Maintaining privacy in RFID enabled environments – Proposal for a disable-model

Sarah Spiekermann
Institute of Information Systems
School of Business and Economics
Humboldt University Berlin
Spandauer Strasse 1
10 178 Berlin
Germany
sspiek@wiwi.hu-berlin.de

Oliver Berthold
Department of Computer Science
Humboldt University Berlin
Unter den Linden 6
10 099 Berlin
Germany

berthold@informatik.hu-berlin.de

Abstract

RFID technology will be a ubiquitous reality in every-day life in the near future. This paper describes a number of reasons why manufacturers, retailers and consumers want to maintain an RFID tag's functionality both in retail environments and after a purchase has been made. On this basis it is argued that current tags' killing functionality cannot be a long-term solution. However, it is also shown that leaving an RFID chip alive can lead to an unprecedented level of privacy intrusion. All borders constituting peoples' private lives could systematically be undermined with RFID tags remaining active. The authors therefore argue that the current RFID tag classes 0 and 1 must be enhanced with privacy functionality. Two levels of privacy protection are suggested leading to a class 2 and 3 proposal for tag specification.

I. Introduction

RFID technology is a major enabler of ubiquitous computing environments.

In the context of the research project InterVal[1], investigations are being made in the potential impact of Radio Frequency Identification (RFID) technology on marketing and privacy. Insights gained are used to support the design of future RFID enabled environments.

Today, RFID technology is mainly used to facilitate supply chain management. Yet, as the technology's cost decreases it also allows for new business models beyond the original logistics function. In fact, manufacturers, retailers and consumers can all take advantage of the technology's ability to uniquely identify objects, view their characteristics and relate to their owners.

At the same time, considerable privacy issues overshadow the introduction of RFID technology. Public debate is rising over the *conditions* of RFID presence in consumer markets and private home environments.

The current article suggests to add privacy enhancing functionality to the current RFID tag specification version 1.0 as formulated by the AutoID Centre (or respectively EPC Global) (EPC Global, 2003). To justify this suggestion, the article sets out (section 2) with a description of long-term industry business models and consumer benefits arising from RFID technology. These benefits make plain that it is unrealistic to expect a widespread use of current tags' 'killing' functionality as it is foreseen in the class 0 and class 1 tag specification. However, if tags are not killed privacy will systematically be sacrificed (section 3). We therefore argue that more thought must be put into the privacy and security design of RFID tags. We present a simple concept on how the current specification can be enhanced (section 4).

[1] InterVal is *InterVal* focuses on the design and analysis of Internet technologies in the context of modern supply chain management. One focus is the study of *privacy and security* issues affecting the acceptance of new technologies such as RFID. The Berlin-based research center unites researchers from three Berlin universities and the Fraunhofer Institute for Software and System Engineering (ISST).

II. Consumer incentives and market models for RFID adoption

RFID technology implies benefits for retailers, manufacturers and consumers. In the current article, only those processes are considered where end-users are in touch with RFID technology. Thus, the role of RFID in pre-shopping logistics is excluded from the discussion.

Retailer benefits from RFID on the shop-floor

Beyond cost reduction in the supply chain (currently estimated at around 5%[2]), retail outlets derive several major benefits from RFID technology. First, cost savings will be made through automated store logistics. Fewer personnel are needed to supervise self-serving cash-registers and watch over automated shelf-management (currently estimated at 10%[2]). Second, theft protection is often cited as a reason for RFID introduction in retail environments. Third, increase is expected from personalized information and recommendation services. In fact, RFID technology (combined with some smart applications) promises a whole new class of one-to-one promotions and information services in the retail outlet. For example, consumers could request guidance on products that are genetically modified Finally, RFID allows for better tracking of peoples' movements through the store, measuring time spent in front of product categories and gaining a better insight into the product selection process. This information can be used to understand media effectiveness, improve product portfolios on offer in the store and test for the roots of product attractiveness. This new type of business intelligence will not only benefit retailers, but also product suppliers who then eventually want to buy this whole new type of data available on consumer shopping behavior.

Based on these arguments, we strongly believe that it is unrealistic to expect retailers to forgo the benefits of RFID technology in their stores. Consequently, RFID tags will remain active (not-killed) in store environments.

Consumer benefits from RFID tags

Due to retailers adopting RFID in their stores, consumers take advantage of personalized information services and potential time savings when shopping. However, also after product purchase consumer potential benefits arise from RFID tags stored on products.

First, many of today's visions encompassed in intelligent home environments reside on RFID technology. New service dimensions are planned and technologies are in the development pipeline of many major IT system manufacturers.[3] For example, the refrigerator could order new food or give a warning signal if a product has passed its eat-by date. Also, many product categories' security, safety and convenience features are planned to be enhanced. RFID is thus seen as a means to differentiate products and brands in the consumer market.

A second argument for RFID introduction is the information value created for consumers. EPC related data can contribute to the convenience, security and entertainment of consumers. Consumers may, for example, be interested to know more about the products they own. In a convenient way they can use the EPC to access information about their objects, view their guarantees and usage manuals, FAQ lists or even find other people who bought from the same product line. One may say that consumers can have something like an online-diary of their objects. Where appropriate, they may also gain an insight into the "family" of their objects, other products from the same manufacturer. In some situations this information could even enhance consumer safety. For example, when they are able to check the compatibility of their pharmaceuticals at home.

Third, RFID can in a few occasions contribute to consumer security. If product flaws are identified after a sale or products are poisoned it is possible to discern exactly what product objects are affected. Consumers can then either be warned directly and individually (if the consumer's identity is known to the sales channel) or hearing

[2] The figures relate to a study published by strategic management consultancy A.T.Kearney., "RFID/EPC Managing the Transition (2004-2007)", 2004

[3] A good insight is given by HP's promotion video called " Cool Town"

about the danger can verify to what extend their particular product is affected (by reading out their respective EPC).

Based on these arguments, we strongly believe that it is unrealistic to expect consumers to have an interest in killing tags at the store exit. We believe that in order to make those visions a reality, RFID tags will have to be kept ‘alive’.

Manufacturer benefits from RFID tags

Current supply chains have led to an increased distancing of manufacturers from their customer base. Big retail chains usually “sit in the middle” and have cut manufacturer's direct access to those who consume their products. RFID technology has the potential to change this dynamic to a certain extend. EPC is designed to directly access manufacturers’ product databases or web pages over the Internet.

Since manufacturers embed the EPC in their products they are also the most likely party to hold the ownership of the respective information related to each object (the “family” information). Thus, when people access information directly about “their” belongings based on their EPCs they are most likely to hit the manufacturer's website first. One could think of an EPC related website as person's personal web-diary on his/her possessions. And since people can get quite attached to their possessions it is not too far fetched to postulate that manufacturers have the potential to establish customer relationships here that were difficult to obtain in the past. Manufacturers (especially of shopping and luxury goods) have the potential to build user relationships around their products in a new fashion. They can up-sell customers to more enhanced versions of what they already own, they can cross-sell to other product categories, build user communities, etc. Direct customer access being a continued vision of manufacturers in the context of today’s standard electronic commerce practices gains a new level of feasibility in environments of ambient intelligence.

Another reason for manufacturers to push for RFID is that it is an efficient means to prevent forgery, because the tags can be programmed to prove their authenticity.

As a result of these arguments we argue that at least for high-involvement goods it is realistic to expect manufacturers to take a long-term interest in RFID technology (which they currently seem to see rather as a nuisance than an opportunity).

Impact of RFID on Privacy

Around 44% of retailers use RFID technology in their supply chains or consider its introduction (Forrester, 2003). One important dimension of the current public debate on RIFD though is marked by rising concern over the technology's impact on privacy.

Consumer privacy can be impacted in two distinct temporal phases: First, in an RFID enabled retail outlet and second after the sale has taken place and RFID tagged products are taken home. The current article focuses on the second phase. It looks at privacy intrusion when RFID hits the street.

The current RFID specifications for class 0 and 1 tags (see below for more detail) foresee that each tag contains a unique electronic product code (EPC). In some respects, the EPC is similar to the bar code. It contains a serial number that can be related to a product category and a manufacturer. However, the EPC is longer and therefore more comprehensive: each *individual* object (rather than an object class) is identified. This allows to retrieve information on the manufacturer, product category as well as (and most important) individual product traits. Furthermore, while the traditional bar code can only be read out via a scanner pointing directly to it, EPCs on an RFID tag can be read out quasi simultaneously, unnoticed and from a distance. The EPC on the object and the scanner (reader) do not need to be in a line of sight. As a result, privacy concerns have mounted.

Privacy concerns usually take two major directions: One is about the direct abuse of RFID tags' ‘uncontrolled willingness to tell’ the EPC code to unauthorized readers. Thus, privacy is intruded when people with readers can spy unrecognized on the belongings of others. The other thread of fear circles around the combination of highly granular EPC data with personal identity data. Personal identity data is usually collected with the help of loyalty cards. Combining a person's identity with such detailed product information then allows for a degree of psychographic segmentation of individuals that has not been available ever before. The ‘transparent customer’ that has often been cited in the past has become a reality. [4]

To address privacy concerns, RFID developers have included a password protected “kill-function” in both RFID tag classes 0 and 1 [EPC Global, 2003]. Retailers in turn have started to offer customers the possibility to kill a tag's EPC before leaving the store. However, as the discussion in section II has shown it is unrealistic to expect that killing RFID tags is a long term solution. In store environments RFID technology plays a major role for retailers. And even if tags were killed at the store exit, the combination of EPC data with personal data at the moment of purchase would not be prohibited (assuming that consumers own loyalty cards).

However, **if tags are *not* killed** privacy intrusion outside of the store can occur. Two conditions of misuse should be distinguished:

1. RFID tags exist on products, but no electronic reference to the product owner is in existence (for example, somebody has bought a product and paid for it cash without using a loyalty card).
2. RFID tags exist on products and an electronic transaction has occurred which has the potential to establish a link between the product and its owner (for example, somebody has bought a product and paid for it via credit card or by using a loyalty card).

In the first condition ‘only’ natural privacy borders can be intruded by others without peoples’ knowledge and consent. [5]

- Natural borders

stand for peoples' desire to sometimes be physically unobserved or secluded. For example, to pursue activities unobserved within one’s own walls, to be let alone in one’s room or to communicate via sealed letters. As described above, RFID has the potential to intrude in this natural privacy, because readers can (even without any authorization) read out a person's belongings. A first series of focus groups conducted by the AutoID Center has shown that consumers are particularly alert to this type of intrusion (Duce, 2003). Natural borders may also be impacted if people in a shop are observed in a targeted manner by RFID-triggered video cameras (FoeBuD e.V, November 2003).

In the second condition where a link is established between an RFID enabled object and its owner, several additional scenarios of breaking down personal ‘privacy borders’ may be expected:

- Ephemeral borders

Ephemeral borders stand for peoples' desire to sometimes have information on them simply pass away unnoticed or forgotten. For example, if someone has thrown his candy bar wrapping-paper into the city lake or not sorted garbage according to the rules. Active RFID tags would be able to uniquely identify the ‘sinner’.

- Social borders

Social borders stand for peoples’ expectation that some of their activities or proclamations are treated confidentially by the social group in which they have been performed (family, doctor, prostitute, etc.). For example, if someone visits a prostitute he may not want this to be known to others. Yet, RFID tags can easily be used to track the movements of people.

[4] For example, in such a pooling scenario, it is not only known that a person A buys something to wear or spends an amount x per year on cloths, but that person A, female, age 17, buys a specific type and color of trouser that is of size XL. From there, more conclusions can be drawn, e.g. that she is overweight.

[5] The notion of personal borders framing out perception of privacy has been commented on in the in the context of ambient intelligence by (Bohn et al., 2003) who refer to (Marx, 2001).

- Temporal and spatial borders

Temporal and spatial borders relate to the "… expectation by people that parts of their lives can exist in isolation from other parts, both temporally and spatial. For example, a previous wild adolescent phase should not have a lasting influence on current life of a father of four…" (Bohn et al., 2003). RFID technology can be used to support this lasting influence. For example, if somebody has been registered in his youth as a football hooligan and now (perhaps years later) wants to visit a football game. His RFID enabled ticket to the game may identify him already at the entry point to the stadium as a hooligan. As a result, he may not be allowed to enter the stadium or endure other kinds of special treatment.

IV. Privacy enhancing functionality for RFID tags

Background

The discussion has shown that privacy concerns around RFID technology arise within retail environments as well as outside of them. Concurrent with the above discussion, we will hereafter concentrate on how privacy can be maintained *outside* of retail environments when people take RFID tagged products home. We assume that people will increasingly pay for their products electronically (e.g. with a credit card) and thus imply that a link can be established between a product and its owner. The role of RFID technology in pre-shopping logistics is excluded from the discussion. All proposed tag enhancements will not change their basic functionality. All existing components and systems used in pre-shopping logistics are maintained.

Version 1.0 of the EPC Network Specification (EPCGlobal, 2003) distinguishes 2 classes of tags labeled class 0 and class 1. Both classes foresee tags to be equipped with a password protected killing function in order to address the privacy issue. Based on the arguments provided in section II we argue that this killing function is not a tangible solution for the future. More thought must be put into tags' privacy functionality in order to prevent the misuse outlined in section III while allowing for the benefits and business models described in section II. The essence of our proposal is that consumers should have the control over their RFID tags' communication. They can gain this control with the help of a password protection scheme embedded in the RFID tag.

Our solution puts emphasis on the fact that tag cost is the major bottleneck for RFID introduction in many product categories. Especially low-cost and low-involvement goods which will only be equipped with passive tags[6] cannot afford to integrate sophisticated security solutions (in the foreseeable future). Therefore, we focus hereafter on an economically feasible solution for passive tags that is 'good-enough' to meet a majority of security threats.

The disable model: a new proposition for privacy perseverance

(Passive) RFID tag specification as-is

Table 1 gives an overview of today's main components of an RFID tag relevant for the privacy/security context. Features marked in bold are the minimum requirement for a tag of the respective class. Studying the table some issues arise:

The table shows that from a privacy perspective one major difference exists between class 0 and class 1 tags: Class 1 tags' killing function may only be protected by an 8-bit password (specified for the frequency range of 860MHz-930MHz). Even though an 8-bit memory solution may be cheaper for tag manufacturers it implies security risks for both retailers and consumers. Since an 8-bit password can be deciphered by common computing equipment in seconds, it provides little security. Retailers and consumers alike therefore face the risk

[6] As opposed to active tags passive tags do not have their own power supply. As a result, they are cheaper and smaller and may therefore be those present in the majority of consumer objects.

of ‘kill-attacks’ on their stores and homes (e.g. by people who oppose the technology introduction). We therefore argue, that a 24-bit password should be foreseen as the minimum protection required by retailers generally.

The most important drawback of both current classes of tags though is the killing function. Since the killing function is economically unrealistic (see section II) it is not a feasible long-term solution. Consequently, we expect the EPC to lie “bare”; at least if the current specification approach is maintained. The EPC would thus be accessible to any party equipped with a reader, regardless of access authorization. With this, all privacy abuses outlined in section III become possible. The tag’s readiness to tell its EPC to anyone deprives an owner of controlling the information traces left by his objects.

RFID tag specification	**Class 0**	**Class 1**
Memory		
ROM (read only)	**x**	**x**
EPROM (write once)	x	x
RAM	x	x
Objects in memory		
Electronic Product Code (EPC) (x bit)	**x**	**x**
8 bit password related to kill-function		**x**
24 bit password related to kill-function	**x**	x
Operations		
Receive requests (from reader or kill-device)	**x**	**x**
Send EPC number (to reader)	**x**	**x**
Self-test EPC or random number for anti-collusion	**x**	**x**
Kill EPC function	**x**	**x**
Verify kill-password	**x**	**x**

Table 1: Current dimensions of EPCGlobal’s RFID specification for passive tags relevant in the privacy context

RFID tag specification to-be

In order to create user control of tag communication we suggest the addition of a password-protection scheme to access a product’s EPC. This password protection scheme puts information revelation under the sole control of the owner once an object is sold and leaves the retail environment. We call this approach ‘the disable-model’.

The scheme we propose distinguishes two levels of security with different tag cost levels attached to them. The appropriateness of each level depends on the cost acceptable for a tag relative to an object’s value.

Class 2 enhancements

A simple enhancement to class 0 and 1 tags is to integrate an EPC *disable*-function instead of a kill-function. When a product is passed to a consumer we suggest to generally disable EPCs instead of killing them.

We refer to RFID tags including enable/disable functionality as “class 2” tags.

The way we envision the disabling process to flow is as follows: Instead of storing the kill password and function, the RFID tag stores a 24-bit *enable/disable* password and function. When a consumer pays for his products all tags are automatically disabled instead of killed. The disabling process is handled by the cash-register in order to avoid consumer time cost. With disablement a new password is randomly set on all tags. This password is then printed out on the customer's receipt. [7] It can be used by the new product owner to potentially re-enabling the EPC if he wishes to use intelligent home applications later or other feature available with the product.. [8]

If now unauthorized reader devices request the EPC from a disabled tag without the correct password the tag denies access to the EPC stored on it. From a layman perspective this means that *by default* objects bought do not communicate with any reading device except at one's personal request. The approach thus lends itself to calm all those privacy concerns related to unauthorized 'spying'. At the same time, all economically driven intelligent home appliances and future consumer information needs are maintained.

From a technical perspective, of course, the tag still reacts for processing re-enable requests. If the re-enabling password is not correct, the reader denies transmission of the objects EPC. At this point several issues can arise from a security perspective: The most important one challenging our approach is that it is possible that a reader identifies the EPC by not attempting to decipher the password at all, but instead by miming an anti-collusion method. Anti-collusion is a function used to uniquely recognize and communicate with one tag when several tags respond at the same time.[9] If anti-collusion is now based on the EPC - the structure of which is standardized - our disable-proposition could easily be circumvented. Our solution therefore relies on the fact that the EPC itself (or at least not the entire EPC) is used for anti-collusion. At first sight, this may be considered a major drawback of our solution. Yet, technical analysis of logistics requirements has suggested that full EPCs are not really suited as a numbering scheme for anti-collusion anyways. The time it takes for readers to forge through a full EPC is very time consuming. Also, EPCs are similar for many products and product categories. Therefore, other numbering schemes have been proposed for anti-collusion including EPC dependent hash-values, a random number pre-integrated in the tag, RNG integrated into tags or a 12 to 14-bit serial number extract from the full 96-bit EPC. For all these suggestions, our solution is feasible.

The second security weakness that may be argued is that a 24-bit password scheme is not a 'good-enough' protection from a serious attack. The effort required by an attacker to decipher a 24-bit protection though (which currently lies around X hours) may not really be worthwhile when the result is nothing, but the EPC of a low-cost/low involvement product. We therefore argue that the cost-benefit rationale of most attackers would effectively protect consumers.

The third drawback of class 2 tags is that there will be authorized readers (e.g. at the cash-register or in the consumer's smart home) which send the new owner's home-password around in plain text without encryption. A serious attacker, e.g. a thief, could therefore sniff on the cash register or home environment and retrieve the password. Again, we would argue that for low-cost products the incentive for thieves or other attackers is rather low.

Yet, for higher value objects (such as CD players, TVs, etc.) a systematic 'spying-attack' of this sort, e.g. on private homes could be realistic. Consequently we argue that for high-value goods another (more sophisticated) class of RFID tag is necessary. We refer to this class as class 3 RFID tag.

[7] Another long-term possibility would be to transfer the password to an identity device such as a PDA owned by consumer. Smart homes could then automatically read out the product password, change it and eventually set it to the user's common smart home password.

[8] The password may be changed at home by the consumer or by the consumer's smart home agent to match the smart home's password. We believe that a common password architecture for home readers or smart homes makes sense as consumers can access their devises more easily. A back-end database containing all tag data (as proposed by Weis, S., 2003 and Juels, A., 2003) and processing infrastructure to test all possible passwords is not required.

[9] In essence, anti-collusion (tree-walking method) implies that a reader says (to each tag in the area): "Respond if your EPCS begins with number x". If more than one chip responds, the reader than says" Respond if your EPC begins with xx". This process continues until only one tag remains to respond.

- **Class 3 enhancements**

In order to defeat sniffing practices on high-value goods, class 3 tags employ a challenge response method to verify the (class 2) password. This method is based on a cryptographic one-way[10] function: First the tag sends a randomly generated value to a reader. Here, a pseudoRNG may be the most realistic solution for 'good-enough' security, when a standard RNG solution is too costly. The reader answers with a combined hash from the random value and the password. Using the same one-way function, the tag can then verify the reader's password. In detail the process would flow as follows:

Step 1	Reader sends a request to a tag (e.g. enable EPC).
Step 2	Tag responds with a random value of 128 bit average length.
Step 3	Reader concatenates the 128 bit random value and the (class 2) password. Then, it performs the cryptographic one-way function. The result is sent to the tag.
Step 4	Tag performs the same algorithm outlined in step 3. Upon reception of the reader result, the tag compares its own result with the received result. If results match (<true>), the tag performs the reader request.

The vulnerability of this procedure is that ithe moment of resetting the password the new password is transmitted in plain text. An attacker could thus sniff on the new password (e.g. at the cash register). In order to defeat such an attack an XOR function is applied for password re-set.[11]

Compared to solutions proposing published hash functions or symmetric encryption (Weis, 2003; Kinosita et al., 2003, Ohkubo et al., 2003) our solution does not require a database for personal tag management. Only one common password is used. Switching product ownership implies just two password changing steps using a randomly selected temporary password. Key management is equally not required.

Table 2 gives an overview of our proposed privacy enhancements to the current class 0 and 1 specification.[12] It also specifies what and how many extra requirements would arise for tag manufacturers if our solution was to be adopted.

Obviously, both class enhancements we propose do imply some additional cost for tag manufacturers. Tags of class 2 and 3 need ROM instead of RAM, need to process two (or even five) additional functions[13] and need at least one additional bit in memory. Yet, especially as far as low cost passive tags are concerned, our solution is very lean in terms of additional cost arising. It makes a realistic trade-off between privacy and security concerns on one side and economic feasibility on the other.

[10] In [1] a solution for a low-cost hash (one-way) function for RFID tags was proposed.

[11] The XOR function allows for hiding the new password. The retailer's cash-register or check-out apparatus would transmit the XOR result based on old and new password instead of transmitting the new password in plain text. The tag would decrypt the binary XOR code with the held of the old password and derive the new password.

[12] In addition to this proposal it would be possible to include a proof-of-authenticity concept into a tag of this class. This could be considered for luxury goods or other kind of highly brand-reliant items. In this case, the manufacturer would have to embed a secret (of additional 64 bit) in the tag's memory. Assuming access to a manufacturer database and with the help of the (existent) challenge-response function a reader would be able to verify the authenticity of a product.

[13] Only two of the functions needed for class 3 tags (Cryptographic one-way function and random number generator), have a significant effect to manufacturing costs of tags.

RFID tag specification	**Class 0**	**Class 1**	**Class 2**	**Class 3**
Memory				
ROM	**X**	**X**	x	x
EPROM	x	x	x	x
RAM	x	x	**X**	**X**
Minimum memory type required	***ROM***	***ROM***	***RAM***	***RAM***
Objects in Memory				
Electronic Product Code (EPC) (x bit)	**X**	**X**	**X**	**X**
8 bit password related to kill-function		x		
24 bit password related to kill-function	**X**	x		
24 bit password to disable or enable the EPC			**X**	**X**
Status (enabled/disabled)			**X**	**X**
Memory space required (incl. 96 bits for EPC)	***136 bits***	***136 bits***	***137 bits***	***137 bits***
Operations				
Receive requests (from reader or kill-device)	**X**	**X**	**X**	**X**
Send EPC number (to reader)	**X**	**X**	**X**	**X**
Self-test EPC or random number for anti-collusion	**X**	**X**	**X**	**X**
*Kill*_EPC function	**X**	**X**		
Verify (kill-)password	**X**	**X**		
Cryptographic one-way function				**X**
Disable function (to disable EPC based on password)			**X**	**X**
Enable function (to enable EPC based on password)			**X**	**X**
Verify_password to disable/enable EPC			**X**	**X**
Change_password			**X**	**X**
Generate random number (pseudoRNG)				**X**
XOR function				**X**
Number of functions required	***5***	***5***	***7***	***10***

Table 2: Current and future RFID tag components relevant in the privacy context

Conclusion

RFID technology will be a ubiquitous reality in every-day life in the future. This paper shows why manufacturers, retailers and consumers want to maintain an RFID tag's functionality both in a store and after a purchase has been made. On this basis it is argued that killing RFID tags is an unrealistic solution to preserve privacy in the long run. However, it is also shown that leaving an RFID chip alive can lead to an unprecedented level of privacy intrusion. The authors conclude that the current RFID tag classes 0 and 1 as outlined in the specification 1.0. must therefore be enhanced with privacy functionality. Two levels of low-cost privacy protection are suggested. The approach is called the 'disable-model'.

The major benefit of the solution outlined is that a compromise is made between state-of-the-art security and what is economically feasible. Only 'good-enough' security is used to develop a proposition that will meet the privacy needs in a majority of situations. Secondly, the disable-model puts RFID communication into the sole control of the user. With this, the solution embraces current thinking in the development of PET technologies which takes a user-centric view. Finally, the model is the only proposition to our knowledge which allows for a realistic compromise between RFID-based market aspirations and business models on one side and peoples' desire for privacy on the other. In doing so it remains simple and cost efficient. Consequently, we believe that the disable-model is a good road to take.

Literature

Bohn, J., Coroama V., Langheinrich, M., Mattern, F., Rohs, M., „Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing“, Working Paper, Institute of Pervasive Computing, ETH Zürich, Zürich, Switzerland, 2003

Duce, Helen, “Public Policy: Understanding Public Opinion”, Executive Briefing Document of the AutoIDCentre, Cambridge, UK, February 2003

EPC Global: Version 1.0 Specifications for RFID Tags., 2003; http://www.epcglobalinc.org/standards_technology/specifications.html

FoeBuD e.V., “Positionspapier über den Gebrauch von RFID auf und in Konsumgütern“, Presseerklärung vom 19. November 2003, see: http://www.foebud.org/texte/aktion/rfid/positionspapier.pdf

Forrester’s Business Technographic’s, North American Benchmark Study, November 2003

Juels, A., “Privacy and Authentication in Low-Cost RFID Tags”, Submission to RFID Privacy Workshop @ MIT, November 15, 2003.

Marx, G., “Murky Conceptual Waters: The Public and the Private”, Ethics and Information Technology, volume 3, number 3, July 2001, pp. 171-180

Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita: Cryptographic Approach to “Privacy-Friendly” Tags. Submission to RFID Privacy Workshop @ MIT, November 15, 2003.

Sarma, S., Weis, S., Engels, D. „RFID Systems: Security and Privacy Implications“, White Paper published by the AutoID Centre, November 2002

Shingo Kinosita, Fumitaka Hoshino, Tomoyuki Komuro, Akiko Fujimura and Miyako Ohkubo: Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection. to appear in CSS 2003 in Japanese.

Weis, S., “Security and Privacy in Radio-Frequency Identification Devices”, Disseration at Massachusetts Institute of Technology (MIT), May 2003.