

Radio-frequency identification

Radio-frequency identification (**RFID**) uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver and transmitter. When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifying inventory number, back to the reader. This number can be used to track inventory goods.^[1]

Passive tags are powered by energy from the RFID reader's interrogating radio waves. Active tags are powered by a battery and thus can be read at a greater range from the RFID reader, up to hundreds of meters.

Unlike a barcode, the tag does not need to be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture (AIDC).^[2]

RFID tags are used in many industries. For example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line, RFID-tagged pharmaceuticals can be tracked through warehouses, and implanting RFID microchips in livestock and pets enables positive identification of animals.^{[3][4]} Tags can also be used in shops to expedite checkout, and to prevent theft by customers and employees.^[5]

Since RFID tags can be attached to physical money, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns.^[6] These concerns resulted in standard specifications development addressing privacy and security issues.

In 2014, the world RFID market was worth US\$8.89 billion, up from US\$7.77 billion in 2013 and US\$6.96 billion in 2012. This figure includes tags, readers, and software/services for RFID cards, labels, fobs, and all other form factors. The market value is expected to rise from US\$12.08 billion in 2020 to US\$16.23 billion by 2029.^[7]

Contents

History

Design

Tags

Readers

Frequencies

Signaling

Bulk reading

Miniaturization

TFID (Terahertz Frequency Identification)

Uses

Commerce

Retail

Access control

Advertising

Promotion tracking

Transportation and logistics

Infrastructure management and protection

Passports

Transportation payments

Animal identification

Human implantation

Institutions

Hospitals and healthcare

Libraries

Museums

Schools and universities

Sports

Complement to barcode

Waste management

Telemetry

Regulation and standardization

EPC Gen2

Problems and concerns

Data flooding

Global standardization

Security concerns

Health

Shielding

Controversies

Privacy

Government control

Deliberate destruction in clothing and other items

See also

References

External links

History

In 1945, Léon Theremin invented the "Thing", a listening device for the Soviet Union which retransmitted incident radio waves with the added audio information. Sound waves vibrated a diaphragm which slightly altered the shape of the resonator, which modulated the reflected radio frequency. Even though this device was a covert listening device, rather than an identification tag, it is considered to be a predecessor of RFID because it was passive, being energised and activated by waves from an outside source.^[8]

Similar technology, such as the Identification friend or foe transponder, was routinely used by the Allies and Germany in World War II to identify aircraft as friendly or hostile. Transponders are still used by most powered aircraft.^[9] An early work exploring RFID is the landmark 1948 paper by Harry Stockman,^[10] who predicted that "Considerable research and development work has to be done before the remaining basic problems in reflected-power communication are solved, and before the field of useful applications is explored."



FasTrak, an RFID tag used for electronic toll collection in California

Mario Cardullo's device, patented on January 23, 1973, was the first true ancestor of modern RFID,^[11] as it was a passive radio transponder with memory.^[12] The initial device was passive, powered by the interrogating signal, and was demonstrated in 1971 to the New York Port Authority and other potential users. It consisted of a transponder with 16 bit memory for use as a toll device. The basic Cardullo patent covers the use of radio frequency (RF), sound and light as transmission carriers. The original business plan presented to investors in 1969 showed uses in transportation (automotive vehicle identification, automatic toll system, electronic license plate, electronic manifest, vehicle routing, vehicle performance monitoring), banking (electronic chequebook, electronic credit card), security (personnel identification, automatic gates, surveillance) and medical (identification, patient history).^[11]

In 1973, an early demonstration of *reflected power* (modulated backscatter) RFID tags, both passive and semi-passive, was performed by Steven Depp, Alfred Koelle and Robert Frayman at the Los Alamos National Laboratory.^[13] The portable system operated at 915 MHz and used 12-bit tags. This technique is used by the majority of today's UHFID and microwave RFID tags.^[14]

In 1983, the first patent to be associated with the abbreviation RFID was granted to Charles Walton.^[15]

In 1996, the first patent for a batteryless RFID passive tag with limited interference was granted to David Everett, John Frech, Theodore Wright, and Kelly Rodriguez.^[16]

Design

A radio-frequency identification system uses *tags*, or *labels* attached to the objects to be identified. Two-way radio transmitter-receivers called *interrogators* or *readers* send a signal to the tag and read its response.^[17]

Tags

RFID tags are made out of three pieces:

- a micro chip (an integrated circuit which stores and processes information and modulates and demodulates radio-frequency (RF) signals)
- an antenna for receiving and transmitting the signal
- a substrate^[18],^[19]

The tag information is stored in a non-volatile memory.^[19] The RFID tag includes either fixed or programmable logic for processing the transmission and sensor data, respectively.

RFID tags can be either passive, active or battery-assisted passive. An active tag has an on-board battery and periodically transmits its ID signal.^[19] A battery-assisted passive tag has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than an active tag for signal transmission.^[20] This makes a difference in interference and in exposure to radiation.

Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user. Field programmable tags may be write-once, read-multiple; "blank" tags may be written with an electronic product code by the user.^[21]

The RFID tag receives the message and then responds with its identification and other information. This may be only a unique tag serial number, or may be product-related information such as a stock number, lot or batch number, production date, or other specific information. Since tags have individual serial numbers, the RFID system design can discriminate among several tags that might be within the range of the RFID reader and read them simultaneously.

Readers

RFID systems can be classified by the type of tag and reader. There are 3 types:^[22]

- A **Passive Reader Active Tag (PRAT)** system has a passive reader which only receives radio signals from active tags (battery operated, transmit only). The reception range of a PRAT system reader can be adjusted from 1–2,000 feet (0–600 m), allowing flexibility in applications such as asset protection and supervision.
- An **Active Reader Passive Tag (ARPT)** system has an active reader, which transmits interrogator signals and also receives authentication replies from passive tags.
- An **Active Reader Active Tag (ARAT)** system uses active tags activated with an interrogator signal from the active reader. A variation of this system could also use a Battery-Assisted Passive (BAP) tag which acts like a passive tag but has a small battery to power the tag's return reporting signal.

Fixed readers are set up to create a specific interrogation zone which can be tightly controlled. This allows a highly defined reading area for when tags go in and out of the interrogation zone. Mobile readers may be handheld or mounted on carts or vehicles.

Frequencies

RFID frequency bands^{[23][24]}

Band	Regulations	Range	Data speed	ISO/IEC 18000 section	Remarks	Approximate tag cost in volume (2006)
LF: 120–150 kHz	Unregulated	10 cm (4 in)	Low	Part 2 (http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=46146)	Animal identification, factory data collection	US\$1
HF: 13.56 MHz	ISM band worldwide	0.1–1 m (4 in – 3 ft 3 in)	Low to moderate	Part 3	Smart cards (ISO/IEC 15693, ISO/IEC 14443 A, B), ISO-non-compliant memory cards (Mifare Classic, iCLASS, Legic, FeliCa ...), ISO-compatible microprocessor cards (Desfire EV1, Seos)	US\$0.05 to US\$5
UHF: 433 MHz	Short range devices	1–100 m (3–300 ft)	Moderate	Part 7 (https://www.iso.org/standard/57336.html)	Defense applications, Underground Miner Tracking with active tags	US\$5
UHF: 865–868 MHz (Europe) 902–928 MHz (North America)	ISM band	1–12 m (3–40 ft)	Moderate to high	Part 6 (https://www.iso.org/standard/59644.html)	EAN, various standards; used by railroads ^[25]	US\$0.04 to US\$1.00 (passive tags)
microwave: 2450–5800 MHz	ISM band	1–2 m (3–7 ft)	High	Part 4 (http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62539)	802.11 WLAN, Bluetooth standards	US\$25 (active tags)
microwave: 3.1–10 GHz	Ultra wide band	up to 200 m (700 ft)	High	Not defined	Requires semi-active or active tags	US\$5 projected
mm-wave: 24.125 GHz ^{[26][27][28]}	ISM band worldwide	10–200 m (30–700 ft)	High	Not defined	Requires semi-passive tags. Uses retrodirective backscatter approaches to achieve extended ranges	US\$10 projected

Signaling

Signaling between the reader and the tag is done in several different incompatible ways, depending on the frequency band used by the tag. Tags operating on LF and HF bands are, in terms of radio wavelength, very close to the reader antenna because they are only a small percentage of a wavelength away. In this near field region, the tag is closely coupled electrically with the transmitter in the reader. The tag can

modulate the field produced by the reader by changing the electrical loading the tag represents. By switching between lower and higher relative loads, the tag produces a change that the reader can detect. At UHF and higher frequencies, the tag is more than one radio wavelength away from the reader, requiring a different approach. The tag can backscatter a signal. Active tags may contain functionally separated transmitters and receivers, and the tag need not respond on a frequency related to the reader's interrogation signal.^[29]

An Electronic Product Code (EPC) is one common type of data stored in a tag. When written into the tag by an RFID printer, the tag contains a 96-bit string of data. The first eight bits are a header which identifies the version of the protocol. The next 28 bits identify the organization that manages the data for this tag; the organization number is assigned by the EPCGlobal consortium. The next 24 bits are an object class, identifying the kind of product. The last 36 bits are a unique serial number for a particular tag. These last two fields are set by the organization that issued the tag. Rather like a URL, the total electronic product code number can be used as a key into a global database to uniquely identify a particular product.^[30]

Often more than one tag will respond to a tag reader, for example, many individual products with tags may be shipped in a common box or on a common pallet. Collision detection is important to allow reading of data. Two different types of protocols are used to "singulate" a particular tag, allowing its data to be read in the midst of many similar tags. In a slotted Aloha system, the reader broadcasts an initialization command and a parameter that the tags individually use to pseudo-randomly delay their responses. When using an "adaptive binary tree" protocol, the reader sends an initialization symbol and then transmits one bit of ID data at a time; only tags with matching bits respond, and eventually only one tag matches the complete ID string.^[31]

Both methods have drawbacks when used with many tags or with multiple overlapping readers.

Bulk reading

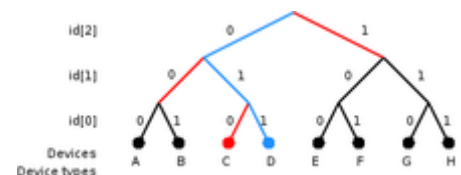
"Bulk reading" is a strategy for interrogating multiple tags at the same time, but lacks sufficient precision for inventory control. A group of objects, all of them RFID tagged, are read completely from one single reader position at one time. However, as tags respond strictly sequentially, the time needed for bulk reading grows linearly with the number of labels to be read. This means it takes at least twice as long to read twice as many labels. Due to collision effects, the time required is greater.^[32]

A group of tags has to be illuminated by the interrogating signal just like a single tag. This is not a challenge concerning energy, but with respect to visibility; if any of the tags are shielded by other tags, they might not be sufficiently illuminated to return a sufficient response. The response conditions for inductively coupled HF RFID tags and coil antennas in magnetic fields appear better than for UHF or SHF dipole fields, but then distance limits apply and may prevent success.^[33]

Under operational conditions, bulk reading is not reliable. Bulk reading can be a rough guide for logistics decisions, but due to a high proportion of reading failures, it is not (yet) suitable for inventory management. However, when a single RFID tag might be seen as not guaranteeing a proper read, multiple RFID tags,



RFID hard tag



An example of a binary tree method of identifying an RFID tag

where at least one will respond, may be a safer approach for detecting a known grouping of objects. In this respect, bulk reading is a fuzzy method for process support. From the perspective of cost and effect, bulk reading is not reported as an economical approach to secure process control in logistics.^[34]

Miniaturization

RFID tags are easy to conceal or incorporate in other items. For example, in 2009 researchers at Bristol University successfully glued RFID micro-transponders to live ants in order to study their behavior.^[35] This trend towards increasingly miniaturized RFIDs is likely to continue as technology advances.

Hitachi holds the record for the smallest RFID chip, at 0.05 mm × 0.05 mm. This is 1/64th the size of the previous record holder, the mu-chip.^[36] Manufacture is enabled by using the silicon-on-insulator (SOI) process. These dust-sized chips can store 38-digit numbers using 128-bit Read Only Memory (ROM).^[37] A major challenge is the attachment of antennas, thus limiting read range to only millimeters.

TFID (Terahertz Frequency Identification)

In early 2020, MIT researchers demonstrated a terahertz frequency identification (TFID) tag that is barely 1 square millimeter in size. The devices are essentially a piece of silicon that are inexpensive, small, and function like larger RFID tags. Because of the small size, manufacturers could tag any product and track logistics information for minimal cost.^{[38][39]}

Uses

An RFID tag can be affixed to an object and used to track tools, equipment, inventory, assets, people, or other objects.

RFID offers advantages over manual systems or use of barcodes. The tag can be read if passed near a reader, even if it is covered by the object or not visible. The tag can be read inside a case, carton, box or other container, and unlike barcodes, RFID tags can be read hundreds per second; barcodes can only be read one at a time using current devices. Some RFID tags, such as battery-assisted passive tags, are also able to monitor temperature and humidity.^[40]

In 2011, the cost of passive tags started at US\$0.09 each; special tags, meant to be mounted on metal or withstand gamma sterilization, could cost up to US\$5. Active tags for tracking containers, medical assets, or monitoring environmental conditions in data centers started at US\$50 and could be over US\$100 each.^[41] Battery-Assisted Passive (BAP) tags were in the US\$3–10 range.

RFID can be used in a variety of applications,^{[42][43]} such as:

- Access management
- Tracking of goods
- Tracking of persons and animals^[44]
- Toll collection and contactless payment
- Machine readable travel documents
- Smartdust (for massively distributed sensor networks)
- Locating lost airport baggage^[45]
- Timing sporting events
- Tracking and billing processes

■ Monitoring the physical state of perishable goods^[46]

In 2010, three factors drove a significant increase in RFID usage: decreased cost of equipment and tags, increased performance to a reliability of 99.9%, and a stable international standard around HF and UHF passive RFID. The adoption of these standards were driven by EPCglobal, a joint venture between GS1 and GS1 US, which were responsible for driving global adoption of the barcode in the 1970s and 1980s. The EPCglobal Network was developed by the Auto-ID Center.^[47]

Commerce

RFID provides a way for organizations to identify and manage stock, tools and equipment (asset tracking), etc. without manual data entry. Manufactured products such as automobiles or garments can be tracked through the factory and through shipping to the customer. Automatic identification with RFID can be used for inventory systems. Many organisations require that their vendors place RFID tags on all shipments to improve supply chain management. Warehouse Management System incorporate this technology to speed up the receiving and delivery of the products and reduce the cost of labor needed in their warehouses.^[48]

Retail

RFID is used for item level tagging in retail stores. In addition to inventory control, this provides both protection against theft by customers (shoplifting) and employees ("shrinkage") by using electronic article surveillance (EAS), and a self checkout process for customers. Tags of different types can be physically removed with a special tool or deactivated electronically once items have been paid for.^[49] On leaving the shop, customers have to pass near an RFID detector; if they have items with active RFID tags, an alarm sounds, both indicating an unpaid-for item, and identifying what it is.

Casinos can use RFID to authenticate poker chips, and can selectively invalidate any chips known to be stolen.^[50]

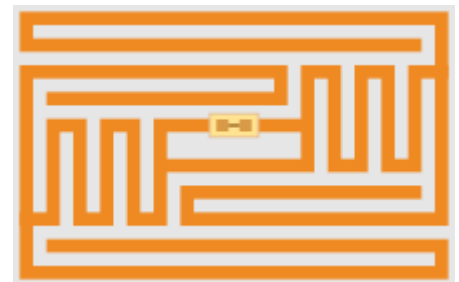
Access control

RFID tags are widely used in identification badges, replacing earlier magnetic stripe cards. These badges need only be held within a certain distance of the reader to authenticate the holder. Tags can also be placed on vehicles, which can be read at a distance, to allow entrance to controlled areas without having to stop the vehicle and present a card or enter an access code.

Advertising



Electronic key for RFID based lock system



An EPC RFID tag used by Wal-Mart



Sewn-in RFID label in garment manufactured by the French sports supplier Decathlon. Front, back, and transparency scan.

In 2010 Vail Resorts began using UHF Passive RFID tags in ski passes.^[51]

Facebook is using RFID cards at most of their live events to allow guests to automatically capture and post photos.

Automotive brands have adopted RFID for social media product placement more quickly than other industries. Mercedes was an early adopter in 2011 at the PGA Golf Championships,^[52] and by the 2013 Geneva Motor Show many of the larger brands were using RFID for social media marketing.^[53]

Promotion tracking

To prevent retailers diverting products, manufacturers are exploring the use of RFID tags on promoted merchandise so that they can track exactly which product has sold through the supply chain at fully discounted prices.^[54]

Transportation and logistics

Yard management, shipping and freight and distribution centers use RFID tracking. In the railroad industry, RFID tags mounted on locomotives and rolling stock identify the owner, identification number and type of equipment and its characteristics. This can be used with a database to identify the type, origin, destination, etc. of the commodities being carried.^[55]

In commercial aviation, RFID is used to support maintenance on commercial aircraft. RFID tags are used to identify baggage and cargo at several airports and airlines.^{[56][57]}

Some countries are using RFID for vehicle registration and enforcement.^[58] RFID can help detect and retrieve stolen cars.^{[59][60]}

RFID is used in intelligent transportation systems. In New York City, RFID readers are deployed at intersections to track E-ZPass tags as a means for monitoring the traffic flow. The data is fed through the broadband wireless infrastructure to the traffic management center to be used in adaptive traffic control of the traffic lights.^[61]

Where ship, rail, or highway tanks are being loaded, a fixed RFID antenna contained in a transfer hose can read an RFID tag affixed to the tank, positively identifying it.^[62]

Infrastructure management and protection

At least one company has introduced RFID to identify and locate underground infrastructure assets such as gas pipelines, sewer lines, electrical cables, communication cables, etc.^[63]

Passports



RFID antenna for vehicular access control



RFID E-ZPass reader attached to the pole and mast arm (right) used in traffic monitoring in New York City

The first RFID passports ("E-passport") were issued by Malaysia in 1998. In addition to information also contained on the visual data page of the passport, Malaysian e-passports record the travel history (time, date, and place) of entry into and exit out of the country.

Other countries that insert RFID in passports include Norway (2005),^[64] Japan (March 1, 2006), most EU countries (around 2006), Australia, Hong Kong, the United States (2007), the United Kingdom and Northern Ireland (2006), India (June 2008), Serbia (July 2008), Republic of Korea (August 2008), Taiwan (December 2008), Albania (January 2009), The Philippines (August 2009), Republic of Macedonia (2010), Argentina (2012), Canada (2013), Uruguay (2015)^[65] and Israel (2017).

Standards for RFID passports are determined by the International Civil Aviation Organization (ICAO), and are contained in ICAO Document 9303, Part 1, Volumes 1 and 2 (6th edition, 2006). ICAO refers to the ISO/IEC 14443 RFID chips in e-passports as "contactless integrated circuits". ICAO standards provide for e-passports to be identifiable by a standard e-passport logo on the front cover.

Since 2006, RFID tags included in new United States passports will store the same information that is printed within the passport, and include a digital picture of the owner.^[66] The United States Department of State initially stated the chips could only be read from a distance of 10 centimetres (3.9 in), but after widespread criticism and a clear demonstration that special equipment can read the test passports from 10 metres (33 ft) away,^[67] the passports were designed to incorporate a thin metal lining to make it more difficult for unauthorized readers to skim information when the passport is closed. The department will also implement Basic Access Control (BAC), which functions as a personal identification number (PIN) in the form of characters printed on the passport data page. Before a passport's tag can be read, this PIN must be entered into an RFID reader. The BAC also enables the encryption of any communication between the chip and interrogator.^[68]

Transportation payments

In many countries, RFID tags can be used to pay for mass transit fares on bus, trains, or subways, or to collect tolls on highways.

Some bike lockers are operated with RFID cards assigned to individual users. A prepaid card is required to open or enter a facility or locker and is used to track and charge based on how long the bike is parked.

The Zipcar car-sharing service uses RFID cards for locking and unlocking cars and for member identification.^[69]

In Singapore, RFID replaces paper Season Parking Ticket (SPT).^[70]

Animal identification

RFID tags for animals represent one of the oldest uses of RFID. Originally meant for large ranches and rough terrain, since the outbreak of mad-cow disease, RFID has become crucial in animal identification management. An implantable RFID tag or transponder can also be used for animal identification. The transponders are better known as PIT (Passive Integrated Transponder) tags, passive RFID, or "chips" on animals.^[71] The Canadian Cattle Identification Agency (<http://www.canadaid.com/>) began using RFID tags as a replacement for barcode tags. Currently CCIA tags are used in Wisconsin and by United States farmers on a voluntary basis. The USDA is currently developing its own program.

RFID tags are required for all cattle sold in Australia and in some states, sheep and goats as well.^[72]

Human implantation

Biocompatible microchip implants that use RFID technology are being routinely implanted in humans. The first-ever human to receive an RFID microchip implant was American artist Eduardo Kac in 1997.^{[73][74]} Kac implanted the microchip live on television (and also live on the Internet) in the context of his artwork *Time Capsule*.^[75] A year later, British professor of cybernetics Kevin Warwick had an RFID chip implanted in his arm by his general practitioner, George Boulos.^{[76][77]} In 2004 the 'Baja Beach Clubs' operated by Conrad Chase in Barcelona^[78] and Rotterdam offered implanted chips to identify their VIP customers, who could in turn use it to pay for service. In 2009 British scientist Mark Gasson had an advanced glass capsule RFID device surgically implanted into his left hand and subsequently demonstrated how a computer virus could wirelessly infect his implant and then be transmitted on to other systems.^[79]

The Food and Drug Administration in the United States approved the use of RFID chips in humans in 2004.^[80]

There is controversy regarding human applications of implantable RFID technology including concerns that individuals could potentially be tracked by carrying an identifier unique to them. Privacy advocates have protested against implantable RFID chips, warning of potential abuse. Some are concerned this could lead to abuse by an authoritarian government, to removal of freedoms,^[81] and to the emergence of an "ultimate panopticon", a society where all citizens behave in a socially accepted manner because others might be watching.^[82]

On July 22, 2006, Reuters reported that two hackers, Newitz and Westhues, at a conference in New York City demonstrated that they could clone the RFID signal from a human implanted RFID chip, indicating that the device was not as secure as was previously claimed.^[83]

Institutions

Hospitals and healthcare

Adoption of RFID in the medical industry has been widespread and very effective.^[84] Hospitals are among the first users to combine both active and passive RFID.^[85] Active tags track high-value, or frequently moved items, and passive tags track smaller, lower cost items that only need room-level identification.^[86] Medical facility rooms can collect data from transmissions of RFID badges worn by patients and employees, as well as from tags assigned to items such as mobile medical devices.^[87] The U.S. Department of Veterans Affairs (VA) recently announced plans to deploy RFID in hospitals across America to improve care and reduce costs.^[88]

Since 2004 a number of U.S. hospitals have begun implanting patients with RFID tags and using RFID systems, usually for workflow and inventory management.^{[89][90][91]} The use of RFID to prevent mix-ups between sperm and ova in IVF clinics is also being considered.^[92]



A surgeon implants British scientist Dr Mark Gasson in his left hand with an RFID microchip (March 16, 2009)

In October 2004, the FDA approved the USA's first RFID chips that can be implanted in humans. The 134 kHz RFID chips, from VeriChip Corp. can incorporate personal medical information and could save lives and limit injuries from errors in medical treatments, according to the company. Anti-RFID activists Katherine Albrecht and Liz McIntyre discovered an FDA Warning Letter that spelled out health risks.^[93] According to the FDA, these include "adverse tissue reaction", "migration of the implanted transponder", "failure of implanted transponder", "electrical hazards" and "magnetic resonance imaging [MRI] incompatibility."

Libraries

Libraries have used RFID to replace the barcodes on library items. The tag can contain identifying information or may just be a key into a database. An RFID system may replace or supplement bar codes and may offer another method of inventory management and self-service checkout by patrons. It can also act as a security device, taking the place of the more traditional electromagnetic security strip.^[94]

It is estimated that over 30 million library items worldwide now contain RFID tags, including some in the Vatican Library in Rome.^[95]

Since RFID tags can be read through an item, there is no need to open a book cover or DVD case to scan an item, and a stack of books can be read simultaneously. Book tags can be read while books are in motion on a conveyor belt, which reduces staff time. This can all be done by the borrowers themselves, reducing the need for library staff assistance. With portable readers, inventories could be done on a whole shelf of materials within seconds.^[96] However, as of 2008 this technology remained too costly for many smaller libraries, and the conversion period has been estimated at 11 months for an average-size library. A 2004 Dutch estimate was that a library which lends 100,000 books per year should plan on a cost of €50,000 (borrow- and return-stations: 12,500 each, detection porches 10,000 each; tags 0.36 each). RFID taking a large burden off staff could also mean that fewer staff will be needed, resulting in some of them getting laid off,^[95] but that has so far not happened in North America where recent surveys have not returned a single library that cut staff because of adding RFID.^[97] In fact, library budgets are being reduced for personnel and increased for infrastructure, making it necessary for libraries to add automation to compensate for the reduced staff size.^[97] Also, the tasks that RFID takes over are largely not the primary tasks of librarians.^[97] A finding in the Netherlands is that borrowers are pleased with the fact that staff are now more available for answering questions.^[97]

Privacy concerns have been raised surrounding library use of RFID.^{[98][99]} Because some RFID tags can be read up to 100 metres (330 ft) away, there is some concern over whether sensitive information could be collected from an unwilling source. However, library RFID tags do not contain any patron information,^[100] and the tags used in the majority of libraries use a frequency only readable from approximately 10 feet (3.0 m).^[94] Another concern is that a non-library agency could potentially record the RFID tags of every person leaving the library without the library administrator's knowledge or consent. One simple option is to let the book transmit a code that has meaning only in conjunction with the library's database. Another possible enhancement would be to give each book a new code every time it is returned. In future, should readers become ubiquitous (and possibly networked), then stolen books could be traced even outside the library. Tag removal could be made difficult if the tags are so small that they fit invisibly inside a (random) page, possibly put there by the publisher.



RFID tags used in libraries: square book tag, round CD/DVD tag and rectangular VHS tag

Museums

RFID technologies are now also implemented in end-user applications in museums.^[101] An example was the custom-designed temporary research application, "eXspot," at the Exploratorium, a science museum in San Francisco, California. A visitor entering the museum received an RF tag that could be carried as a card. The eXspot system enabled the visitor to receive information about specific exhibits. Aside from the exhibit information, the visitor could take photographs of themselves at the exhibit. It was also intended to allow the visitor to take data for later analysis. The collected information could be retrieved at home from a "personalized" website keyed to the RFID tag.^[102]

Schools and universities

In 2004, school authorities in the Japanese city of Osaka made a decision to start chipping children's clothing, backpacks, and student IDs in a primary school.^[103] Later, in 2007, a school in Doncaster, England is piloting a monitoring system designed to keep tabs on pupils by tracking radio chips in their uniforms.^[104] St Charles Sixth Form College in west London, England, started in 2008, uses an RFID card system to check in and out of the main gate, to both track attendance and prevent unauthorized entrance. Similarly, Whitcliffe Mount School in Cleckheaton, England uses RFID to track pupils and staff in and out of the building via a specially designed card. In the Philippines, during 2012, some schools already use RFID in IDs for borrowing books.^[105] Gates in those particular schools also have RFID scanners for buying items at school shops and canteens. RFID is also used in school libraries, and to sign in and out for student and teacher attendance.^[97]

Sports

RFID for timing races began in the early 1990s with pigeon racing, introduced by the company Deister Electronics in Germany. RFID can provide race start and end timings for individuals in large races where it is impossible to get accurate stopwatch readings for every entrant.

In races utilizing RFID, racers wear tags that are read by antennas placed alongside the track or on mats across the track. UHF tags provide accurate readings with specially designed antennas. Rush error, lap count errors and accidents at race start are avoided, as anyone can start and finish at any time without being in a batch mode.



ChampionChip

The design of the chip and of the antenna controls the range from which it can be read. Short range compact chips are twist tied to the shoe, or strapped to the ankle with hook-and-loop fasteners. The chips must be about 400mm from the mat, therefore giving very good temporal resolution. Alternatively, a chip plus a very large (125mm square) antenna can be incorporated into the bib number worn on the athlete's chest at a height of about 1.25 m (4.10 ft).

Passive and active RFID systems are used in off-road events such as Orienteering, Enduro and Hare and Hounds racing. Riders have a transponder on their person, normally on their arm. When they complete a lap they swipe or touch the receiver which is connected to a computer and log their lap time.

RFID is being adapted by many recruitment agencies which have a PET (physical endurance test) as their qualifying procedure, especially in cases where the candidate volumes may run into millions (Indian Railway recruitment cells, police and power sector).



J-Chip 8-channel receiver next to timing mat. The athlete wears a chip on a strap around his ankle. Ironman Germany (<https://web.archive.org/web/19961218232821/http://www.ironman.de/>) 2007 in Frankfurt.

A number of ski resorts have adopted RFID tags to provide skiers hands-free access to ski lifts. Skiers do not have to take their passes out of their pockets. Ski jackets have a left pocket into which the chip+card fits. This nearly contacts the sensor unit on the left of the turnstile as the skier pushes through to the lift. These systems were based on high frequency (HF) at 13.56 megahertz. The bulk of ski areas in Europe, from Verbier to Chamonix, use these systems.^{[106][107][108]}

The NFL in the United States equips players with RFID chips that measures speed, distance and direction traveled by each player in real-time. Currently cameras stay focused on the quarterback; however, numerous plays are happening simultaneously on the field. The RFID chip will provide new insight into these simultaneous plays.^[109] The chip triangulates the player's position within six inches and will be used to digitally broadcast replays.

The RFID chip will make individual player information accessible to the public. The data will be available via the NFL 2015 app.^[110] The RFID chips are manufactured by Zebra Technologies. Zebra Technologies tested the RFID chip in 18 stadiums last year to track vector data.^[111]

Complement to barcode

RFID tags are often a complement, but not a substitute, for UPC or EAN barcodes. They may never completely replace barcodes, due in part to their higher cost and the advantage of multiple data sources on the same object. Also, unlike RFID labels, barcodes can be generated and distributed electronically by e-mail or mobile phone, for printing or display by the recipient. An example is airline boarding passes. The new EPC, along with several other schemes, is widely available at reasonable cost.

The storage of data associated with tracking items will require many terabytes. Filtering and categorizing RFID data is needed to create useful information. It is likely that goods will be tracked by the pallet using RFID tags, and at package level with Universal Product Code (UPC) or EAN from unique barcodes.

The unique identity is a mandatory requirement for RFID tags, despite special choice of the numbering scheme. RFID tag data capacity is large enough that each individual tag will have a unique code, while current barcodes are limited to a single type code for a particular product. The uniqueness of RFID tags means that a product may be tracked as it moves from location to location while being delivered to a person. This may help to combat theft and other forms of product loss. The tracing of products is an important feature that is well supported with RFID tags containing a unique identity of the tag and the serial number of the object. This may help companies cope with quality deficiencies and resulting recall campaigns, but also contributes to concern about tracking and profiling of persons after the sale.

Waste management

Since around 2007 there been increasing development in the use of RFID in the waste management industry. RFID tags are installed on waste collection carts, linking carts to the owner's account for easy billing and service verification.^[112] The tag is embedded into a garbage and recycle container, and the RFID reader is affixed to the garbage and recycle trucks.^[113] RFID also measures a customer's set-out rate and provides insight as to the number of carts serviced by each waste collection vehicle. This RFID process replaces traditional "pay as you throw" (PAYT) municipal solid waste usage-pricing models.

Telemetry

Active RFID tags have the potential to function as low-cost remote sensors that broadcast telemetry back to a base station. Applications of tagometry data could include sensing of road conditions by implanted beacons, weather reports, and noise level monitoring.^[114]

Passive RFID tags can also report sensor data. For example, the Wireless Identification and Sensing Platform is a passive tag that reports temperature, acceleration and capacitance to commercial Gen2 RFID readers.

It is possible that active or battery-assisted passive (BAP) RFID tags could broadcast a signal to an in-store receiver to determine whether the RFID tag – and by extension, the product it is attached to – is in the store.

Regulation and standardization

To avoid injuries to humans and animals, RF transmission needs to be controlled.^[115] A number of organizations have set standards for RFID, including the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), ASTM International, the DASH7 Alliance and EPCglobal.^[116]

Several specific industries have also set guidelines, including the Financial Services Technology Consortium (FSTC) for tracking IT Assets with RFID, the Computer Technology Industry Association CompTIA for certifying RFID engineers, and the International Airlines Transport Association IATA for luggage in airports.

Every country can set its own rules for frequency allocation for RFID tags, and not all radio bands are available in all countries. These frequencies are known as the ISM bands (Industrial Scientific and Medical bands). The return signal of the tag may still cause interference for other radio users.

- Low-frequency (LF: 125–134.2 kHz and 140–148.5 kHz) (LowFID) tags and high-frequency (HF: 13.56 MHz) (HighFID) tags can be used globally without a license.
- Ultra-high-frequency (UHF: 865–928 MHz) (Ultra-HighFID or UHFID) tags cannot be used globally as there is no single global standard, and regulations differ from country to country.

In North America, UHF can be used unlicensed for 902–928 MHz (± 13 MHz from the 915 MHz center frequency), but restrictions exist for transmission power. In Europe, RFID and other low-power radio applications are regulated by ETSI recommendations EN 300 220 and EN 302 208, and ERO recommendation 70 03, allowing RFID operation with somewhat complex band restrictions from 865–868 MHz. Readers are required to monitor a channel before transmitting ("Listen Before Talk"); this requirement has led to some restrictions on performance, the resolution of which is a subject of current research. The North American UHF standard is not accepted in France as it interferes with its military bands. On July 25, 2012, Japan changed its UHF band to 920 MHz, more closely matching the United States' 915 MHz band, establishing an international standard environment for RFID.

In some countries, a site license is needed, which needs to be applied for at the local authorities, and can be revoked.

As of 31 October 2014, regulations are in place in 78 countries representing approximately 96.5% of the world's GDP, and work on regulations was in progress in three countries representing approximately 1% of the world's GDP.^[117]

Standards that have been made regarding RFID include:

- ISO 11784/11785 – Animal identification. Uses 134.2 kHz.
- ISO 14223 – Radiofrequency identification of animals – Advanced transponders
- ISO/IEC 14443: This standard is a popular HF (13.56 MHz) standard for HighFIDs which is being used as the basis of RFID-enabled passports under ICAO 9303. The Near Field Communication standard that lets mobile devices act as RFID readers/transponders is also based on ISO/IEC 14443.
- ISO/IEC 15693: This is also a popular HF (13.56 MHz) standard for HighFIDs widely used for non-contact smart payment and credit cards.
- ISO/IEC 18000: Information technology—Radio frequency identification for item management:
- ISO/IEC 18092 Information technology—Telecommunications and information exchange between systems—Near Field Communication—Interface and Protocol (NFCIP-1)
- ISO 18185: This is the industry standard for electronic seals or "e-seals" for tracking cargo containers using the 433 MHz and 2.4 GHz frequencies.
- ISO/IEC 21481 Information technology—Telecommunications and information exchange between systems—Near Field Communication Interface and Protocol –2 (NFCIP-2)
- ASTM D7434, Standard Test Method for Determining the Performance of Passive Radio Frequency Identification (RFID) Transponders on Palletized or Unitized Loads
- ASTM D7435, Standard Test Method for Determining the Performance of Passive Radio Frequency Identification (RFID) Transponders on Loaded Containers
- ASTM D7580, Standard Test Method for Rotary Stretch Wrapper Method for Determining the Readability of Passive RFID Transponders on Homogenous Palletized or Unitized Loads
- ISO 28560-2— specifies encoding standards and data model to be used within libraries.^[118]

In order to ensure global interoperability of products, several organizations have set up additional standards for RFID testing. These standards include conformance, performance and interoperability tests.

EPC Gen2

EPC Gen2 is short for *EPCglobal UHF Class 1 Generation 2*.

EPCglobal, a joint venture between GS1 and GS1 US, is working on international standards for the use of mostly passive RFID and the Electronic Product Code (EPC) in the identification of many items in the supply chain for companies worldwide.

One of the missions of EPCglobal was to simplify the Babel of protocols prevalent in the RFID world in the 1990s. Two tag air interfaces (the protocol for exchanging information between a tag and a reader) were defined (but not ratified) by EPCglobal prior to 2003. These protocols, commonly known as Class 0 and Class 1, saw significant commercial implementation in 2002–2005.^[119]

In 2004, the Hardware Action Group created a new protocol, the Class 1 Generation 2 interface, which addressed a number of problems that had been experienced with Class 0 and Class 1 tags. The EPC Gen2 standard was approved in December 2004. This was approved after a contention from Intermec that the standard may infringe a number of their RFID-related patents. It was decided that the standard itself does not infringe their patents, making the standard royalty free.^[120] The EPC Gen2 standard was adopted with minor modifications as ISO 18000-6C in 2006.^[121]

In 2007, the lowest cost of Gen2 EPC inlay was offered by the now-defunct company SmartCode, at a price of \$0.05 apiece in volumes of 100 million or more.^[122]

Problems and concerns

Data flooding

Not every successful reading of a tag (an observation) is useful for business purposes. A large amount of data may be generated that is not useful for managing inventory or other applications. For example, a customer moving a product from one shelf to another, or a pallet load of articles that passes several readers while being moved in a warehouse, are events that do not produce data that are meaningful to an inventory control system.^[123]

Event filtering is required to reduce this data inflow to a meaningful depiction of moving goods passing a threshold. Various concepts have been designed, mainly offered as middleware performing the filtering from noisy and redundant raw data to significant processed data.

Global standardization

The frequencies used for UHF RFID in the USA are as of 2007 incompatible with those of Europe or Japan. Furthermore, no emerging standard has yet become as universal as the barcode.^[124] To address international trade concerns, it is necessary to use a tag that is operational within all of the international frequency domains.

Security concerns

A primary RFID security concern is the illicit tracking of RFID tags. Tags, which are world-readable, pose a risk to both personal location privacy and corporate/military security. Such concerns have been raised with respect to the United States Department of Defense's recent adoption of RFID tags for supply chain management.^[125] More generally, privacy organizations have expressed concerns in the context of ongoing efforts to embed electronic product code (EPC) RFID tags in general-use products. This is mostly as a result of the fact that RFID tags can be read, and legitimate transactions with readers can be eavesdropped on, from non-trivial distances. RFID used in access control,^[126] payment and eID (e-passport) systems operate at a shorter range than EPC RFID systems but are also vulnerable to skimming and eavesdropping, albeit at shorter distances.^[127]

A second method of prevention is by using cryptography. Rolling codes and challenge-response authentication (CRA) are commonly used to foil monitor-repetition of the messages between the tag and reader, as any messages that have been recorded would prove to be unsuccessful on repeat transmission. Rolling codes rely upon the tag's ID being changed after each interrogation, while CRA uses software to ask for a cryptographically coded response from the tag. The protocols used during CRA can be symmetric, or may use public key cryptography.^[128]

While a variety of secure protocols have been suggested for RFID tags, in order to support long read range at low cost, many RFID tags have barely enough power available to support very low-power and therefore simple security protocols such as cover-coding.^[129]

Unauthorized reading of RFID tags presents a risk to privacy and to business secrecy.^[130] Unauthorized readers can potentially use RFID information to identify or track packages, persons, carriers, or the contents of a package.^[128] Several prototype systems are being developed to combat unauthorized reading, including RFID signal interruption,^[131] as well as the possibility of legislation, and 700 scientific papers

have been published on this matter since 2002.^[132] There are also concerns that the database structure of Object Naming Service may be susceptible to infiltration, similar to denial-of-service attacks, after the EPCglobal Network ONS root servers were shown to be vulnerable.^[133]

Health

Microchip-induced tumours have been noted during animal trials.^{[134][135]}

Shielding

In an effort to prevent the passive “skimming” of RFID-enabled cards or passports, the U.S. General Services Administration (GSA) issued a set of test procedures for evaluating electromagnetically opaque sleeves.^[136] For shielding products to be in compliance with FIPS-201 guidelines, they must meet or exceed this published standard; compliant products are listed on the website of the U.S. CIO's FIPS-201 Evaluation Program.^[137] The United States government requires that when new ID cards are issued, they must be delivered with an approved shielding sleeve or holder.^[138] Although many wallets and passport holders are advertised to protect personal information, there is little evidence that RFID skimming is a serious threat; data encryption and use of EMV chips rather than RFID makes this sort of theft rare.^{[139][140]}

There are contradictory opinions as to whether aluminum can prevent reading of RFID chips. Some people claim that aluminum shielding, essentially creating a Faraday cage, does work.^[141] Others claim that simply wrapping an RFID card in aluminum foil only makes transmission more difficult and is not completely effective at preventing it.^[142]

Shielding effectiveness depends on the frequency being used. Low-frequency LowFID tags, like those used in implantable devices for humans and pets, are relatively resistant to shielding, although thick metal foil will prevent most reads. High frequency HighFID tags (13.56 MHz—smart cards and access badges) are sensitive to shielding and are difficult to read when within a few centimetres of a metal surface. UHF Ultra-HighFID tags (pallets and cartons) are difficult to read when placed within a few millimetres of a metal surface, although their read range is actually increased when they are spaced 2–4 cm from a metal surface due to positive reinforcement of the reflected wave and the incident wave at the tag.^[143]

Controversies

Privacy

The use of RFID has engendered considerable controversy and some consumer privacy advocates have initiated product boycotts. Consumer privacy experts Katherine Albrecht and Liz McIntyre are two prominent critics of the “spychip” technology. The two main privacy concerns regarding RFID are as follows:

- As the owner of an item may not necessarily be aware of the presence of an RFID tag and the tag can be read at a distance without the knowledge of the individual, sensitive data may be acquired without consent.

- If a tagged item is paid for by credit card or in conjunction with use of a loyalty card, then it would be possible to indirectly deduce the identity of the purchaser by reading the globally unique ID of that item contained in the RFID tag. This is a possibility if the person watching also had access to the loyalty card and credit card data, and the person with the equipment knows where the purchaser is going to be.



Logo of the anti-RFID campaign by German privacy group digitalcourage (formerly FoeBuD)

Most concerns revolve around the fact that RFID tags affixed to products remain functional even after the products have been purchased and taken home and thus can be used for surveillance and other purposes unrelated to their supply chain inventory functions.^[144]

The RFID Network responded to these fears in the first episode of their syndicated cable TV series, saying that they are unfounded, and let RF engineers demonstrate how RFID works.^[145] They provided images of RF engineers driving an RFID-enabled van around a building and trying to take an inventory of items inside. They also discussed satellite tracking of a passive RFID tag.

The concerns raised may be addressed in part by use of the Clipped Tag. The Clipped Tag is an RFID tag designed to increase privacy for the purchaser of an item. The Clipped Tag has been suggested by IBM researchers Paul Moskowitz and Guenter Karjoth. After the point of sale, a person may tear off a portion of the tag. This allows the transformation of a long-range tag into a proximity tag that still may be read, but only at short range – less than a few inches or centimeters. The modification of the tag may be confirmed visually. The tag may still be used later for returns, recalls, or recycling.

However, read range is a function of both the reader and the tag itself. Improvements in technology may increase read ranges for tags. Tags may be read at longer ranges than they are designed for by increasing reader power. The limit on read distance then becomes the signal-to-noise ratio of the signal reflected from the tag back to the reader. Researchers at two security conferences have demonstrated that passive Ultra-HighFID tags normally read at ranges of up to 30 feet can be read at ranges of 50 to 69 feet using suitable equipment.^{[146][147]}

In January 2004 privacy advocates from CASPIAN and the German privacy group FoeBuD were invited to the METRO Future Store in Germany, where an RFID pilot project was implemented. It was uncovered by accident that METRO "Payback" customer loyalty cards contained RFID tags with customer IDs, a fact that was disclosed neither to customers receiving the cards, nor to this group of privacy advocates. This happened despite assurances by METRO that no customer identification data was tracked and all RFID usage was clearly disclosed.^[148]

During the UN World Summit on the Information Society (WSIS) between the 16th to 18 November 2005, founder of the free software movement, Richard Stallman, protested the use of RFID security cards by covering his card with aluminum foil.^[149]

In 2004–2005 the Federal Trade Commission staff conducted a workshop and review of RFID privacy concerns and issued a report recommending best practices.^[150]

RFID was one of the main topics of the 2006 Chaos Communication Congress (organized by the Chaos Computer Club in Berlin) and triggered a large press debate. Topics included electronic passports, Mifare cryptography and the tickets for the FIFA World Cup 2006. Talks showed how the first real-world mass

application of RFID at the 2006 FIFA Football World Cup worked. The group monochrom staged a special 'Hack RFID' song.^[151]

Government control

Some individuals have grown to fear the loss of rights due to RFID human implantation.

By early 2007, Chris Paget of San Francisco, California, showed that RFID information could be pulled from a US passport card by using only \$250 worth of equipment. This suggests that with the information captured, it would be possible to clone such cards.^[152]

According to ZDNet, critics believe that RFID will lead to tracking individuals' every movement and will be an invasion of privacy.^[153] In the book *SpyChips: How Major Corporations and Government Plan to Track Your Every Move* by Katherine Albrecht and Liz McIntyre, one is encouraged to "imagine a world of no privacy. Where your every purchase is monitored and recorded in a database and your every belonging is numbered. Where someone many states away or perhaps in another country has a record of everything you have ever bought. What's more, they can be tracked and monitored remotely".^[154]

Deliberate destruction in clothing and other items

According to an RSA laboratories FAQ, RFID tags can be destroyed by a standard microwave oven;^[155] however some types of RFID tags, particularly those constructed to radiate using large metallic antennas (in particular RF tags and EPC tags), may catch fire if subjected to this process for too long (as would any metallic item inside a microwave oven). This simple method cannot safely be used to deactivate RFID features in electronic devices, or those implanted in living tissue, because of the risk of damage to the "host". However the time required is extremely short (a second or two of radiation) and the method works in many other non-electronic and inanimate items, long before heat or fire become of concern.^[156]

Some RFID tags implement a "kill command" mechanism to permanently and irreversibly disable them. This mechanism can be applied if the chip itself is trusted or the mechanism is known by the person that wants to "kill" the tag.

UHF RFID tags that comply with the EPC2 Gen 2 Class 1 standard usually support this mechanism, while protecting the chip from being killed with a password.^[157] Guessing or cracking this needed 32-bit password for killing a tag would not be difficult for a determined attacker.^[158]

See also

- AS5678
- Balise
- Bin bug
- Campus card
- Chipless RFID
- Internet of Things
- Mass surveillance
- Microchip implant (human)
- Near Field Communication (NFC)
- PositiveID
- Privacy by design
- Proximity card
- Resonant inductive coupling
- RFdump
- RFID in schools
- RFID Journal
- RFID on metal
- RSA blocker tag
- Smart label
- Speedpass
- TecTile
- Tracking system

References

1. "RFID Inventory Tracking" (<https://www.controltekusa.com/news/rfid-inventory-tracking/>). *CONTROLTEK*. February 28, 2014. Retrieved May 12, 2022.
2. Automatic Identification and Data Collection (AIDC) (<http://www.mhi.org/fundamentals/automatic-identification>) Archived (<https://web.archive.org/web/20160505190510/http://www.mhi.org/fundamentals/automatic-identification>) May 5, 2016, at the [Wayback Machine](#)
3. Bhise, Kshama S. (February 2016). "Wildlife Animal Tracking Using RFID and GSM Technology" (<https://www.ijser.org/researchpaper/WILDLIFE-ANIMAL-TRACKING-USING-RFID-AND-GSM-TECHNOLOGY.pdf>) (PDF). *International Journal of Scientific & Engineering Research*. 7: 1–2 – via IJSER.
4. "USDA Announces Intent to Pursue Rulemaking on Radio Frequency Identification (RFID) Use in Animal Disease Traceability" (https://www.aphis.usda.gov/aphis/newsroom/news/sa_by_date/sa-2021/rfid-traceability-rulemaking). *USDA APHIS*. March 23, 2021. Retrieved May 12, 2022.
5. D'Onofrio, Tony (2022-05-01). "Then and Now: RFID, Self-Checkout, and IoT" (<https://losspreventionmedia.com/then-and-now-rfid-self-checkout-and-iot/>). *Loss Prevention Media*. Retrieved 2022-05-12.
6. Angell, I., Kietzmann, J. (2006). "RFID and the end of cash?" (https://web.archive.org/web/20140224155226/http://beedie.sfu.ca/files/Research/Journal_Articles/Journal_Articles_misc/RFID_and_the_end_of_Cash.pdf) (PDF). *Communications of the ACM*. 49 (12): 90–96. doi:10.1145/1183236.1183237 (<https://doi.org/10.1145/1183236.1183237>). S2CID 3559353 (<https://api.semanticscholar.org/CorpusID:3559353>). Archived from the original (http://beedie.sfu.ca/files/Research/Journal_Articles/Journal_Articles_misc/RFID_and_the_end_of_Cash.pdf) (PDF) on 2014-02-24. Retrieved 9 November 2013.
7. *RFID Forecasts, Players and Opportunities 2019-2029* (<https://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2019-2029/700>). IDTechEx. 2020-02-27.
8. *Hacking Exposed Linux: Linux Security Secrets & Solutions* (<https://books.google.com/books?id=f5Vz08spzw8C>) (third ed.). McGraw-Hill Osborne Media. 2008. p. 298. ISBN 978-0-07-226257-5.
9. "What are IFF Technologies?" (<https://www.baesystems.com/en-us/definition/what-are-iff-technologies>). *BAE Systems | United States*. Retrieved 2021-03-29.
10. Stockman, Harry (October 1948), "Communication by Means of Reflected Power", *Proceedings of the IRE*, 36 (10): 1196–1204, doi:10.1109/JRPROC.1948.226245 (<https://doi.org/10.1109/2FJRPROC.1948.226245>), S2CID 51643576 (<https://api.semanticscholar.org/CorpusID:51643576>)
11. "Genesis of the Versatile RFID Tag" (<http://www.rfidjournal.com/article/view/392/1/2>). *RFID Journal*. 10 October 2012. Retrieved 2013-09-22.
12. US 3713148 (<https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US3713148>), Cardullo, Mario W. & Parks, William L., "Transponder apparatus and system", published May 21, 1970, issued Jan 23, 1973
13. Landt, Jerry (2001). "Shrouds of Time: The history of RFID" (https://web.archive.org/web/20090327005501/http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf) (PDF). *AIM, Inc.* Archived from the original (http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf) (PDF) on 2009-03-27. Retrieved 2006-05-31.
14. "Real Time Location Systems" (http://www.clarinox.com/docs/whitepapers/RealTime_main.pdf) (PDF). clarinox. Retrieved 2010-08-04.
15. Charles A. Walton "Portable radio frequency emitting identifier" U.S. Patent 4,384,288 (<http://patents.google.com/patent/US4384288>) issue date May 17, 1983

16. David F. Everett, John W. Frech, Theodore Wright, Kelly M. Rodriguez "Identification system and method with passive tag" U.S. Patent 5,491,468 (<https://patents.google.com/patent/US5491468>) issue date February 13, 1996
17. "RFID-Tag" (<https://www.behance.net/gallery/67918923/RFID-Tag>). Behance. Retrieved 15 July 2018.
18. **SUBSTRATE** The substrate holds all other tag components together. The tag antenna is deposited or printed on the substrate, and the IC is then attached to this antenna. A substrate is usually made from flexible material such as thin plastic, but it may also be made from rigid material.
19. "Construction of RFID Tags - RFID chip and antenna" (<https://rfid4u.com/rfid-basics-resource/s/dig-deep-rfid-tags-construction/>). *RFID4U*. n.d. Retrieved 2020-03-01.
20. Bays, Barbara; McGowan, Mike (2016). "Use of RFID for Tracking Government Property - Proof of Concept/Pilot". *Sandia National Laboratories*. Sandia Corporation: 24.
21. Want, Roy (January–March 2006). "An Introduction to RFID Technology" (https://home.cs.colorado.edu/~rhan/CSCI_7143_001_Fall_2002/Papers/rfid_intro_01593568.pdf) (PDF). *Pervasive Computing*. January - March 2006: 25–33. doi:10.1109/MPRV.2006.2 (<https://doi.org/10.1109%2FMPRV.2006.2>). S2CID 130729 (<https://api.semanticscholar.org/CorpusID:130729>). Retrieved 2021-04-09 – via <https://home.cs.colorado.edu/>. {{cite journal}}: External link in |via= (help)
22. "How Does RFID Technology Work?" (<https://www.makeuseof.com/tag/technology-explained-how-do-rfid-tags-work/>). *MakeUseOf*. June 2017. Retrieved 2019-04-22.
23. Sen, Dipankar; Sen, Prosenjit; Das, Anand M. (2009), *RFID For Energy and Utility Industries*, PennWell, ISBN 978-1-59370-105-5, pp. 1-48
24. Weis, Stephen A. (2007), *RFID (Radio Frequency Identification): Principles and Applications*, MIT CSAIL, CiteSeerX 10.1.1.182.5224 (<https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.5224>)
25. "RFID and Rail: Advanced Tracking Technology – Railway Technology" (<http://www.railway-technology.com/features/feature1684/>). 16 March 2008. Retrieved 14 March 2018.
26. Kaleja, M. M., Herb, A. J., Rasshofer, R. H., Friedsam, G., & Biebl, E. M. (1999). "Imaging RFID system at 24 GHz for object localization". *IEEE MTT-S International Microwave Symposium Digest*. 4: 1497–1500. doi:10.1109/MWSYM.1999.780237 (<https://doi.org/10.1109%2FMWSYM.1999.780237>). ISBN 0-7803-5135-5. S2CID 22463766 (<https://api.semanticscholar.org/CorpusID:22463766>).
27. Hester, Jimmy GD, and Manos M. Tentzeris. (2017). "A mm-wave ultra-long-range energy-autonomous printed rfid-enabled van-atta wireless sensor: At the crossroads of 5G and IoT". *IEEE MTT-S International Microwave Symposium*: 1557–1560. doi:10.1109/MWSYM.2017.8058927 (<https://doi.org/10.1109%2FMWSYM.2017.8058927>). ISBN 978-1-5090-6360-4. S2CID 20439390 (<https://api.semanticscholar.org/CorpusID:20439390>).
28. Soltanaghaei, E., Prabhakara, A., Balanuta, A., Anderson, M., Rabaey, J. M., Kumar, S., & Rowe, A. (2021). "Millimetro: mmWave retro-reflective tags for accurate, long range localization". *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*: 69–82. doi:10.1145/3447993.3448627 (<https://doi.org/10.1145%2F3447993.3448627>). S2CID 231833014 (<https://api.semanticscholar.org/CorpusID:231833014>).
29. Daniel M. Dobkin, *The RF in RFID: Passive UHF RFID In Practice*, Newnes 2008 ISBN 978-0-7506-8209-1, chapter 8
30. John R. Vacca *Computer and information security handbook*, Morgan Kaufmann, 2009 ISBN 0-12-374354-0, page 208

31. Bill Glover, Himanshu Bhatt, *RFID essentials*, O'Reilly Media, Inc., 2006 ISBN 0-596-00944-5, pages 88–89
32. "Frequently Asked Questions - RFID Journal" (<https://www.rfidjournal.com/site/faqs>). *www.rfidjournal.com*. Retrieved 2019-04-22.
33. Paret, Dominique. *RFID at ultra and super high frequencies: theory and application*.
34. "STGF Report" (http://www.nerc.com/files/SGTF_Report_Final_posted_v1.1.pdf) (PDF).
35. "Ants' home search habit uncovered" (<http://news.bbc.co.uk/1/hi/england/bristol/8011998.stm>). *BBC News*. 2009-04-22. Retrieved 2013-09-03.
36. "Hitachi's RFID powder freaks us the heck out" (<https://www.engadget.com/2007/02/14/hitachi-his-rfid-powder-freaks-us-the-heck-out>). Engadget. Retrieved 2010-04-24.
37. TFOT (2007). "Hitachi Develops World's Smallest RFID Chip" (<https://web.archive.org/web/20090416235559/http://thefutureofthings.com/news/1032/hitachi-develops-worlds-smallest-rfid-chip.html>). Archived from the original (<http://thefutureofthings.com/news/1032/hitachi-develops-worlds-smallest-rfid-chip.html>) on 2009-04-16. Retrieved 2009-03-27.
38. Zewe, Adam (2021-11-18). "Pushing the limits of electronic circuits" (<https://news.mit.edu/2021/ruonan-han-circuits-1118>). *MIT News*. Retrieved 2021-11-18.
39. Matheson, Rob (2020-02-20). "Cryptographic "tag of everything" could protect the supply chain" (<https://news.mit.edu/2020/cryptographic-tag-supply-chain-0220>). *MIT News*. Retrieved 2021-11-18.
40. "EPTLS | The Electronic Product Tag & Labelling Scheme" (<http://eptls.org/rfid.html>). *eptls.org*. Retrieved 2019-04-22.
41. "Barcoding Inc. - FAQ - How much does an RFID tag cost?" (<https://web.archive.org/web/20111007191020/http://www.barcoding.com/faq/rfid-tag-cost.shtml>). 2011-10-07. Archived from the original (<http://www.barcoding.com/faq/rfid-tag-cost.shtml>) on 7 October 2011. Retrieved 2022-03-06.
42. Martein Meints (June 2007). "D3.7 A Structured Collection on Information and Literature on Technological and Usability Aspects of Radio Frequency Identification (RFID), FIDIS deliverable 3(7)" (<http://www.fidis.net/resources/deliverables/hightechid/#c1782>). Retrieved 2013-09-22.
43. Paolo Magrassi (2001). "A World Of Smart Objects: The Role Of Auto Identification Technologies" (<http://www.gartner.com>). Retrieved 2007-06-24.
44. Silva, S., Lowry, M., Macaya-Solis, C., Byatt, B., & Lucas, M. C. (2017). Can navigation locks be used to help migratory fishes with poor swimming performance pass tidal barrages? (<https://www.sciencedirect.com/science/article/pii/S0925857417300940>) A test with lampreys. *Ecological engineering*, 102, 291–302.
45. Pete Harrison (2009-07-28). "EU considers overhauling rules for lost air luggage" (<https://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSLS63631320090728>). *Reuters*. Retrieved 2009-09-09.
46. Vivaldi, F.; Melai, B.; Bonini, A.; Poma, N.; Salvo, P.; Kirchhain, A.; Tintori, S.; Bigongiari, A.; Bertuccelli, F.; Isola, G.; Di Francesco, F. (October 2020). "A Temperature-Sensitive RFID Tag for the Identification of Cold Chain Failures" (https://figshare.com/articles/A_Temperature-Sensitive_RFID_Tag_for_the_Identification_of_Cold_Chain_Failures/12197784). *Sensors Actuators A: Physical*. **313**: 112182. doi:10.1016/j.sna.2020.112182 (<https://doi.org/10.1016/6%2Fj.sna.2020.112182>). S2CID 224856329 (<https://api.semanticscholar.org/CorpusID:224856329>).
47. [Miles, Stephen Bell (2011). *RFID Technology and Applications*. London: Cambridge University Press. pp. 6–8]

48. "Crucial Factors for Implementing Warehouse Management System | SIPMM Publications" (<https://publication.sipmm.edu.sg/crucial-factors-implementing-warehouse-management-system/>). *publication.sipmm.edu.sg*. 2021-12-19.
49. "Benefits of RFID in Theft Protection – CONTROLTEK" (<http://www.controltekusa.com/controltek-news/benefits-of-rfid-in-theft-protection/>). *Controltek*. 14 February 2014. Retrieved 11 October 2017.
50. Rohrllich, Justin (15 December 2010). "RFID-Tagged Gaming Chips Render Hotel Bellagio Robbery Haul Worthless" (<http://www.minyanville.com/businessmarkets/articles/bellagio-wynn-casino-rfid-gambling-las/12/15/2010/id/31714>). *Minyanville Financial Media*. Retrieved 16 December 2010.
51. "RFID use raises on-slope privacy concerns" (<https://www.espn.com/action/news/story?id=5810585>). *ESPN.com*. 2010-11-15. Retrieved 2021-03-23.
52. "Mercedes Provides RFID Facebook Checkins at PGA Championship" (<http://mashable.com/2011/08/11/mercedes-rfid-facebook/>). *Mashable.com*. 2011-08-11. Retrieved 2013-09-22.
53. Patrick Sweeney (2013-03-26). "Social Media Winner's Circle at Geneva Motor Show [Video]" (<https://web.archive.org/web/20130927053606/http://socialmediatoday.com/pjsweeney/1322626/social-media-winner-s-circle-geneva-motor-show>). *Social Media Today*. Archived from the original (<http://socialmediatoday.com/pjsweeney/1322626/social-media-winner-s-circle-geneva-motor-show>) on 2013-09-27. Retrieved 2013-09-22.
54. James P. Farrell & Ralf Saykiewicz. "Keeping Track of Promotion Progress: How Marketing Will Become the Greatest Advocate of RFID" (<https://web.archive.org/web/20080411211453/http://www.consumergoods.com/ME2/dirmod.asp?sid=&nm=&type=Publishing&mod=Publications%3A%3AArticle&mid=8F3A7027421841978F18BE895F87F791&tier=4&id=07CA1C544D3E4FD1916C7A6D2638913E>). *Consumer Goods Technology*. Archived from the original (<http://www.consumergoods.com/ME2/dirmod.asp?sid=&nm=&type=Publishing&mod=Publications%3A%3AArticle&mid=8F3A7027421841978F18BE895F87F791&tier=4&id=07CA1C544D3E4FD1916C7A6D2638913E>) on 2008-04-11. Retrieved 2008-04-10.
55. "AEI technology" (<https://web.archive.org/web/20080406031000/http://www.aeitag.com/aeirfidtec.html>). *Softail*. Archived from the original (<http://www.aeitag.com/aeirfidtec.html>) on 2008-04-06. Retrieved 2008-10-12.
56. "Qantas Next Generation Check-in" (<http://www.qantas.com.au/travel/airlines/next-generation-checkin/global/en>). *Qantas Airways Limited*. Retrieved 2010-12-27.
57. [1] (<http://www.cargo-box.com>) Archived (<https://web.archive.org/web/20150801102438/http://www.cargo-box.com/>) August 1, 2015, at the Wayback Machine
58. "Bermuda's RFID Vehicle Registration System Could Save \$2 Million/Year" (<http://www.rfidjournal.com/article/view/3321>). *Rfidjournal.com*. 2007-05-18. Retrieved 2013-09-03.
59. "Smart License May Cut Car Theft" (<http://www.rfidjournal.com/article/view/89>). *Rfidjournal.com*. 2002-10-11. Retrieved 2013-09-03.
60. "Mexico's Electronic Vehicle Registration system opens with Sirit open road toll technology, Dec 29, 2009" (<https://web.archive.org/web/20130703170620/http://www.tollroadsnews.com/node/4513>). *Tollroadsnews.com*. Archived from the original (<http://www.tollroadsnews.com/node/4513>) on 2013-07-03. Retrieved 2013-09-03.
61. "New York's award-winning traffic control system" (<http://www.itsinternational.com/sections/nafta/features/new-yorks-award-winning-traffic-control-system/>). *ITS International*. January–February 2013. Retrieved 3 May 2014.
62. Rosová, Balog, and Šimeková., Andrea, Michal, and Žofia (2013). "The use of the RFID in rail freight transport in the world as one of the new technologies of identification and communication" (<https://www.researchgate.net/publication/292665484>). *Acta Montanistica Slovaca*. **18** (1): 26–32.

63. "Locating and Marking Products" (http://solutions.3m.com/wps/portal/3M/en_US/Telecom/Home/Products/LocatingMarking/). 3M Company. Retrieved 25 June 2012.
64. "Datatilsynet misfornøyd med nye pass" (<https://web.archive.org/web/20080405212252/http://www.digi.no/php/art.php?id=275753>). Digi.no. Archived from the original (<http://www.digi.no/php/art.php?id=275753>) on 2008-04-05. Retrieved 2013-09-22.
65. "Uruguay a la vanguardia con nuevo pasaporte electrónico" (https://web.archive.org/web/20210223164859/https://www.minterior.gub.uy/index.php?option=com_content&view=article&id=3227). Ministerio del Interior. 2015-10-15. Archived from the original (https://www.minterior.gub.uy/index.php?option=com_content&view=article&id=3227) on 2021-02-23. Retrieved 2021-02-23.
66. "Contactless inlays from SMARTRAC ordered for US ePassport project" (<http://www.contactlessnews.com/2006/11/30/contactless-inlays-from-smartrac-ordered-for-us-epassport-project/>). Retrieved 2009-03-25.
67. Lettice, John (30 January 2006). "Face and fingerprints swiped in Dutch biometric passport crack: Chip skimmed, then security breached" (https://web.archive.org/web/20060131005717/https://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/). *The Register*. Archived from the original (https://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/) on 31 January 2006. Retrieved 9 September 2013.
68. "United States sets date for E-passports" (<http://rfidjournal.com/article/articleview/1951/1/132/>).
69. Mary Catherine O'Connor (7 January 2008). "RFID Is Key to Car Clubs' Success" (<http://www.rfidjournal.com/article/view/3839/2>). RFID Journal. Retrieved 9 May 2011.
70. Tay, Lay (2007-11-01). "HDB Introduces RFID Season Parking Ticket" (<http://www.rfid-asia.info/2007/11/hdb-introduce-rfid-season-parking.htm>). RFID Asia. Retrieved 2009-10-17.
71. *USDA Bets the Farm on Animal ID Program (http://www.thenation.com/doc/20071231/pentl_and_gumpert)
72. "National Livestock Identification System" (<https://web.archive.org/web/20130820085741/http://www.mla.com.au/Meat-safety-and-traceability/National-Livestock-Identification-System>). Meat & Livestock Australia Limited. Archived from the original (<http://www.mla.com.au/Meat-safety-and-traceability/National-Livestock-Identification-System>) on 2013-08-20. Retrieved 2013-09-03.
73. Carvalho, Mario Cesar (November 11, 1997). "Artista implanta hoje chip no corpo" (<https://acervo.folha.com.br/leitor.do?numero=13700&keyword=Kac&anchor=282247&origem=busca&originURL=&pd=e5616b5794dde0ab6a687a693c931980/>). *Folha de S.Paulo* (in Portuguese). Retrieved 14 June 2021.
74. Esnal, Luis (December 15, 1997). "Un hombre llamado 026109532" (<https://web.archive.org/web/20170201160159/http://www.ekac.org/lanacion.html>). *Internet Archive Wayback Machine* (in Spanish). La Nación. Archived from the original (<http://www.ekac.org:80/lanacion.html>) on 1 February 2017. Retrieved 14 June 2021.
75. "1º implante de chip ao vivo - Jornal das 10 - Canal 21 - SP - 1997" (<https://www.youtube.com/watch?v=7y2tbPaYqfQ>). *YouTube*.
76. Witt, Sam. "CNN – Is human chip implant wave of the future? – January 14, 1999" (<http://edition.cnn.com/TECH/computing/9901/14/chipman.idg/>). *edition.cnn.com*. Retrieved 14 March 2018.
77. "Professor has world's first silicon chip implant" (<https://www.independent.co.uk/news/professor-has-worlds-first-silicon-chip-implant-1174101.html>). 26 August 1998. Retrieved 14 March 2018.
78. "Technology | Barcelona clubbers get chipped" (<http://news.bbc.co.uk/2/hi/technology/3697940.stm>). *BBC News*. 2004-09-29. Retrieved 2013-09-22.

79. Gasson, M. N. (2010). "Human Enhancement: Could you become infected with a computer virus?" (http://centaur.reading.ac.uk/29329/1/GASSON_ISTAS2010.pdf) (PDF). *2010 IEEE International Symposium on Technology and Society*. pp. 61–68.
doi:10.1109/ISTAS.2010.5514651 (<https://doi.org/10.1109%2FISTAS.2010.5514651>).
ISBN 978-1-4244-7777-7. S2CID 3098538 (<https://api.semanticscholar.org/CorpusID:3098538>).
80. Greene, Thomas C. (2004). "Feds approve human RFID implants" (https://www.theregister.co.uk/2004/10/14/human_rfid_implants/). *The Register*. Retrieved 2007-03-01.
81. Monahan, Torin and Tyler Wall. 2007. Somatic Surveillance: Corporeal Control through Information Networks ([http://www.surveillance-and-society.org/articles4\(3\)/somatic.pdf](http://www.surveillance-and-society.org/articles4(3)/somatic.pdf)). *Surveillance & Society* 4 (3): 154–173 Archived ([https://web.archive.org/web/20160615201126/http://www.surveillance-and-society.org/articles4\(3\)/somatic.pdf](https://web.archive.org/web/20160615201126/http://www.surveillance-and-society.org/articles4(3)/somatic.pdf)) 2016-06-15 at the Wayback Machine
82. Kietzmann, J., Angell, I. (2010). "Panopticon revisited" (https://web.archive.org/web/20140224154000/http://beedie.sfu.ca/files/Research/Journal_Articles/Journal_Articles_2010/Panopticon_revisited.pdf) (PDF). *Communications of the ACM*. **53** (6): 135–138.
doi:10.1145/1743546.1743582 (<https://doi.org/10.1145%2F1743546.1743582>).
S2CID 10487109 (<https://api.semanticscholar.org/CorpusID:10487109>). Archived from the original (http://beedie.sfu.ca/files/Research/Journal_Articles/Journal_Articles_2010/Panopticon_revisited.pdf) (PDF) on 2014-02-24. Retrieved 9 November 2013.
83. Fulton, Nic (2006-07-22). "Reuters" (<https://web.archive.org/web/20170202020437/http://blogs.reuters.com/mediafile/2006/07/22/high-tech-cloning/>). *Blogs.reuters.com*. Archived from the original (<http://blogs.reuters.com/mediafile/2006/07/22/high-tech-cloning/>) on 2017-02-02. Retrieved 2013-09-03.
84. Rosenbaum, Benjamin P. (28 February 2014). "Radio Frequency Identification (RFID) in Health Care: Privacy and Security Concerns Limiting Adoption". *Journal of Medical Systems*. **38** (3): 19. doi:10.1007/s10916-014-0019-z (<https://doi.org/10.1007%2Fs10916-014-0019-z>). PMID 24578170 (<https://pubmed.ncbi.nlm.nih.gov/24578170/>). S2CID 11368940 (<https://api.semanticscholar.org/CorpusID:11368940>).
85. Lahtela, Antti. "A Short Overview of the RFID Technology in Healthcare" (<https://www.academia.edu/703195>). *2009 Fourth International Conference on Systems and Networks Communications*.
86. "RFID Frequently Asked Questions" (<http://www.rfidjournal.com/faq/show?68>). *RFIDJournal.com*. Retrieved 2013-05-20.
87. "Group Health Reinvents Patient Care With RTLS" (<http://www.rfidjournal.com/article/print/9828>). *RFID Journal*. 22 August 2012.
88. "Veterans Affairs to Install RFID in Hospitals across America" (<https://web.archive.org/web/20140319083312/http://www.impinj.com/blog/veteran-affairs-to-install-rfid-in-hospitals-across-america/>). *Impinj*. 14 June 2013. Archived from the original (<http://www.impinj.com/blog/veteran-affairs-to-install-rfid-in-hospitals-across-america/>) on 19 March 2014.
89. Fisher, Jill A., Monahan, Torin (2012). "Evaluation of Real-time Location Systems in their Hospital Contexts" (http://publicsurveillance.com/papers/Fisher_Monahan_IJMI-2012.pdf) (PDF). *International Journal of Medical Informatics*. **81** (10): 705–712.
doi:10.1016/j.ijmedinf.2012.07.001 (<https://doi.org/10.1016%2Fj.ijmedinf.2012.07.001>).
PMID 22857790 (<https://pubmed.ncbi.nlm.nih.gov/22857790/>).
90. Fisher, Jill A., Monahan, Torin (2008). "Tracking the Social Dimensions of RFID Systems in Hospitals" (http://publicsurveillance.com/papers/Fisher_Monahan_RFID_IJMI.pdf) (PDF). *International Journal of Medical Informatics*. **77** (3): 176–183.
doi:10.1016/j.ijmedinf.2007.04.010 (<https://doi.org/10.1016%2Fj.ijmedinf.2007.04.010>).
PMID 17544841 (<https://pubmed.ncbi.nlm.nih.gov/17544841/>).

91. Fisher, Jill A. 2006. Indoor Positioning and Digital Management: Emerging Surveillance Regimes in Hospitals (http://media.wix.com/ugd/e5e1e1_9618d4aaaa1240f4bfa2e6fc8178b144.pdf). In T. Monahan (Ed), *Surveillance and Security: Technological Politics and Power in Everyday Life* (pp. 77–88). New York: Routledge.
92. "Electronic tags for eggs, sperm and embryos – life – 30 March 2005" (<https://www.newscientist.com/article.ns?id=dn7209>). *New Scientist*. Retrieved 2010-04-24.
93. "Verichip Special Report" (<https://web.archive.org/web/20120323031257/http://www.spychips.com/devices/verichip-fda-report.html>). spychips.com. Archived from the original (<http://www.spychips.com/devices/verichip-fda-report.html>) on 2012-03-23. Retrieved 2013-09-22.
94. Butters, Alan (December 2006). "Radio Frequency Identification: An Introduction for Library Professionals" (<http://search.informit.com.au/documentSummary;dn=312996058408409;res=IELHSS>). *Australasian Public Libraries and Information Services*. **19** (4): 164–74. ISSN 1030-5033 (<https://www.worldcat.org/issn/1030-5033>).
95. Sing, Jay; Brar, Navjit; Fong, Carmen (2013). "The State of RFID Applications in Libraries" (<https://doi.org/10.6017%2Fital.v25i1.3326>). *Information Technology and Libraries*. 25–32: 24. doi:10.6017/ital.v25i1.3326 (<https://doi.org/10.6017%2Fital.v25i1.3326>).
96. Wadham, Rachel (2003). "Radio Frequency Identification". *Library Mosaics*. **14** (5): 22.
97. Chellappandi, P; Sivankalai, S (October 2013). ISSN: 2321 – 788X. "Implementation Of RFID Technology In Library – Book Exhausting and Retrieval For Readers" (<https://www.researchgate.net/publication/259854363>). *Shanlax International Journal of Arts, Science & Humanities*. **1** (2): 25–32 – via ResearchGate.
98. Molnar, David; Wagner, David (June 8, 2004). "Privacy and Security in Library RFID: Issues, Practices, and Architectures" (<https://www.researchgate.net/publication/221609472>). *Conference: Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25–29, 2004*. **1**: 1–20 – via ResearchGate.
99. Ferguson, Stuart; Thornley, Clare; Gibb, Forbes (2015), "How do libraries manage the ethical and privacy issues of RFID implementation? A qualitative investigation into the decision-making processes of ten libraries" (<https://www.researchgate.net/publication/270618836>), *Journal of Librarianship and Information Science*, **47** (2): 117–130, doi:10.1177/0961000613518572 (<https://doi.org/10.1177%2F0961000613518572>), hdl:10197/5242 (<https://hdl.handle.net/10197%2F5242>), S2CID 28009426 (<https://api.semanticscholar.org/CorpusID:28009426>)
100. Dorman, David (December 2003). "RFID Poses No Problem for Patron Privacy" (<http://www.ala.org/PrinterTemplate.cfm?section=archive&template=/ContentManagement/ContentDisplay.cfm&ContentID=50931>). *American Libraries*. **34** (11): 86.
101. Rowe, Paul (November 9, 2011). "RFID Technology in use at the Otago Museum" (<https://vernonsystems.com/rfid-technology-in-use-at-the-otago-museum/>). *Vernon Systems*.
102. Hsi, Sherry; Fait, Holly (2005). "RFID enhances visitors' museum experience at the Exploratorium". *Communications of the ACM*. **48** (9): 60–5. doi:10.1145/1081992.1082021 (<https://doi.org/10.1145%2F1081992.1082021>). S2CID 8334725 (<https://api.semanticscholar.org/CorpusID:8334725>).
103. "Schoolchildren to be RFID-chipped" (<https://web.archive.org/web/20120427003216/http://networks.silicon.com/lans/0,39024663,39122042,00.htm>). Networks.silicon.com. Archived from the original (<http://networks.silicon.com/lans/0,39024663,39122042,00.htm>) on April 27, 2012. Retrieved 2013-09-03.
104. Williams, Christopher (2007-10-22). "Schoolkid chipping trial 'a success'" (https://www.theregister.co.uk/2007/10/22/kid_chipping_doncaster_go/). *Theregister.co.uk*. Retrieved 2013-09-03.

105. Baghya Lakshmi (2012-09-16). "Using rfid technology to develop an attendance system and avoid traff..." (<https://www.slideshare.net/baghyaharini/using-rfid-technology-to-develop-an-attendance-system-and-avoid-traffic-1>).
106. "Epic Mix – Skiers [sic] and Snowboarders Social Media Dream" (<http://cliqology.com/2010/09/epic-mix-skiers-and-snowboards-social-media-dream/>). 2010-09-07. Retrieved 2013-09-22.
107. "Vail Resorts Launches Epic Mix | SNOWBOARD MAGAZINE" (<https://web.archive.org/web/20100904085254/http://snowboard-mag.com/content/vail-resorts-launches-epic-mix-39814>). Archived from the original (<http://snowboard-mag.com/content/vail-resorts-launches-epic-mix-39814>) on 2010-09-04. Retrieved 2020-03-01.
108. Kinsella, Bret. (2010-09-07) Vail shows that Consumer RFID delivers a better experience (<http://blog.odintechnologies.com/odin-rfid-blog/bid/51179/Vail-shows-that-Consumer-RFID-delivers-a-better-experience>) Archived (<https://web.archive.org/web/20101106030526/http://blog.odintechnologies.com/odin-rfid-blog/bid/51179/Vail-shows-that-Consumer-RFID-delivers-a-better-experience>) 2010-11-06 at the [Wayback Machine](#). [Blog.odintechnologies.com](http://blog.odintechnologies.com). Retrieved on 2013-08-16.
109. "How a pair of microchips could transform football into an intricate dance of data" (<http://www.dailydot.com/technology/nfl-rfid-player-tracking-zebra-technologies/>). *DailyDot*. 2015-08-12. Retrieved 1 September 2015.
110. "The NFL has a (RFID) Chip on its shoulder" (<https://web.archive.org/web/20150906105747/http://news.surgogroup.com/nfl-has-a-rfid-chip-on-its-shoulder/>). *News Surgo Group*. Archived from the original (<http://news.surgogroup.com/nfl-has-a-rfid-chip-on-its-shoulder/>) on 2015-09-06. Retrieved 1 September 2015.
111. Moynihan, Tim (2015-08-07). "All NFL Players Are Getting RFID Chips This Season" (<https://www.wired.com/2015/08/nfl-players-getting-rfid-chips-season/>). *Wired*. Retrieved 1 September 2015.
112. Chowdhury, Belal; Chowdhury, Morshed (December 2, 2007). "RFID-based Real-time Smart Waste Management System" (<http://dro.deakin.edu.au/eserv/DU:30008105/chowdhury-rfid-based-2007.pdf>) (PDF). *2007 Australasian Telecommunication Networks and Applications Conference December 2nd – 5th 2007*. **1**: 175–180. doi:10.1109/ATNAC.2007.4665232 (<https://doi.org/10.1109%2FATNAC.2007.4665232>). hdl:10536/DRO/DU:30008105 (<https://hdl.handle.net/10536%2FDRO%2FDU%3A30008105>). ISBN 978-1-4244-1557-1. S2CID 18506491 (<https://api.semanticscholar.org/CorpusID:18506491>) – via Deakin University DRO.
113. "RFID Still In Early Stages of Adoption by Waste Industry" (<http://www.waste360.com/route-optimization/rfid-still-early-stages-adoption-waste-industry>). 2016-08-10.
114. 0001-0782 (<https://www.worldcat.org/search?fq=x0:jrn&q=n2:0001-0782>)
115. "RFID Regulations" (<https://rfid4u.com/rfid-basics-resources/basics-rfid-regulations/>). *RFID4U*. n.d. Retrieved 2020-03-01.
116. Yang, Kuo-pao; Beaubouef, Theresa (2011-04-01). "Radio frequency identification (RFID) projects for computer science" (<https://dl.acm.org/doi/abs/10.5555/1953573.1953586>). *Journal of Computing Sciences in Colleges*. **26** (4): 78–84. ISSN 1937-4771 (<https://www.worldcat.org/issn/1937-4771>).
117. "Regulatory status for using RFID in the EPC Gen 2 band (860 to 960 MHz) of the UHF spectrum" (http://www.gs1.org/docs/epc/UHF_Regulations.pdf) (PDF). GS1.org. 2014-10-31. Retrieved 2015-03-23.
118. "ISO 28560-2:2011 – Information and documentation – RFID in libraries – Part 2: Encoding of RFID data elements based on rules from ISO/IEC 15962" (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50997). *www.iso.org*. Retrieved 14 March 2018.

119. "RFID Standards and Mandates" (<https://rfid4u.com/rfid-basics-resources/how-to-select-a-correct-rfid-tag-standards-mandates/>).
120. Roberti, Mark (2004-12-16). "EPCglobal Ratifies Gen 2 Standard" (<http://www.rfidjournal.com/article/view/1293>). RFID Journal. Retrieved 2011-07-07.
121. Catherine O'Connor, Mary (2004-07-12). "Gen 2 EPC Protocol Approved as ISO 18000-6C" (<http://www.rfidjournal.com/article/view/2481/1/1>). RFID Journal. Retrieved 2011-07-07.
122. Roberti, Mark (2006-05-06). "A 5-Cent Breakthrough" (<http://www.rfidjournal.com/article/articleview/2295/1/128/>). RFID Journal. Retrieved 2007-01-26.
123. Bill Glover, Himanshu Bhatt, *RFID Essentials*, O'Reilly Media, Inc., 2006 ISBN 0-596-00944-5 page 43
124. "Radio Silence" (http://economist.com/printedition/displaystory.cfm?story_id=9249278). *The Economist*. 7 June 2007.
125. "What's New" (<https://web.archive.org/web/20060228101133/http://www.acq.osd.mil/log/rfid/index.htm>). *Radio Frequency Identification (RFID)*. 4 April 2007. Archived from the original (<http://www.acq.osd.mil/log/rfid/index.htm>) on 28 February 2006.
126. S. A. E., Elshrief; R. A. Sadek; A. Ghalwash (March 2014). "Comparative analysis of authentication techniques to Secure Low Level Reader Protocol (LLRP)". *2014 31st National Radio Science Conference (NRSC), Cairo, Egypt*: 73–81. doi:10.1109/NRSC.2014.6835063 (<https://doi.org/10.1109%2FNRSC.2014.6835063>). S2CID 21520509 (<https://api.semanticscholar.org/CorpusID:21520509>).
127. Hancke, Gerhard P (2011). "Practical eavesdropping and skimming attacks on high-frequency RFID tokens" (<https://web.archive.org/web/20160527141257/http://iospress.metapress.com/content/xx855446h2kh84r2/>). *Journal of Computer Security*. **19** (2): 259–288. CiteSeerX 10.1.1.169.9341 (<https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.169.9341>). doi:10.3233/JCS-2010-0407 (<https://doi.org/10.3233%2FJCS-2010-0407>). Archived from the original (<http://iospress.metapress.com/content/xx855446h2kh84r2/>) on 27 May 2016. Retrieved 10 August 2012.
128. Ilyas, edited by Syed Ahson, Mohammad (2008). "26.5" (<https://books.google.com/books?id=q4aCyZnq0cwC&q=Rather,+the+reader+issues+a+challenge+to+the+tag,+which+responds+with+a+result+computed+using+a+cryptographic+circuit+keyed+with+some+secret+value&pg=PA478>). *RFID handbook : applications, technology, security, and privacy* ([Online-Ausg.] ed.). Boca Raton: CRC Press. p. 478. ISBN 9781420054996. Retrieved 7 August 2012. {{cite book}}: |first= has generic name (help)
129. "RFID: Social Implications" (<https://polygait.calpoly.edu/what-rfid/social-implications>).
130. "Business risks from naive use of RFID in tracking, tracing and logistics - Conference papers - VDE Publishing House" (<https://www.vde-verlag.de/proceedings-en/453168007.html>). *www.vde-verlag.de*. Retrieved 2019-12-09.
131. "RFID Privacy and Security" (<https://web.archive.org/web/20061218210709/http://www.rsasecurity.com/rsalabs/node.asp?id=2115>). RSA Laboratories. Archived from the original (<http://www.rsasecurity.com/rsalabs/node.asp?id=2115>) on 2006-12-18. Retrieved 2013-09-22.
132. "RFID Security and Privacy Lounge" (<http://avoine.net/rfid/>). Avoine.net. Retrieved 2013-09-22.
133. Tedjasaputra, Adi (2006-12-11). "Putting RFID Network Security in Perspective" (<http://www.rfid-asia.info/2007/02/putting-rfid-network-security-in.htm>). RFID Asia. Retrieved 2007-08-03.
134. Albrecht, Katherine (2010). *Microchip-induced tumors in laboratory rodents and dogs: A review of the literature 1990–2006*. IEEE. pp. 337–349. doi:10.1109/ISTAS.2010.5514622 (<https://doi.org/10.1109%2FISTAS.2010.5514622>). ISBN 978-1-4244-7777-7. S2CID 2813360 (<https://api.semanticscholar.org/CorpusID:2813360>).

135. Lewan, Todd (8 September 2007). "Chip Implants Linked to Animal Tumors" (https://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html). *Washington Post*.
136. "Electromagnetically Opaque Sleeve Test Procedure version 3.0.0" (https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1171/2017/01/GSA_EP_Electromagnetic_v13.1.pdf) (PDF). GSA.
137. "FIPS 201 Evaluation Program Approved Products List (APL)" (<https://www.idmanagement.gov/approved-products-list>). U.S. CIO and the Federal CIO Councils.
138. "FIPS-201, Personal Identity Verification (PIV) of Federal Employees and Contractors" (<http://web.archive.org/web/20101226075308/http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>) (PDF). NIST. Archived from the original (<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>) (PDF) on 2010-12-26. Retrieved 2019-01-10.
139. Oremus, Will (2015-08-25). "Do You Really Need an RFID-Blocking Wallet?" (<https://slate.com/human-interest/2015/08/credit-cards-passports-and-rfid-fraud-are-special-blocking-wallets-necessary.html>). *Slate Magazine*. Retrieved 2019-11-10.
140. "There Are Plenty Of RFID-Blocking Products, But Do You Need Them?" (<https://www.npr.org/sections/alltechconsidered/2017/07/04/535518514/there-are-plenty-of-rfid-blocking-products-but-do-you-need-them>). *NPR.org*. Retrieved 2019-11-10.
141. "Can Aluminum Shield RFID Chips?" (https://web.archive.org/web/20140330050519/http://www.rfid-shield.com/info_doesitwork.php). RFID Shield. Archived from the original (http://www.rfid-shield.com/info_doesitwork.php) on 2014-03-30. Retrieved 2007-03-27.
142. "Aluminum Foil Does Not Stop RFID" (<http://www.omniscienceisbliss.org/rfid.html>). Omniscience is Bliss.
143. "A Primer on RFID" (http://www.falkensecurenetworks.com/PDFs/A_Primer_on_RFID.pdf) (PDF).
144. Markus Hansen, Sebastian Meissner: Identification and Tracking of Individuals and Social Networks using the Electronic Product Code on RFID Tags (<https://tepin.aiki.de/blog/uploads/2007-hansen-meissner-tracking-epc-rfid-ifip.pdf>), IFIP Summer School, Karlstad, 2007, Slides (<https://tepin.aiki.de/blog/uploads/20070807-ifip-hansen-meissner-tracking-rfid-epc.pdf>).
145. "How to read data from rfid reader" (<http://0y3v.errandrunner.org/onbqfGf>). *0y3v.errandrunner.org*. Retrieved 2019-04-22.
146. [2] (<http://blogs.pcworld.com/staffblog/archives/000798.html>) Archived (<https://web.archive.org/web/20110928040106/http://blogs.pcworld.com/staffblog/archives/000798.html>) September 28, 2011, at the *Wayback Machine*
147. [3] (http://blog.makezine.com/archive/2005/07/_defcon_rfid_wo.html) Archived (https://web.archive.org/web/20090207081350/http://blog.makezine.com/archive/2005/07/_defcon_rfid_wo.html) February 7, 2009, at the *Wayback Machine*
148. Katherine Albrecht; Liz McIntyre. "The METRO "Future Store" Special Report" (<https://web.archive.org/web/20050508083244/http://www.spychips.com/metro/overview.html>). Spychips. Archived from the original (<http://www.spychips.com/metro/overview.html>) on 2005-05-08. Retrieved 2005-05-05.
149. Richard M Stallman. "The WSIS in Tunis" (<http://www.fsf.org/blogs/rms/entry-20060125.html>). Fsf.org. Retrieved 2013-09-22.
150. "Radio Frequency Identification: Applications and Implications for Consumers" (<http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf>) (PDF). Ftc.gov. March 2005. Retrieved 2013-09-22.
151. monochrom. "R F I D" (<https://web.archive.org/web/20100220122421/http://www.monochrom.at/rfid/>). Archived from the original (<http://www.monochrom.at/rfid/>) on 2010-02-20. Retrieved 2007-01-04.

152. Iain Thomson in San Francisco. "Hacker clones passports in drive-by RFID heist – V3.co.uk – formerly vnunet.com" (<https://web.archive.org/web/20100324060524/http://www.v3.co.uk/vnunet/news/2235666/hackers-clones-passports-drive>). V3.co.uk. Archived from the original (<http://www.v3.co.uk/vnunet/news/2235666/hackers-clones-passports-drive>) on 2010-03-24. Retrieved 2010-04-24.
153. "Human chips more than skin-deep | Tech News on ZDNet" (https://web.archive.org/web/20100324122642/http://news.zdnet.com/2100-9584_22-138001.html). News.zdnet.com. Archived from the original (http://news.zdnet.com/2100-9584_22-138001.html) on 2010-03-24. Retrieved 2010-04-24.
154. Katherine Albrecht; Liz McIntyre (2005). *Spychips: how major corporations and government plan to track your every move with RFID* (<https://books.google.com/books?id=YDxDuMYVJdcC&q=RFID+Government&pg=PR9>). Thomas Nelson Inc. ISBN 978-1-59555-020-0.
155. "FAQ on RFID and RFID privacy" (<http://www.emc.com/emc-plus/rsa-labs/research-areas/faq-on-rfid-and-rfid-privacy.htm#13>). rsa.com. Retrieved 2015-03-23.
156. "Declara | Your Personal Knowledge Engine" (<https://declara.com/content/kaZAL635>). *declara.com*. Retrieved 2019-04-22.
157. "EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID, Version 2.0.0" (http://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_2_0_0_standard_20131101.pdf) (PDF). GS1.org. November 2013. Retrieved 23 March 2015.
158. "EPC Gen 2 FAQ" (<https://web.archive.org/web/20150320225151/http://www.smartcardalliance.org/publications-epc-gen2-faq/>). Smart Card Alliance. July 2006. Archived from the original (<http://www.smartcardalliance.org/publications-epc-gen2-faq/>) on 2015-03-20. Retrieved 2015-03-25.

External links

- An open source RFID library used as door opener (<https://www.codeproject.com/Articles/1096861/DIY-electronic-RFID-Door-Lock-with-Battery-Backup>)
- UHF regulations overview by GS1 (http://www.gs1.org/docs/epc/UHF_Regulations.pdf)
- What is RFID? Educational video by The RFID Network (<https://web.archive.org/web/20100530071726/http://rfid.net/basics>)
- How RFID Works (<http://www.howstuffworks.com/rfid.htm>) at HowStuffWorks
- Privacy concerns and proposed privacy legislation (<http://www.privacyrights.org/ar/RFIDposition.htm>)
- RFID (https://curlie.org/Society/Issues/Science_and_Technology/RFID/) at Curlie
- What is RFID? – animated explanation (<https://web.archive.org/web/20120322194318/http://www.explanian.com/en/channels/technology/detail/what-is-rfid>)
- Hardgrave, Bill C.; Aloysius, John; Goyal, Sandeep (2009). "Does RFID improve inventory accuracy? A preliminary analysis". *International Journal of RF Technologies: Research and Applications*. **1** (1): 45–56. doi:10.1080/17545730802338333 (<https://doi.org/10.1080%2F17545730802338333>).
- IEEE Council on RFID (<http://www.ieee-rfid.org/>)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Radio-frequency_identification&oldid=1103405784"

This page was last edited on 9 August 2022, at 15:02 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License 3.0; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

