RZ 3597 (# 99607) 03/15/05
Computer Science 12 pages

Research Report

Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced

Günter Karjoth

IBM Research GmbH
Zurich Research Laboratory
8803 Rüschlikon
Switzerland
Email: gka@zurich.ibm.com

Paul Moskowitz

IBM Research
T.J. Watson Research Laboratory
P.O. Box 218
Yorktown Heights, N.Y. 10598
Email: mosk@us.ibm.com

IBM Research
Almaden · Austin · Beijing · Delhi · Haifa · T.J. Watson · Tokyo · Zurich

Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced

Günter Karjoth[1] and Paul Moskowitz[2]

[1] IBM Research, Zurich Research Laboratory,
gka@zurich.ibm.com
[2] IBM Research, Watson Research Laboratory
mosk@us.ibm.com

March 15, 2005

Abstract. Existing solutions to protect consumer privacy 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. These properties make clipped tags superior to other privacy-enhancing technologies, in particular the kill command.

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 bar codes", with the advantage 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 [14]. Many large retailers have instructed their suppliers to tag pallets and cases with RFID tags carrying the Electronic Product Code (EPC$^{\mathrm{TM}}$), a "license plate" with a hierarchical structure that can be used to express a wide variety of different, existing numbering systems. EPCglobal[3] has approved a new communications protocol for UHF tags that

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

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. Even though some experiments on item tagging have been conducted by retailers, the enormous number of tags needed, in the many trillions, and the current costs of tags, US $0.25 to $0.50, indicate that it will be several years before large-scale item tagging becomes a reality.

Given that the ultimate vision is to tag all products at the item level, consumers will be affected. 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 and thus tags can be read without explicit user action [5]. Although tags that can be read at a distance cannot be as small as a grain of rice, as stated for example in [20], the aforementioned characteristics of RFID tags have raised privacy concerns, see for example [15, 18].

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 [18] 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 is inhibited. We call such structures 'clipped tags' as the body (chip) becomes separated from the head (antenna). Such a physical 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 and thus could not be undertaken without the owner's knowledge unless the item were either stolen or left unattended.

In Section 2, we give a brief introduction to the fundamentals of RFID technology. Privacy concerns and associated reactions are discussed in Section 3. In Section 4, we elaborate on standard protection mechanisms based on blocking the RF signals, killing the tags, or protecting the air protocol by cryptography. Clipped tags and three ways of implementation are presented in Section 5.

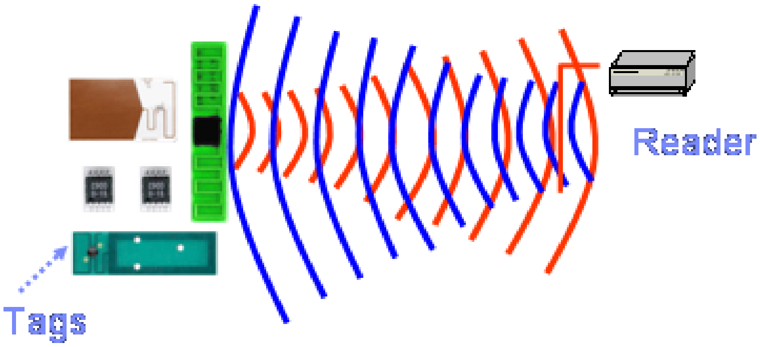


Fig. 1. Schematic of an RFID system. (Reprinted with permission by Intermec Technologies)

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. Fig. 1 shows its main principal functionality.

RFID tags come in many form factors, for example, embedded in a car key to work as 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 when they detect a radio frequency signal from a reader over a range of distances. Passive tags, i.e., tags without battery, can only send information back to the reader on the reflected signal. Readers then either send tag information over the enterprise network to back-end systems for processing or display it to the end user. When the reader broadcasts a request in its interrogation zone, the tags send back their answers, which will then be sent to the (back-end) data processing system. The simplest RFID tag will send the reader its unique ID serial number, which may be 64, 96, or 256 bits in length.

RFID tags differ in the frequencies used, ranging from 100 kHz (access control, animal tracking) to 2.45 GHz (item management), in power consumption, memory (read-only, write-once (identity tags), (multiple) 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.

As an RFID tag reader is only able to communicate with a single RFID tag at a time, a “singulation protocol” is used to overcome “collisions” [13, 19]. The tree-walking singulation algorithm enables an RFID tag reader to identify the serial numbers of nearby tags individually by means of a bit-by-bit query process resembling a depth-first search of a binary tree. In the ‘Aloha’ singulation protocol, tags respond to reader queries by randomly selecting a ‘slot’ within a given time interval.

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, and currency tags. RFID systems are primarily designed to uniquely identify items by affixing a tag containing a unique identifier to every item of interest. To identify an individual tag in a group, tags usually store at least a unique ID (UID). A tag may only carry a unique ID, where information is encoded in this identifier (as in the EPC) or its memory is partioned into a random serial number identifying the tag and additional memory to store information about the item to which the tag is attached [6].

RFID tags, in particular those used in high quantities, for example in supply-chain management and retail, must be very inexpensive (a few cents only). Besides being passive tags, they have limited storage (tag identifier only), limited computation power (only a few thousands logic gates, in particular no cryptography [19]), and low bandwith. In addition, their communication time must be short as hundreds of tags have to 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 [7]. Consumer organizations and data commissioners have taken a proactive stands on privacy, and develop policies and guidelines for appropriate implementation of RFID technology. Data commissioners have reacted and propose guidelines or regulations. On the other hand, there are RFID proponents who argue that RFID privacy concerns are exaggerated and legislation is premature [3].

The RFID Position Statement of Consumer Privacy and Civil Liberties Organizations of November 20, 2003, raises the following privacy concerns with RFID:

- hidden placement of tags;
- unique identifiers for all objects worldwide;
- massive data aggregation;
- hidden readers;
- 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,[4] enable inferences about the tagged item to be made. In the following, we describe possible attacks on privacy.

[4] RFID tags with EPC reveal information about the manufacturer and class of product they are attached to.

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 [16].

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.

In 2002, Garfinkel proposed "An RFID Bill of Rights", inspired by the Principles of Fair Information Practices, in which consumers should have the following rights [8]:

Notice The right to know whether products contain RFID tags. The right to know when, where and why the tags are being read.

Choice The right to have RFID tags removed or deactivated when a product is purchased. The right to use RFID-enabled services without RFID tags.

Transparency The right to access an RFID tag's stored data.

Organizations followed to state RFID policies such as Privacy Commissioners [4], the German Computer Society (GI), European Commission [1], and EPCglobal.

4 Approaches to protect consumer privacy

We categorize the technologies for protecting consumer privacy according to the responsibility of provision. 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,[5] 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 to scan products after purchase.[6] 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 to jam RF signals, such as jamming stations have been used to disable the operation of cell phones. A device that broadcasts radio signals to block/disrupt nearby RFID readers would work. However, this crude approach raises legal issues relating to illegal broadcasting. Alternatively, the RSA blocker tag [13] is an elegant mechanism to interfere with the reading of RFID tags, and is described in more detail in Section 4.1.

[5] As an example, see the products of mobileCloak (`www.mobilecloak.com`).

[6] Prototypes are already available, either in the form of a bracelet or as a self-assembly kit to function at 13.56 MHz ('RFID-Detektor' and 'Tag-Finder' at eMedia, `www.emedia.de`).

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. Problems with this approach are described in Section 4.2. There is a steadily increasing number of proposals for "smart" tags. These proposals include hash locks, re-encryption, silent tree-walking, or other cryptography-based approaches to prevent the unauthorized reading of RFID tags. We comment on some of them in Section 4.3.

4.1 RSA blocker tags

The most prominent example of a consumer self-protection device is the RSA Blocker Tag [13], which prevents the reading of other RFID tags in its proximity by spamming the RFID reader. In the basic form, the blocker tag responds in the singulation phase to any query related to tags whose ID share the same prefix by broadcasting simultaneously both a '0' and a '1' bit. This forced collision drives the reader to recurse on all nodes that lie in the common subtree. Thus, the blocker tag simulates all possible serial numbers for tags, thereby obscuring the serial numbers of other tags. When carried by a consumer, it effectively mounts a denial-of-service attack.

Selective blocker tags, however, only simulate a given subset of serial numbers. Such ranges of serial numbers may constitute "privacy zones". Each zone (subtree) is identified by its common prefix $b_1, \ldots, b_d$ or, equivalently, by the position of the last common bit on the serial number (the "privacy bit" at position d). Tags can be transferred to a privacy zone if the corresponding privacy bit is switched on. If zero, the selective blocker tag is silent and only the tag responds to queries related to its ID. Otherwise, the selective blocker tag responds to any query related to tags whose identifiers are in the privacy zone.

Thus, when the RFID tag reader at a cash register scans an item for purchase by a customer, it also transmits a tag-specific key to the RFID tag on the item. This causes the privacy bit in the serial number of the tag to flip to a '1'. However, a password needs to be managed for each standard RFID tag, to authorize it to change privacy zones. Further, the reader protocol must be augmented with a special query to ask whether there is a subtree blocked by a selective blocker tag ("polite blocking"). Otherwise, the reader may never get around to reading identifiers outside of privacy zones.

Blocker tags are expensive and place the onus of privacy protection solely on consumers [4]. 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. Furthermore, retailers have to provide appropriate equipment at checkout where either staff or the consumers disable tags if wanted. Finally, it may be possible that the jamming can be overcome in time [5].

4.2 Kill command

Concerned over public perceptions of RFID tags embedded in products (Benetton, Gillette), chip makers have introduced a “kill command” into their RFID chips. This special command causes a permanent state change in the tag, which prevent it from responding to any interrogations from any readers. Applied upon purchase of tagged products, “a killed tag is truly dead and can never be re-activated” [13], and thus provides post-purchase privacy.

While the kill command requires only limited changes to tag hardware, there are also some weaknesses [5, 13]. 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.

As with the blocker tag, “passwords” are needed to prevent unauthorized killing of tags. Depending on the RFID tag specification, passwords range from trivial eight bits up to 32 bits. However, if the password(s) become known, the consequences for the retail supply chain are much severe, as this would allow a malicious customer or competitor to silently deactivate numerous tags while he or she is walking along the shelves.

4.3 Cryptography

Current RFID technology for the retail space imposes severe constraints on deploying cryptography on the RFID tags. Because of stringent cost pressure, tags are passive and have extremely few gates [19]. As an RFID tag is only powered when within range of a reader, it only has an extremely limited amount of time to carry out computations. Precomputation of results is also impossible when the tag is out of range [16]. Although recent breakthroughs have been reported in implementing ciphers, for example NtruEncrypt, with no more than 3000 gates [9], we assume that encryption, hash functions, or pseudo-random functions are not possible on today’s RFID tags. Realistically, only simple password comparison and XOR operations can be expected [16].

Only recently have privacy-preserving authentication protocols been proposed that are based on randomized hash-lock [19], re-encryption [12], hash chains [17], one-time authenticators [10], PIN-protected read commands to authenticate readers against tags [11], and others. In the remainder of this section, we briefly elaborate on their basic characteristics and limitations. For a more in-depth discussion on many of these protocols, we refer to [2, 13, 16].

Even if a tag only transmits a fixed identifier, it can be used to trace an object in time and space [2]. However, as noted earlier (see Section 2), a tag must first be singulated before the reader can start to send commands. Thus, any tag that uses a static identifier in the collision-avoidance protocol can be uniquely identified [2, 16].

To achieve location privacy, the information sent by the tag to the reader has to change at each identification. This information is either the identifier of the tag or an encrypted value of it. It implies that the information sent by the tag has to be indistinguishable (by an adversary) from a random value and must be used only once. When the reader is involved in the regeneration of the information, access to a central database is needed. Otherwise, the tag must be able to generate new information by itself, which requires corresponding cryptographic primitives.

Passwords and secret keys for RFID tags must be securely managed. Good security practice further demands that different passwords or keys per tag are used. This may impose a workload on the reader that is on the order of the number of keys. Only Molnar and Wagner have shown a private authentication scheme, for which the reader workload is logarithmic in the number of tags [16]. On the other hand, this protocol needs a logarithmic number of message exchanges. Because of chip cost and time consumption, it therefore does not offer an alternative technology for today's retail business.

5 Clipped Tags

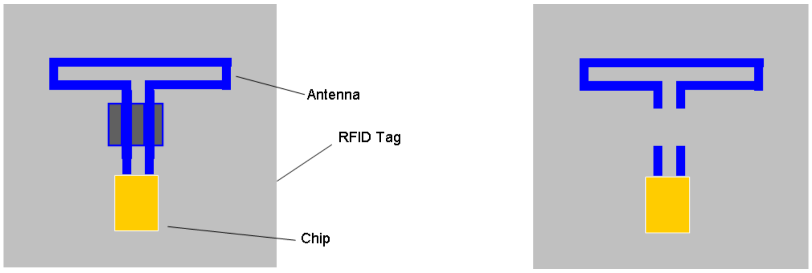
As discussed in the preceeding section, existing solutions to protect consumer privacy either put the burden on the consumer, including the risk of illegal behavior, or are hampered by the very limited capabilities of the so-called 5-cent RFID tags. The kill command seems to be the solution with the 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 deactivatede (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.

In the remaining section, we show three possible realizations of clipped tags, which address different physical environments and needs. Whereas a physical destruction of the tags would likely damage the original item [14], we show practical ways to physically separate the chip from its antenna.

5.1 Removable Electrical Conductor

In Fig. 2, 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



(a) tag with connected antenna

(b) tag with disconnected antenna

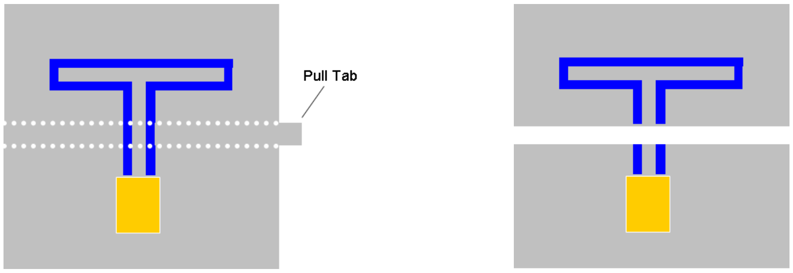
Fig. 2. RFID tags with removable electrical conductor

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.

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. 3 shows another realization of clipped tags. Perforations such as those used to separate postage stamps[7] 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.

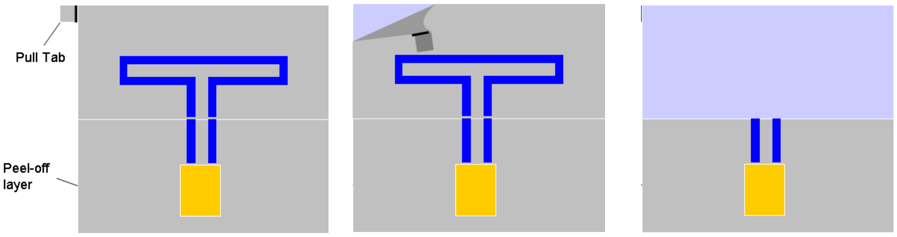


(a) tag with connected antenna

(b) tag and antenna separated

Fig. 3. RFID tags with perforation

[7] See Wikipedia article “Postage stamp separation” at `en.wikipedia.org/wiki/Postage_stamp_separation`.



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

Fig. 4. RFID tags with a peel-off layer

5.3 Peel-off layer

Fig. 4 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 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.

6 Conclusion

In this paper, we proposed a simple and practical privacy-enhancing technique for RFID retail. Clipped tags offer a number of advantages compared with other technologies, in particular the kill command. No special devices are needed by retailers. There is no "interruption" of the flow at the checkout counter. Deactivation can be performed by the consumer 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.

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-check out 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 [5] or P3P-like protocols [6] 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.

References

1. ARTICLE 29 Data Protection Working Party. Working document on data protection issues related to RFID technology. 10107/05/EN WP 105, Jan. 2005. `europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf`.
2. G. Avoine and P. Oechslin. RFID Traceability: A multilayer problem. In *Financial Cryptography – FC'05*, Lecture Notes in Computer Science. Springer, 2005.
3. 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`.
4. 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`
5. K.P. Fishkin, S. Roy, and B. Jiang. Some methods for privacy in RFID communication. In *European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, Lecture Notes in Computer Science 3313, pages 42–53. Springer, 2004.
6. C. Floerkemeier, R. Schneider, and M. Langheinrich. Scanning with a purpose – supporting the fair information principles in RFID protocols. To appear in *2nd International Symposium on Ubiquitous Computing Systems (UCS 2004)*, Lecture Notes in Computer Science. Springer, 2005.
7. R.A. Fusaro. None of our business? *Harvard Business Review*, 82(12):33–38, Dec. 2004.
8. S. Garfinkel. An RFID bill of rights. *MIT Technology Review*, page 35, Oct. 2002.
9. G. Gaubatz, J.-P. Kaps, and B. Sunar. Public key cryptography in sensor networks – revisited. In C. Castelluccia, H. Hartenstein, and C. P. et al., editors, *European Workshop on Security in Ad-hoc and Sensor Networks (ESAS 2004)*, Lecture Notes in Computer Science 3313, pages 2–18. Springer, 2004.
10. A. Juels. Minimalist cryptography for low-cost RFID tags (extended abstract). In C. Blundo and S. Cimato, editors, *Fourth International Conference on Security in Communication Networks – SCN 2004*, Lecture Notes in Computer Science 3352, pages 149–164. Springer, 2004.

11. A. Juels. Strengthening EPC tags against cloning. Manuscript, October 2004.
12. A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In R. Wright, editor, *Financial Cryptography*, Lecture Notes in Computer Science 2742, pages 103–121. Springer, 2003.
13. A. Juels, R.L. Rivest, and M. Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *10th ACM Conference on Computer and Communication Security*, pages 103–111. ACM Press, 2003.
14. D. Luckett. The supply chain. *BT Technology Journal*, 22(3):50–55, July 2004.
15. M. McGinity. RFID: Is this game of tag fair play? *Commun. ACM*, 47(1):15–18, 2004.
16. D. Molnar and D. Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In *11th ACM Conference on Computer and Communications Security (CCS)*, pages 210–219. ACM Press, 2004.
17. M. Ohkubo, K. Suzuki, and S. Kinoshita. A cryptographic approach to “privacy-friendly” tags. RFID Priavcy Workshop, 2003.
18. R. Want. RFID: A key to automating everything. *Scientific American*, 290(1):46–55, Jan. 2004.
19. S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *First International Conference on Security in Pervasive Computing*, Lecture Notes in Computer Science 2802, pages 201–212. Springer, 2003.
20. A. Weiss. Me and my shadow. *ACM netWorker*, 7(3):24–30, 2003.