have also designed a " blocker tag" technology that prevents RFID devices being read. This system is software based and prevents readers from gathering data from other tags in

their immediate vicinity[33]. RFID readers are unable to read multiple tags simultaneously. Anti-collision protocols allow multiple tags to be read within a very short timeframe. However, " blocker tags" confuse the reader by always responding and thereby prevent any tags being read[34]. Blocker tags could, for example, be incorporated into shopping bags at provided at the checkout. Without this technology, readers could access any tag within range.

The Auto-ID Center specification includes a " kill" command to permanently deactivate a tag. Earlier kill codes were 8 (Class 1) and 24 (Class 0) bit codes, which are relatively trivial defence to a brute force or DOS attack. The new specification for Class 1 tags incorporates a 32-bit kill code. Separate and random kill codes for each RFID tag, which would then have to be retrieved from a secure database, can be used and activated at the checkout. A variation is to disable the tag's unique identifier. Keeping other identifiers in the chip, such as what the item is, could be useful, for example, for sight impaired people who can use a reader to identify medicines and dosages.

One further technique proposed is using antenna energy analysis to enhance security[35]. There are two variations in this technique. In the first, signal analysis estimates the reader distance, distance implying degrees of trust with greater distance equating to less trust. In the second, antenna energy is used to power a tiered authentication scheme in which tags provide more information to more trusted readers.

In New Zealand

There is some use of RFID in New Zealand, mainly EAS, access cards and similar access control applications and some dairy applications for animal tracking and husbandry. Indications are, however, that increasing use can be expected over the next few years.

While EAS tags have been used in New Zealand by retailers for many years, one of the early adopters of new developments in RFID technologies is the Manukau City Council's library in Botany Downs. The library is the first in New Zealand to use RFID tags to track and manage its book collection. Wellington Libraries are expected to follow suit in two to three years[36]. Libraries in the US and UK are deploying the technology with about 250 libraries in the US already using the technology[37]. Singapore implemented the technology in 1998 under the leadership of the National Library Board[38].

Supermarket group Progressive Enterprises which includes Woolworths, Foodtown and Countdown, is trialling RFID to track meat from processing plants to its butcheries[39]. RFID tags will be incorporated into specialised meat containers to assist in supply chain management.

Hastings based Richmond Meats has been evaluating RFID for animal tracking. This will allow shipments to be traced through processing plants back to the livestock[40].

Preliminary discussions between a Canadian RFID vendor, AdvancedID and New Zealand sheep industry officials are underway to establish field demonstrations of RFID technology[41].

Some practical issues

At present, RFID systems do not have high reliability, particularly in a retail environment. . UHF tags are virtually unreadable near the human body because of its high water content[42]. Many retailers have difficulty in getting an accurate, consistent reading when the tag is any distance (sometimes more than a few centimetres) from the reader. With low-cost, passive tags, readers have to be in close proximity to the tag.

Many Customer Relations Management (CRM) systems today, store more data than organisations can use which raises the question why they would want to go to the expense and trouble of collecting more data? The technology does not yet reliably exist for a retailer to drive through a suburb collecting information from the roadside and again there is little desire for retailers so to do.

RFID technologies have been in use for many years (for example access control, toll collection and animal tracking systems) without any significant privacy or security violations. A greater privacy concern is, for example, the cell-phone and particularly the latest feature-rich devices with cameras and location tracking. Loosely speaking, your cell-phone is a sophisticated, active RFID tag[43]! Privacy concerns are unlikely to constrain the use of cell-phones.

Using RFID tags in pallets and cartons to facilitate consignment, distribution and inventory management does not raise major privacy issues[44]. However, where tags are related to individual products, there are legitimate privacy and security concerns. These will have to addressed if RFID is going to find the same widespread acceptance as bar codes.

As with many new technologies there is potential for great benefit and misuse, particularly in supply chain management. But before we see widespread adoption of RFID, tag prices will have to fall significantly, clear benefits will have to be demonstrated and consumers will have to embrace the technology.

[1] " The History of RFID" , Association for Automatic Identification and Data Capture Technologies, October 2001 www.aimglobal.org

[2] RFID Journal Frequently Asked Questions, www.rfidjournal.com

[3] Data from " Radio Frequency Identification - A Basic Primer" , Association for Automatic Identification and Data Capture Technologies, August 2001 www.aimglobal.org and from Wikipedia Encyclopaedia, http://en.wikipedia.org/wiki.RFID.

[4] Radio Frequency Identification Ready to Deliver, Signal Magazine January 2005, Armed Forces Communications and Electronics Association (AFCEA), http://www.afcea.org/

[5] RFID Gazette June 28 2004, www/rfidgazette.org/2004/06/rfid_101.html

[6] RFID Journal Sept 28 2004, www.rfidjournal.com/article/articleprint/1139/-1/1/

[7] The Nation, 3 February 2004, www.thenation.com/doc.mhtml?i=20040216&s=garkinkel

[8] The Register, 27 June 2003, www.theregister.co.uk/2003/06/27/rfid_chaips_are_here/ptint.html

[9] At Delta, tracking bags with radio tags, Ron Coates, CNET News, 1 July 2004, http://news.com.com/2102-1012_3-5254118.html

[10] British Airways likely to invest in RFID, Jo Best, CNET News 7 June 2005, http://news.com.com/2102-1039_3-573582.html

[11] Vegas Casino bets on RFID, Alorie Gilbert, CNET News 9 February 2005, http://news.com.com/2102-7355_3-5568288.html

[12] EETimes December 19 2001, " Euro bank notes to embed RFID chips by 2005" ,www.eetimes.com/

[13] Radio Frequency Identification Ready to Deliver, Signal Magazine January 2005, Armed Forces Communications and Electronics Association (AFCEA), http://www.afcea.org/

[14] Ibid

[15] San Francisco Business Times, March 24 2004, Surging Market for RFID security predicted.

[16] RFID:Robot for infinite decluttering, Kevin Maney, USA Today, 5 October 2004. http://usatoday.com/money/industries/technology/maney/2004-10-05-maney_x.htm

[17] RFID: The Next Generation of AIDC, Application White Paper, Zebra Technologies

[18] Security and Privacy in Radio-Frequency Identification Devices by Stephen August Weis; Massachusetts Institute Of Technology, May 2003

[19] Auto-ID Center, Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag, 23 February 2003

[20] RFID in the Supply Chain, A Balanced View A Business Briefing Paper, Amcor Australasia and Hewlett Packard, 2004 Hewlett-Packard Development Company, L.P.

[21] RFID Devices and Privacy, Junkbusters, www.junkbusters.com/rfid.html

[22] An RFID Security Module, http://www.siliconchip.com.au/cms/A_101658/article.html

[23] Radio Frequency Identification: Security Risks and Challenges, Sarma, Weis and Engels, RSA Laboratories Cryptobytes Volume 6 No.1 Spring 2003

[24] Radio tags set to short circuit supply chains, Peter Griffin, The New Zealand Herald, 07.09.2004, http://www.nzherald.co.nz

[25] RFID: Is that a radio in your toothpaste?, Francis Till, The National Business Review, 20 January 2004, www.nbr.co.nz

[26] EPCGlobalinc Consumer Information; http://www.epcglobalinc.org/consumer/

[27] States Move on RFID Privacy Issue, Claire Swedberg, RFID Journal, 30 April 2004, www.rfidjournal.com

[28] RFID Explained, IDTechEx White Paper, IDTechEx Limited, 2004

[29] Ibid

[30] RFID Security, Dan Kaminsky, Doxpara Research, November 2002, www.doxpara.com/read.php/security/rfid.html

[31] RSA Laboratories; Technical Characteristics of RFID,www.rsasecurity.com

[32] RSA Laboratories, A Primer on RFID, www.rsasecurity.com

[33] RSA Keeps RFID Private, Dennis Fisher, eWeek, 23 February 2004, www.eweek.com

[34] RSA Security Designs RFID Blocker, RFID Journal, 28 August 2003, www.rfidjournal.com

[35] Enhancing RFID Privacy via Antenna Energy Analysis, Kenneth P. Fishkin and Sumi Roy, MIT RFID Privacy Workshop, Boston, November 2003

[36] RFID Library Opens Tomorrow, The Dominion Post, 4 October 2004.

[37] Are Book Tags a Threat?, Andrew Heining and Christa Case, The Christian Science Monitor, October 5 2004, www.csmonitor.com/2004/1005/p17s01-legn.htm

[38] Singapore Seeks Leading RFID Role, RFID Journal, 12 July 2004, http://216.121.131.129/article/articleprint/1024/-1/1/

[39] Progressive Tags Meat, Tom Pullar-Strecker, The Dominion Post, 4 October 2004

[40] RFID - tracking every step you take, iStart, April 2004, www.istart.co.nz

[41] Globalisation of RFID boots AdvancedID sales, Food Production Daily, 5 October 2004, www.foodproductiondaily.com

[42] RSA Laboratories; FAQ on RFID and RFID Privacy, www.rsasecurity.com

[43] RSA Laboratories; Technical Characteristics of RFIDs, www.rsasecurity.com

[44] Privacy Groups Tag RFID, Roy mark, July 14 2004, Internet New, www.internetnews.com/security/article.php/3381261