Privacy Enhancing Technologies for RFID – A Critical State-of-the-Art Report

Dr. Sarah Spiekermann & Sergei Evdokimov
Institute of Information Systems
Humboldt University Berlin
Spandauer Street 1
10178 Berlin
Germany
e-mail: {sspiek}{evdokim}|wiwi.hu-berlin.de

Abstract

Radio Frequency Identification (RFID) is a technology that allows for automatic and remote identification of objects and is currently discussed as one of the most important technical enablers of Pervasive Computing, boosting economic processes and home computing applications. However, as far as privacy is concerned RFID is still in its 'kindershoes'. A public outcry as to the privacy and security limitations of RFID has fostered the development of myriad privacy enhancing proposals. In this article we review and categorize the state-of–the-art of research work in this domain. We compare proposed solutions from a technological and economic point of view and we critically review their ability to give users real control over their privacy vis-à-vis RFID readers. Considering over 200 scientific publications in the field we come to the conclusion that the most promising and low cost approach does hardly get any attention from academia.

Keywords RFID, privacy, security, authentication

1. Introduction

Radio Frequency Identification (RFID) technology has become a subject of unprecedented attention. The technology was first described in 1948 and has since been widely adopted for access control and electronic toll collection. The basic idea of RFID is communication by means of reflected power. Data (i.e. an identification number) is stored on a tiny chip. Joint with an antenna, the chips forms a tag that can either be attached to an object or directly integrated into its fabric. A device called RFID reader communicates with the chip by transmitting commands as a radio signal. The signal induces an electrical current in the antenna powering up a chip's circuitry that reads its memory, performs certain computation and backscatters a response.

RFID was chosen as the transmission standard that subsequently replaces currently used UCC and EAN barcode systems.[1] Experts expect that the technology will be a core enabler for pervasive computing environments. It is forecasted that 87 million tags will be sold in Europe alone by 2022.

What makes RFID so attractive is that it allows for higher automation of goods identification and registration process. Depending on the radio frequency spectrum used, the distance between readers and objects can reach several meters and no line of sight to the tags is required. Consequently, supply chain processes can be better controlled and optimized. An RFID tag can store a unique structured number, a so called Electronic Product Code (EPC), that serves as object identifier and carries information about the object type and its manufacturer. In addition, the EPC will be associated with certain data that are stored in a backend (a data-on-network architecture), thus providing a fine-grained access to product information and better product control. Figure 1 summarizes technology basics.

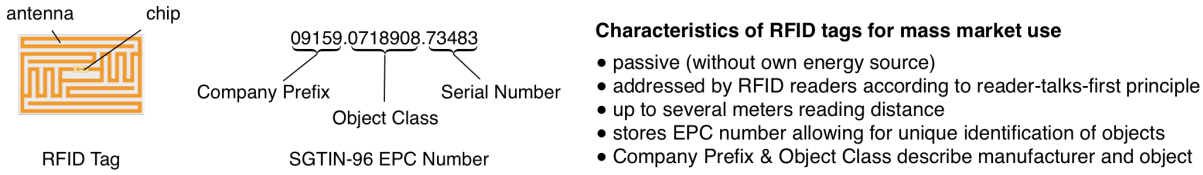


Figure 1: RFID Technology Basics

These architectural proposals as well as RFIDs technical characteristics stir strong privacy debates. If more than six million RFID readers will be deployed by 2022 (as GS1 forecasts), who will be authorized to read out EPCs, in particular once products leave supply chains and enter the private sphere of the home? Will read-processes be recognizable and controllable by the people? And who will have access to the information stored about tags on the network? Some privacy advocates refer to RFID tags as "spychips" [1] and have rolled out public "STOP RFID" campaigns. In the US, a 'Boycott Benetton' campaign was launched upon the news that RFID chips would be embedded in the company's clothes. The retailer Metro Group decided to withdraw 10.000 customer loyalty cards that embedded RFID. The German Association for Computer Science has established a catalogue of provisions to *"minimize the potential dangers of transponders for citizens and society"*.

Consumer studies confirm that people become concerned about their privacy when hearing about RFID. The main issues they have are [2]: (1) concern of one's personal belongings to be assessed without one's knowledge and consent, (2) concern to become known to and classified by others, (3) concern to be followed, (4) concern to be victimized, (5) concern to sign responsible for each object one owns, (6) concern about being restricted, educated or exposed through automatic object reactions.

As people desire to have control over RFID read processes the privacy and security research community has started to develop privacy enhancing technologies (PETs) aimed on preventing any unauthorized access to RFID tags. The goal is to establish secure tag-reader communication and to give consumers means to effectively manage their privacy in RFID enabled environments. Yet, tags' modest computational capabilities and the necessity to keep their prices low present a challenging problem that goes beyond the well-studied problems of traditional authentication and access management.

---

[1] EAN and UCC merged in 2004 to form the global standardization body GS1. Within GS1 the Unit EPCglobal is responsible for developing next generation barcode standards and technologies. EPCglobal currently represents around 1100 companies from diverse industries and, in particular, the consumer goods and retail sector.

This article categorizes, summarizes and critically discusses the state-of–the-art of research work in this domain and it discusses current PET proposals against three user control requirements: (1) cognitive control in the sense that consumers are aware of read-processes happening, (2) decisional control or choice to consent or deny to read processes and (3) behavioral control to effectively stop or launch read processes

2. Technical Options to Address Consumer Concerns

In order to gain an overview of the main research directions and findings we analyzed all scientific papers accumulated in a list managed by Gildas Avoine that pools research on security and privacy in RFID systems.[2] It contains literature from a wide collection of scientific conferences and journals with authors originating from all continents, We added all privacy related standardization documents published by GS1 and consulted with experts in the RFID research community for their perspective on the main privacy papers. We were particularly interested in research dealing with privacy challenges arising uniquely in RFID systems. Therefore, tag-reader security was a main focus of our analysis. Table 1 shows 179 papers we accumulated for analysis. 123 out of these 179 publications (69%) investigate security and privacy mechanisms for RFID tag-reader communication. Of these, 73 (59% of the total) describe their main motivation as end-user privacy protection. End-user RFID PETs described in these 73 papers can be generally divided into five categories:

1. RFID Kill Function: RFID tags are deactivated (software initiated tag 'killing').
2. Physical Privacy: Reading of RFID tags is physically restricted.
3. On-tab Scheme: Readers communicate directly with tags which self-control access to their content.
4. Agent Scheme: Users delegate privacy management to a privacy agent.
5. User Scheme: Users authorize each individual read-out process themselves.

[2] Website: 'Security and Privacy in RFID Systems' by Gildas Avoine. The website says to exclusively reference work *"which has been published in journals and conference proceedings, as well as technical reports, thesis, and eprints";* Avoine, G., Security and Privacy in RFID Systems, 2007; available at http://lasecwww.epfl.ch/~gavoine/rfid/.

		2002	2003	2004	2005	2006	2007	Total
Number of papers analysed on security and privacy in RFID systems		1	11	23	59	66	58	218
Number of papers containing technical proposals to control information flow between tag and reader		1	8	17	32	52	39	149
…of these, those which describe their motivation as protecting *end-user* privacy		1	4	14	26	22	30	97
DEALING WITH...								
	Important Selected References	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**Total**
Physical Privacy	Karjoth, G. & P.A. Moskowitz. *Disabling RFID Tags with Visible Confirmation: Clipped Tags are Silenced.* in *ACM Workshop on Privacy in the Electronic Society*. 2005. Alexandria, VA, USA: ACM Press.				1			2
RFID Kill Function	EPCglobal, *EPC™ Radio-Frequency Identity Protocols Class-1 Gen-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz - Vers. 1.0.9*, *Specification for RFID Air Interface*, 2005, Cambridge, MA, USA.	1			1			2
User Scheme	- Spiekermann, S. & O. Berthold, *Maintaining privacy in RFID enabled environments - Proposal for a disable-model*, in *Privacy, Security and Trust within the Context of Pervasive Computing*, P. Robinson, H. Vogt, and W. Wagealla, Editors. 2004, Springer Verlag: Vienna, Austria. - Inoue, S. and H. Yasuura. *RFID Privacy Using User-controllable Uniqueness*. in *RFID Privacy Workshop*. 2004. Massachusetts Institute of Technology (MIT), Cambridge, MA, USA.		1	2	2			5
Agent Scheme	- Juels, A. and S. Weis. *Authenticating Pervasive Devices with Human Protocols*. in *25th Annual International Cryptology Conference*. 2005. Santa Barbara, California, USA: Springer Berlin / Heidelberg. - Rieback, M.R., B. Crispo, and A. Tanenbaum. *RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management*. in *10th Australiasian Conference on Information Security (ACISP 2005)*. 2005. Brisbane, Australia.		1	1	3	3		8
On-tag Scheme	- Molnar, D. and D. Wagner. *Privacy and Security in Library RFID. Issues, Practices, and Architectures*. in *11th ACM Conference on Computer and Communications Security*. 2004. Washington DC, USA: ACM Press. - Engels, D., et al. *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*. in *1st International Conference on Security in Pervasive Computing, SPC 2003*. 2003. Boppard, Germany: Springer Verlag.		2	11	19	19	30	81

Table 1 A snapshot of the technical literature on RFID privacy and security

Killing RFID tags at store exits

The most straightforward approach to give people control over information flows between RFID tags and readers is to completely prohibit them. This can be achieved by simply disabling RFID tags' ability to transmit information as they leave the point of sale. Exercising the kill function on a software basis can be done automatically by cashier systems. Alternatively, it could be offered to customers as a separate option apart from the main payment process. IBM suggested a clip tag that allows buyers of RFID tagged products to physically destroy chips' antennas if they want to disable future read processes.

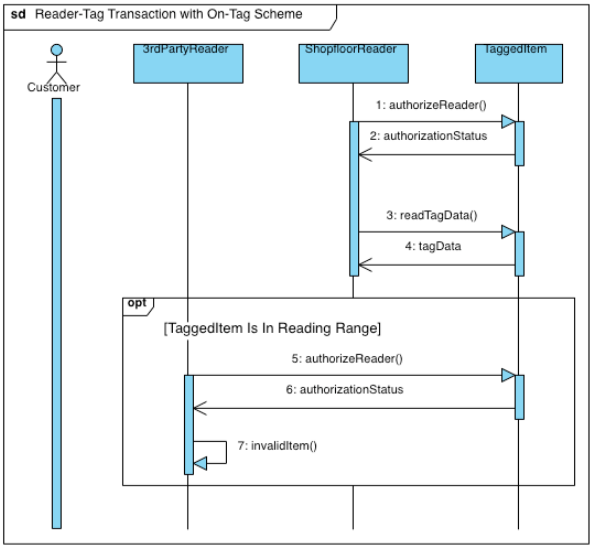
From a technical perspective, the software based kill-function presents the most advanced privacy solution existing today since its properties have been integrated in the communication protocols for EPC Class1/Generation 2 UHF tags (Table 1) and there are already low cost tags available supporting kill functionality. The main technical challenge associated with kill-commands is that they imply vulnerability for supply-chain transactions and point of sale operations if kill-passwords are not properly secured. If kill

passwords were compromised, an attacker could deactivate RFID tag functionality and threaten supply chain transactions.

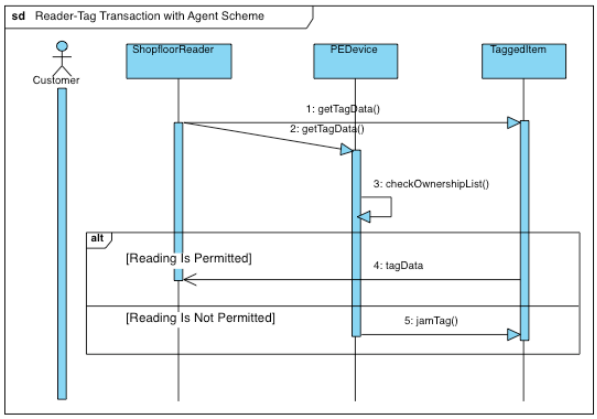
Assuming that password distribution can be effectively organized and secured, the crucial drawback of the RFID kill function is that it disallows transactions beyond the point of sale. All use cases propagated by industry today for after-sales RFID smart home services as well as electronic warranty, recycling- and return management would be thwarted. Consequently, some scholars have argued *"if you consider that RFID tags represent the future of computing technology, this proposal [the kill function] becomes as absurd as permanently deactivating desktop PCs to reduce the incidence of computer viruses and phishing" (p. 92 in [3])*

On-tag Scheme

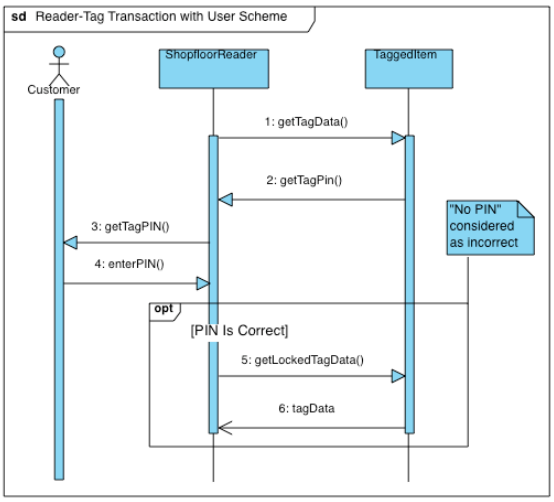
Table 1 shows that 82% of the PETs proposed could be characterized as *On-tag Schemes*. We define the On-tag Scheme as a privacy approach where only those RFID readers can access a tag that can authorize themselves vis-à-vis the tag. As the UML sequence diagram in Figure 1a shows, such an authorization process implies that a reader directly addresses an object's tag to ask for read permission and, if authorized, reads the tag's content. An early and relatively simple example for this kind of technology is the randomized hash-lock procedure proposed by [4]. It relies on a hash function that is implemented by the tag's circuitry. When a product is sold, the tag's content is locked by storing a hashed randomly generated key k: h=Hash(k) on the tag. Both values h and k form a dataset (h,k) which needs to be known by any party wanting to access the tag. When a reader attempts to access the tag, it receives h as the tag's response. Looking up the corresponding k value in a back-end database, the reader sends k as an authentication response that is hashed by the tag; and, in case the resulting hash is equal to h, the tag releases its content.



(a) On-Tag Scheme



(b) Agent Scheme



(c) User Scheme

Figure 1 UML Diagrams: RFID-based communication in an intelligent mall

The functionality required to implement such an authentication protocol on the tag is quite complex: The tag needs to compute a cryptographic hash function. Additionally, communication typically requires a network connection for key retrieval. Moreover, if the tracking of a tag via its h-value is to be avoided, then an even more sophisticated randomized hash-lock procedure would be needed requiring a random number generator on the tag and imposing significant performance overhead on the back-end.

An alternative approach that does not require reader-backed communication is to use public-key authentication. In these protocols readers and tags store public and private keys. To establish communication the reader sends a notification and receives a random challenge from the tag. The reader uses its private key to encrypt the challenge and sends it back to the tag. By decrypting the received cipher text and comparing it against the original challenge, the tag verifies whether the reader possesses the required private key and establishes the communication session if the resulting plaintext is equal to the issued challenge.

Unfortunately public-key cryptography requires the tag to be able to perform complex mathematical computations. Considering extremely limited resources available in low-cost RFID tags, it may, therefore, be problematic to implement a public-key authentication protocol while keeping the tag at low cost. At the time of writing the most compact implementation of a public-key encryption scheme is ECC (elliptic-based public-key encryption) cipher that requires about 15.000 logical gates on a tag. Cryptographic primitives required to implement hash-based authentication schemes are more compact. The SHA-1 hash function, for example, only requires about 4.300 gates. AES symmetric cipher requires about 3.400 gates. The On-tag Scheme requires the tag to implement at least one of these primitives. Yet, [5] argue that current RFID chips costing below $ 0.50 dispose of only 2.000 – 10.000 logical gates, 200 – 2.000 of which are approximately available for security

needs. Consequently, at the present time there are simply not enough resources to implement any of the proposed authentication mechanisms.

Besides the fact that the On-tag Scheme assumes the availability of complex security functionality on tags, it also imposes a key management challenge. Assuming the availability of hash-based authentication protocols, parties wishing to access tags will need to constantly communicate with back-end databases storing the data required by the protocol (e.g. the (h,k) pairs). Furthermore, making stored data on a tag available to its current owners (e.g. buyers) would require the owner to have access to these databases as well. This leads to the question of how key distribution and access can be managed. How can users ensure that keys maintained with retailers are not shared with 3rd parties? No answer is yet being provided by RFID security researchers on this crucial question.

Another drawback linked to key management is the sacrifice of user control over tag-reader communication. According to existing proposals for On-tag Schemes, users are not notified of any read processes or read attempts taking place. If it is not the object owner himself who triggers the read process, but instead some other 3rd party consumers need to trust that only authorized readers access their tags. Once keys are accessible anywhere outside of a user's sphere of influence, cognitive and behavioral control are lost. Cognitive control is lost, because a user has no way to know when, where, and by whom he is read out. And, even if the user knew, there would be no way in which he could stop the reading process from happening (exercising behavioral control). The UML sequence diagram depicted in Figure 2 visualizes the On-tag Scheme. It shows how users are kept out of the loop of their tags' activities.

Agent Scheme

Due to the drawbacks of the pure On-tag Scheme scholars have started to suggest tag-reader mediation systems. Users delegate privacy management to a privacy agent that mediates tag-reader communication based on general privacy preferences. We call this approach *Agent Scheme* (some also call it 'Off-tag'). Agent schemes are represented in 11% of the publications reviewed. Early versions for such mediating systems have been suggested in the form of a "watchdog" device [7] that informs users ex-post about reading processes. Alternatively, scholars have suggested a 'blocker tag' that can block all RFID communication [8].

More advanced mediating privacy agents [3, 9] explored the use of a device serving as a proxy and emulating tag behavior [9] or the selective jamming of reader-tag communication with the help of a 'Privacy Guardian' [10]. For the former approach RFID tags need to be cryptographically enabled and dispose of some centralized storage of RFID tag keys (as in the On-tag Scheme). In contrast, Privacy Guardian is much simpler. It can be part of a smart phone where it will have enough power and processing resources to maintain a centralized security policy. This security policy dictates which RFID readers in which situations have access to which tags. It is implemented as an Access Control List (ACL) that manages RFID traffic based on the data that includes the identity of the querying reader, the targeted tag(s), issued commands and context data (i.e. location of the user). If a reader is not authorized to access a person's tags, the Guardian selectively jams reader-tag communication.

Three major challenges are inherent in the Agent approach: First, agents need to effectively cut off tag-reader communication. Second, users need to manually specify their security policies. This implies non-negligible transaction costs for users as well as acquaintance with IT. The third challenge relates to context recognition. An Agent PET would need to recognize when (time) and where (location) and under what circumstances (conditions, purposes) readers are allowed to access tags in order to apply a user's security policies. However, how is the Agent PET supposed to understand and interpret context? Context sensitivity is still an unresolved challenge for Ubiquitous Computing scholars.

For Privacy Guardian it is foreseen that "context updates are provided either by users (via the user interface), or by authenticating "Guardian aware RFID readers" (p. 98 in [3]). The latter implies that Guardian software would need to be a standard component of RFID readers, an assumption that is hard to be met by reality if Guardian software does not become a de-jure or de-facto standard. However, the approach makes plain that RFID standardization committees should generally consider adding space for authentication information to the RFID air interface. This would allow embedding privacy enabling purpose information, such as fair information practices into the reader protocol [7].

Experience collected with E-Commerce Agent PETs which reside on similar preference specification procedures (such as the Platform for Privacy Preferences Project, P3P [11]) has shown that generalized privacy rules are not always applicable to specific contexts. Consequently, it may be that in some cases read processes occur or do not occur despite or against user permission. This possibility deprives users of full cognitive control or knowledge about what is going on as well as behavioral control to intervene. This again can undermine trust in the

protective abilities of the PET. Only if protection mechanisms are enhanced over time and perform well upon user inspection, might users develop trust and believe they exercise behavioral control by using an Agent PET.

Figure 1b shows the sequence of transactions taking place between RFID readers, Agent PETs, tags, and users. It shows that in the long run users can remain private and in control if they make the effort to specify their privacy preferences in great details and if a lightweight approach can be found to precisely jam tag-reader communication. It also circumvents the challenge of tag complexity and cost. Password or key management is simplified as the Agent PET automates it. All in all, the Agent Scheme can therefore be recognized as an important advance when compared to the On-tag Scheme. However, as the discussion has also shown, control perceptions of users over individual readout processes are still not optimal. Beyond the challenge of a trustworthy technical enforcement of privacy rules, tags are left unlocked by default. It is not the user who initiates a communication, but the network. As a result, the user is forced to trust PET performance to properly block undesired network requests. Many technical hurdles, such as context recognition, make this technique a very long-term vision rather than a short-term solution.

User Scheme

PETs for RFID may also be designed so that users exert immediate control over their RFID tags [4, 12]. We have coined these solutions (which represents 7 % of the classified literature) *User Scheme*. Solutions in this direction are proposing that tags are locked before people are leaving the stores. Therefore, they do not a priori respond to network requests. If the owner of an object has some benefit from reviving an object's RFID tag and transmitting its information, she can do so by authenticating herself vis-à-vis the tag and give the tag explicit permission to release its data. The authentication process could be handled via a user password. Figure 3 illustrates the approach.

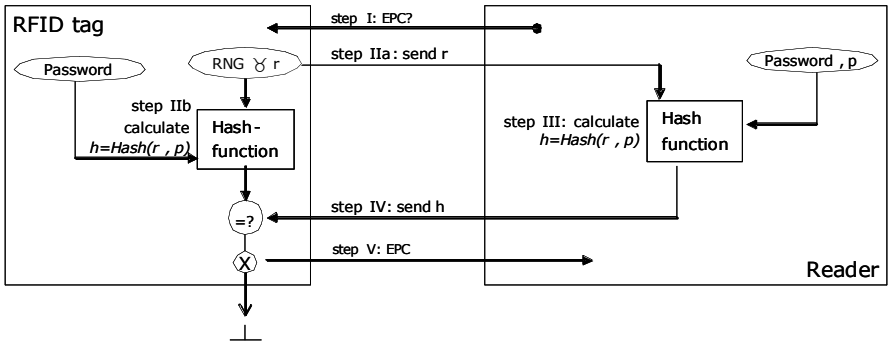


Figure 2 The Password Model (Spiekermann, S. & Berthold, O., 2004)

In this scenario the pre-configured kill-password coming with EPC Class1/Generation2 tags is being replaced at cash registrars with the personal password of an object owner. Object owners may in the simplest scenario possess only one password that allows them to manage their tags (analogue to other individual passwords they typically possess to access their e-mail, bank accounts or other sensitive electronic services). When an interrogating reader requests a tag's EPC, the tag sends a random challenge r to the reader. The reader uses password p for calculating a hash value h=Hash (r,p) and sends h back to the tag. The tag performs the same operation and compares its internal h value with the one received from the reader. If the password used by the reader is correct, the values will be equal and the tag releases its data.

In comparison to the previous two approaches, the User Scheme is much easier to implement. It does not rely on any auxiliary devices and needs no communication with a back-end and no public-key cryptography. Only to prevent a tracking attack the tag would be required to embed some cryptographic primitives, such as a random generator and a hash function. But even this can be circumvented when no random generator is involved and a tag instead issues an internal counter that is incremented after each read request. More simple even, authorized readers could directly send the password to a tag when requesting its EPC [13]. This solution would leave the user in control and be extremely cost effective. However, password sniffing by attackers could then, of course, not be prohibited.

The most important benefit of the User Scheme is that it puts the user in the role of the initiator of communication with the intelligent infrastructure. Before communication can take place, the user actively takes the context decision on whether he would like his object to release tag data or not. Theoretically, she, thus, has a high degree of control: cognitive control, because she is aware of the specific setting for which data exchange is

about to take place and decisional control, because she can take the context dependent decision on whether she would like to open the reader-tag communication channel or not.

The main challenge associated with the User Scheme becomes apparent when studying the UML sequence diagram of the User Scheme (Figure 1c): Password management leaves users with considerable transaction cost to initiate reading processes. Therefore, the existence of some user controlled password database may be required if more security is desired (similar to the On-tag Scheme). In this case, the same key management problem outlined above for the On-tag Scheme would apply. A 'good enough' but challengeable privacy approach would reside in employing just one password for all products.

Conclusion on current PET schemes

The analysis of the four privacy management models currently proposed for RFID privacy and security shows that none of them is truly optimal. Trade-offs are inherent in each proposal concerning security levels, tag cost, key management complexity and user transaction cost. Furthermore, the level of user control achieved is very different from one solution to the other.

The On-tag Scheme is costly and complex in terms of key management, but it may be highly secure. Most of the research efforts focus on this approach so far, probably because embedding security mechanisms into low-resource RFID tags is an interesting engineering challenge as such. However, we show that the On-tag process is not very sensible from a user perspective. People are left with only one choice, that is, either to allow all parties possessing the valid credentials to read tag information or completely disable the tag. If the tag is disabled, they deprive themselves of after-sales services and neither they nor industry have any benefit from the sophisticated privacy solution on the tag. If they leave the tag enabled, they either deprive themselves of any further control over read-out processes (and privacy is effectively lost) or they require a key management PET that registers key sharing for all transactions. Once users need such a sophisticated PET though, the question arises why not to adopt a more an Agent Scheme.

An Agent PET includes key management, but also aims to relieve users of the transaction costs implied in the privacy monitoring of individual transactions. It takes privacy decisions for users and, depending on its implementation, it can even be considerably less expensive, as far as tag cost is concerned. However, even though Agent PETs promise to relieve users from individual transaction monitoring, they also imply one major fallacy: They need to be able to make sound context decisions and people need to trust that these context decisions are well done and in their best interest. If research in context sensitivity advances and if RFID standardization committees agree on embedding privacy related context data into reader protocols, then smart RFID Privacy Agents could become an interesting technological option for users to gain control over RFID data exchange.

The question arises why not to opt for a much simpler User Scheme from the beginning. Here, no a priori RFID tag-reader data exchange takes place. Only if users feel that they want to use a certain service they provide their password. A prime difference between this user driven solution and the Agent Scheme is that the user initiates the data exchange selectively and upon taking the context decision himself to interact with an intelligent environment. This kind of interaction design puts the user literally 'into the driver's seat'. It is conceptually close to the interaction paradigm of most Near Field Communication (NFC) systems today.

It could be argued that in the very far future the line between User Scheme and Agent Scheme may blur. When users generally possess reader devices, these could contain algorithms that learn their owners' privacy preferences and subsequently automate individual password provisioning and management. Indeed, this potential long-term merging of the two approaches is a viable scenario. However, the two PET schemes differ in one major dimension: In the User Model, the user takes the context decision to read out his tags and initiates tag-reader communication. In the Agent Scheme it is the network that does so. Consequently, an intelligent RFID infrastructure evolving around a User Scheme in the long term may have different characteristics as compared to an infrastructure evolving alongside an Agent Scheme. In a User Scheme read-out points would probably be limited to a few places where they are requested by people and attractive service benefits from tag use are offered. In addition, a smart device used for accessing tags in limited circumstances would learn a user's privacy preferences on the basis of a series of 1:1 exposure decisions. People could be slowly led to delegating individual repetitive read processes to their read devices. In contrast, an intelligent infrastructure evolving around an Agent Scheme would most likely evolve in a similar way as today's E-Commerce infrastructures. People may be unwilling to specify and manage complex privacy preferences. This leads to an a-priori openness vis-à-vis collecting entities. This again could be an incentive for infrastructure investors to increase the number of read-points in order to collect more data. We therefore conclude that from a privacy perspective the User Scheme is

an important strategy and we call for the privacy research community to put more effort into this line of thinking about RFID privacy.

1. Albrecht, C., *SPYCHIPS: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move*. 2006, Nashville, Tennessee, USA: Plume (Penguin).
2. Spiekermann, S., *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*

. 2008, Berlin: Books on Demand.

3. Rieback, M.R., et al. *A Platform for RFID Security and Privacy Administration*. in *20th Large Installation System Administration Conference (LISA'06)*. 2006. Washington D. C., USA: USENIX The Advanced Computing Systems Association.
4. Engels, D., et al. *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*. in *1st International Conference on Security in Pervasive Computing, SPC 2003*. 2003. Boppard, Germany: Springer Verlag.
5. Lehtonen, M., et al. *From Identification to Authentication - A Review of RFID Product Authentication Techniques*. in *Workshop on RFID Security 2006 (RFIDSec 06)*. 2006. Graz: Springer Verlag.
6. Juels, A. and S. Weis. *Authenticating Pervasive Devices with Human Protocols*. in *25th Annual International Cryptology Conference*. 2005. Santa Barbara, California, USA: Springer Berlin / Heidelberg.
7. Floerkemeier, C., R. Schneider, and M. Langheinrich, *Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols*, in *Ubiquitious Computing Systems.* , H. Murakami, et al., Editors. 2004, Springer-Verlag: Tokyo, Japan.
8. Juels, A., R. Rivest, and M. Szydlo. *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*. in *10th ACM Conference on Computers and Communications Security (CCS 2003)*. 2003. Washington, USA.
9. Juels, A., P. Syverson, and D. Bailey. *High-Power Proxies for Enhancing RFID Privacy and Utility*. in *5th International Workshop on Privacy Enhancing Technologies (PET 2005)*. 2005. Cavtat, Croatia: Springer.
10. Rieback, M.R., B. Crispo, and A. Tanenbaum. *Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags*. in *13th Security Protocol International Workshop*. 2005. Cambridge, USA.
11. Cranor, L.F., et al. *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification - W3C Working Group Note 13 November 2006*. 2006 [cited 2007 July 17th, 2007]; Available from: http://www.w3.org/TR/P3P11/.
12. Engberg, S., M. Harning, and C. Damsgaard Jensen. *Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience*. in *2nd Annual Conference on Privacy, Security and Trust*. 2004. New Brunswick, Canada.
13. Spiekermann, S. and O. Berthold, *Maintaining privacy in RFID enabled environments - Proposal for a disable-model*, in *Privacy, Security and Trust within the Context of Pervasive Computing*, P. Robinson, H. Vogt, and W. Wagealla, Editors. 2004, Springer Verlag: Vienna, Austria.