Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience

Stephan J. Engberg, Morten B. Harning, Christian Damsgaard Jensen

Abstract - Radio frequency identification (RFID) technology is expected to enhance the operational efficiency of supply chain processes and customer service as well as adding digital functionality to products that were previously non-digital such as, e.g., washing machines automatically adapting to the clothes put into the machine. However, consumer response clearly shows significant concern and resistance related to consumer tracking and profiling as well as problems related to government tracking, criminal or terrorist abuse etc. Multiple conferences warn that RFID take-up is likely dependant on solving the privacy and security problems early. These concerns are not adequately addressed by current technology and legislation.

In this paper, we present a model of the lifecycle of RFID tags used in the retail sector and identify the different actors who may interact with a tag. The lifecycle model is analysed in order to identify potential threats to the privacy of consumers and define a threat model. We suggest that the in-store problem is more related to lack of privacy solutions for the consumer himself than for the RFID. We propose a solution to the RFID privacy problem, which through zero-knowledge protocols and consumer control of keys has the potential to ensure consumer privacy needs without reducing corporate value from utilising the potential of RFID. We propose that securing RFIDs will require a physical redesign of RFIDs but that this can be done without leaving security and privacy issues to consent or regulation.

***Index Terms*— Privacy Enhancing Technologies, Radio Frequency Identification (RFID), Security, Zero Knowledge Protocols.**

I. INTRODUCTION

In today's hyper-competitive business environment, companies are increasingly forced to reduce costs, rather than increase price, in order ensure return on investments. Studies have shown that companies spend between 12%-15% of their revenue on supply chain related activities [9], so supply chain efficiency has become a necessary condition for survival. Radio frequency identification (RFID) technology is expected to enhance the operational efficiency of supply chain management in both manufacturing and retail industries by embedding small silicon chips (RFID tags) in products or packaging [8]. An RFID tag provides a unique identification number (an electronic product code or an individual serial number) that can be read by contact-less readers, which enables automatic real-time tracking of items as they pass through the supply chain. Depending on the RFID tag it may contain addition storage for application specific use (such as product descriptions, certifications or temporary storage related to process support) or generic functionality embedded into the hardware (such as sensor interfaces, cryptographic primitives etc.).

Moreover, RFID technology is already used to prevent shoplifting and the tamper resistance of RFID tags (similar to smart-cards) makes them well suited to protect against counterfeiting, e.g., the European Central Bank is known to consider embedding RFID chips in the larger denomination bank notes for this purpose [7]. Finally, when RFID tags are embedded into artefacts of everyday life, they will enable a wide range of innovative end-user applications, e.g., in the areas of home automation and ambient intelligence environments. This only requires that the tag is left active after it passes the point of sale. Examples of such applications are: location service that helps find mislaid property, tags embedded in clothes may provide washing instructions to washing machines (thereby preventing the washing machine from washing a woolly jumper too hot) and an RFID reader embedded in the frame of the front door may warn the owner of the house if he is about to leave home without his keys/wallet/mobile phone. Such applications are likely to increase user acceptance of RFID technology and may create a demand for products with embedded RFID tags, provided that important privacy issues are adequately addressed. An enabled RFID tag allows anyone with an RFID reader, which is able to generate an electromagnetic field powerful enough to drive the tag, to identify the item and thereby to track the location of the item and (indirectly) its owner. This ability to locate and identify the property of ordinary consumers has already raised concerns, among consumer organizations and civil liberties groups, about privacy in RFID systems and may result in a general consumer backlash against products with active RFID tags, e.g., Benetton has already been forced to reconsider its plans to embed RFID tags in every new garment bearing Benetton's Sisley [11] brand name and Tesco (a UK

Stephan J. Engberg is founder and CEO of Open Business Innovation, 2800 Kgs. Lyngby, Denmark (e-mail: Stephan.Engberg@obivision.com).

Morten B. Harning is with Open Business Innovation, 2800 Kgs. Lyngby, Denmark (e-mail: Morten.harning@obivision.com).

Christian Damsgaard Jensen is with the Department of Informatics & Mathematical Modelling,, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark (e-mail: Christian.Jensen@imm.dtu.dk).

supermarket chain) in Cambridge was forced to abandon their experiments with an RFID based "smart shelf" technology developed by Gillette [REF]. Lately METRO was forced to back down on already implemented customer loyalty cards with RFIDs due to privacy concerns [10]. Finally, multiple conferences, such as the EU SmartTags workshop in spring 2004 [22], have isolated privacy enhancing solutions as important to ensure end-user acceptance.

The most common solution to the RFID privacy problem is to disable ("kill") the tag at the point of sale. While some RFID tags can be disabled at the point of sale, other tags, e.g., tags in library books or toll road subscriptions, have to remain active while in the possession of the customer. Another solution is to encrypt the identifier so that only the intended recipient will be able to read the identifier. However, encryption creates a new unique identifier, which allows the tag to be tracked and thereby the location of the customer to be monitored.

In this paper, we propose a solution that allows the tag to require an authentication from the reader and only return its identifier to anyone with a legitimate need to know defined as anyone able to authenticate accordingly. This authentication mechanism employs relatively cheap symmetric cryptography and can easily be extended to a group authentication scheme and asymmetric encryption. The rest of this paper is organized in the following way: Section 2 gives a short introduction to RFID technology, including applications, and privacy issues. Section 3 describes our proposal for zero-knowledge device authentication, which solves the privacy problem in RFID systems. Related work is presented in Section 4 and conclusions are presented in Section 5.

II. Consumer Privacy in RFID Systems

As mentioned above, the use of RFID tags in supply chain management and retail is expected to increase dramatically in the near future. In order to analyse the possible threats to consumer privacy, we need to examine the technology itself, the way RFID tags will be used and the actors (stakeholders) in an RFID enabled system.

A. RFID Tags and Readers

RFID-technologies consist of chips that can be very small and incorporated in all sorts of wrapping, cards or product themselves. They come in both active and passive versions where the passive versions utilise the energy from the radio beam of a RFID reader to get enough power to carry out simple calculations and respond with is normally a unique number. The unique number or ePC numbers are to be standardized and stored in a central database, which will provide instant access, but thereby also linkability, across locations and various readers. It is important to emphasize that RFID tags are normally considered as resource constrained, but that the most important limiting factor is price and that there is an important trade off between the price and the computational/cryptographic capabilities of the tag.

The term active tag is often referred to as tags with a power source such as a battery or part of a device with a power cord and as such having fewer restrictions on computational ability. However in the following the term Active means that Tag require or have required Active involvement of the Owner or bearer of a tag.

B. RFID Tag Life Cycle

An RFID tag, which is embedded in product or packaging, passes through many hands in an RFID enabled environment. In the following, we present the typical lifecycle of an RFID tag embedded into a consumer product and identify the typical actors in RFID systems.

The typical RFID tag lifecycle consists of four main phases, defined by the ownership of the product in which the RFID tag is embedded:

1. Supply Chain Management: the tag delivers a unique electronic product code (ePC) [18,19,20], which replaces and surpasses existing bar codes;
2. In-store & Point-of-Sales; the tag may be used by the retailer to track and support consumer interaction with products and provide services and purchase support.
3. Customer Control & After Sales Services: the tag may be used by consumers as an enabling technology for ambient intelligence applications, after sales services may use the ePC to record product service record or protect against counterfeiting;
4. Recycling & Waste Management: the tag's ePC may be used to automatically sort recyclable material and will also identify manufacturer, type and weight of disposable materials (the manufacturer of a product that will eventually constitute hazardous waste may ultimately have to pay for its safe disposal, this closes the cycle).

In this paper we focus on the second and third phases and the privacy implications of keeping enabled RFID tags in products, e.g., in order to enable some of the advanced applications in Phase 3. However, it is useful to examine all four phases in order to identify requirements for an acceptable solution to the consumer privacy problem.

C. Actors in RFID Systems

The typical actors in the RFID system outlined above will be:

1. the manufacturer, who embeds an RFID tag in the product or the packaging;
2. the logistics and wholesale companies that transport the product from the manufacturer to the retailer and who rely on RFID tags for supply chain management;
3. the retailer, who uses RFID tags for automatic inventory, re-stocking and cash registers and who sells the product to the customer;
4. the after sales service providers, e.g., warranty repairs, who may use the ID from the tag to record product history;

5. the infrastructure service providers, providing for instance RFID name services to link the Tag ePc number to the Producer or Retailer database with detailed information related to the application
6. the consumer, who buys a product with an embedded RFID tag and who may benefit from novel new applications of RFID tags;
7. the waste management company, who may use RFID tags to automatically sort garbage and recyclable materials and to levy waste charges based on the nature and the volume of garbage collected.

The RFID lifecycle allows us to identify two important features that a privacy solution for RFID must support: *transfer of ownership* and *multiple authorisations*. Transfer of ownership means that the set of readers able to read the tag will change at certain points in time and multiple authorisations means that readers belonging to several actors may be able to read the tag at the same point in time, e.g., the consumer and the after sale service provider may both access the tags while the product is under warranty. These properties indicate that simple solutions based on a single shared secret will not be sufficient to enhance privacy in RFID systems.

In order to simplify the presentation, we focus on protecting the privacy of the customers in this paper. For instance there are few obvious privacy threats in the supply chain process, but there can be threats of industrial espionage or shipments can be made to impersonate another security cleared shipment through some of the man-in-the-middle attack scenarios discussed later. However, the proposed solution may be extended to protect the privacy of all parties in the obvious way.

D. Understanding Privacy and Security

In the following discussion we take an objective approach to privacy and security meaning that we focus on risks without considering trust or consent perspectives.

The reason is two-fold; first a risk elimination approach would integrate privacy and security discussion making objectively better privacy solutions; second in the area of socio-economics there is increasingly focus on privacy from a control ("power") paradigm rather than a consent ("trust") paradigm in order to describe the connection between behaviour and real threats.

The linkage is however not straightforward as perceived control by consumers can be very different from their real control. Also in some aspects individuals prefer to give up privacy in order to gain for instance recognition or their 15 minutes of fame. We will not try to discuss this further nor try to give an overview of the vast number of articles produced except assuming that the difference between perceived control and real control will reduce as consumers gets more informed. Also we assume that consumers want both control and convenience in a complex, subjective and likely also context-dependant balance[1]. The optimal will therefore be to ensure convenience without reducing control.

As the paper will show, we do not see an inherent trade-off between these parameters – if only technology is designed accordingly. On the contrary if privacy is designed into the system most security threats are also taken care of. If privacy is designed into the system the consumer have no privacy argument NOT to share information or use RFID tags..

E. Consumer Privacy Threat Model

Consumer privacy may be threatened whenever the user interacts with a RFID enabled product, both pre purchase, e.g., when the product is in the user's trolley in the shop, and post purchase, e.g., when the product is carried around or when the user interacts with the RFID tag in the product.

1) In store Consumer Tracking

The process from the consumer picks the product from the shelf until payment allows consumer tracking, e.g., knowing what products have been returned to the shelf, when the total price of the trolley exceeds the consumer ability to pay, or the consumers pattern of movements around the store reveals a lot about the preferences and priorities of the consumer.

This does in many ways resemble traditional closed circuit TV (CCTV) surveillance, which means that the privacy threats are well understood. However, the logs of RFID tracking are significantly smaller than output from traditional CCTV cameras. Moreover, the RFID tracking logs can be directly processed by machine, which means that the threat to consumer privacy can be significantly higher in RFID tracking systems that traditional CCTV systems — provided the shop is able to link the RFID to an individual customer. It is therefore important to prevent the shop from keeping persistent records traceable to an identified consumer of in store RFID tracking.

We believe that this problem is similar to the issue of location privacy for mobile phone users. The main point is that this is not a problem of detailed information being collected or stored per se, but a problem of tracking the consumer himself and thereby making the information abusable creating privacy risks. Both problems must be solved by using privacy enhancing technologies to pseudonymise or anonymise the consumer in the shopping process itself. One way to do this is discussed in Privacy Authentication – Persistent non-identification in Ubiquitous Environments [3] and the broader infrastructure support [14]. We do not consider the issue of consumer PETs, we simply assume that these exist or that the consumer pays using either physical or digital cash and have total discretion to decide on transaction linking[2].RFIDs would thereby only be traceable to the

[1] For a discussion covering many angles see for instance Demos, *The Future of Privacy ([23])*

[2] It should be noted that we don't see an inherent trade-off between convenience and security/privacy as long as the consumer has control and each decision is implemented with the minimum necessary level of linkability. See the discussion under related work.

transaction/invoice or perhaps even an anonymous/pseudonymous customer number, but not to the specific identified consumer. In other words, RFID only adds to already existing privacy problems in this phase. To ensure security and privacy in digitally supported retail transactions, these problems needs to be addressed separately by other PETs such as Digital Cash and redesign of communication etc.

2) Post purchase use

After a product with an active RFID tag has been bought by the consumer, it will continue to interact with both the consumer and active RFID readers in his environment — these readers are not necessarily controlled by the consumer, but could be part of an eavesdropping or man-in-the-middle attack creating consumer's privacy risks.

The current RFID standard infrastructure is highly centralized requiring a central database to translate the unique number (e.g. ePC) to the location where detailed information about the product is stored. In other words whenever the unique number is available to any reader, the reader can in collaboration with infrastructure link the presence of a tag to detailed tag information and to the purchase transaction. By definition revealing the unique number in open communication presents the ability to establish easy linkability among databases creating serious privacy threats. It is therefore important that the tag is able to enter into some form of privacy solution, which prevents the store and infrastructure from tracking the product once it has been bought by the customer.

F. Consumer Security Threat Model

Privacy threats often also present a security threat to the system application. If a corporate database contain identified information related to a consumer, this is vulnerable to hackers, errors, information selling, criminals searching for potential victims, government confiscation etc.

Broadcasting or automatically revealing any persistent identifier is in itself a source of security threats, e.g., it is not a good idea to equip a soldier in a war zone with an active RFID tag, because it could be used by the enemy to track the soldier's unit or to trigger a bomb that could even be targeted to a specific soldier. Similarly, a consumer can be tracked exiting and leaving various shops linking the various transactions or providing a target for criminals, government or executive authority tracking or other abuse.

The combination is worse. If a potential attacker can access some database with any means to access RFIDs related to targeted persons or devices, he can then feed this information into any application equipped to monitor for such RFIDs. A simple example is tickets for a specific event or car road pricing schemes using unsecured RFIDs – the attacker knows that this specific RFID will eventually pass by a specific location and be easily detectable. Also wireless communication can be eavesdropped upon from a distance.

Other security threats are even more dangerous for criminal or terrorist abuse. For instance when RFIDs are deliberately used as passive proximity tags for convenient identification, access control, and payment or ticketing, there is an inherent risk of man-in-the-middle attacks. Unless there is special protection, any Challenge/Response protocol with an automatically responding and passive entity presents not only a threat to privacy, but also an open threat of impersonation or identity theft. A simple way to do Identity Theft is to use two RFID readers that are able to communicate with each other, thereby simulating the chess-players problem. The first RFID reader catches the Challenge and relay the request to the second RFID reader presenting the Challenge to the victim. When the victim returns the correct response, this message is then transferred to the first RFID reader who impersonates the victim and gets clearance.

Depending on the system application, this can present an unlimited risk such as for instance impersonating a security cleared person in an airport, authenticating signatures to payments/loans or even worse a person cleared to authenticate new fake identification papers or access to sensitive information.

In particular, applications using passive RFID-chips as proximity tags implemented under the skin present some seriously dangerous identity theft scenarios and these are already today available in commercial applications labeled as "security".

The RFID security and privacy challenges are significant. We need solutions that prevent the RFIDs from broadcasting identifiers and we need solutions to the issue of vulnerability to linking through infrastructure.

III. Zero-Knowledge Device Authentication

Existing proposals for privacy protection in RFID systems [6, 15] focus on either legislation that limits a company's ability to collect personally identifiable data or technology to deactivate the tag (kill it) when the ownership of the product is transferred to the customer. However, solutions based on consumer consent offer no guarantee for privacy protection and often turn into some sort of advanced blackmail, where a desirable service will only be made available to consumers who agree to the collection of personally identifiable information. Deactivation of the tag at the point of sale ensures the privacy of the consumer (if the tag is properly killed,) but it prevents natural post-purchase services such as warranty, access to product support, authenticity, recycling and waste management, advanced home applications, advanced recycling and waste management and all the other applications in the two last phases of the RFID-tag life cycle.

Finally, a number of technologies have been proposed to protect the communication between tags and readers from eavesdropping, but common to most of these proposals is that they require a trusted infrastructure, which excludes applications where authorised third parties may be given access to the RFID, e.g., toll passes, transport cards for public transport, ski passes, etc. We review these proposals in our related work section.

As indicated above, different actors should be authorized to read the tag at different times in the tag life cycle, so it is important to differentiate between first the Consumer controlling the RFID post-purchase, the in-store purchase process and the use of RFID as a proximity solution such as a ticket. The main focus is on the post-purchase problem to eliminate the trade-of between convenience and security by ensuring the device owner control of information leakage.

We propose to change the design of the RFID tags, so that they upon entering into the post-purchase phase support the ability to change into Privacy mode where they only accept zero-knowledge device authenticated requests, which ensures that RFID tags only reply to authorised requests.

The central property of Zero-Knowledge authentication protocols is to prevent an eaves-dropper and infrastructure to learn about which entities are communicating and make it significantly harder to do brute force attacks on the protocol. The Owner shall be able to communicate with the tag without leaking identifiers. The tag must be able to authenticate the reader BEFORE it returns any identifier or response that can reveal tracking information.

RFID tags with limited computational resources cannot handle advanced cryptography, but it will be able to perform basic operations like XOR and hash functions which can be handled even in the cheaper versions, but not in the cheapest Read-Only RFID Tags. These operations are sufficient to support the device authentication protocol proposed in this paper.

In the following, we present the basic zero-knowledge device authentication protocol and describe a few scenarios where the protocol may be applied.

A. Basic Zero-Knowledge Device Authentication Protocol

We propose a basic zero-knowledge device authentication protocol designed for resource-constrained devices, such as RFID tags.

The core zero-knowledge authenticated request is not generated by the RFID reader itself, but by an actor using any device under his control, which is able to generate a request which is then forwarded to the RFID reader and communicated to the RFID tag. Upon proper authentication the TAG will respond in a similar manor to the RFID reader which returns the reply to the actor, who can then initiate the next step. This can be simply detecting the presence of the specific tag and do nothing or instructing the Tag to do some operation such as revealing the ePC to a retailer. Normally we would however assume that the actor device itself will handle communication towards third parties and the tag itself only communicates with the actor device ensuring the ePC is NOT stored on the tag.

The reader and device can of course be the same such as a PDA that is NOT revealing any persistent device identifier. In the following we assume for simplicity that the actor is the tag owner equipped with some sort of PDA with inventory management similar to an address book and the ability to communicate accordingly.

It is noteworthy that this approach explicitly is open to broadcasting and message relaying, but only when the actor is actively involved in the authentication process.

An important aspect of the zero knowledge property is that the tag itself is not tamper resistant. A security parameter is that the ePC number does not have to remain stored on the tag and the ability to identify the tag is therefore transferred to the owner. In other words – the tag itself does not need to know the real secret which is the identity of the tag. The shared secret operates as an indirect identifier which only the actor can translate into meaning and only the Owner can translate into tag identification

The generic approach to authentication with this serious lack of asymmetric or symmetric primitives is based on two main aspects with three variables; A non-encrypted nonce is used in combination with a shared secret to communicate a second nonce. Verification of the knowledge of the shared secret is then based on an operation involving a combination of the second nonce and the shared secret.

For the specific application of RFID we use the one-time-pad aspect of XOR and the one-way aspect the hash algorithms as the main security properties.

Our specific suggestion for the core RFID authentication protocol incorporates additional security features. The Actor authenticates to the RFID-tag by sending a Zero-knowledge Authentication Message (ZAM).

The format of the Zero-knowledge Authentication Message[3] is:

Authentication: [DT ; (RSK XOR Hash(DT XOR SSDK)) ; Hash(RSK XOR SSDK)]

In the above DT is the first nonce, RSK is the second nonce and SSDK the shared secret.

We propose to use the first nonce (DT) to prevent replay attacks. After each successful authentication DT is stored by the RFID tag and authentication attempts with counter values below or equal to this stored value will be ignored. Therefore we propose to use a Date Timestamp (or any solution with similar properties). A request is ignored if the DT of the request is smaller that the DT of the last authenticated

[3] Variations of the basic idea are straightforward and will not be considered here.

request[4].

The second part provides input to make the RFID-tag able to recover the second nonce or the random session key, RSK.

The third part of the ZAM allows the RFID-tag to verify that this is a valid authentication. Validation of the third part provides an authentication proof that the authenticator knows the shared secret device key. This step is a vital novelty as it makes it possible to authenticate a valid Actor BEFORE the tag even responds.

The shared secret device key (SSDK) must be known by the specific tag and authorised Actors. Proving knowledge of the SSDK is necessary and sufficient to authenticate the reader, while the tag being able to reply is necessary to authenticate the RFID-tag towards the actor but NOT to anyone else.

It is important to note that the RFID tag will only respond if the authentication validates successfully as it would otherwise leak data about presence even though this might not be an identifier. To prevent against fake acknowledgement an acknowledgement is also zero-knowledge by containing a function of the shared secret such as a hash of the concatenation or XOR of the random session key, the shared secret and the nonce date-time stamp.

Tag response: [Hash(RSK XOR SSDK XOR DT)]

The outcome is that the Actor can communicate with the tag without revealing identifiers of the tag or the device in the protocol. The Actor can for instance release the ePC value stored in the inventory management in the PDA by letting the RFID reader impersonate the tag according to the ePC standard, i.e. without any change to the ePC protocol.

The zero-knowledge property of this solution is that - even though the protocol itself is a identity-secured shared secret protocol and as such might not abide perfectly to the traditional understanding of a zero knowledge protocol - the underlying property is that the tag does not even need to know the real tag secret which is the identity of the tag, its owner or any other external reference.

.

B. Augmented Protocol

The device authentication protocol can in itself act as a toggle switch (turn on theft alarm, open door), a locater (respond with presence) or a session initiation (respond with presence plus await command). Here DT could be used as a session identifier.

Application specific commands could also be added as a fourth parameter for instance as in a hash/XOR combinations with RSK or simply as a relative commend ("use key 4" - see below) to support tag efficiency.

Additional security features could be added but only on expense of either storage, energy consumption or adding complexity in the vital key management;

Backward secrecy can be incorporated using the RSK in a hash combination to change the SSDK on a per session basis. This would also incorporate Forward Secrecy unless an attacker is able to eavesdrop on every session. This would require careful attention to key synchronization.

The tag could incorporate multiple SSDK in parallel of which several different types can be identified; Access level for tag modification, Group Authentication with Category Data, Group Authentication in Trusted Environment and Tag Identification and Group Authentication in Untrusted environments WITHOUT tag ever gets identified.

For instance the Owner can add new or temporary SSDKs or change the overall tag mode back to ePC. This would either require the device to traverse through multiple keys requiring energy or to reduce the energy drain require building in a relative key reference to help the tag chose which SSDK to verify against.

The issue of Group Authentication of sharing the same SSDK between multiple tags and/or multiple Actors depends on the application and especially on whether the Actor is trusted (i.e. another device of Owner or for instance belonging to the same Group/Family as the Owner).

Foreign Actors with SSDK keys to a consumer tag represent a basic threat both to the zero-knowledge property and to security as such. Without ignoring that many applications can be of this nature (e.g. Product Authenticity), solutions to this group of problems require new solutions to Identity management or Agent Support which is outside the scope of this paper.

For the rest of the paper we assume that the RFID tag even if physically broken does not store identifiers that can is traceable to the consumer by third-parties. All keys and references are generated by the consumer and can be randomly changed.

Even if the tag contains its ePC number in for example ROM shielded by ZAM authentication, we assume the tag has never been linked to the real identity of the owner and therefore would not reveal information beyond linkage to an anonymous (or even pseudonymous) transaction. From a security and privacy perspective the overall Zero-knowledge properties would still be strong as data linking would still be contained.

[4] Using a DT introduces the problem of clock synchronization among all the readers, but this can be solved in the usual way.

And even if the tag contains an ePC in ROM and the store transaction was linked to an identified consumer, we suggest that PRIVACY MODE still represents a strong protection of post-purchase privacy and security. Even if the zero-knowledge property would not be perfect.

IV. Privacy Protection with Zero-Knowledge Device Authentication

Focussing on the Life Cycle, Phase 1 has no privacy threats, but as shown can have multiple security threats. ZAM might provide valuable security for this phase which should be investigated further.

From the analyses, it is clear that in Phase 2 prior to the User taking ownership of the Tag, the privacy and security Threats are not so much related to the RFID Tag itself, but more to the fact that the Tag adds information to the transaction which might be linkable to the consumer.

This is only a real privacy or security problem if the consumer is not protected by PET for authentication (including passive identification such as video cameras with face recognition), payments, communication etc.

Therefore if Security and Privacy is to be maintained when introducing Tags to the pervasive space, we must assume PET implemented for the consumer. This includes but is not limited to Smartcards, Payments, Communication Devices and Surveillance (e.g. Cameras) should all be designed with security and privacy in mind.

Assuming that consumers is not persistently identified a RFID tag in Phase 2 would be highly useful for customer service while maintaining privacy.

This would be beneficial for theft protection as product tags not paid for suddenly disappearing would signal attempted theft and only then would surveillance cameras or other theft protection be necessary. RFID could as such provide privacy-preserving or non-intrusive in-store theft protection.

In Phase 3 from Point-of-Sales to Recycling, the Tag turns into an active security and Privacy threat. By using devices with Zero Knowledge Device Authentication, these threats effectively blocked by creating an asymmetry between the consumer and other Actors such as the Retailer or infrastructure ensuring that the Tag.

When the consumer leaves the store, one of two scenarios may apply; either Total KILL or Privacy Mode:

1. Total KILL
   The consumer distrust the technology entirely, is not able to digitally manage the authentication information or the tag does not support Privacy Mode. The store issues a total KILL command that ERASE all identifiers or physically remove/destroy the tag and in every aspect leaves the RFID-tag untraceable even when physically examined.
2. PRIVACY MODE
   The consumer take active control of the product tag and prepare the product for intelligent linking within the consumer sphere such as for instance a shirt being prepared for the washing machine etc. When payment is ensured and authentication information has been transferred to the consumer, the store issues a TRANSFER[5] command in order to enable PRIVACY MODE. The consumer leave the store and may later use the received one-time-only authentication key to create a new key only known to the Product tag and the consumer.

A third intermediate Passive PRIVACY MODE may be built-in for consumers that are not yet actively using the possibility to authenticate purchased products, but desire the ability to do so in the future[6]. This should be regarded as a temporary intermediate stage as an alternative to KILL in order to facilitate market change. The product tag will remain silent, but the consumer can at any time resume control of the Product tag and integrate the product within the consumer sphere. Until then the tag appear as if it is not there – perhaps for ever.

With PRIVACY MODE activated the consumer can make use of intelligent privacy-enhanced communication services including authenticating the RFID tag towards third-parties such as customer service or integrating the acquired product into an intelligent home environment.

RFID Product Lifecycle

Phase / Tool	I Supply Chain	II In-store	III Post-Purchase	IV Re-cycling
RFID ePC Mode	+	!!/+	!!	+
RFID Privacy Mode			+	
Consumer PET		+	+	

+ Fine - !! Don't - !! /+ Conditional

In Phase 3 a product with a Tag may change ownership several times.

In Privacy Mode, the previous Owner initiate a TRANSFER command in parallel with the change from Phase 2 to Phase 3.

When returning the product for recycling in Phase 4,

[5] Transferring control and eestablishing a new SSDK safe from retailer in-store eaves-dropping is not trivial. See the section of Key Management.

[6] Passive PRIVACY MODE seems obvious for products requiring some sort of registration with the producer for service, firmware upgrades or products with home intelligence features or integration possibilities.

consumer can disable PRIVACY MODE and restore the Tag to continue the original ePC mode in Phase 1,

A. Key Management

Transferring control require that the Owner is able to manage the keys. The challenge is to balance usability and security as control transfer from the former Owner (e.g. Retailer) to the new Owner (e.g. the consumer).

One principle to follow is this:

The former Owner will transmit the ePC number and a related Ownership SSDK key to the New Owner in digital form to his Device such as a an anonymous PDA, a pseudonymous Privacy Authenticating Devices [3] or other PET Shopping Assistant Device implementing an Inventory Manager. If the session includes encryption this would prevent third-party eaves-dropping on the transfer.

The New Owner sends a TRANSFER command (for instance in the form of the combination of a ZAM message and <Transfer-code>+Hash(<Transfer> XOR RDK)) as a fourth parameter to the tag. By acknowledging transfer the tag verifies it has entered PRIVACY MODE and that all other keys including the ePC number are deleted in the tag. The new Owner then moves out of bounds from the former Owner and authenticates the tag with a change key[7].

Ownership SSDK keys are specific and not reused across multiple tags as these are not tamper-resistant. Multiple devices can coordinate key sharing and synchronize key changes using the Inventory management data within an Inventory domain such as a household sharing a Home Server.

But as mentioned the Ownership key could authenticate additional keys on the same tag depending on application purposes:

Group Authentication key with Segment Data: This would be highly useful for a washing machine which can use the same persistent SSDK for many tags. Critical for security of this simple application is that the response from the tag is not an identifier but rather category or segment data that would not distinguish the tag from a lot of other tags. Such a non-identifying response could be “Color Red, Max 60C”.

Group Authentication within Trusted environments:

For readers sharing the same inventory domain a natural question would be “Which tags are present?” without having to attempt authentication for each item in inventory. Application examples are household, or office applications.

For this purpose an additional Group Key shared between many tags is one solution. In order to prevent a physical intrusion in one tag making anyone able to access tags a two-step approach is suggested. First a Group key is used to get a tag-specific one-time-only reference which is then by the Inventory manager who can maintain a reference table and translate the one-time-only reference into the specific tag. If necessary a second authentication can be carried out to authenticate the specific tag if more than identifying is relevant. New One-time-only references can either be added or generated from the Group RSK combined with the one-time-only reference being used. This is not trivial but is parallel to managing backward and forward secrecy of Ownership SSDK keys.

Group Authentication in Hostile environments:

When foreign readers should be able to access tags from different owners the Inventory Management approach is insufficient unless the same tag is accessed only once such as en event ticket. Multiple requests to the same tag would create linkability and tracking. Applications would include road tools, transport ticket machines, ecommerce shipping etc. These applications require additional identity management solutions and are as such outside the scope of this paper.

It should be noted here that even through the principles described in this paper would add to the security of, they are severely insufficient to solve the massive security problems related to for instance national passports with biometrics or National Id Cards which are presently suggested to be implemented without any security.

B. Resulting Security and Privacy Properties

This approach is based on the principle of designing the optimal security and privacy properties into the technology. Security and Privacy in this understanding both related to the principle of Risk minimisation. Since no privacy threat is ever created, there is no need to regulate the use of data, no source of privacy-related distrust, no need for consent and no blackmail like trade-of decisions forced upon the consumer.

With Zero-knowledge Device Authentication RFID tags will remain silent until activated providing inherent protection against any unauthorised data collection. Even when activated the sessions will in most cases not reveal any information except when authenticated to respond for instance as part of a customer service session and even then linkage to a purchase is sufficient.

An attacker might not even know a two-party communication had occurred as the message can be broadcasted over a wide area and only the consumer knows what to expect as a response (e.g. a windows opens, a door unlocks - “is it activating the alarm, the heating being turned two degrees down or both”?). Each authenticated session is non-linkable to other sessions to anyone but the owner himself

[7] The main aspect here is that the New Owner can verify that the former Owner is not doing a man-in-the-middle based n the knowledge of the SSDK Ownership key and eaves-dropping on the Transfer ZAM message. This is another argument for including forward and backward secrecy.

even in the case of persistent wiretapping incorporating all external parties working together

The protocol is highly useful for applications where the signal is relayed over open networks or other protocols. For instance this could implement a broadcast anti-theft control for a car using FM radio or other long-range radio signals which is picked up by for instance the car FM radio and relayed to toggle the built-in theft control which would initiate either a silent alarm, switch of the petrol or both. A key aspect here is that no tracking of the car is necessary until the car theft control itself starts to emit tracking signals.

C. Resulting Legal Properties

If the Tag is never linked to an identified or identifiable consumer and the Tag post-purchase remain in absolute consumer control there are no privacy or security threats to regulate.

Regulation could focus on the situations where security and privacy risks are created maliciously or though neglect, i.e. when RFID enter the store without consumer PET protection or when unsecured RFIDs are not removed at Point of Sales.

The main issue is to prevent the serious risk of unsecured RFID tags in public spaces. This approach prevents persistent device identifiers turning into person identifier or giving raise to any of a long array of security problems described independent of in-store consumer protection

Beyond all the obvious risks more advanced legal risks are avoided. For instance an ownership change in Phase 3 will avoid problems where an action of the New Owner through the ePC and the retail transaction is linked to the first Owner. The first Owner this way avoid reverse burden of proof. Similar, legally, change of Ownership does not lead to secondary use problems of the New Owner being associated with something related to the First Owner.

Another security threat to prevent is tracking or identification of individuals without absolute individual control Direct or indirect Identification should not take place without the individual active involvement. Otherwise the risks of Identity Theft and criminal abuse of fake identities are significant.

D. Resulting Business value Properties

The key aspect of this approach is that it creates security without destroying business value for tags without Privacy Mode ability. Very cheap tags naturally are killed at Point of Sales without affecting their positive business value for the Supply Chain Management and in-store support. If the product is intended for post-purchase consumer applications, they can be equipped with RFID with Privacy Mode.

A key aspect is the perfect symmetry of consumer and retailer interests. If the tag is still responding when the consumer leaves the store one of two possibilities exists: 1) the consumer is stealing the product or 2) privacy mode was never activated. Either way an active tag will trigger store security. The Tags thereby present active theft protection and at the same time reduce the need for secondary surveillance. This means that the proposed model does not interfere with the common use of RFID tags as active theft protection.

If the product was properly purchased but the tag is still responding either the store made an error or the tag is not respecting basic privacy requirements. The consequence is either the store or the producer is guilty of attempted privacy violation. Since the consumer can check this using any RFID reader and bounty bonuses can be applied, privacy violations are rapidly detected and stopped. The tag thereby creates protection against privacy violations.

A particular interesting aspect of this approach is the open road to implementation. Since the RFID is dual-mode, current RFID standards can be supported at the same time as new Privacy Mode enabled RFID tags are introduced.

Another aspect is the potential for unsynchronised implementation of active tags and consumer Tag handling devices. Even if the consumer is not able to make use of the Tag when the product is purchased, he can later acquire that ability and make use of the built-in tags

The consumer can release linkable information to get convenience and services if the retailer or other service provider makes this valuable to him. If the consumer wants Post-purchase RFID support of his property that was originally equipped with a non-secured tag, he can attach his own RFIDs with Privacy Mode without any reduction in functionality and even link this back to the transaction and original ePC number if the retailer or producer is able to support this step. If he wants to he can even instruct the RFID tag to remain in ePC mode even though this would in most case be a bad idea compared to implementing some sort of specific key.

In short, it is difficult to see what kind of business value is lost. But the causes of privacy and security concern are removed reducing the barriers for RFID take-up and the tag can remain usable for customer service and Home intelligence Post-purchase without creating security threats.

E. Attack analysis

In order to analyse the privacy properties of the proposed mechanism, we consider the commonly used Dolev & Yao model, where an attacker has the following properties:

1. the attacker can obtain/decompose any message send over the network (in this case any message exchanged between RFID reader and tag);
2. the attacker can remember/insert messages using messages that was already seen;
3. the attacker can initiate communication with either tag or reader;
4. given the key, the attacker can encrypt/decrypt all messages;

5. the attacker cannot get partial information, guess the key or perform statistical analysis; and
6. without the key, the attacker can neither alter nor read encrypted messages.

For the purpose of this analysis, we assume that the attacker cannot interfere with the physical artefacts in the system (RFID tags and readers) or with the backend system. However, we do expect the attacker to attempt to masquerade as one of the physical artefacts.

1) Attacking RFID Tags

Attacks where the attacker masquerades as a valid reader.

This kind of attack is defeated by the shared secret because the tag does not recognise valid readers per se, but only readers able to present a valid authentication requests.

Care should be given to designing the messages in specific applications to minimize the ability to learn from the message size and especially not ignoring that the setup assumes relaying.

2) Attacking RFID Readers

Attacks where the attacker masquerades as a valid tag.

This kind if attack is defeated by the shared secret because the Actor does not identify the tag, but only recognise that the tag is able to decrypt the authentication message and respond accordingly.

.

3) Attacking the Communication between tags and readers

Eavesdropping on a single session is not providing information because communication is encrypted and zero-knowledge.

Modification attacks, where the attacker interferes with the communication by changing elements – results in a Denial of Service as all three elements of the ZAM protocol are linked and one part cannot be changed without making the tag ignore the authentication request as invalid.

Only successful authentication will result in Tag activation creating a change in the tag (updating the last successful DT, potentially changing the SSDK and initiating a session mode according to the specific application). The ZAM protocol in itself protects against replay attacks. Attempts to overload the Tag by external Distributed Denial of service attacks should not produce any serious problem as Tags naturally is discarding non-verifiable authentication requests without responding. The tag automatically resets when the induced power is insufficient to operate.

4) Man-in-the-Middle attacks.

Defeated since the authentication procedure require the Actor to initiate the authentication protocol. Multiple applications would actually benefit by the fact that the protocol can work from a distance assuming "man-in-the-middle" relaying the authentication protocol for instance in Key toggling modes.

The setup is transparent to man-in-the-middle as responses are also zero-knowledge. An attacker can through direct reading learn that a present device and a present RFID tag communicate, but he cannot learn an identifier of either device. Masquerading require access or brute force guessing the shared secret SSDK.

5) *Brute-force attack on session key and shared secret*

An attacker can record the authentication and attempt to do offline brute-force attack. Notice that even guessing the correct Random Session Key (RSK) does not provide access to the shared secret SSDK. The attacker would not even be able to verify that he had guessed the Random Session key.

We have not analysed the optimal brute-force attack approach, but expect that this would be to run through combinations of RSK and SSDK and trying to verify the authentication request. This should be sufficient for all applications where RFIDs is a likely choice as key size can be chosen accordingly.

High-value or sensitive applications would either move to device with more computational power or ensure damage control for instance so that an attacker would not have time to do a brute-force attack on the session before the keys have changed.

However a successful brute-force attack on a reused Shared Secret would potentially make the attacker able to take over control of the tag. Damage control against this attack would likely incorporate changing the shared secret on a per session basis.

Changing keys with backward secrecy can be implemented changing the shared secret SSDK on a per session basis using the Random Session Key in a combination with a hashing or other non-reversible algorithm. To ensure forward secrecy can be implementing for sensitive application is best done as a social procedure by changing the SSDK in different locations as the attacker only need to miss one session to loose the ability to use a brute-force broken key to gain control of the tag.

A combination of eaves-dropping and using the knowledge of the original keys can be defeated through changing the SSDK outside the reach of the eaves-dropper. This would also apply to attacks incorporating physically inspecting the keys while leaving the tag intact.

Using the Retailer knowledge of the original key to track a Tag in Passive Privacy Mode can be made detectable by making the original key a one-time-only key requiring change on first use.

Attacks including interference with the physical artefacts

The attacker can physically get access to the keys in the Tag

Damage control can be incorporated by removing any external keys and using the SSID as an intermediate tag Identifier. SSDK should NOT be reused across multiple Tags. A combination of a Physical Attack and eaves-dropping is unlikely but would be highly effective. The main protection against this kind of attack is by changing the keys outside the eaves-droppers reach

A more advanced and serious attack model is where RFID producers of the original Tags incorporate a hidden backdoor. Since the same protocol described here can be used to create sleeping agents that can only be activated by those with access to the shared SSDK key provided by the producer, the only way to detect this privacy/security threat is through physical inspection.

When the violation occur it is difficult to detect as even then the protocol is zero-knowledge and the only detectable aspect is that the Tags apparently responded to some undetermined request. This attack incorporating tracking or additional functionality would be difficult to detect in specific attacks targeted at a specific consumer similar to any attack incorporating huge resources and faked products with backdoors.

What is important is that such an attack would be highly vulnerable to physical inspection of the RFID tags as they are not tamper-resistant. For commercial approaches this seems unrealistic as the risk and consequences of exposure would be out of proportion with the business value in normal context. For government to do generic tracking this would require the use of the same key in all devices and thereby building in both vulnerabilities and risk of detection.

V. Related Work

Two approaches have been proposed to address the privacy concerns in RFID systems: Legislation (data protection laws) and technology (privacy enhancing technologies).

A. Legal Framework

There is much consideration on how to regulate the RFID space to prevent the strongly privacy invasive aspects of RFID. Two main approaches have been considered – KILL and Policy-based approaches.

Much consideration focuses on deactivating the RFID tag either physically or by issuing a KILL command. However, this prevents the use of RFID tags for other purposes, such as warranty, authenticity, return of goods, use of presents with purchase information attached and home intelligent applications, i.e., second and third phase of the RFID tag life cycle. Moreover, the KILL approach is not usable in many situations such as proximity use in toll booths, tickets, access etc.

Another approach is to inform consumers about the embedded RFID tags, in order to make the privacy violation acceptable. However, this approach will often turn into an advanced form of blackmail where consumers have the impossible choice of not getting a service or accepting a service designed using privacy-invasive principles.

Using this approach it can be shown that the entire shopping process can be fully anonymous EVEN with self-service shopping. Since no collection of identifiable personal data takes place, a perfect balance between consumer convenience and the shop desire for supply chain efficiency and customer relationship support can be established.

The outcome is that the only need for legal regulation is to handle the situations where RFIDs still respond post-purchase. This translates into one of two scenarios; either the product is being stolen and doors can close and surveillance cameras be activated OR either the shop or one of the suppliers have integrated non-privacy respecting RFIDs into the product in which case this translates into a violation of consumer privacy.

In other words RFIDs responding post-purchase should in any case translate into an offence. Legal regulations can simply state that if anyone is able to pick up an unauthenticated signal from a RFID there is a legal violation.

B. Privacy Enhancing Technologies

Ari Juels [4] suggest a key change protocol based on a double hash focussing on backward secrecy. This approach is not implementing consumer privacy towards the infrastructure as the key is suggested to have a direct translation to the ePC key framework. Moreover, this approach has significant problems related to key synchronisation, as each request will result in a secret key change.

In another paper [16], Ari Juels proposes various approaches to protect the RFID tag which may be embedded in EURO-notes using participants as trusted parties to re-encrypt the information stored in the RFID tag. This approach both leak information and require the constructive participation of entities that may prefer to jam the trace process.

Stephen Weis [12, 13] suggest a protocol where a consistent shared secret key is shielded using a random key generated by the RFID itself and authentication requires transmission of the shared secret itself. This approach will require comprehensive searches and as soon as the shared secret is transmitted in the open the RFID will be have no backward secrecy.

Engberg & Harning [3] show how a reverse authentication towards infrastructure can be used to establish location privacy in wireless environments using a modified mobile communicating device called a Privacy Authenticating Device. This principle turns wireless devices into session-only linkable transaction which combined with an RFID reader can be shown to create the basis of a privacy infrastructure support for in-store active RFID tags that has not yet entered privacy Mode.

Inoue et al. [17] suggest a basic solution where a shared secret makes the RFID remain silent hiding the persistent key. This approach contains no authentication mechanism or suggestions on how to work in real-world settings.

Other approached can be based on the blocker tags where the consumer carries a special protection tag responding to confuse any reader and hide the real tags carried. As a general rule it is wrong leaving it to the consumer to try protecting himself from a bad technology design. In addition this approach requires the protection device to be able to protect against any protocol in any frequency jamming the actual response which must be considered a highly vulnerable and risky approach.

VI. Future Work

The main activity we would like to look into is a detailed crypto analysis to determine the ZAM protocol resistance to especially brute force and various other attacks.

The current system relies on a permanent shared secret between the RFID reader and tag, which may introduce problems. However, we believe that the random session key can be shown to provide a good basis for changing the shared secret SSDK on a per session basis, which will provide backward secrecy (using for instance a hash combination) and forward secrecy (an attacker needs to record every change as there is no algorithmic link between the various SSDK). Synchronisation of changing shared secrets can be established based on the acknowledgment as the coordinating mechanism. This is easier because the Random Session key is chosen by the Actor. We would like to further develop the protocol to incorporate these ideas.

We have focused on zero-knowledge securing seriously resource constrained devices in this paper. However, the principles presented in this paper can easily be shown to port to stronger asymmetric encryption as well as most protocols and devices.

It is important to develop handover protocols for the point of purchase, which will minimise the risk of future man-in-the-middle attacks by previous owners. We would like to explore solutions based on intelligent agents that help automate the handover process and increases convenience for the consumer.

We wish to explore how the proposed protocol can securely be extended into a group authentication protocol within a trusted infrastructure, such as home intelligence or certain workplace intelligence applications, using one-time-only identifiers.

One of the advantages of the proposed protocol, compared to other privacy enhancing technologies proposed for RFID systems, is however that it does not require a trusted infrastructure. We therefore believe that this protocol can securely extend into a group authentication protocol within an untrusted infrastructure, such as car road tolls, event tickets etc. using a combination of one-time-only identifiers and consumers identity PETs. This would allow an advanced anonymous implementation with authentication to authorize the release of centrality stored tickets and still ensuring instant revocability in case of theft etc. Finally, development of a group authentication protocol should make it possible to add new one-time-only references dynamically over open channels.

An important area to look deeper into is the problem were seemingly mutually excluding security needs meet such as for instance Product Authenticity vs. Owner Control, Anti-money laundering vs. Data Protection or even worse Digital Rights vs. Consumer Fair Use and the serious problem of Trusted Computing vs. Freedom. Product Authenticity can be solved to a satisfying level by ensuring consumer ability to demonstrate a purchase – but making this required would create reverse burden of proof so that inability to demonstrate purchase and product authenticity is proof of theft.

This leads to the generic discussion of free consumer choice at Point of Sales directing market development. The question of maintaining a RFID tag without security makes little sense as the consumer has likely no idea of the potential consequences, cannot detect or see the data collection, have unclear causal understanding between the collection of data and the abuse potential, have little impact as the real decision is dependant on a long supply chain that is really controlled by industry standards and finally the consumer can easily be faced with a deliberate unbalanced choice of accepting an undeterminable threat compared to loosing real services such as warranty, intelligence or upgrades. Due to this we suggest that this discussion will be very difficult to leave to the consumer choice at point of sales as it would become a destructive debate between consumer rights organizations and industry rather than a question of individual choice directing market trends.

Behind this is an even more fundamental question for market theorists on how market dynamics work in a digital world, for socio/economics on how people behave and make decisions, for technicians on how to design technology with security and privacy incorporated, questions for industry on how to ensure that real market demand is feed back into the standards and design processes, to marketers on the logic in building barriers between the company and customers and of course regulatory questions for politicians on what all this means for policy. We need better balances both within and between all these areas. If not we risk damaging the market forces and the very fundamentals of prosperity, stability and quality of life.

VII. Conclusion

RFID tags without security used for consumer applications incorporate serious risk of abuse for commercial, political, social or criminal purposes. But especially the risk of identity theft of passive proximity tags, tracking or targeting devices could easily lead to serious breaches of security and privacy.

From the analysis in this paper we conclude that incorporating PETs in the RFID tag would not only solve the RFID Security and Privacy problems but it would do so without reducing the obvious value for process efficiency, customer service, recycling and also security purposes such as theft protection.

We conclude that Zero-Knowledge Device Authentication would provide such a PET solution as a general solution for resource constrained devices in the ambient space and RFID in particular.

The attack analysis shows that even though the computational resources are scarce, the solution is highly resistible to realistic attacks. Also there are additions that would make this approach resisting even resourceful attacks or implement operational damage control even in the case of physical intrusion to access keys in the RFID tag.

We suggest that even though there are strong reasons to require KILL of RFIDs without security at Point-of- Sales this should not apply to RFID redesigned to meet security and privacy requirements for consumer applications.

We conclude that the in-store privacy problem is not related to RFID per se but that RFID used in-store is escalating existing security and privacy problems related to lack of attention to Consumer PETs for payments, communication and security purposes. We suggest that further attention should be given to the question of in-store consumer PETs.

From the analysis it is also clear that many present commercial applications for the consumer space lack even basic security properties and are open to a multitude of abuse attacks. Without discussing this in further detail, we have indicated generic ways to solve most of these problems using a combination of Zero Knowledge Device Authentication, Group Authentication, one-time-only identifiers, intelligent linking of surveillance equipment with PET solutions and privacy enhanced Identity management integrated in infrastructure.

We consider it highly likely that most applications such as ID cards, communication, payments, car tolls, ticketing, access control, libraries, home intelligence, mobile intelligence etc. can be technically designed or redesigned to incorporate basic security and privacy requirements. If industry will not do it themselves and consumers can do it through the market, then other means should be considered.

We suggest that we can and should make Privacy Default, i.e. preserve individual ownership and control of personal data. What we set out to show in this paper was that in the area of RFID this does NOT lead to loss of business value – on the contrary, balanced security and privacy might eliminate critical barriers to economic growth by ensuring end-user control and eliminate sources of risk and distrust.

REFERENCES

[1] Auto-ID Center, *Consumer Privacy Concerns* - http://www-mmd.eng.cam.ac.uk/automation/w_papers/cam-autoid-eb002.pdf - (Auto-ID Center moved - link checked May 2004)

[2] *Convenience Triumphs Privacy* - http://www.cio.com/archive/092203/saffo.html

[3] ENGBERG, S., HARNING, M, *Privacy Authentication – Persistent Non-identification in Ubiquitous Environments*, Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, at UbiComp2002, Gothenburg, September 2002, http://www.obivision.com/papers/privacyauthentication.pdf (checked January 17, 2004).

[4] JUELS, A., *Privacy and Authentication in Low-Cost RFID Tags*, In submission 2003, http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pt-rfid/index.html

[5] Gillette/Tesco Case - http://www.out-law.com/php/page.php?page_id=tescousingrfidtag1059647038&area=news

[6] Privacy Conference 2003, *Privacy Commissioners resolution on RFID*, http://www.privacyconference2003.org/resolutions/res5.DOC

[7] YOSHIDA, J., *Euro bank notes to embed RFID chips by 2005*, EE Times, December 19, 2001, http://www.eetimes.com/story/OEG20011219S0016 (checked January 17, 2004).

[8] SAP AG*: Adaptive Supply Chain Networks*, SAP White Paper, 2002.

[9] QUINN, F.J., The Payoff Potential in Supply Chain Management, ASCET: *Achieving Supply Chain Excellence through Technology*, 1999, http://quinn.ascet.com (checked January 17, 2004).

[10] RFID *in customer cards: Test is discontinued*, 2004, http://www.future-store.org/servlet/PB/menu/1002376_l2/index.html

[11] *Benetton Explains RFID Privacy Flap*, RFID Journal, June 23, 2003, http://www.rfidjournal.com/article/articleview/471/1/1/

[12] WEIS, S.A., *Security and Privacy in Radio-Frequency Identification Devices*, M.Sc. Dissertation, M.I.T., May 2003.

[13] Weis, S.A., Sarma S.E., Rivest, R.L., Engels D.W., Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, 1st Annual Conference on Security in Pervasive Computing, Boppard, Germany, March, 2003.

[14] Engberg, Stephan, 2002, EU-IST workshop Living with Security, *Privacy through Virtual Identities in Infrastructure*, http://www.obivision.com/Papers/IST_Living_with_security_20021106.PDF

[15] *Bowen seeks balance in RFID law*, 2004, http://www.rfidjournal.com/article/articleview/812/1/1/

[16] Juels, A., Pappu, R., *Squealing Euros: Privacy Protection in RFID-Enabled Banknotes*, Seventh International Financial Cryptography Conference, Gosier, Guadeloupe, January 2003.

[17] Inoue, S., Konomi S., Yasuura., *Privacy in Digitally Named World with RFID Tags*, Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, at UbiComp2002, Gothenburg, September 2002.

[18] Brock, D., *The Electronic Product Code (ePC) – A Naming Scheme For Physical Objects,* White Paper MIT-AUTOID-WH002, Auto-ID Center, January 2001.

[19] Brock, D., *The Compact Electronic Product Code – A 64-Bit Representation of the Electronic Product Code*, White Paper MIT-AUTOID-WH008, Auto-ID Center, November 2001.

[20] Engels, D., *ePC-256: The 256-bit Electronic Product Code™ Representation,* Technical Report MIT-AUTOID-TR010, Auto-ID Center, February 2003.

[21] Dolev, D., Yao, A., *On the Security of Public Key Protocols*, IEEE Trans. on Information Theory, 29(2), (1983) 198-208.

[22] EU Smarttags Workshop, Bruxelles 2004, Final Report http://www.cordis.lu/ist/directorate_d/ebusiness/workshop.htm

[23] Demos, *The Future of Privacy, 1998.*