Author manuscript, published in Digital Privacy: Theory, Technologies, and Practices, Auerbach Publications, pp. 285-306, December, 2007
https://www.nics.uma.es

RFID: Technological issues and privacy concerns

Pablo Nájera, Javier Lopez
Computer Science Department, Univesity of Malaga, Spain
{najera, jlm}@lcc.uma.es

1. Introduction

RFID (Radio Frequency Identification) is a type of automatic identification system: portable tags stuck on any kind of product (clothes, smartcards, currency) transmit data wirelessly to readers, which are often connected to computer networks, facilitating the transfer of data to databases and software applications that process the data according to the needs of a particular use.

The data stored by the tag may provide identification or location of the product attached to, or specifics characteristics about the product tagged, such as price, color, or date of purchase.

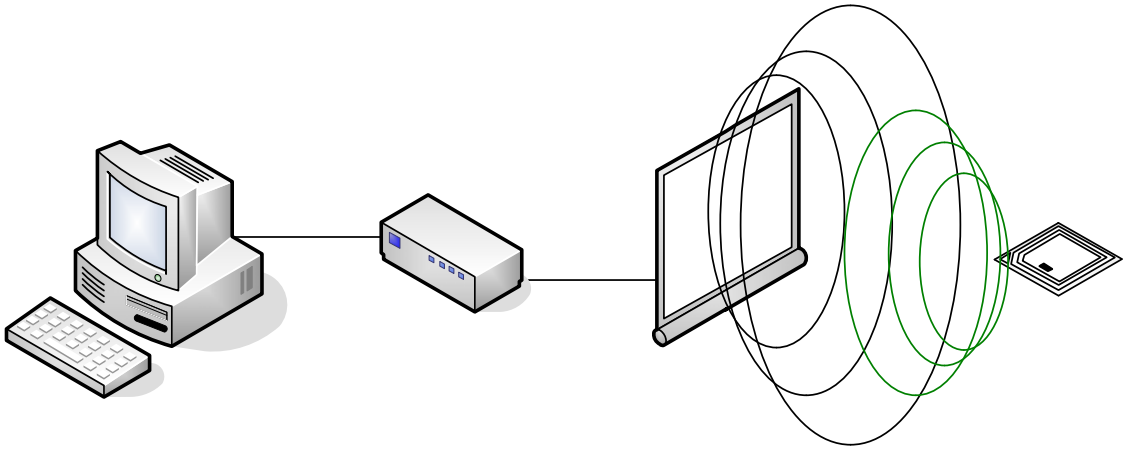

Figure 1. Diagram of a basic RFID system

As can be seen in Figure 1, a basic RFID system consists of two main components: (i) *Tag*: Attached to or embedded in the object to be identified. It typically contains a coupling element so that it can communicate with readers and an integrated circuit used to manipulate and store the data. (ii) *Reader*: the device that communicates with tags and is able to read or write their memories. It contains an antenna and a control unit to manipulate the data, and is connected to a communication network to transfer tag's identity and data to the central system.

There are two kinds of tags: *passive* tags, which lack an independent power source and need to harvest energy from the reader's signal before they can communicate with it. Their range of readability is quite reduced (up to distances of five meters). An example Gen2 UHF passive tag is shown in Figure 2. And *active* tags, which have on board batteries that dramatically increase their read range and functionality.

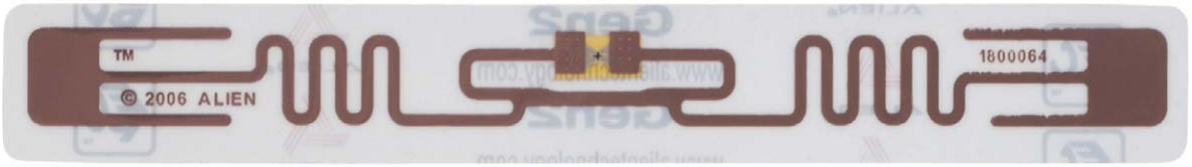

Figure 2. Alien Technology Gen2 EPCGlobal tag based on UHF frecuency

The most typical data that a tag stores is a code to uniquely identify the physical object it is attached to. Since passive tags (the most widespread type of tags) can only work in presence of a reader, they store the data that a reader writes onto it or the data that was originally stored at the factory. Such information is usually limited to basic aspects of the object. The reading of a tag usually lasts a fraction of a second and its storage capacity range from no memory to 128 kilobytes of data.

There is a wide variety of RFID systems that work on nearly any frequency range from LF (e.g. automobile inmobilizer systems) to microwave (e.g. toll collection systems), but leading applications work in HF (e.g. contactless smart cards) and UHF (e.g. supply chain management).

As barcodes, RFID tags may provide product identification. Due to this fact, they are often said to be a new and improved generation of barcodes, but there are some important differences between them. While bar codes are identical for every unit of the same product, RFID tags provide for unique identification of each tagged unit. Also, their storage and capacity for interactive communication and their read/write capability make them much more powerful. The ability to perform non line of sight reading at production speeds is one of its best advantages.

Tags implement low to moderate security features like memory write protection and basic encryption schemes. As for the price, it depends on their functionality and sophistication. While tags with advanced security measures, as those used in bank applications have an approximate value of ten euros, most typical tags with basic features used in supply chain and logistics cost a few cents of an Euro.

3. RFID Technology applications

Based on essential developments in technology such as the transistor, the integrated circuit and communication networks, RFID technology showed up during the second half of the twentieth century. The first RFID [1,2] use was in the 1960's, when Checkpoint and Sensomatic were created. They developed the Electronic Articicle Surveillance (EAS) equiment to countertheft. It could only detect the presence or absence of a tag attached to an object, but it could not determine the identitiy of the tag. After that, in the 1970's both the private and public sectors were involved in RFID technology. During this decade applications for factory automation, animal and vehicle tracking came up. The 1980's were a decade of different RFID implementations around the world: while in Europe the main interest was in short-range systems for animal and industrial applications, in the United States transportation, personnel access and animal tracking were of interest. During the 1990's, different systems for electronic toll collection proliferated in the United States that allowed vehicles be driven without having to stop at toll collection points.

The beginning of the 21st Century is becoming the breaking point for RFID technology development where international standards are being finally set and cost is rapidly decreasing, showing, a promising future for technology adoption. One of the leads applications of this technology is told to be in the supply chain management [3], providing automation to the warehouse and manufacturing process. Thanks to RFID, it is possible to track trailer and merchandise shipments from suppliers to stores. This technology helps to streamline the receiving/check-in process, tracking trailers and associated merchandise and providing visibility at any point. These facts improve customer

experience through out-of-stock reductions, as well as benefits retailers reducing on-hand inventory and less use of "safety stock", increase potential for sales generation, inventory visibility and internal inventory management and increase store, manufacturing and distribution operational efficiency. It even reduces shrink and theft in the supply chain due to the enhanced control on the goods.

It can help also costumers through easier identification on recalls and on high cost goods using it for warranty information or for software upgrades and it can also be used to reverse the supply chain (if a product is returned, the tag can be used to track the product to supplier for repair and resell of for destruction). Improved product selection or freshness for dated goods are also useful advantages.

Most product identification uses require a unique code stored in the RFID tag. These codes are managed by EPCglobal [5]. EPCglobal, which was formed in November 2003, is a joint venture of the *Uniform Code Council* (UCC) and EAN International. Taking the *Electronic Product Code* (EPC) from its development at the MIT Auto-ID Center to the global marketplace, its mission is to create global standards for the EPCglobal Network.

But there is a wide variety of application areas, other than in the supply chain management, that benefit from the wireless identification provided by RFID systems. These predominant application types include: electronic payment (at banks, mass transportation or by means of automatic toll collection systems), access control systems (controlling building access or implemented as automobile inmobilizers), animal tracking, and prevention of counterfeiting.

One of the emerging fields where RFID technology is being widely implemented is in the medical area. RFID tags fit into many health care scenarios [4], for example, in tasks like detecting pill expiration date or preventing mis-medication: the information provided by the tag can inform about the expiration date of a product and the software that receives the data from the reader can check it with the actual date and issue a warning if it is wrong or, using the identification data of the medicine, query a database about contraindications and instructions and warn the doctor about possible

problems. With the aid of larger readers, it can be used in hospital to know where a determined doctor or a chart is at any time. It can be a useful tool to asses med school students and, in the long term, help doctors and nurses proactively through their jobs. Thanks to the tracking ability that RFID technology provides, it is possible to infer *Activities of Daily Living* (ADL) including medication taking which can help doctors at the supervision of their patients. It is also being used in test tube tracking, ensuring accuracy and tube identification and protecting patient safety.

The range of options that RFID offers for tomorrow uses list is endless: smart appliances, refrigerators that automatically create shopping lists, closets that tell you what clothes you have available and search the web for advice on current styles, aids for physically and cognitively impaired, environmental care and recycling help such as plastics that sort themselves and so on and so far.

However, not every use of RFID provides an advantage to clients or citizens and important privacy and anonymity threats rise with the use of this new technology.

4. Threats to anonymity and privacy

4.1 A double-edge sword

RFID is a promising technology whose ability to provide automatic identification in nearly any scenario is revolutionizing many industrial fields. However, it has several features that working together can turn it into a double edged sword and threaten privacy and civil liberties. Next, we analyze those features.

- *No tag presence awareness.*

Current miniaturization level allows manufacture RFID tags embedded in any object type without being notice. Integrated circuit's size is comparable to a grain of salt, and antennas that need a few square centimetres surface can now be printed with conductive ink, making them nearly imperceptible. As a result, product owner may not be aware of tag's presence.

- *No reader presence awareness.*

RFID readers can be installed invisibly in all kind of objects. Places where readers can be embedded in covers: walls, doorways, floor tiles, carpeting, vehicles, roads, sidewalks, furniture and so on. Some manufacturers also distribute handheld devices with readers integrated or in Compact Flash format.

- *Silent readings.*

Due to lack of contact needed to read tags, they can be accessed from a distance in a virtually silent and invisible way because human can not sense RF radiation. Therefore, readings can be performed without individual's knowledge or consent.

- *Line of sight.*

With RFID, non direct line of sight is required to identify and access data stored in a tag. As a consequence, private items kept out of view (i.e. in a wallet, pocket, backpack or car boot) are not protected against an evil reader.

- *ID disclosure. Public identification.*

Prior to any reader-tag data transmission, the RFID label needs to be recognized so its unique code is sent to the reader. Even if a tag implements security measures or a cryptographic coprocessor (which is not present in EPC tags used in consumer products), they usually provide authentication and encryption for tag's stored data reading and writing once tag's identification has been done. Accordingly, any (authorised or unauthorized) reader can obtain tag's electronic code. If no security features are implemented (as in ISO/IEC 15693 tags with no onboard encryption or authentication and only optional protection on write command), even stored data can be accessed and modified.

- *Unique identification.*

A tag's electronic code is a globally unique ID number (except for ISO 11784 and ISO 11785 tags used in animal tracking which serial numbers can collide). Label's id does not provide identification

at product type level (i.e. barcodes), but at item level. Consequently, data inferred from a positive identification surpass owner's anonymity.

- *Global database.*

EPC provides a unique link to individual product data. The data is stored in the *Object Name Service* (ONS), a globally distributed, but centrally managed, electronic database. Tag readers in remote physical locations can connect to the ONS via the Internet to read and modify the item ONS dossier throughout its lifecycle. From a query to the EPC network using a tag's serial number is possible to know the manufacturer and product type that serial number identifies to. Due to the nature of RFID tags the number does not identify only the product type, but a unique item.

Not only a specific reader would be able to identify tags that belong to its own database, but, due to the worldwide standard of identification codes managed by EPCglobal, it would be possible to identify any tag that a person would carry on if he/she is near enough (which products he has, even if they are inside a bag, when they were bought or how much cost them).

This multi-identification ability is not a dream, in the words of Jack Grasso from EPCglobal, "Companies would 'join the EPCglobal universe' which means they would get an identification number, and they would have access to the network where all of the codes would be stored". This system is already working.

Candidates for associating with the tag (in EPCglobal database or in particular databases) include: date of purchase, name of individual, date of sale, price of sale, warranty and many other possibilities.

Even the company which manages this database is not completely trustable: Verisign was chosen to manage the name service due to its similarity with the *Domain Name Service* (DNS) which it already provided for some top level domains. In 2003, Verisign used its control over DNS servers to promote their own services redirecting mistyped URLs during web browsing, activity that meant a lawsuit

from ICANN. Email servers were also redirected to their own servers which imply a potential risk for consumer's privacy.

- *No human intervention.*

Detection and identification of tags in a reader's perimeter is triggered automatically. What is more, data processing and database updating can be made without needing any human intervention. Due to this fact, the amount of data that can be automatically gathered for subsequent data mining increases noticeably. At the same time, the chance to be under observation in any circunstance is remarkably higher.

So, an RFID infrastructure that identifies, compiles, stores, and analyzes the vast amounts of data generated as tagged products make their way from factory to the point of sale and perhaps beyond could be deployed [6].

- *Lifetime.*

In contrast to active or battery-assisted tags that require an external power source with a maximum lifetime of 10 years, passive tags operate with no power source (gathering reader's radiation) and contain no mechanical parts offering a virtually unlimited operational lifetime. Therefore, an item embedded with a live RFID tag can be tracked during its whole life span.

4.2 Privacy threats

Due to the particular aspects of RFID technology, a wide range of potential privacy and anonymity threats appear for both individuals and organizations. We analyze them in this subsection.

- *Product information leakage.*

Without a security mechanism to conceal tag's ID, any unauthorised reader can obtain its unique electronic code. In case of an EPC code, EPCglobal product info database can be queried all around the world to know the connection between the tag and the product. It does not contain information

about the owner, but allows a reader to know the manufacturer and product type. If the tag provides no protection on the read command (authentication protocol or password based access), not only the identity, but data stored in the tag can also be compromised.

Added to no line of sight requirement, technology offer an stranger a kind of x-ray vision to identify items an individual is wearing or carrying. In a classical example, a thief could target victims based on their belongings.

- *Association.*

RFID tags are embedded in items to allow objects' automatic identification, but these unique IDs can also be associated with their owners' identity (e.g. at checkout) causing a privacy threat. Associations between users and tagged objects created by organizations or governments could cause future problems or incoveniences to item's owners. Consumers could be not aware of the tag embedded in the object or that their identity has been associated with it. As a result, owner would get rid of the object without destroying the tag first or requesting to update databases. If any dishonest act is performed carrying these objects in the future, the original owner would be under suspicion. Keeping track of which objects contains tags and which databases link these items with their identities would be a heavy burden for consumers, if possible.

- *Individual's tracking.*

Due to the fact that tagged objects contain a globally unique identifier, virtually unlimited operational lifetime and permanent association between tags and owner, an individual can be tracked based on his possessions. As a consequence, the following threats arise:

    - *Location information.*

      If a product ID is uniquely associated to an individual (i.e. tagged items like shoes, glasses or wallets) it is possible to track person movements and obtain individual's physical location. In fact, it is not necessary that an individual carries the same RFID tag all the time to establish his electronic identifier, not even that tagged objects he uses belong to him exclusively. An

individual's electronic signature can be derived from the cloud of tags usually carried by him. The identification of some tags related to the set would denote individual's presence.

- *Individual's profiling.*

Linking item-level data on the tag with personally identifiable information generates a risk of creating a comprehensive infrastructure for individual profiling. Consumer profiles can be generated by means of compiling and analyzing information provided by working tags. Tracking a person movements over an extended period would allow organizations determine which products a consumer purchases and make inferential assumptions about a consumer lifestyle, income, health and buying habits. For instance, a retailer may use the purchase database going beyond polite uses and rank individuals based on previous purchase history. At shop entrance, consumers would be silently identified restricting customer support to valuable clients.

- *Corporations privacy threat.*

Not only individuals, but any entity related with RFID can suffer from privacy threats [20] derived from controversial technology applications. As a side effect of using RFID in the supply chain and stores, organizations can suffer industrial espionage. Readers strategically placed and hidden by competitors (e.g. readers concealed at a shop entrance and supply doors) could gather data about products flow inferring internal business operation knowledge such as stocks, rate of sales or consumers profiles and preferences.

Another threat that is not a privacy threat, but a potential attack is due to the nature of RFID technology which radio frequency signals can be easily jammed. In fact, this jamming procedure is one of the options to protect consumer privacy, but used by dishonest third parties can cause malfunctioning or even render the network non-functional. Such kind of denial of service attack oriented to a business infrastructure could cause big losses.

In conclusion, tagged items can be easily tracked at business level to infer internal operation or associated with personally identifiable information providing individual tracing and consumers' profiling creating a potential for abuses of consumer data and individual privacy.

4.3 Organizations position on RFID

Maybe, killing RFID tags attached to consumer products once the product is sold would reduce privacy threats, but there are evidences that show that companies are not interest in killing them [7].

Wired magazine published on April 2004 [8] that "P&G and other companies suggested they want to keep RFID tags active after checkout, rather than disabling them with so-called 'kill machines'. The companies also want to match the unique codes emitted by RFID tags to shoppers' personal information", reporting on statements made by Sandy Hughes in Chicago at the RFID Journal Live conference.

According to Wal-Mart, the US largest retailer, "Consumers may wish to keep RFID tags on packaging to facilitate returns and warranty servicing", so individuals may not be able to choice whether they want to keep live tags on their products or not once they have been bought without sacrificing reliable customer support.

Privacy advocates even argue that forcing companies to kill tags would not give an assurance that it has been really done. According to CASPIAN [9] in its 'Position Statement On Use of RFID On Consumer Products' [10], "Stores would only pretend to kill a tag, when in reality they would make it dormant and then later reactivate it to track you."

Also, Cedric Laurent, from EPIC [11] said that "Government would prevent stores from killing them, thereby creating a "surveillance society."

People in favour of RFID technology have stated that the privacy community has intentionally exaggerated the threats to privacy to stop RFID rollout. Much of what privacy advocates warn will happen is already standard practice in commerce with few or no privacy or consumer issues occurring.

Meeting the concerns of the privacy advocates is not costless, and due to RFID is only in its initial stages, it is obvious that legislation and regulation is premature yet, but, examining the results of a survey carried out by Direct Marketing Association which found out that nowadays 62% of companies gather personal information without telling customers, while 75% use customers' personal data without asking permission, we can conclude that the threat really exists.

4.4 Real life scenarios.

There are already several examples that prove that companies are using RFID technology or analogous devices to track customer behaviour without warnings. Path Tracker system is a good example of this. PathTracker records the coordinates of a shopper from the time they enter the store and select their shopping cart until check out. Each shopping cart is fitted with an emitter that sends a uniquely coded signal to an array of antennae every four seconds. Using state-of-the-art technology, the path taken and stops made (location and duration) become a database for each shopper tracked. In addition, every actual purchase made can be tied to the specific shopper's path, allowing analysis on a specific brand and item level. All kind of stores are nowadays using this technology (i.e. Wal-Mart Stores, Best Buy, CompUSA and Office Depot).

Another brand that has already used RFID technology in a controversial application is Gillette. The razor manufacturer developed at the MIT Auto-ID Center an RF enabled shelf oriented to theft prediction and deterrence. The smart shelf detected when inventory had been reduced or gone below a threshold and triggered a hidden camera to take close-up photographs of the shopper’s face inferring a possible theft in progress. A second picture was taken as they paid for the razors at checkout. After

testing the monitoring system at a British Telco store, Caspian launched a boycott campaign against Gillette's products [12].

A similar experiment was conducted by Wal-Mart and Proctor & Gamble[13] embedding RFID tags in Max Factor Lipfinity products and mounting cams near the shelves to keep watch costumers and track lipsticks leaving the shelves. A sign at the display alerted customers that closed-circuit televisions and electronic merchandise security systems were in place in the store.

Therefore, it is obvious that RFID raises security problems, most of them based on tracking of personal information and loss of anonymity and privacy. Situations like the one described by Barry Steinhardt, where a man walking around the city and stopping in front of a sex shop (with a radio customer identification system installed using chips in credit cards) for a moment to look at the curious items in the store windows and a few weeks later receiving at home advertising sex material is no so unlikely.

5. Technology based solutions

5.1 Security mechanisms in actual RFID standards

A wide range of RFID systems are available nowadays to fulfil the needs of each type of application depending on users' needs. Features include attenuation from water resistance, minimum read range, improved read accuracy, fast read rate, low tag's cost or high security features. As a result, a variety of RFID product categories have been defined, such as passive, active, semi-passive or semi-active, based on different frequency ranges (i.e. LF, HF, UHF or microwave) that implement particular onboard features.

Each RFID standard has being focused on a different set of requirements and implements a particular trade-off between tag's characteristics, performance and security features. In fact, security mechanisms as encryption or authentication, on the one hand, increase tag's cost and latency of read

and write processes, and on the other hand, reduce onboard storage capacity and the number of tag reads per second.

Most of the RFID standards include security features [14] to provide some level of confidentiality or integrity. Mechanisms used to provide confidentiality include password protection on read commands (e.g. ISO/IEC 18000-3), tags addressed by random numbers (e.g. EPC Class 1 Gen 2, ISO 11784-11785 and 10536), masked reader to tag communications (e.g. EPC Class 1 Gen 2 and ISO 10536), "reader-talks-first" protocol (e.g. ISO/IEC 18000-2 and 18000-3) and "quiet mode" (ISO 18000-3, 11784-11785 and 10536). Integrity is addressed by means of protection on write commands (e.g. ISO/IEC 18000-3 Mode 2, optional in ISO 15693) and CRC error detection.

A particularly noteworthy example addressing security issues is the ISO 14443 designed for proximity smart cards, that includes cryptographic challenge-response authentication and triple-DES, AES and SHA-1 algorithms. These proximity cards have been used in environments such as gas stations, public transport services and banks as a contactless payment method. Most commercial cards belong to proprietary specifications based on the standard such as Philips' Mifare or Calypso family products. The recent adoption of the ePassport, an internationally accepted Machine Readable Travel Document (MRTD), is based on the ICAO standards that specify the use of the ISO 14443. Countries such as Germany, Holland, Belgium and the United States have started issuing these electronic passports containing RFID tags. Unfortunately, secret keys needed in order to access information on the RFID chips are derived from basic personal information (passport holder's birth date, passport number and expiry date) that can be read from the data page or hacked [15], enabling a way to clone ePassports[16].

EPC standards applies to supply-chain and logistical applications. Main design goals focus on low tag's cost and fast read rate. As a result, EPC tags lack the computational resources to implement strong cryptographic encryption or authentication. EPC Class 0 and EPC Class 1 Generation 1 tags did not implement any security feature to provide privacy protection. Due to the tag sorting protocol

used in Gen 1 based on a binary tree algorithm, in order for readers to singulate a unique tag before communication begins, Generation 1 required the transmission of an entire tag's EPC code (96 bits). Therefore, tag's identification and tracing on EPC Gen 1 tags is possible, rising several privacy threats. EPC Generation 2 uses a new tag sorting protocol called "Q" algorithm that does not require the communication of an entire tag code over the air until secure communication is established. Instead, a pair of randomly generated numbers is used for tag singulation. This approach prevents eavesdropping data by a third party device on tag-reader communications, although does not address direct EPC code identification requesting. EPC Generation 2 specifications are being adopted in ISO standardization as ISO 18000-6c.

Most privacy threats are caused by unauthorised readers being able to identify RFID tags, even if they are not able to access the data stored inside. At the same time, most security features implemented in tags nowadays focus on authentication schemes to prevent read, write or lock commands on tag's memory and provide encryption once the tag has been singulated and identified. In fact, readers usually need to know tags' ID in order to select the right keys or password. Actual standards lack from the definition of a coherent key-management infrastructure designed for environments full of RFID tags. Consequently, real life applications resort to the used of the same password for all the tags or weak and predictable ones (e.g. ePassports). This inappropriate security architecture entails poor protection to organizations and individual's privacy.

Several privacy-protection schemes have been proposed to prevent RFID tags identification from unauthorised devices. The range of approaches extends from out-of-tag mechanisms to tags with lightweight cryptographic circuits, all the way up to basic tags with simple modifications.

Kill command.

EPCglobal standards approach to provide permanent consumer's privacy protection does not require any advanced security framework or onboard cryptographic circuits. It uses a simple, but effective solution: killing the tag. The kill command is a function that must be implemented in EPC tags that

allows permanently deactivating a tag. It can be used at the point-of-sale preventing any malicious (or legitimate) applications. To execute a successful kill command a weak 8-bit password is used for EPC Class 1 Gen 1 tags; anyway a tag lockouts after several incorrect queries. In EPC Class 1 Gen 2, a stronger 32 bit password is necessary.

At first sight, this scheme can provide complete consumer's privacy protection, but it shows some drawbacks. First, privacy is not protected until the tag is deactivated; thus, it does not address organizational privacy threats or in-store tracking. Second, it is a manual process that adds a burden on shop assistants or consumers; some proposals as the placement of kiosks in stores where individuals could deactivate their tags would leave a high ratio of live RFID tags due to unaware customers. Third, deactivating the tags avoids any further legitimate uses of them as envisioned by ubiquitous computing environments, home automation systems or future post sale services. In the field of emerging services based on live RFID tags, due to the lack of an appropriate key-management infrastructure, the same password is usually required to kill any tag used in the same application, opening a gap for a kind of permanent denial-of-service attack.

5.2 Proposed solutions

5.2.1 Out-of-tag privacy mechanisms

ID disclosure can be avoided without modifying a tag's design. Thus, in normal tag's operation, its specifications remain the same (e.g. privacy protection does not suppose any alteration of read rate speed or onboard storage capacity) and the most appealing factor, cost of tag, is not changed. Two main approaches remain in this category.

- *Faraday cage.*

This solution appeals to block the output from a tag by means of an enclosure that avoids the establishment of any reader-tag communication. Metal materials and water in contact or in the proximity of a RFID tag can attenuate radiofrequency waves shielding it against any unauthorised reading. Sensitive level depends on the frequency range. For example, UHF tags in contact with a

human body can not be read, but HF tags are still functional. e-Passports issued in some countries like the United States are adopting this shielding solution embedding a web of metal fibres in the front cover, so that passports can not reveal their presence at least they are physically opened. In this scheme, individuals need to insure that a Faraday cage is protecting every RFID tag their own in order to be 'safe'. So, in most scenarios, it is not a practical solution and human error is possible. Finally, it also blocks any ubiquitous computing application.

- *Active jamming.*

Based on the same idea that the Faraday cage, in this case, a device is used to broadcast a signal that prevents unauthorised readers from accessing the RFID tag.

  - *Blocker tag.* A noteworthy example is the blocker tag scheme [17], an RFID tag that identifies itself with all possible tag's ID, thus avoiding a malicious reader to know which tags are really present. The classic blocker tag implementation takes advantage of the tree sorting protocol used to singulate a tag. Using this algorithm, a reader needs to travel across the binary tree of tag's codes (where each leaf represents an entire tag's ID and intermediate nodes correspond to an identifier prefix). At root's state, no bit prefix of any present RFID tag is known; therefore, the reader asks for the first bit value of tags in the reader's perimeter. From this point on, a recursive search is conducted based on tags' responses. A blocker's tag strategy is to broadcast both values for each reader's request, simulating that all possible tags are present. Under these circumstances, the reader would hang trying to scan the complete tree. A selective blocker tag would only disrupt a reader's search if it goes deep into a predefined subtree, for instance, a privacy zone.

  - Soft blocking [18]. Instead of misleading a reader's search, soft blocking alternative approach leans to warn the reader about the presence of private tags, thus requiring the reader to give up the search. In order to achieve this, a special prefix that identifies "blocker tags" could be defined and commercial readers' firmware would need to be tested to carry out the policy. The threat of a rogue reader would always exist.

Any of these active jamming solutions entail the same drawbacks commented for the Faraday cage approach: they add a burden on individuals and suffer from scalability problems

5.2.2 Non cryptographic tags

In most proposed privacy schemes [19,20], tags themselves need to provide specific features in order to prevent unauthorised identification by third party readers. At the same time, these solutions do not avoid tag identification and communication with legitimate readers, solving one of the problems of out-of-tag solutions.

- *Tags with rewritable memory [21,22,23,24]*. At a minimum requirement level, tags that only implement rewritable memory can be used without needing any onboard cryptographic circuit. In this scenario, tags store encrypted versions of their serial numbers preventing third party readers from knowing their real IDs. As static encrypted serial numbers can also be traced by malicious devices, the legitimate readers are in charge of refreshing the encrypted serial number versions as often as possible. A central server accessible by the authorised devices is queried to obtain decrypted versions of tag IDs and, optionally, a new encrypted ID to update tag's memory. Thus, servers are a critical infrastructure resource and can turn into a bottleneck. Since a tag's encrypted ID can be traced until it is refreshed, the level of privacy protection achieved depends on the frequency of update. On the positive side, low cost tags can be used.

- *Tag pseudonyms [23]*. This solution can be seen as a improved version of the previous one. In this case, a tag contains not one, but a set of pseudonyms or encrypted versions of the original ID and implements a policy for pseudonym selection. Each time a tag's identifier is requested one from the set is provided, thus making it harder to trace real tag's identity for unauthorised readers. In a hostile environment, an insistent reader could obtain all available pseudonyms repeating the identification process multiple times. To prevent this, the pseudonym selection

policy could use a kind of time control before cycling pseudonyms. Unfortunately, passive tags lack from onboard clocks. As in the previous solution, updating the set of alternative IDs as often as possible improves the security level.

- *Tags with antenna energy analysis [25]*. In this case, a tag tries to guess which readers are legitimate based on the quality of the signal received. For this distinction, two special considerations are made. First, an unauthorised reader usually queries the tag from a longer distance than an authorised one. Second, signal to noise ratio increases as the reader gets closer to the tag. Based on this, a tag can measure this value and decrease the amount of information provided as the reader gets further (such as providing a generic product type instead of its unique identifier code). Although this approach is error-prone, it can be implemented as a complement to other solutions.

- *Password checking tags.* In order to provide any private data including its unique electronic code, a tag could request a password to the reader. At a negligible cost, this solution could provide privacy protection because onboard circuitry needed to check a password is inexpensive. This scheme is already been used in some implementations to control read/write operations on data stored in the tag, but it does not address ID disclosure: a reader needs to know tag's identity in order to provide the right password. As a workaround, in controlled contexts where every tag could be programmed sharing the same secret key (e.g. a consumer's home), ID publication could also be addressed by this scheme.

5.2.3 Tags with cryptographic circuits.

In this category, tags are equipped with cryptographic circuits to perform onboard operations such as encrypt their IDs. The implementation of cryptographic primitives may have a negative impact on other tag’s specifications as has already been commented and increases tag’s cost. Envisioned applications of RFID technology requires tagging products at item level regardless of its own cost. As a result, tag’s price needs to be nearly zero-cost. For these reasons, only minimalist and lightweight

cryptographic operations are acceptable on most RFID tags. Instead of static encrypted versions of stored electronic codes as provided by rewritable memory tags, these tags can perform their own encryption functions and generate dynamic identifiers, which avoid tracking from malicious readers.

- Hash-chain scheme [26]. A noticeable example is the hash-chain scheme where two hash functions are implemented in the tag. The tag also contains rewritable memory that stores the last key used to generate a new identifier. The secret key *s* is share with a central server that knows the link between the key and the real ID. The first hash function G is used to generate the next identifier based on the actual key s (the output value is broadcast to the reader), while the second has function H is used to update the key (the output value overwrite the last key in memory). Even if the secret value is hacked, due to the one-way nature of hash functions, the past tag history is not compromised.

6. Policy and legal solutions

Technological solutions alone may not be enough to alleviate privacy threats arisen by radiofrecuency identification. It is necessary to mitigate possible abuses by means of regulations and law.

It is known that individuals value anonymity and do not trust companies to administer personal data, and fear both private sector and government abuses of privacy. Also, users want to realize of how their personal information is collected, used, and with whom it is shared.

According to an American survey, the public considers opt-in (the principle that a company must have the consumer's permission prior to gather or use personally identifiable information) as one of the most important privacy rights.Laws must ensure that unscrupulous companies do not take advantage of the ability of RFID technology to identify customers and produce interesting data by means of spy readings of tags they own. Companies need to be forced to follow a set of "fair-play" guidelines that assures that not evil uses of RFID take place [27]. A good starting point in the regulation of the use of personal information is the use of the Fair Information Practices.

- *Fair Information Practices.*

In 1972, the U.S. Department of Health Education and Welfare proposed a Code of Fair Information Practices in a report on Automated Personal Data Systems exploring the impact of computerized record keeping on individuals. These principles were the basis for the Privacy Act of 1974 that recommended a series of information practices to protect the use of personal data addressing issues of privacy and accuracy. These principles have been widely accepted and are the basis for many privacy laws in the United States, Canada, Europe and other parts of the world. All these documents share five core principles of privacy protection: awareness of data recopilation, consent, access, integrity and data security and, finally, remedy.

In 1980, the OECD (Organization for Economic Co-operation and Development) rearticulated the Fair Information Practices in its Guidelines for the Protection of Privacy and Transborder Flows of Personal Data [38] as a set of eight principles which cover the collection of data, security, data quality and use limitation. These principles have been used as the baseline for evaluating data protection and privacy initiatives.

Specific guidelines that consider the unique aspects of RFID have been derived from Fair Information Practices and OECD principles. In 2002, Simson Garfinkel expounded “An RFID Bill of Rights” [29] as a framework of guidelines that companies could voluntary and publicly adopt. In 2003, Caspian introduced “RFID Right to Know Act of 2003” [31], a proposed legislation to mandate labeling of RFID-enabled products and consumer privacy protections. In 2004, EPIC rearticulated Fair Information Practices as guidelines [30] that guide the use of RFID technology to protect consumer privacy from private enterprises and enterprise interests at the same time.

According to these guides, Table 1 illustrates practices that companies must follow in order to mitigate possible abuses to privacy.

Practice issue	Description
Consent	Individual's written consent should be obtained before associate any personal data with RFID tags.
RFID system presence	Any tagged item or location equipped with readers should be clearly identifiable by means of labels or logos. Information displayed should reference the nature of the system and be easily understood.
Removal	Individuals should decide if they want live tags in the products they own, so tags must be attached in a way that they can be easily removed or permanently deactivated by the customer.
Reading awareness	Any reading activity must be clearly identifiable through a recognized signal (i.e. a tone or light). Individuals must know when tags are being read, by whom and why.
No coerce	RFID enabled services should be accessible without RFID tags. In particular, customers should not be forced to keep tags for benefits as warranty tracking.
Data access	Personally identifiable data collected through and RFID system should be accessible to the individual including tag's data and information stored in databases.
Data association	Corporations should not link personal information with tag's data if there are alternatives which achieve the same goal.
Profiling or tracking	Tagged items should not be used to create customer's profile obtaining individual shopping habits or tracking location.

Table 1.Industrial Practices to mitigate possible abuses to privacy

EPIC guidelines (see Table 2) also establish the requirements that must be satisfied if personal information is collected and associated with tag data.

Requirement	Description

Purpose	Prior to obtain consent, individual must be informed about the purpose of the data association.
Use limitation	Data should not be used out of the original scope and keep only as long as it is necessary.
No third party disclosure	Data should not be disclosed to third parties.
Data quality	Data used in approved applications must be kept accurate and updated.
Security	Appropriate security measures must be used in data transmission, storing and accessing.
Openness	Policies and practices applied to RFID systems must be easily accessible for individuals.

Table 2.Requirements for personal data collection and association according to EPIC guidelines

Nowadays, state of laws protecting personal information is not homogeneous all around the globe. In particular, Europe has enacted two data protection directives (in 1995 [32] and 2002 [33]) that defend individuals against personal information processing adopting the Fair Information Practices with modifications. Therefore, controversial applications of RFID technology like association of data with personal identification or individual tracking are already regulated and involve a number of data protection obligations. The Directives grant data subjects a serie of important rights including the right of access to personal data, know where data originated and the right to withhold permission to use data. In particular, location data requires consumer's permission prior to collecting or using information, without consent data should be anonymous.

Consequently, the development of technical measures that prevent privacy abuses and the establishment of regulations that ensure consumers rights is a must.

7. Conclusions

It is possible that potential risks and abuses arisen by RFID technology have been exaggerated by privacy advocates. Anyway, alarms and suspicions raised have allowed preventing potential problems and treating them during technology development phase, so they are being considered during the design of new standards that include security measures to alleviate privacy threats. Measures to control privacy threats created by this technology need to be taken both in technology and legal ways, but citizens must also be informed, to warn them about possible troubles that this technology can cause, without generating an irrational alarm and fear that can curb the development of this promising technology.

Nevertheless, an irrational fear of possible consequences due to technology adoption in our lifes could cause massive consumer's rejection that avoid further technology development or force tag to implement excessive security measures incompatible with tag's purpose and target scenario (e.g. high cost tags or crippled features such as reduced operational reading distance or speed). Anyway, privacy threats caused by this emerging technology are a reality, so a trade-off allowing an adequate and safe use of RFID is necessary.

References

[1] Jeremy Landt, "The History of RFID", IEEE Potentials, Vol. Oct/Nov, pp. 8-11, 2005.

[2] Cedric Laurent, Workshop comment on "Radio Frequency Identification: Applications and Implications for Consumers", Electronic Privacy Information Center, 2004.

[3] Wal Mart RFID presentation, FTC RFID Conference, June 21, 2004.

[4] Ken Fishkin, "RFID for Healthcare: Some Current And Anticipated Uses", Radio Frequency IDentification: Applications and Implications for Consumers, Washington, June 21, 2004.

[5] EPCglobal homepage: http://www.epcglobalinc.org/ , accessed on January 2007.

[6] Declan McCullagh, "RFID tags: Big Brother in small packages", Cnet News, January 13 2003, http://news.com.com/2010-1069-980325.html

[7] Zombie Jo Best, "Zombie RFID tags may never die", ZDNet News, May 18, 2004, http://zdnet.com.com/2100-1103_2-5214648.html

[8] Mark Baard, “Watchdogs Push for RFID Laws”, Wired 2004, http://www.wired.com/news/privacy/0,1848,62922,00.html

[9] CASPIAN homepage: http://www.nocards.org , accessed on January 2007.

[10] CASPIAN, RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, Privacy Rights Clearinghouse, November 20, 2003.

[11] EPIC (Electronic Privacy Information Center) homepage: http://www.epic.org/ , accessed on January 2007.

[12] Boycott Gillette campaign, www.boycottgillette.com , accessed on January 2007.

[13] WorldNetDaily, "Wal-Mart used microchip to track customers", November 15, 2003, http://worldnetdaily.com/news/article.asp?ARTICLE_ID=35629http://worldnetdaily.com/news/article.asp?ARTICLE_ID=35629

[14] T. Phillips, T. Karygiannis, R. Kuhn, “Security Standards for the RFID Market”, IEEE Security & Privacy, pp. 85-89, 2005.

[15] Harko Robroch, “ePassport Privacy Attack”, Cards Asia Singapore, April 26, 2006, http://www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf

[16] Kim Zetter, “Hackers Clone E-Passports”, Wired, 2006, http://www.wired.com/news/technology/0,71521-1.html

[17] A. Juels, R. Rivest, M. Szydlo, The blocker tag : Selective blocking of RFID tags for consumer privacy, In Porceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 27-30, ACM Press, New York, 2003, 103-111.

[18] A. Juels and J. Brainard, “Soft Blocking: Flexible Blocker Tags on the Cheap,” Workshop on Privacy in the Electronic Society, ACM Press, 2004, pp. 1–7.

[19] M. Ohkubo, K. Suzuki, S. Kinoshita, “RFID Privacy Sigues and Technical Challenges”, Communications of the ACM, Vol. 48, No. 9, Sept. 2005, pp. 66-71.

[20] S. Garfinkel, A. Juels, “RFID Privacy: An Overview of Problems and Proposed Solutions”, IEEE Security & Privacy, 2005, pp. 34-43.

[21] A. Juels, R. Pappu, Squealing Euros: Privacy protection in RFID-enabled banknotes, In Proceedings of Financial Cryptography, Gosier, Jan. 27-30, Springer-Verlag, 2003.

[22] S. Kinoshita, F. Hoshino, T. Komuro, A. Fujimura, M. Ohkubo, Low-cost RFID privacy protection écheme, IPS Journal 45, 8, Aug, 2004, pp. 2007-2021 (in Japanese).

[23] A. Juels, “Minimalist Cryptography for RFID Tags,”4th Conf. Security in Comm. Networks, C.Blundo and S. Cimato, eds., Springer-Verlag, 2004, pp.149-164.

[24] P. Golle et al., “Universal Re-encryption for Mixnets,” Proc. RSA Conference Cryptographer’s Track, T.Okamoto, ed., Springer-Verlag, 2004, pp. 163–178.

[25] K.P. Fishkin and S. Roy, “Enhancing RFID Privacy via Antenna Energy Analysis,” IRS-TR-03 -012, Intel Research Seattle, 2003.

[26] M. Ohkubo, K. Suzuki, S. Kinoshita, A cryptographic approach to ‘privacy-friendly’ tags, RFID Workshop, Cambridge, Nov. 15, 2003.

[27] Eduardo Ustaran, “Data Protection and RFID systems”, Privacy and Data Protection, Vol. 3 Issue 6.

[28] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, ns Service, OECD Publications Service, 2001.

[29] Simson Garfinkel, “An RFID Bill of Rights”, MIT Enterprise technology review, October 2002, http://www.simson.net/clips/2002/2002.TR.10.RFID_Bill_Of_Rights.htm

[30] Epic, “Guidelines on Commercial Use of RFID Technology”, Electronic Privacy Information Center, July 9, 2004.

[31] K. Albrecht, Zoe Davidson, “RFID Right to Know Act of 2003”, Caspian, http://www.nocards.org/rfid/rfidbill.shtml

[32] Directive 95/46/EC of the European Parliament and of the Council, "Protection of individuals with regard to the processing of personal data and on the free movement of such data", 24 October 1995.

[33] Directive 2002/58/EC of the European Parliament and of the Council, "Directive on privacy and electronic communications", 12 July 2002.