Critical RFID Privacy-Enhancing Technologies

Using RFID technology, people can automatically and remotely identify objects. With the prospects of this technology, however, come many security concerns. The authors review and categorize several RFID security and privacy solutions, and conclude that the most promising and low-cost approach currently attracts little academic attention.

Sarah Spiekermann and Sergei Evdokimov
Humboldt University, Berlin

Recently, RFID technology has become a subject of prime attention. Developed in the middle of the 20th century, today we apply it in such areas as supply chain management, access control, and electronic toll collection.

Although the technology is easy to use—and greatly simplifies and automates many processes such as inventory control (see the "RFID Overview" sidebar for further explanation)—consumer studies show that many people have privacy concerns when they hear about RFID. Primary issues[1] include the following:

- personal belongings could be assessed without prior knowledge or consent,
- consumers might become known and classified by others,
- people could be tracked and followed,
- consumers could be victimized,
- someone could be made responsible for each object that he or she owns, and
- people could be restricted or exposed through automatic object reactions.

In response to the public desire for control over RFID reading processes, the security and privacy research community has begun to develop privacy-enhancing technologies (PETs) aimed at preventing unauthorized access to RFID tags. The goal is to establish secure tag–reader communication and to give consumers the means to effectively manage their privacy in RFID-enabled environments. Still, the fact that tags have only modest computational capabilities, combined with the need for low prices, presents a challenging dilemma that goes beyond the well-studied problems of traditional authentication and access management.

To aid in solving this dilemma, we categorize, summarize, and critically discuss state-of-the-art research in this domain. We also compare current PET proposals to three user-control requirements: cognitive control (the sense that consumers are aware of reading processes as they happen), decisional control (the choice to accept or deny reading processes), and behavioral control (the ability to effectively stop or launch reading processes).

Addressing Concerns

To gain an overview of the primary research trends and findings for RFID, we analyzed every scientific paper that pools research on security and privacy in RFID systems (the complete list of papers, managed by Gildas Avoine, is available at http://lasecwww.epfl.ch/~gavoine/rfid/). Avoine's list contains literature from a wide collection of scientific conferences and journals, with authors originating from all continents. We added every privacy-related standardization document published by the global standardization group GS1, and consulted with experts in the RFID research community for their perspective on the most relevant privacy papers.

We expressed particular interest in research dealing with privacy challenges arising uniquely in RFID systems. Therefore, we primarily analyzed papers that focused on tag–reader security. Table 1 (on p. XX) provides an overview of the 218 papers we accumulated

RFID Overview

The main attraction of RFID technology is that RFID tags communicate using reflected radio frequency, so that they require no power supply. Data (as an identification number) is stored on a tiny chip that joins with an antenna to form a tag that we can either attach to an object or directly integrate into its fabric. A device called an RFID reader then communicates with the chip by transmitting commands via radio signal. The signal induces an electrical current in the antenna, powering up the chip's circuitry. This circuitry reads its memory and performs certain computations before backscattering a response.

To establish a communication, an RFID tag and a reader do not need a line of sight. That makes RFID technology a perfect candidate for replacing the existing US Uniform Commercial Code (UCC) and European Article Number (EAN) barcode systems. Experts expect to see RFID become a core enabler for pervasive computing environments, forecasting that 87 million tags will be sold in Europe alone by 2022 (see www.bridge-project.eu).

Part of what makes RFID so attractive is that it lets users automate procedures, identify goods, and engage in registration processes without much human intervention. Depending on the radio frequency spectrum used, readers and objects can interact while several meters apart, even if the tags are out of sight. Consequently, users can control and optimize supply-chain processes. An RFID tag can store a unique structured number—an electronic product code (EPC) that serves to identify objects and carry information about the object type and manufacturer. Additionally, the reader can associate this EPC with data stored on the back end (via a data-on-network architecture), providing fine-grained access to product information and ensuring better product control. Figure A summarizes the basics of this technology.

The very qualities that make RFID so popular and easily employable, however, are the same traits that create controversy. These architectural proposals, along with RFID's technical characteristics, stir strong privacy debates. If more than six million RFID readers are deployed by 2022, who will be authorized to read the EPCs, especially once consumer products leave supply chains and enter the private sphere of the home? Will reading processes be recognizable and controllable by the people? And who will have access to the tag information stored on the network?

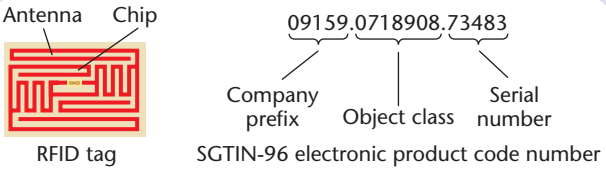

Figure A. RFID technology basics. RFID tags for mass-market use are generally passive (with no self-contained energy source); they work using a reader-talks-first principle, can be read from several meters away, store product code numbers for easy object identification, and store company prefix and object classes that describe the manufacturer and object.

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 with embedded RFID tags.[1] The German Association for Computer Science has established a catalog of provisions to "minimize the potential dangers of transponders for citizens and society" (see www.gi-ev.de/fileadmin/redaction/Presse/RFID-GI040608.pdf).

Reference

1. K. Albrecht and L. McIntyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move*, Plume (Penguin), 2006.

for analysis. Of these 218 publications, 149 (68 percent) investigate security and privacy mechanisms for RFID tag–reader communication. Of these, 97 (44 percent of the total) describe their main motivation as end-user privacy protection. We can divide the end-user RFID PETs described in these 97 papers into five categories:

1. RFID kill function—where RFID tags are deactivated (software-initiated tag "killing");
2. physical privacy—where the reading of RFID tags is physically restricted;
3. on-tag schemes—where readers communicate directly with tags that control access to their content;
4. agent schemes—where users delegate privacy management to a privacy agent; and
5. user schemes—where users personally authorize each individual read-out process.

Killing Function and Physical Privacy

The most straightforward way to give people control over the flow of information between RFID tags and readers is to completely prohibit it. A retailer can achieve this by making RFID tags incapable of transmitting information as they leave the point of sale: cashier systems can automatically exercise the kill function on a software basis. Alternatively, retailers could offer it to customers as an option separate from the main payment process. IBM suggested attaching a clip tag that would allow buyers of RFID-tagged products to physically destroy the chips' antennae if they wanted to disable future reading processes.[2]

From a technical perspective, the software-based kill function presents the most advanced privacy

Table 1. Snapshot of technical literature on RFID security and privacy.

RESEARCH PAPER TOPICS	2002	2003	2004	2005	2006	2007	TOTAL
Security and privacy in RFID systems	1	11	23	59	66	58	218
Controlling the information flow between the tag and reader	1	8	17	32	52	39	149
Of the previous two topics, those papers that describe their main motivation as end-user privacy protection	1	4	14	26	22	30	97
RESEARCH SUBTOPICS REGARDING END-USER PRIVACY	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**TOTAL**
Physical privacy				1			1
RFID kill function	1			1			2
User scheme		1	2	2			5
Agent scheme		1	1	3	3		8
On-tag scheme		2	11	19	19	30	81

solution existing today. Its properties have been integrated into the communication protocols for electronic product code (EPC) Class 1/Generation 2 ultrahigh frequency (UHF) tags, and many low-cost tags already support a kill functionality. The main technical challenge associated with kill commands relates to security: if kill passwords are compromised, an attacker can deactivate RFID tag functionality and threaten supply-chain transactions or point-of-sale operations.

Assuming that it's possible to effectively and securely organize password distribution, the crucial drawback of the RFID kill function is that it bars transactions beyond the point of sale. All industry use cases propagated for after-sales RFID smart home services, as well as those circulated for electronic warranties, recycling, and return management, would be thwarted. Consequently, some scholars have argued that "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."[3]

On-Tag Scheme

Table 1 shows that 84 percent of the PETs proposed could be characterized as *on-tag schemes*. We define an on-tag scheme as a privacy approach in which only RFID readers that can authorize themselves using a particular tag are granted access to that tag.

As the Unified Modeling Language (UML) sequence diagram in Figure 1a shows, this form of authorization process involves a reader directly addressing an object's tag to ask for permission to read. If a system authorizes it, then the reader gains access to the tag's content. An early and relatively simple example of this kind of technology is the randomized hash-lock procedure,[4] which relies on a hash function 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: $h = \text{Hash}(k)$ on the tag. Both values h and k form a data set (h, k) that any party wanting to access the tag must know. 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. The tag hashes the response and, if the resulting hash is equal to h, the tag releases its content.

Because the tag must compute a cryptographic hash function, the functionality required to implement such an authentication protocol is quite complex. Additionally, communication typically requires a network connection for key retrieval. If we want to avoid tracking a tag via its h value, then we need an even more sophisticated randomized hash-lock procedure. Such a procedure would require a random number generator on the tag, imposing significant performance overhead on the back end.

Public-key authentication, an alternative approach, doesn't require reader-backed communication. 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 then sends it back to the tag. By decrypting the received cipher text and comparing it to the original challenge, the tag verifies whether the reader possesses the required private key. If the resulting plain text is equal to the issued challenge, the tag establishes the communication session.

Unfortunately, public-key cryptography requires the tag to perform complex mathematical computations. Because low-cost RFID tags offer extremely limited resources, it could be problematic to imple-

ment a public-key authentication protocol while keeping the tag's cost low.

As of this writing, the most compact implementation of a public-key encryption scheme is the elliptic-based public-key encryption cipher (ECC), which requires roughly 15,000 logical gates on a tag. Cryptographic primitives required to implement hash-based authentication schemes are more compact. The Secure Hash Algorithm 1 (SHA-1), for example, only requires approximately 4,300 gates, whereas the Advanced Encryption Standards (AES) symmetric cipher requires roughly 3,400 gates. An on-tag scheme requires the tag to implement at least one of these primitives. Yet some argue that current RFID chips costing below $0.50 dispose of only 2,000 to 10,000 logical gates, approximately 200 to 2,000 of which are available for security needs.[5] Consequently, not enough resources are currently available to implement any of the proposed authentication mechanisms.

The on-tag scheme not only assumes that complex security functionality will be available on tags, but also imposes a key management challenge. Assuming that hash-based authentication protocols are available, parties who wish to access tags will need to constantly communicate with back-end databases storing the data required by the protocol, such as the (h, k) pairs. Furthermore, for consumers to access data stored on a tag, they'll need access to these databases as well, which raises the question of how to manage key distribution and access. How can users ensure that keys maintained with retailers remain unshared with third parties? RFID security researchers have yet to provide answers to this crucial question.

Another drawback linked to key management is that users sacrifice control over tag–reader communication. With existing proposals for on-tag schemes, nobody notifies users of any reading processes or attempts taking place. If the object owner cedes control over the reading process to a third party, consumers are left wondering if only authorized readers have access their tags. When third parties hold access keys to the user's sphere of influence, the user loses cognitive and behavioral control. Specifically, he or she loses cognitive control because there is no way of knowing when, where, and by whom the user is being read. And even if he or she does know, there's no way to prevent the reading process from happening (exercising behavioral control).

Agent Scheme

Because of the on-tag scheme's drawbacks, some scholars recommend tag–reader mediation systems. In these systems, users delegate privacy management to an agent that mediates tag–reader communication based on general privacy preferences. Researchers mentioned this approach—called an *agent scheme* (some call it *off*

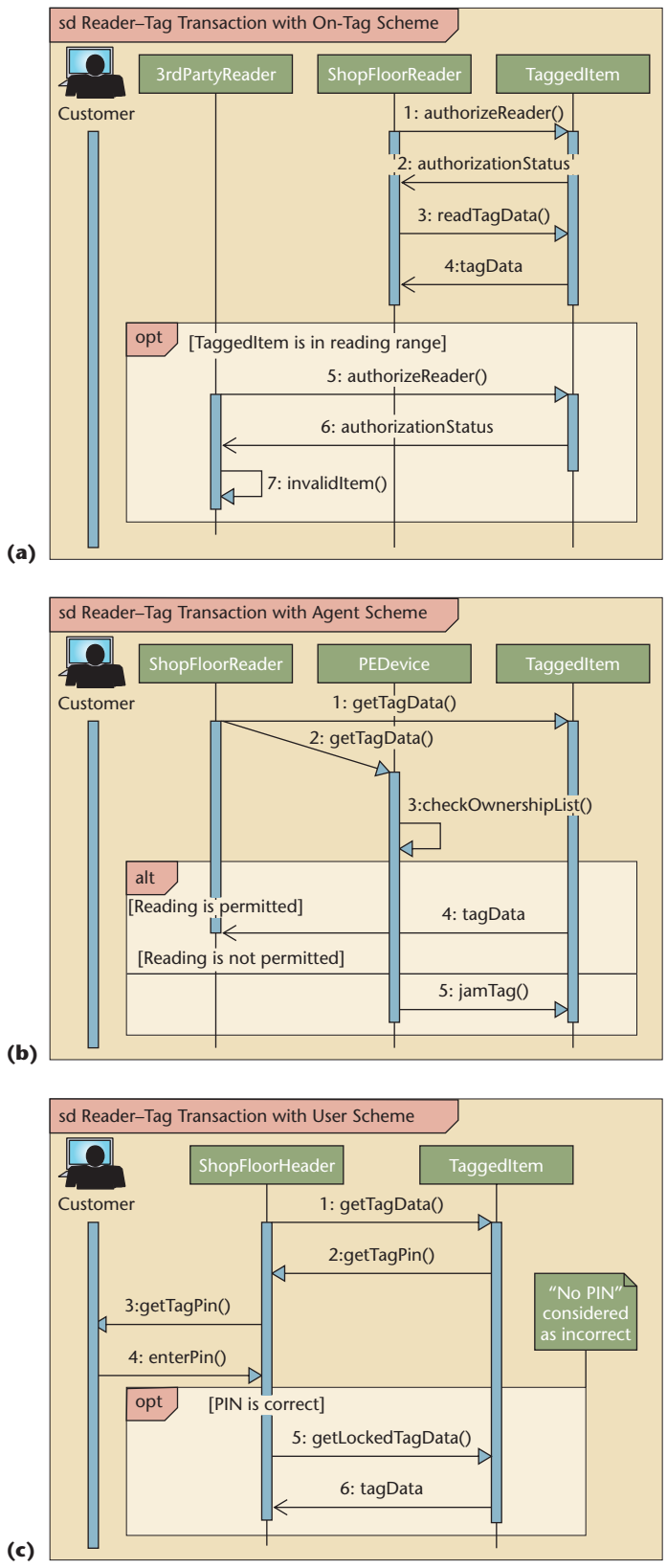

Figure 1. Unified Modeling Language (UML) diagrams. In this example of RFID-based communication in an intelligent mall, we see the interplay of (a) on-tag, (b) agent, and (c) user schemes.

tag)—in 11 percent of the publications reviewed. Early research suggested that this type of mediating system could take the form of a watchdog device[6] that would inform users ex-post about reading processes. Alternatively, some have suggested creating a blocker tag that could block all RFID communication.[7]

More advanced mediating privacy agents[3,8] use either a device that serves as a proxy—emulating tag behavior[8]—or a device that relies on a privacy guardian to selectively jam reader–tag communication.[9] For the former approach, RFID tags must be cryptographically enabled and capable of clearing some centralized storage on RFID tag keys (as is the case with the on-tag scheme). In contrast, a privacy guardian is much simpler: it can be part of a smart phone, where it has access to the power and processing resources needed to maintain a centralized security policy. This security policy dictates which RFID readers in which situations have access to which tags. Implemented as an access control list (ACL), the policy/list manages RFID traffic based on a variety of data, including the querying reader's identity, the targeted tags, the issued commands, and context data (such as the user's location). If a reader isn't authorized to access a person's tags, the guardian selectively jams the reader–tag communication.

Three major challenges are inherent to the agent approach. First, agents must effectively cut off tag–reader communication. Second, users must manually specify their security policies—which implies non-negligible transaction costs for users—and they must be technologically savvy enough to know how to specify such policies. The third challenge relates to context recognition. To apply a user's security policies, an agent PET would need to recognize when (time), where (location), and under what circumstances (conditions and purposes) readers are allowed to access tags. However, how is the agent PET supposed to understand and interpret context? Context sensitivity remains an unresolved challenge for ubiquitous computing scholars.

Some scholars foresee a future for a privacy guardian in which "context updates are provided either by users (via the user interface), or by authenticating guardian-aware RFID readers."[3] The latter proposal assumes that guardian software will become a standard component of RFID readers, but this is wholly dependent on whether the guardian software becomes a de jure or de facto standard. The approach does make plain that RFID standardization committees should consider extending the RFID air interface to specify corresponding authentication mechanisms. This would enable privacy capabilities, such as fair information practices, to be embedded into the reader protocol.[6]

Deployment experience collected with e-commerce agent PETs built on similar preference specification procedures (such as the Platform for Privacy Preferences Project, also known as P3P[10]) has shown that generalized privacy rules might not apply in specific contexts. Consequently, read processes might run counter to what the user desires in some cases. When this occurs, it not only deprives users of full cognitive control (that is, knowledge about what's transpiring) but also behavioral control (the ability to intervene). This can again undermine trust in the PET's protective abilities. In contrast, when protection mechanisms improve over time and consistently hold up to user inspection, users develop trust and believe that using an agent PET helps them exercise behavioral control.

Figure 1b illustrates the sequence of transactions taking place between RFID readers, agent PETs, tags, and users. It shows that, in the long run, users will be able to retain privacy and control if two conditions are met. First, users must make the effort to specify their privacy preferences in great detail. Second, researchers must create a lightweight approach capable of precisely jamming tag–reader communication—an approach that would also circumvent the issues of tag complexity and cost. Users could simplify the password or key management process by using the agent PET to automate it.

All in all, the agent scheme could be an important advance over the on-tag scheme. However, the user's perception concerning control over individual readout processes still isn't optimal. Even if researchers address the technical enforcement of privacy rules, they still have to face the fact that, with this system, tags remain unlocked by default. It's not the user who initiates a communication, but the network. As a result, this forces the user to trust that the PET will properly block undesired network requests. Many technical hurdles, such as context recognition, make this technique a long-term vision rather than a short-term solution.

User Scheme

It's also possible to design PETs for RFID so that users exert immediate control over their RFID tags.[4,11] We term this type of solution (which represents 5 percent of the classified literature) a *user scheme*. Solutions in this direction propose locking tags before people leave stores, thus tags can't respond a priori to network requests. If an object's owner decides that he or she would benefit from a tag–reader communication, the owner can authorize the transmission by giving the tag explicit permission to release its data. He or she could also handle this authentication process via a user password. Figure 2 illustrates the approach.[12]

In this scenario, the preconfigured kill password associated with EPC Class 1/Generation 2 tags is replaced at the cash register by an object owner's personal password. Object owners can, in the simplest scenario,

possess just one password that lets them manage their tags (analog to other individual passwords used to access email, 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 to calculate 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 will release its data.

In comparison to the on-tag or agent schemes, the user scheme is much easier to implement. It doesn't require auxiliary devices, communications with a back end, or forms of public-key cryptography. The tag would only be required to embed a random generator and a hash function if designers wished to prevent a tracking attack. Even more simply, authorized readers can send the password directly to a tag when requesting its EPC,[12] which would leave the user in control and be extremely cost effective. However, this solution couldn't prohibit attackers from engaging in password sniffing.

The user scheme's most important benefit scheme is that it lets the user open communication with the intelligent infrastructure. Before communication can take place, the user must actively make the context decision as to whether he or she would like the object to release tag data. Theoretically, the user thus has a high degree of control: cognitive control, because he or she is aware of the data exchange's specific setting, and decisional control, because he or she can make the context-dependent decision based on whether he or she would like to open the reader–tag communication channel.

The user scheme's main challenge becomes apparent when studying the UML sequence diagram in Figure 1c: password management leads users to incur a considerable transaction cost when they initiate reading processes. If the user desires more security, he or she might need to create a user-controlled password database (similar to the on-tag scheme). In this case, the same key management problem outlined for the on-tag scheme would apply. A privacy approach that some might consider good enough—though not great—would be to use just one password for all products.

Our analysis of the five privacy management models currently proposed for RFID security and privacy shows that none is truly optimal. Each proposal involves trade-offs concerning security levels, tag cost, key management complexity, and user transaction cost. Furthermore, each solution achieves a different level of user control.

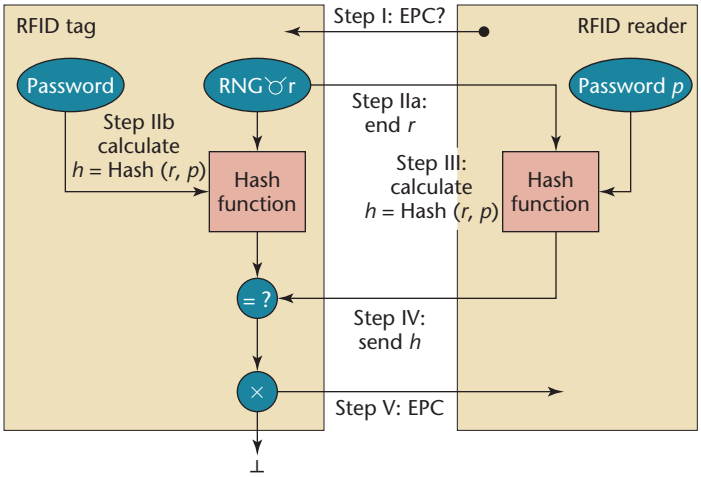

Figure 2. The password model. The user has more control over privacy because he or she has the opportunity to authenticate requests, thereby giving the tag explicit permission to release its data.

The on-tag scheme is costly and complex in terms of key management, but it might be highly secure. Most research efforts to date focus on this approach, probably because embedding security mechanisms into low-resource RFID tags is an interesting engineering challenge. However, we show that the on-tag process isn't terribly sensible from a user perspective. People are left with only one choice: to offer tag information to all parties possessing the valid credentials or to completely disable the tag. If the tag is disabled, users are deprived of after-sales services, and then neither they nor industry benefit from the tag's sophisticated privacy solution. If the tag remains enabled, users either deprive themselves of any further control over read-out processes (and privacy is effectively lost), or they're forced to use a key management PET that registers key sharing for all transactions. However, once users are asked to use such a sophisticated PET, the question arises as to why they shouldn't just adopt an agent scheme.

An agent PET includes key management but also aims to relieve users of the transaction costs implied by the private monitoring of individual transactions. It leaves privacy decisions to users and, depending on its implementation, could even involve dramatically cheaper tags. But even though agent PETs promise to relieve users from individual transaction monitoring, they do have one major flaw: they must be able to make sound context decisions. Furthermore, people must be able to trust that these context decisions are in their best interests. If research in context sensitivity advances, and if RFID standardization committees agree to embed privacy-related context data into reader protocols, then smart RFID privacy agents could become an interesting technological

option for users wishing to gain control over RFID data exchange.

This prompts another question: Why not opt for a much simpler user scheme from the beginning? Compared to the on-tag scheme, it's much easier to implement because it doesn't rely on resource-intensive public-key authentication protocols and doesn't require any data exchange between an RIFD reader and a back-end infrastructure. It's also much more user friendly and user centric. Instead of putting users in a defensive position to protect their privacy—where they must perform nontrivial key management or define privacy preferences for a privacy-mediating device—it provides users with explicit control over their RFID data. Here, no a priori RFID tag–reader data exchange takes place; users only provide their passwords if they want to use a certain service to selectively initiate the data exchange. Then it's the user who makes the context decision and chooses whether to interact with an intelligent environment.

In contrast, an intelligent infrastructure evolving around on-tag and agent schemes would most likely evolve in a manner similar to today's e-commerce infrastructures. People might be unwilling to specify and manage complex privacy preferences. This leads to a priori openness from collecting entities, which might be an incentive for infrastructure investors to increase the number of reading points (to collect more data).

We therefore conclude that, from a privacy perspective, the user scheme is an important strategy for meeting the consumer's needs. Furthermore, we call for the privacy research community to put more effort into this line of thinking about RFID privacy. ❑

References

1. S. Spiekermann, *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*, Shaker Verlag, 2008.
2. P.A. Moskowitz, A. Lauris, and S. Morris, "A Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag," *Proc. 5th IEEE Int'l Conf. Pervasive Computing and Comm. Workshops*, IEEE CS Press, 2007, pp. 348–351.
3. M.R. Rieback et al., "A Platform for RFID Security and Privacy Administration," *Proc. 20th Large Installation System Administration Conf.,* Advanced Computing Systems Assoc., 2006, pp. 92–98.
4. D. Engels et al., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Proc. 1st Int'l Conf. Security in Pervasive Computing*, Springer Verlag, 2003, pp. 201–212.
5. M. Lehtonen et al., "From Identification to Authentication—A Review of RFID Product Authentication Techniques," *Proc. Workshop on RFID Security*, Springer Verlag, 2006, pp. 169–187.
6. C. Floerkemeier, R. Schneider, and M. Langheinrich, *Scanning with a Purpose—Supporting the Fair Information Principles in RFID Protocols in Ubiquitous Computing Systems*, H. Murakami et al., eds., Springer Verlag, 2004.
7. A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. 10th ACM Conf. Computers and Comm. Security*, ACM Press, 2003, pp. 103–111.
8. A. Juels, P. Syverson, and D. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility," *Proc. 5th Int'l Workshop on Privacy Enhancing Technologies*, Springer, 2005, pp. 210–226.
9. M.R. Rieback, B. Crispo, and A. Tanenbaum, "Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags," *Proc. 13th Security Protocol Int'l Workshop*, Springer Verlag, 2005, pp. 51–59.
10. L.F. Cranor et al., "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification," W3C Working Group note, 13 Nov. 2006; www.w3.org/TR/P3P11/.
11. S. Engberg, M. Harning, and C. Damsgaard Jensen, "Zero-Knowledge Device Authentication: Privacy and Security Enhanced RFID Preserving Business Value and Consumer Convenience," *Proc. 2nd Ann. Conf. Privacy, Security, and Trust*, RFIDsec, 2004, www.rfidsec.com/docs/PST2004_RFID_ed.pdf.
12. S. Spiekermann and O. Berthold, "Maintaining Privacy in RFID-Enabled Environments—Proposal for a Disable-Model," *Privacy, Security and Trust within the Context of Pervasive Computing*, P. Robinson, H. Vogt, and W. Wagealla, eds., Springer Verlag, 2004, pp. 137–146.

Sarah Spiekermann *is a faculty member at Humboldt University, Berlin, and an adjunct professor of information systems at the Heinz School of Public Policy and Management at Carnegie Mellon University. Her research interests include electronic privacy, security, and RFID; personalization and user interaction in e-commerce and m-commerce; and knowledge management. Spiekermann has a PhD in information systems from Humboldt University. She's a member of the ACM and the German Society for Informatics. Contact her at sspiek@wiwi.hu-berlin.de.*

Sergei Evdokimov *is a postdoctoral scholar at Humboldt University, Berlin, where he also received a PhD in information systems. His research interests include database security as well as privacy and security issues in ubiquitous computing. Contact him at evdokim@wiwi.hu-berlin.de.*