**RC23710 (W0508-164) August 31, 2005**
**Computer Science**

# IBM Research Report

## Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced

**Günter Karjoth**
IBM Research Division
Zurich Research Laboratory
Rüschlikon, Switzerland

**Paul Moskowitz**
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

**Research Division**
**Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich**

# Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced

Günter Karjoth
IBM Zurich Research Laboratory
Rüschlikon, Switzerland
gka@zurich.ibm.com

Paul Moskowitz
IBM T.J. Watson Research Center
Hawthorne, NY 10532
mosk@us.ibm.com

## ABSTRACT

Existing solutions to protect consumer privacy in RFID either put the burden on the consumer or suffer from the very limited capabilities of today's RFID tags. We propose the use of physical RFID tag structures that permit a consumer to disable a tag by mechanically altering the tag in such a way that the ability of a reader to interrogate the RFID tag by wireless mean is inhibited. In "clipped tags", consumers can physically separate the body (chip) from the head (antenna) in an intuitive way. Such a separation provides visual confirmation that the tag has been deactivated. However, a physical contact channel may be used later to reactivate it. Such a reactivation would require deliberate actions on the part of the owner of the RFID tag to permit the reactivation to take place. Thus reactivation could not be undertaken without the owner's knowledge unless the item were either stolen or left unattended. This mechanism enables controlled reuse after purchase, making clipped tags superior to other RFID privacy-enhancing technologies.

**Categories and Subject Descriptors:** B.0 [**Hardware**]: RFID tags; **General Terms:** Design, Human Factors, Security. **Keywords:** Privacy, RFID

## 1. INTRODUCTION

Radio Frequency Identification (RFID) tags typically are small devices that can be embedded in or attached to objects for the purpose of identifying the object over a radio channel. RFID tags can be thought of as "electronic barcodes", with the advantage that they can not only identify a class of objects but also every instance of that object. Another advantage is that objects tagged with RFID technology can be read more easily and more frequently, thus improving the quality of information on objects in a supply chain or in the inventory of a warehouse. RFID tags can be read if they are in the range (typically up to a few meters) of a reader that communicates with tags over a radio channel.

RFID technology is being introduced for use in the retail supply chain [8]. Many large retailers have instructed their suppliers to tag pallets and cases with RFID tags carrying the Electronic Product Code (EPC$^{TM}$), a "license plate" with a hierarchical structure that can be used to express a wide variety of different, existing numbering systems. EPCglobal[1] has approved a new communications protocol for UHF tags that will standardize tags and readers for the retail supply chain throughout the world. Eventually, many billions of tags will be needed for pallets and cases alone.

If the initiative of the retailers for the tagging of pallets and cases proves successful, then the next step in the process may be to tag individual items and thus affecting consumers. Compared with bar codes, the wireless nature of the communication provides significant qualitative and quantitative advantages: tags can store and communicate many more bits of information, multiple tags can be interrogated by the same reader, and readers do not require line-of-sight to the tag. The aforementioned characteristics of RFID tags have raised privacy concerns, see for example [9, 11, 13].

Shaping of public opinion has been started by consumer advocacy groups, for example, by Consumers Against Supermarket Privacy Invasion And Numbering – CASPIAN, followed by numerous articles in journals and newspapers and not only in those specialized in technology and business [11] but also in the popular press. Perceptions of RFID differ dramatically – ranging from fuzzy fear ("spy chips", "Orwellian Eyes") to unlimited belief in its not yet completely discovered potential.

In this paper, we do not address the political and philosophical controversy about RFID, but focus on technical solutions for consumer privacy in retail. We show that existing solutions to protect consumer privacy either put the burden on the consumer or are hampered by the very limited capabilities of today's RFID tags. One way to disable RFID tags is through a "kill command". This seems to be the solution with the greatest potential. However, it possesses three critical weaknesses: complex key management, no controlled reuse after purchase, and no (visual) confirmation of successful disablement. Instead, we propose to provide RFID tag structures that permit a consumer to disable a tag by mechanically altering the tag in such a way that inhibits the ability of a reader to interrogate the RFID tag by wireless means. We call such structures 'clipped tags' as the body (chip) becomes separated from the head (antenna). Such a physical separation provides visual confirmation that

[1]EPCglobal Inc. is a joint venture between EAN International and the Uniform Code Council (UCC).

the tag has been deactivated. However, a physical contact channel may be used later to reactivate it. Such a reactivation would require deliberate actions on the part of the owner of the RFID tag to permit the reactivation to take place and thus could not be undertaken without the owner's knowledge unless the item were either stolen or left unattended.

## 2. RFID BASICS

RFID is a means of identifying a unique object or person using a radio frequency transmission. It consists of tags (or transponders), which store information that can be transmitted wirelessly in an automated fashion. Readers (or interrogators) both stationary and hand-held read/write information from/to tags.

RFID tags come in many form factors, for example, embedded in a car key to turn off an immobilizer. In this paper, we think of paper labels with an RFID tag inside. The tag consists of an antenna, which is printed, etched or stamped on a substrate, for example a plastic foil, and a silicon chip attached to it. If necessary another plastic foil may cover the tag to protect it from inclement environments. Such labels are then affixed to objects, and stored information may be written and rewritten to an embedded chip in the tag.

Tags can be read remotely via a radio frequency signal from a reader over a range of distances. Passive tags, i.e., tags without a battery, can only send information back to the reader on the reflected signal. Readers then send tag information over the enterprise network to back-end systems for processing or display it to the end user. The simplest RFID tag will send the reader its unique ID serial number.

RFID tags differ in the frequencies used, typically ranging from 100 kHz (access control, animal tracking) to 2.45 GHz (item management), in power consumption, memory (read-only, write-once, read-write with user memory), and in their computation capabilities, for example encryption. These factors influence the price, read range, life time, and type of data collected/stored on RFID tags.

There are many applications and uses of RFID technology, such as in supply-chain management, electronic tolls, libraries, goods and food tracing, pets and cattle tracing, to identifying individuals by ID cards, passports, and implants. RFID systems are primarily designed to uniquely identify items by affixing a tag containing a unique identifier to every item of interest. The EPC, for example, is not only a unique identifier but also encodes information about the manufacturer and product.

RFID tags, in particular those used in high quantities, for example in supply-chain management and retail, must be inexpensive. Tags for pallets and cases are in the $0.25 to $0.50 range. Tags for individual items will have to be only a few cents each. Besides being passive tags, they have limited storage (tag identifier only), limited computation power, and low bandwith. In addition, their communication time must be short as hundreds of tags may be read within a second.

## 3. RFID PRIVACY CONCERNS

Ever since the "sensitivity" of RFID-tagged products was recognized, an informed debate has been taking place. For example, the possible economic consequences are discussed by Fusaro in form of a fictional case study [6]. Consumer organizations and data protection commissioners have taken proactive stands on privacy, and have developed policies and guidelines for appropriate implementation of RFID technology [1, 3]. On the other hand, there are RFID proponents who argue that RFID privacy concerns are exaggerated and legislation is premature [2].

The RFID Position Statement of Consumer Privacy and Civil Liberties Organizations of November 20, 2003, raises privacy concerns with RFID such as the hidden placement of tags and readers, providing unique identifiers for all objects worldwide, massive data aggregation, and individual tracking and profiling.

But what are the problems with RFID? Most of today's RFID tags have a static identifier, which never changes throughout its lifetime and is transmitting unassumingly to any reader requesting it. RFID tags, whose identifiers are globally unique and follow a standardized structure, enable inferences about the tagged item to be made.

Detecting tag presence often implies signaling the presence of a human being. By correlating multiple observations of the tag's identifier, an adversary tracks the item and may profile an individual's associations. Next, the adversary may have a "hotlist" of items/tags in advance that it wishes to detect. Once the adversary succeeds in establishing a link between a tracked item and the owning individual, the individual's history becomes open. If there exists unlocked memory on the tag, an adversary could even write a 'cookie' and thus track tags and bypass other mechanisms intended to prevent tracking or hotlisting [10].

In the retail space, consumer privacy could be affected by target marketing, where the set of products carried by a consumer or the shopping history if known is then used to classify that consumer for focused marketing efforts. It has further been argued that this knowledge about a customer might also lead to price discrimination or embarrassing situations.

## 4. CONSUMER PRIVACY PROTECTION

We categorize the technologies for protecting consumer privacy according to who must provide the technology. Technology deployed by the consumer consists of physical means to detect or block RF signals. A Faraday Cage around the item with an embedded or attached RFID tag will prevent radio waves from reaching the tag. This approach works well with small items, which fit into a purse or bag lined with aluminum foil, but has its limits when goods are large or if the consumer is not aware of tags. RFID sensor detectors indicate the presence of an RFID reader, and, correspondingly, an RFID reader can be used to search for RFID tags by the consumer by scanning products after purchase. A drawback of the sensor detector is that (almost) any source of electromagnetic waves, a wireless LAN for example, may trigger an alarm.

There is also the possibility of jamming RF signals. Such jamming stations have been used to disable the operation of cell phones. A device that broadcasts radio signals to block/disrupt nearby RFID readers could work. However, this crude approach raises legal issues relating to illegal broadcasting. Alternatively, the RSA blocker tag [7] is an elegant mechanism to interfere with the reading of RFID tags. In its basic form, the blocker tag responds in the singulation phase to any query by simulatng all possible serial numbers for tags, thereby obscuring the serial numbers of other tags. Blocker tags are expensive and place the onus of privacy

protection solely on consumers [3]. A blocker tag can only be similar in size and cost to a conventional RFID tag if produced in high quantities. It also suffers from the heterogeneity of current RFID technology: different frequencies, air protocols, etc. It is not likely that tag manufacturers will produce blocker tags as they could be used to interfere with the legitimate reading of RFID tags.

On the other hand, RFID tag manufactures and researchers have developed technologies embedded into RFID tags to protect consumer privacy. The most prominent example of this class is the "kill command" specified by EPCglobal, which allows the deactivation of tags at the point of sale. While the kill command requires only limited changes to tag hardware, there are also some weaknesses [4, 7]. First, it is an "all or nothing" privacy mechanism. Once deactivated, the tag cannot be used for after-sale purposes, no matter how interesting they might be for the consumer. Emerging applications may require that tags still be active while in the consumer's possession. Secondly, consumers have no way of knowing whether the tag has actually been deactivated. The command may have not been received by the tag, or tags can appear to be "killed" when they are really "asleep" and can be reactivated.

There is a steadily increasing number of proposals for "smart" tags,[2] including hash locks, re-encryption, silent tree-walking, or other cryptography-based approaches to prevent the unauthorized reading of RFID tags. Because of stringent cost pressure, in particular within the retail space, tags are passive and have extremely few gates [12]. Realistically, only simple password comparison and XOR operations can be expected [10].

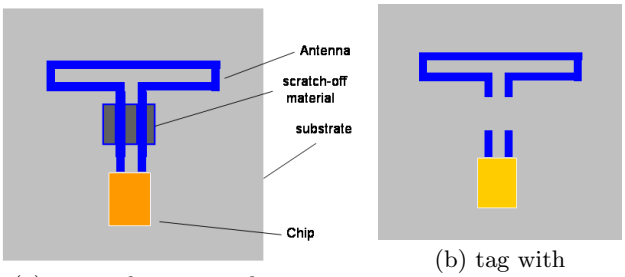
# 5. CLIPPED TAGS

Existing solutions to protect consumer privacy either put the burden on the consumer, including the risk of illegal behavior, or are hampered by the very limited capabilities of inexpensive RFID tags. The kill command seems to be the solution with the greatest potential. However, it is still necessary to overcome its three major weaknesses: complex key management, no controlled reuse after purchase, and no (visual) confirmation of successful disablement.

As an alternative, we propose to provide RFID tags with structures that permit a consumer to disable a tag by mechanically altering the tag in such a way so as to inhibit the ability of a base station or reader to interrogate the RFID tag or transponder by wireless means. This provides visual confirmation that the tag has been deactivated. Once a tag has been deactivated (or "clipped"), only electromechanical means may be used to reactivate it. Such a reactivation would require deliberate actions on the part of the owner of the RFID tag to permit the reactivation to take place, and thus could not be undertaken without the owner's knowledge unless the item were either stolen or left unattended. Whereas a physical destruction of the tags would likely damage the original item [8], we show practical ways to physically separate the chip from its antenna.

## 5.1 Removable Electrical Conductor

In Fig. 1, we show a first possible realization of clipped tags. In this kind of tag, the antenna is constructed of conducting "scratch-off material". This material is familiar to consumers from its use to obscure printed material on lottery tickets or prepaid phone cards. The antenna of the RFID tag is manufactured on a substrate using the scratch-off material. The substrate or mount may be a plastic material such as polyimide or polyester. The chip is mounted on the substrate and is connected to the antenna by an electrical conductor or conductors. The RFID tag is manufactured in such a way that a part or all of the antenna or its connecting wiring is exposed. The electrical conductor or conductors pass through a window, e.g. an exterior portion of the substrate or mount. For instance, an open window in a covering substrate may be built into the tag at or in the region where the antenna is connected to the chip.




(a) tag with connected antenna (b) tag with disconnected antenna

**Figure 1: RFID tags with removable electrical conductor**

Such tags are placed on the article or on its packaging in such a way that the antenna or the antenna-chip connection can be scratched off using a coin, a fingernail, or other such object. Thus, the consumer or a check-out attendant in a retail establishment may perform the scratch-off operation to disable interrogation of the tag. The tag is open for visual confirmation that the tag has been deactivated. Subsequent communication with the tag may be made using mechanical probes to contact the antenna stubs.

## 5.2 Perforation

Fig. 2 shows another realization of clipped tags. Perforations such as those used to separate postage stamps[3] from each other are manufactured into the antenna and its substrate. A separation along the line of small holes or cuts detaches the antenna from the chip, or a sufficient portion of the antenna from itself. In this way, the RFID tag is disabled. A pull tab may facilitate the separation.

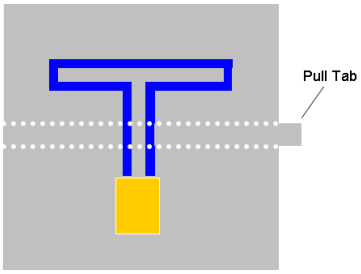



**Figure 2: RFID tags with perforation**

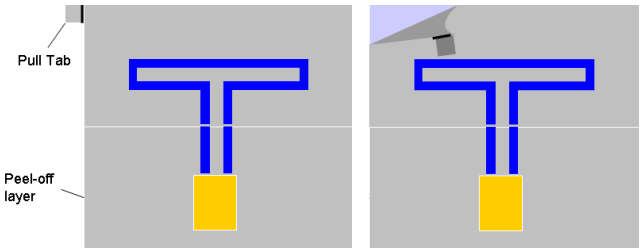
[2]See Gildas Avoine's Web page at `lasecwww.epfl.ch/~gavoine/rfid/` for an exhaustive overview.

[3]See Wikipedia article "Postage stamp separation" at `en.wikipedia.org/wiki/Postage_stamp_separation`.

Experiments have to be performed to identify the most suitable spacing of the holes in respect to the size of the holes. It has also been suggested that the tag may be cut by scissors to obtain the separation.

### 5.3 Peel-off layer

Fig. 3 shows our last example of clipped tags. The antenna or portion of the antenna is sandwiched between two layers of packaging material. In this sandwich, the antenna is connected to the upper layer in such a way that it sticks to it. The lower layer, in turn, is affixed to the purchased item. Adhesion of the antenna to the upper layer of the packaging material is greater than its adhesion to the lower layer. This produces a peel-off layer affixed by an adhesive material or layer to the antenna. The antenna is removed or destroyed by pulling the upper layer of material from the tag, removing the antenna with it.




(a) tag with connected antenna (b) peel-off layer partly lifted

**Figure 3: RFID tags with a peel-off layer**

A pull tab, connected to the upper layer of packaging, facilitates the delamination process. The tag may be designed in such a way that only a portion of the antenna is removed, the portion that is above the peel-off line. This leaves a pair of short antenna lines, or stubs, attached to the chip, which can later be used to reactivate the chip if desirable. Any means for reactivating the tag such as contacting the antenna stubs, repairing the antenna, or adding a new antenna require the cooperation of the owner of the item, thus assuring the privacy of the owner.

## 6. CONCLUSION

Clipped tags are a simple and practical privacy-enhancing technique for RFID retail, which offer a number of advantages compared with other technologies, in particular the kill command. Deactivation can be performed in an easy, reliable, and verifiable way. Even if the RFID tag is "printed" right onto a product, its antenna can be disconnected from the chip. In this way, a post-purchase reactivation is possible, for example to enable after-sale benefits. In the scheme described, reactivation requires deliberate actions on the part of the owner of the RFID tag, and can not be undertaken without the owner's knowledge. Thus, it is an appropriate mechanism to implement consumer consent.

In the retail space, technological solutions are constrained. Stringent cost requirements limit the tag's computational power, which in turn limits the mechanisms to give users options and control over the use of their data in back-end systems. We believe that physical structures described here can be embedded in today's manufacturing process at minimal extra cost.

If deactivation is performed by the consumer no special devices are needed by retailers. There would also be no "interruption" of the flow at the checkout counter. Otherwise, the "clipping" of the tag could for example be integrated into today's devices that disable antitheft tags.

It has always been possible to deactivate an RFID tag by brute force, for example by breaking the antenna or applying a high voltage to the tag. Clipped tags are also subject to fraudulent manipulation, such as other labeling technologies, for example bar codes. Appropriate fraud prevention must be in place, in particular when used in self-checkout applications. The visual inspection capabilities of clipped tags may support the detection of fraud.

Unless RFID chips accommodate enough gates to deploy sufficient cryptography or novel approaches based on reader distance [4] or P3P-like protocols [5] have been adopted, the physical deactivation as described in this paper establishes a practical privacy-enhancing technology.

## Acknowledgments

We thank Robert J. von Gutfeld, who contributed to the idea of clipped tags, Luke O'Connor for valuable discussions, and Charlotte Bolliger for improvements on the readability of the manuscript.

## 7. REFERENCES

[1] ARTICLE 29 Data Protection Working Party. Working document on data protection issues related to RFID technology. EU 10107/05/EN WP 105, Jan. 2005. `europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf`.

[2] J. Brito. Relax, don't do it: Why RFID privacy concerns are exaggerated and legislation is premature. *UCLA Journal of Law and Technology*, 8(2), Fall 2004. `www.lawtechjournal.com/articles/2004/05_041220_brito.pdf`.

[3] A. Cavoukian. Tag, you're it: Privacy implications of radio frequency identification (RFID) technology. Feb. 2004. `www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=15007`

[4] K.P. Fishkin, S. Roy, and B. Jiang. Some methods for privacy in RFID communication. In *Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, Lecture Notes in Computer Science 3313, pg. 42–53. Springer, 2004.

[5] C. Floerkemeier, R. Schneider, and M. Langheinrich. Scanning with a purpose – supporting the fair information principles in RFID protocols. In *Ubiquitous Computing Systems (UCS 2004)*, Lecture Notes in Computer Science. Springer, 2005.

[6] R.A. Fusaro. None of our business? *Harvard Business Review*, 82(12):33–38, Dec. 2004.

[7] A. Juels, R.L. Rivest, and M. Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *Computer and Communication Security (CCS'03)*, pg. 103–111. ACM Press, 2003.

[8] D. Luckett. The supply chain. *BT Technology Journal*, 22(3): 50–55, July 2004.

[9] M. McGinity. RFID: Is this game of tag fair play? *Commun. ACM*, 47(1):15–18, 2004.

[10] D. Molnar and D. Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In *Computer and Communications Security (CCS'04)*, pg. 210–219. ACM Press, 2004.

[11] R. Want. RFID: A key to automating everything. *Scientific American*, pg. 46–55, Jan. 2004.

[12] S. Weis, S. Sarma, R.L. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *Security in Pervasive Computing*, Lecture Notes in Computer Science 2802, pg. 201–212. Springer, 2003.

[13] A. Weiss. Me and my shadow. *ACM netWorker*, 7(3):24–30, 2003.