RFID Security

Prof. Dr. Heiko Knospe, University of Applied Sciences Cologne, Faculty of Information, Media and Electrical Engineering, Betzdorfer Str. 2, D 50679 Köln, Germany. E-mail: heiko.knospe@fh-koeln.de

Prof. Dr. Hartmut Pohl, University of Applied Sciences Bonn-Rhein-Sieg, Fachbereich Informatik, Grantham-Allee 20, D 53754 St. Augustin, Germany. E-mail: Hartmut.Pohl@fh-bonn-rhein-sieg.de

Abstract

Radio Frequency Identification (RFID) systems have become popular for automated identification and supply chain applications. This article describes the technical fundamentals of RFID systems and the associated standards. Specifically, we address the security and privacy aspects of this relatively new and heterogeneous radio technology. We discuss the related security requirements, the threats and the implemented mechanisms. Then the current security and privacy proposals and their enhancements are presented. Finally we discuss the role of this technology in Ubiquitous Computing.

Keywords: RFID, Tag, Transponder, Reader, Security, Privacy

1 Introduction

The automated identification of objects with electromagnetic fields is the major purpose of the RFID (Radio Frequency Identification) technology. An RFID system basically consists of transponders (tags), readers (scanners) and application systems for further processing of the acquired data. There is a large variety of different RFID systems: they may use low, high or ultra high frequencies, the transponder may emit only a fixed identifier or possess significant memory and processing capabilities. Transponders may incorporate no security features at all or realise effective security protocols similar to smartcards. Most transponders are passively powered by the radio field emitted by the reader but there are also active tags with a separate power supply. The transponder design is also little uniform: there are e.g. tiny tags with a size of several millimetres, very thin "smart labels" or standard ID-1 cards [Finkenzeller 2003].

It is expected that this technology will at least partly replace optical barcodes in the future. A significant growth of the RFID market is predicted [Frost 2003] and a major driver for this are the falling prices of RFID–transponders. Tags will soon be available for less than 5 cents a piece [Sarma 2002]. There are various applications for low-cost tags such as logistics, point-of-sale checkouts, animal identification, item management in libraries, and waste management. But, there is also the potential for more sophisticated RFID–transponders (costing approx. 10 cents to 1 EUR) which can be used for higher value items. Current applications include health care, ticketing, road toll, electronic purse, access control for facilities, key, anti-theft device and protection against counterfeiting. These RFID tags have the capability to replace magnetic stripe cards and classical contact smartcards.

The security and privacy aspects of RFID systems have become a major issue. Current RFID–transponders do not protect the unique identifier so that unauthorised readers in the proximity can gather IDs. The collected data (identifying e.g. consumer goods) could be accumulated and linked with location information in order to generate a customer profile. Other security objectives may also be at risk when standard mechanisms can not be realised due to the limited transponder resources.

This article is organised as follows. Chapter 2 describes the functionality of RFID systems and their characteristic properties. Chapter 3 covers the standardisation of radio frequency identification systems. Chapter 4 deals with the security properties of RFID systems: we describe the security requirements and relate them to the RFID standards and implementations. We also discuss a number of current security proposals for RFID systems and put a special emphasis on access control and authentication. Chapter 5 contains the conclusions and an outlook.

2 RFID Fundamentals

2.1 Components and communication model

An RFID system consists at least of *transponder*s *(tags)* and a *reader* (see Figure 1). A tag contains a microchip, capacitors and an antenna coil which is embedded into an encapsulation material, e.g. a coin, a glass body, plastic substrate, smart label or a standard ID-1 card. The coil-on-chip technology allows very small tags with only 6 mm diameter and 1.5 mm thickness [Finkenzeller 2003]. The tags communicate via radio signals with an *RFID–Reader,* which is a central component of an RFID System. A reader can either be a peripheral or a handheld device. Another possibility is that it is integrated into a fixed, installed system. RFID systems usually operate in the ISM (Industry, Scientific, Medical) frequency bands. There are two types of tag-reader couplings [Finkenzeller 2003]:

- *Inductive coupling* uses frequencies below 30 MHz. The reader antenna coil generates an alternating magnetic field and induces a voltage in the tag's coil. The data transfer from the reader to the tag is usually based on amplitude shift keying (ASK) and the tag employs load modulation to transfer data back to the reader.
- *Backscatter coupling* is used for frequencies above 100 MHz. Here the tag antenna receives signals and energy (passive tags only) from the electromagnetic field emitted by the reader. In order to transfer data to the reader, the reflected power is modulated by the transponder (modulated backscatter).

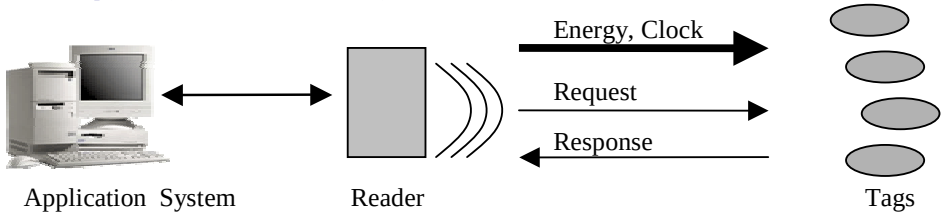

Figure 1: Overview of an RFID system with passive tags.

The reader usually sends the collected tag data to a background *application system* for further processing. Peripheral readers are directly attached to these systems (e.g. via RS 232 or USB interfaces) and standalone readers (e.g. handheld devices) can connect via standard network protocols to background systems, for example via Ethernet (or a wireless link) and TCP/IP.

The transmission range depends on different parameters and ranges from a few centimetres to several meters in practical applications. The communication is (depending on the tag protocol) initiated by the reader ("reader talks first") or by the tag ("tag talks first"). Figure 2 depicts an RFID communication model, but it should be noted that some RFID communication protocols do not clearly separate the different layers.

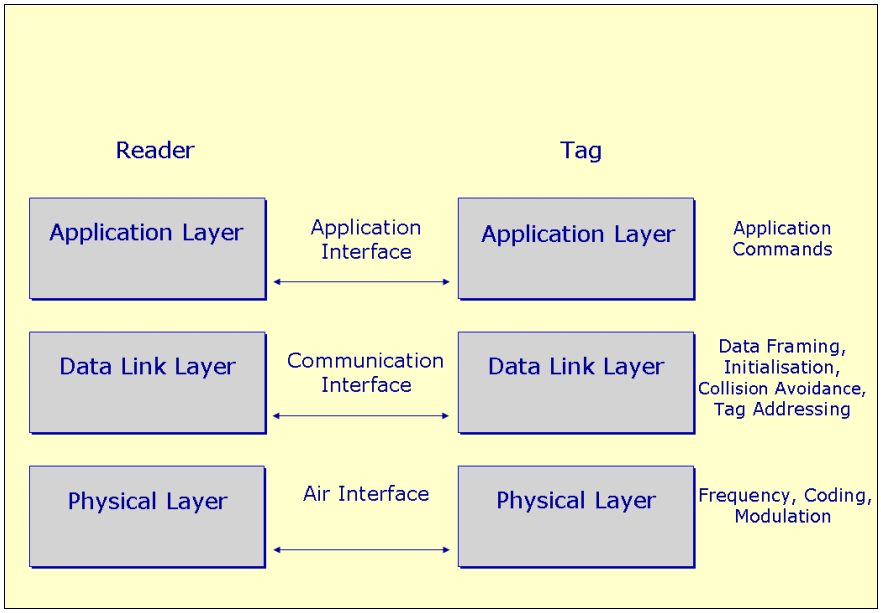

Figure 2: RFID Communication Model

The communication bandwidth for RFID systems is usually relatively low (several kBit/s) compared to other radio technologies but recent modes offer higher data rates (cf. chapter 3). Since little data is exchanged with a single tag, the bandwidth is more relevant in order to scan all tags in the operation range of a reader within a short time.

2.2 Functional properties

The types of RFID transponders considered in this article have the following functional characteristics:

- At a minimum, they are able to send a unique identifier (UID) on request. So called "1 Bit Transponders" without a chip, which are used for electronic article surveillance (EAS), are not considered here.
- There are anti-collision and multi-access protocols (either probabilistic or deterministic) implemented which allow the detection and addressing of multiple tags in the range of a single reader. On the other hand, anti-collision protocols between different readers in the proximity can be considered an open issue.
- Their primary purpose is object identification, so smartcards with considerable processing power (e.g. for advanced cryptographic operations) or even more sophisticated devices are also not considered. But, it should be noted that there is no clear distinction between high-end RFID tags and contactless smartcards (in particular ISO 14443 smartcards, cf. chapter 3).
- The RFID tag *may* possess read and write memory apart from the UID. The memory technology is usually EEPROM (Electrical Erasable and Programmable Read Only Memory) and the capacity typically ranges between a hundred Bits and several Kbytes.
- The transponder is either controlled by a state machine (low-end transponder) or by a microprocessor (high-end transponder).
- The tag *may* possess a crypto unit and implement some security functions, in particular access control, data encryption and message authentication (cf. chapter 4). The purpose of these functions is to protect the tag and its communications.

RFID technology was developed to replace barcodes at some point in the future. The major advantages of RFID systems over optical identification with barcodes are:

- The possibility to rewrite and modify data
- The operation without line-of-sight

On some RFID tags access control is implemented which is not possible with barcodes. The reading speed (in particular relevant for a large number of items) can be higher than using barcodes. Storage may not be an advantage since modern 2D barcodes can store 16 kBit of data or more [Compsee 2004], although many deployed scanners cannot read these codes.

2.3 Different types of RFID systems

There exists a large variety of RFID systems and their main characteristics are defined by standards. In particular, their air interface (frequency, coding, modulations), communication protocol, bandwidth, anti-collision and security mechanisms are standardised (cf. chapter 3 and 4). Other features are at least partly implementation specific (tag read and write memory, type of chip, tag design, communication range).

One important feature of RFID systems is the power supply of the tag. Passive tags do not possess an on-board power source. They are passively powered by the electro-magnetic waves from the reader which restricts the computing power and limits the read and write range.

Active transponders have a battery to power the chip. They may either use the reader's energy for their communication or operate an own radio transmitter. With thin-film batteries or "Power Paper" [Furness 2002], very thin active tags (smart active labels) have been realised. Active transponders are generally more expensive but have better radio characteristics, in particular a larger range, and may integrate other functional components, e.g. sensors.

3 RFID Standards

3.1 Overview

RFID is a relatively heterogeneous radio technology with a significant number of associated standards. Figure 3 contains the most relevant technology standards, i.e. those standards describing the physical and data link layers (air interface, anti-collision, communication protocols, and security functions). Further RFID standards describe test methods and application data standards (format of the Unique Identifier, data protocol and application programming interfaces).

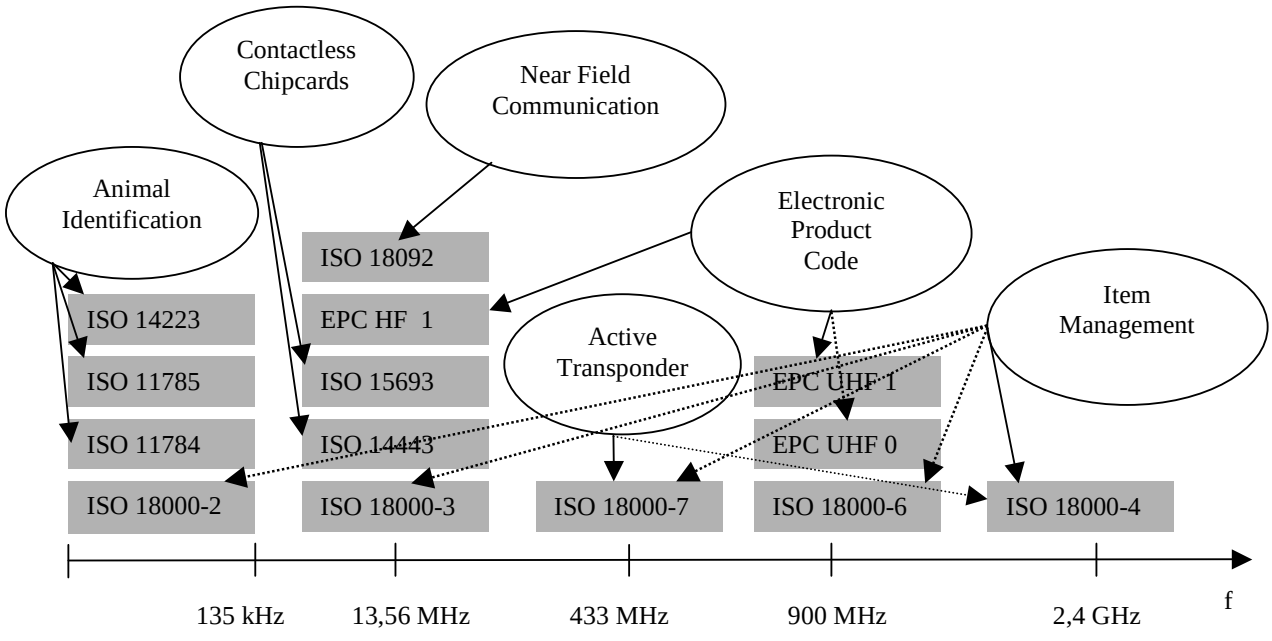

Figure 3: RFID technology standards and frequency bands

3.2 Contactless integrated circuit cards

Contactless integrated circuit cards are special instances of identification cards as defined in ISO 7810. Specifically, there are three types of contactless cards which can be distinguished in terms of their communication range:

- Close-coupled cards (ISO 10536). They operate at a very close distance to the reader (< 1 cm). Since they offer few advantages over classical contact smart cards (ISO 7816) they could not gain a considerable market share. In this article, we will not consider these cards in detail.
- Proximity cards (ISO 14443) operate at approx. 10 centimetres distance from the reader. They usually possess a microprocessor and may be considered as high-end RFID–transponders. These cards can implement more sophisticated applications such as ticketing. There exist two different standards (type A and type B) for the air interface, initialisation and anti-collision. Part 4 of the standard describes the link layer protocol T=CL which is similar to the T=1 protocol (ISO 7816-3) for contact smartcards. Application messages are exchanged with APDUs (Application Protocol Data Units) as specified in ISO 7816-4 or with proprietary protocols, e.g. for the widespread MIFARE® systems [Finkenzeller 2003].
- Vicinity cards (ISO 15693) have a range of up to 1 meter. They usually incorporate inexpensive state machines instead of microprocessors. These cards can be used for identification and simple applications like access control. The standard describes the air interface, anti-collision and the transmission (link layer) protocol.

3.3 RFID in Animals

ISO 11784, ISO 11785 and ISO 14223 specify tags for animal identification in the frequency band below 135 kHz. The original standards defined only a fixed unique 64 bit identifier, but with the more recent ISO 14223 standard further read/write and write-protected data blocks are allowed. The communication protocol of ISO 14223 is closely related to ISO 18000 part 2 (see below) [Finkenzeller 2003].

3.4 Item Management

ISO 18000 (RFID for item management) defines the air interface, collision detection mechanisms and the communication protocol for item tags in different frequency bands. Part 1 describes the reference architecture and parts 2 to 6 specify the characteristics for the different frequencies. Specifically, part 2 specifies low frequency (<135 kHz) tags. Part 3-1 for HF systems (13,56 MHz) is compatible with ISO 15693 (but with more flexibility in tag design), and part 3-2 specifies a next generation RFID system in the same frequency band with higher bandwidth (up to 848 kBit/s) and faster scanning of multiple tags. Part 4 specifies 2,45 GHz systems: in mode 1 a passive backscatter system and in mode 2 a long range, high-data rates system with active tags. Part 5 for the 5,8 GHz band is currently withdrawn. Part 6 defines a passive backscatter system around 900 MHz (the band is only partly available in Europe). Part 7 specifies a RFID system with active transponders and longe range in the 433 MHz band.

3. 5 Near-Field-Communication (NFC)

NFC evolved from RFID technology and is designed for interactions between tags and electronic devices in close proximity (< 10 cm). The standards ETSI TS 102.190, ISO 18092 and ECMA 340 define identically the Near Field Communication Interface and Protocol (NFCIP-1).

They describe the air interface, initialisation, collision avoidance, a frame format and a block oriented data exchange protocol with error handling. There is an active communication mode (both devices use their own RF field) and a passive communication mode (the initiator is generating an RF field and the target uses a load modulation scheme). NFC is not designed for full networking or transmission of large amounts of data, but should allow a convenient data exchange between cheap tags (e.g. smart labels) and electronic devices (e.g. PDAs). Another application is communication between computer peripherals (e.g. for configuration purposes).

The Near Field Communication Interface and Protocol -2 (NFCIP-2) specifies the communication mode selection mechanism (ECMA 352). This protocol deals with the situation that NFCIP-1, ISO 14443 and ISO 15693 devices all operate at 13,56 MHz, but with different protocols. It is specified that NFCIP-2 compliant devices can enter each of these three communication modes and are designed not to disturb other RF fields at 13,56 MHz.

3.6 Electronic Product Code (EPC)

EPC was developed by the AutoID (Automatic Identification) Centre of the MIT. The standardisation is now within the responsibility of EPCglobal which is a joint venture between EAN International and the Uniform Code Council (UCC) [EPCglobal 2003]. The so-called EPC network is composed of five functional elements:

- The Electronic Product Code is a 96 Bit number identifying the EPC version number, domains, object classes and individual instances [EPCglobal 2004]. EPC evolved from the widely used EAN-UCC (European Article Numbering/Universal Code Council) barcodes which identify products but not individual objects.
- An Identification System which consists of RFID tags and readers. Class 0 tags offer only a factory programmed EPC and higher class tags provide additional functionality, e.g. security functions. The AutoID Centre published a protocol specification for Class 1 tags in the HF band (compatible with ISO 15693 and ISO 18000-3), and Class 0 and 1 tags in the UHF band [Auto-ID

Center 2003a, 2003b, 2002a].

- The Savant Middleware offers "Processing Modules or Services" to reduce load and network traffic within the back-end systems. It can perform various tasks related to the acquired tag information [Auto-ID Center 2002c].
- The Object Naming Service (ONS) is a networking service similar to the Domain Name Service (DNS). With ONS, the Electronic Product Code can be linked to detailed object information. The ONS servers return the IP address of the EPC information service which stores the associated information [Auto-ID Center 2002b].
- The Physical Markup Language (PML) is XML-based and provides a standardised representation of information from the EPC network [Brock 2001, Auto-ID Center 2003c].

There are ongoing discussions on the harmonisation of EPC and ISO 18000 air interfaces for the UHF frequency band. It should be noted that EPCglobal specified a complete RFID system including the application layer which is not the case with ISO 18000.

4 Security of the RFID technology

4. 1 Security Objectives

The radio communications between RFID transponders and readers raises, as basically all wireless technologies, a number of security issues. Fundamental information security objectives, such as confidentiality, integrity, availability, authentication, authorisation, non-repudiation and anonymity [Pohl 2004] are often not achieved unless special security mechanisms are integrated into the system.

The privacy aspect has gained special attention for RFID systems. Consumers may carry objects with silently communicating transponders without even realising the existence of the tags. Passive tags usually send their identifier without further security verification when they are powered by electromagnetic waves from a reader. The ID information can also be linked to other identity data and to location information. Consumers might employ a personal reader to identify tags in their environment but the large number of different standards (see chapter 3) may render this difficult. Companies are facing customer fears and the privacy issues may become a major obstacle to further RFID proliferation. There are suggestions for a policy framework (e.g. the "RFID Bill of Rights" [Garfinkel 2002]).

4.2 Security Properties

Confidentiality

The communication between reader and tag is unprotected in most cases (with the exception of some high-end ISO 14443 systems). Eavesdroppers may thus listen in if they are in immediate vicinity. The forward channel from the reader to the tag has a longer range and is more at risk than the backward channel [Weis et al. 2003]. Furthermore, the tag's memory can be read if access control is not implemented.

Integrity

With the exception of high-end ISO 14443 systems which use message authentication codes (MACs), the integrity of transmitted information cannot be assured. Checksums (CRCs) are often employed on the communication interface but protect only against random failures. Furthermore, the writable tag memory can be manipulated if access control is not implemented.

Availability

Any RFID system can easily be disturbed by frequency jamming. But, denial-of-service attacks are also feasible on higher communication layers. The so called "RFID Blocker" [Juels et al. 2003] exploits tag singulation (anti-collision) mechanisms to interrupt the communication of a reader with all or with specific tags.

Authenticity

The authenticity of a tag is at risk since the unique identifier (UID) of a tag can be spoofed or manipulated. The tags are in general not tamper resistant.

Anonymity

The unique identifier can be used to trace a person or an object carrying a tag in time and space. This may not even be noticed by the traced person. The collected information can be merged and linked in order to generate a person's profile. A similar problem occurs in supply-chain applications where undesired product scans are possible. The automated reading of tags permits the counting of objects (e.g. banknotes with attached tags) which may be undesired.

4.3 Security Mechanisms and Proposals

Effective security mechanisms can provide protection against the described threats. But it should be taken into account that the primary purpose of the RFID technology is the realisation of cheap and automated identification. Thus, standard security mechanisms

can hardly be implemented because of their relative complexity compared with the constrained tag computing resources. AES, SHA-1 and efficient public-key protocols like NTRU [Hoffstein 1998] are too elaborate for low-cost tags [Weis et. al. 2003]. In the following, we describe implemented and proposed RFID security mechanisms.

Access Control and Authentication

Some tags implement access control mechanisms for their read/write memory. Access to the UID is mostly unrestricted, and the strength of memory access control procedures varies a lot (e.g. nothing, clear text password, challenge-response protocol).

Current RFID tags do not protect the Unique Identifier which raises the above mentioned privacy concerns. Some tags (in particular ISO 14443 and MIFARE® tags) enforce authentication mechanisms before granting read or write access to specific memory blocks. Here, either a simple password authentication or a unilateral or bilateral challenge-response authentication [e.g. ISO 9798-2] with symmetric keys are realised in practice. The authorisation may be granular and depend on the key which is used by the supplicant (i.e. the reader). For the forthcoming part 4 of the ISO 15693 standard a challenge-response authentication protocol with DES or 3DES is proposed. High-end transponders which comply with ISO 14443-4 can also employ application level authentication like contact smart cards.

The security and privacy risks induced by the unprotected tag identifier gave reason to a number of contributions and protocol propositions. Again, the resource constraints of low-cost tags have to be considered.

One option would be to 'kill' the tag after it has been used [Sarma et al. 2000], e.g. at the point of sale. A password protected 'destroy' command has also been integrated into the Electronic Product Code (EPC) specifications. But this would also destroy valuable resources and delete information which may still be useful [Juels et al. 2003]. The customer or his/her domestic appliances may for example obtain product related information or the tag could be used for recycling management.

[Juels et al. 2003] invented a 'RFID blocker tag' which exploits tag singulation (anti-collision) protocols in order to interrupt the communication with all tags or tags within a specific ID range. The blocker works for the most relevant anti-collision protocols (tree walking and ALOHA) and may be used for privacy protection but it can also be misused for mounting denial-of-service attacks.

[Juels 2003b] proposes a system of multiple tag pseudonyms which renders tracking by external entities more difficult. Only authorised entities can link the different pseudonyms.

[Ishikawa et al. 2003] propose that the tag emits only an 'Anonymous EPC'. A back-end security centre then delivers the clear text Electronic Product Code (EPC) over a secure channel to authorised entities. In an extended version, the readers can send a reanonymising request to the security centre which generates a new 'Anonymous EPC'. The tag is then updated with this ID.

[Weis et al. 2003] propose a 'Hash-Based Access Control Protocol'. The tag is first in a 'locked' state and transmits only a 'Meta ID' which is the hash value of a key. An authorised reader looks up the corresponding key in a backend system and sends it to the tag. The tag verifies the key by hashing it, returns the clear text ID and remains only for a short time in an 'unlocked' state. This would provide reader authentication and a modest level of access security. Privacy would still be at risk when the 'Meta ID' remains constant over time. Hence, [Weis et al. 2003] proposed a 'Randomized Access Control' in another mode of operation where tags respond with a randomised hash value. Since the reader would have to compute hash values for all possible IDs, this mode would only be feasible with a small number of tags.

[Engberg et al. 2004] argue that privacy and security enhancements should be adapted to the RFID tag lifecycle:

Supply-chain management → In-store and Point-of-Sale → Customer Control and After-Sales → Recycling & Waste Management

They propose a solution to the RFID privacy problem through zero knowledge (bilateral) authentication protocols which are based on a shared secret and use hash and XOR operations. At the point of sale, the tag changes from the "ePC" (electronic Product Code) mode to the privacy mode and a new authentication key – only known to the customer and the tag – is produced and stored. When returning the product for recycling, the privacy mode can be disabled and the tag returns to the original "ePC" mode.

[Avoine et al. 2004] describe the multi-layer aspects of the privacy problem. It may not be sufficient to ensure privacy on the application layer. Lower layers also have to be considered. On the data link layer, a unique identifier is required for deterministic singulation (collision avoidance) protocols. Even on the physical layer the radio fingerprint can distinguish a single tag.

Tag authentication

There are also proposals for protocols which authenticate the tag to the reader and protect against tag counterfeiting. [Vajda et al. 2003] propose and analyse several lightweight tag authentication protocols. [Feldhofer 2004] proposes the Simple Authentication and Security Layer (SASL) protocol [RFC 2222: Myers 1997] with AES encryption and analyses the hardware requirements.

Encryption and Message Authentication:

Some high-end RFID systems (ISO 14443 and MIFARE® based) are able to encrypt and authenticate the data traffic with proprietary protocols. Since data exchange apart from identifiers does not play a major role for RFID systems, secure messaging is often not regarded as a key issue. Encryption of memory blocks may be realised on the application layer, which is transparent for the RFID tag. The Unique Identifier (UID) is usually read-only and many RFID–transponders (e.g. ISO 15693 or 18000-3 tags) permit a permanent write lock of memory blocks. This can ensure data integrity but, of course, not message authentication.

5 Conclusions

RFID systems are already used for a large number of applications related to object identification. But, there remain still a number of issues to be resolved: the multiple standards and specifications need to be further harmonised, in particular those from ISO/IEC and EPCglobal. Open technical issues are e.g. related to tag orientation, reader coordination and the relatively short range [Want 2004]. Furthermore, a number of security and in particular privacy questions are still open. Consumer concerns may form an obstacle to further commercial deployment. Although today sophisticated mechanisms can not be implemented on a 5-cent tag, a number of proposals exist even for very restricted resources.

RFID systems may play an important role in the future, not only in marking and identifying objects but also in Body Area Networks (BAN), where tags can be equipped with sensors and actors and become part of a Personal Area Network (PAN) or so-called Wearable Computing. Since the tags are also used for personal identification and access control, new challenges for identity management arise. Privacy-enhancing identity management systems could provide a higher level of transparency and control for the user [Hansen et al. 2004]. Another interesting development is the Near Field Communication (NFC) protocol which allows a simplified exchange between electronic devices based on the RFID-technique in the 13,56 MHz band.

Falling prices will make the RFID–technique especially relevant for pervasive or ubiquitous computing. This enables situation and location based computing, where the status of the surrounding real world is recorded and communicated; a space model and a digital image of the real world may then be generated using the information collected by sensors. Such a digital model can be used by context related applications. An example is the silent commerce, where commercial transactions are carried out without human intervention.

6 References

Auto-ID Center (ed.): Technical Report - 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification. Version 1.0.0. Cambridge 2003a. http://www.epcglobalinc.org/standards_technology/Secure/v1.0/HF-Class1.pdf

Auto-ID Center (ed.): Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag. Cambridge 2003b. http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

Auto-ID Center (ed.): Technical Report – 860 MHz-930 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification. Version 1.0.1. Cambridge 2002a. http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

Auto-ID Center (ed.): Technical Manual: The Object Name Service. Version 0.5 (Beta). Cambridge 2002b. http://archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TM-004.pdf

Auto-ID Center (ed.) Techical Manual: The Savant. Version 0.1 (Alpha). Cambridge 2002c. http://archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TM-003.pdf

Auto-ID Center (ed.): PML Core Specification 1.0. Cambridge 2003c. http://www.epcglobalinc.org/standards_technology/Secure/v1.0/PML_Core_Specification_v1.0.pdf

Avoine, G.; Oechslin, P.: RFID Traceability: A Multilayer Problem (Draft), Lausanne 2004 http://lasecwww.epfl.ch/~gavoine/rfid/

Brock, D. L .: The Electronic Product Code (EPC) - A Naming Scheme for Physical Objects. Cambridge 2001a. http://www.autoidcenter.org/research/MIT-AUTOID-WH-002.pdf

Compsee Inc. (ed.): So What's a Bar Code? A Brief Discourse on Bar Code Symbologies. Palm Bay 2004 http://www.compsee.com/Media/Bar%20Code%20Symbologies%20-%20The%20Basics.pdf

ECMA-340: Near Field Communication - Interface Protocol (NFCIP-1) adopted by fast track procedure in ISO/IEC 18092. Geneva 2002. http://www.ecma-international.org/publications/files/ecma-st/ECMA-340.pdf

ECMA-352: Near Field Communication - Interface Protocol - 2 (NFCIP-2) adopted by fast track procedure in ISO/IEC 21481. Geneva 2003. http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-352.pdf

Engberg, S.; Harning, M.; Jensen, C.: Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. The Second Annual Conference on Privacy, Security and Trust (PST), New Brunswick, Canada 2004

EPCglobal Inc. (ed.): About EPCglobal Inc. Brussels 2003. http://www.epcglobalinc.org/about/about.html

EPCglobal Inc. (ed.): EPC Tag Data Standards Version 1.1. Brussels 2004. http://www.epcglobalinc.org/standards_technology/EPCTagDataSpecification11rev124.pdf

ETSI TS 102 190 v1.1.1 Near Field Communication (NFC) IP–1; Interface and Protocol (NFCIP–1). Technical Specification. Sophia Antipolis 2003

Feldhofer, M.: A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags. In: The 12th IEEE Mediterranean Electrotechnical Conference (MELECON), Dubrovnik 2004

Finkenzeller, K.: RFID-Handbook, Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd edition. Wiley and Sons, 2003

Frost&Sullivan (ed.): RFID Technology: Taking Product Tracking to the Next Level. New York 2003. http://www.frost.com

Furness, A: Present and Future of Smart Active Label Technology – An Overview. Birmingham 2002. http://www.sal-c.org/resources.html

Garfinkel, S.: RFID Bill of Rights. Technology Review 10, 35, 2002. http://www.simson.net/clips/2002/2002.TR.10.RFID_Bill_Of_Rights.htm

Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A., Waidner, M.: Privacy-Enhancing Identity Management. Information Security Technical Report. Vol. 9, No. 1, p. 35-44, 2004.

Hoffstein, J.; Pipher, J.; Silverman, J: NTRU: A ring based public key cryptosystem. In ANTS III (LCNS 1423), p. 267-288, 1998

Ishikawa, T.; Yumoto, Y.; Kurata, M.; Endo, M.; Kinoshita, S.; Hoshino, F.; Yagi, S.; Nomachi, M.: Applying Auto-ID to the Japanese Publication Business, 2003. http://www.autoidlabs.com/whitepapers/KEI-AUTOID-WH004.pdf

ISO/IEC 7810: Identification Cards – Physical Characteristics. Geneva 2003

ISO/IEC 7816: Identification Cards – Integrated circuit(s) cards with contacts. Geneva 1998

ISO/IEC 9798: Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms. Geneva 1999

ISO/IEC 11784: Radio frequency identification of animals -- Code structure**.** Geneva 1996

ISO/IEC 11785: Radio frequency identification of animals -- Technical concept. Geneva 1996

ISO/IEC 14223: Radio frequency identification of animals – Advanced Transponders. Part 1. Geneva 2003

ISO/IEC 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards. Parts 1 to 4, Geneva 2000

ISO/IEC 15693: Identification Cards – contactless integrated circuit(s) cards – Vicinity Cards. Parts 1 to 3, Geneva 2000

ISO/IEC 18000: RFID for Item Management: Air Interface. Parts 1,2,3,4,6,7, Geneva 2004

Juels, A.; Rivest, R.L.; Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. *CCS'03,* October 27–30, 2003, Washington http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf

Juels, A: Minimalist cryptography for RFID tags for low-cost RFID tags. In submission, 2003

Myers, J.: Simple Authentication and Security Layer (SASL). Internet RFC 2222, 1997. Updated by RFC 2444

Pohl, H.: Taxonomie und Modellbildung in der Informationssicherheit. Datenschutz und Datensicherung 11, 2004

Sarma, E.; Weis, S.; Engels, D.: RFID Systems and Security and Privacy Implications. In: Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, Volume 1965, p. 302-317, 2000

Sarma, E: Towards the 5c Tag. Auto-ID Center White Paper, 2002. http://archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-006.pdf

Vajda, I.; Buttyan, L.; Lightweight Authentication Protocols for Low-Cost RFID Tags. Second Workshop on Security in Ubiquitous Computing (Ubicomp), Seattle 2003

Want, R.: The Magic of RFID. acm queue, October 2004. http://www.acmqueue.com

Weis, S.; Sarma, S.; Rivest, R.; Engels, D.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Security in Pervasive Computing, Lecture Notes in Computer Science, Volume 2802, p. 201-212, Berlin 2003