WHITE PAPER SERIES / EDITION 1

AUTO-ID LABS

BUSINESS PROCESSES & APPLICATIONS
SOFTWARE & NETWORK
HARDWARE

AUTOIDLABS-WP-BIZAPPS-012

Extending the EPC Network — The Potential of RFID in Anti-Counterfeiting

Thorsten Staake, Frédéric Thiesse, Elgar Fleisch

University of St. Gallen

thorsten.staake@unisg.ch
frederic.thiesse@unisg.ch
elgar.fleisch@unisg.ch
www.autoidlabs.org

Abstract

The International Chamber of Commerce estimates that seven percent of the world trade is in counterfeit goods, with the counterfeit market being worth 500 billion USD in 2004. Many companies already use overt anti-counterfeiting measures like holograms to confine counterfeiting and product piracy. However, current techniques are not suited for automated tests of product authenticity as required in warehouses, or do not provide the required level of security. In this context, Radio Frequency Identification (RFID) is a promising approach, providing an extensible, flexible and secure measure against counterfeiting. Unique product identification numbers together with an infrastructure to seamlessly share RFID-related data over the Internet are a basis of efficient Track & Trace applications. An emerging infrastructure is the EPC Network, which can be used to provide pedigree information of products and makes plausibility checks possible. In this paper, we propose a solution for products requiring authentication mechanisms that go beyond track & trace. Therefore, the evolving EPC Network should comprehend the functionality to handle tags which support strong cryptography. We suggest extending the upcoming EPC Network infrastructure with an EPC Product Authentication Service. Moreover, the development of cost-effective, dedicated authentication devices as well as the belonging standardization is motivated.

1. Introduction

Counterfeiting imposes a menace to industry worldwide. The problem is not specific for certain products or countries. It is a global phenomenon affecting a wide range of industries. Counterfeit, whether of clothes, medicines or CDs, cost hundreds of billions of US dollars globally every year [1]. The effects of these crimes range from loss of company revenues to threats to public health and safety.

Companies are becoming increasingly aware of intellectual property rights (IPR) infringements. Many already use anti-counterfeiting measures such as holograms or elaborated packaging designs to confine counterfeiting and product piracy. However, current techniques are not suited for automated tests or do not provide the required level of security.

Radio Frequency Identification (RFID) is a promising technology to fight counterfeiting. In this context, Koh et al. describe an RFID based track & trace solution on the example of the pharmaceutical supply chain [2]. They use an infrastructure referred to as EPC Network [3] which enables the seamless sharing of RFID-related data over the Internet. The approach is sufficient in many cases, but certain products require secure authentication mechanisms that go beyond track & trace. For this reason, the scientific community is encouraged to extend the EPC infrastructure such that it provides an opportunity to securely authenticate RFID tags.

The structure of the paper is as follows: Section 2 points out the economic impact of counterfeiting and shows the relevance of doing research in this field. Section 3 concerns itself with the technologies which are currently used, followed by a discussion on the applicability of RFID as an anti-counterfeiting measure in section 4. Section 5 closes with concluding remarks.

2. The Economic Impact of Counterfeiting

The International Chamber of Commerce estimates that seven percent of the world trade is in counterfeit goods, with the counterfeit market being worth 350 billion USD in 2001. Similar data is available from the Counterfeiting Intelligence Bureau, assessing that global counterfeiting was worth 385 billion USD in 2001. In 2004, the International Chamber of Commerce expects the counterfeit market to exceed 500 billion USD per year [1]. Figure 1 illustrates the expansion of counterfeiting compared to the development of world merchandise trade.

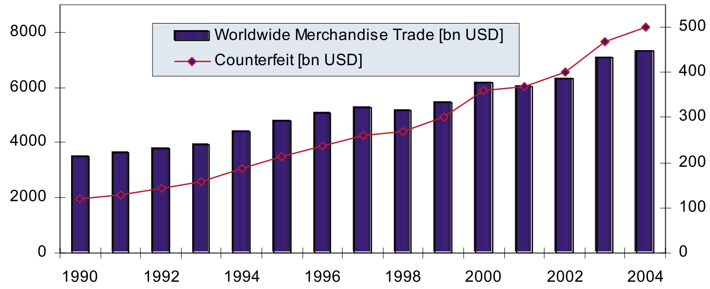

Fig. 1. Developement of counterfeiting compared to worldwide merchandise trade, based on [20,21]

2.1 The Scale of Counterfeiting

The extent of counterfeiting is highly sector specific. For some industries, the scale is stated in the following:

- In the *Copyright Industry*, almost half of all motion picture videos, more than 40 percent of all business software, and a third of all music recordings were pirated copies [4].
- About 10 percent of *clothing*, *fashion* and *sports wear* are plagiarism. Referring to estimates by the Counterfeiting Intelligence Bureau of the International Chamber of Commerce, online sales of faked luxury goods are worth 25 billion USD per year.
- In the *automotive industry*, 5 to 10 percent of all spare parts are counterfeits. This includes factory overruns, recycled items, copy parts and stolen goods [5]. Although very stringent controls exist for the supply of spare aircraft parts, the number of counterfeit or suspected unapproved components installed each year around the world rising [4].
- Between 5 to 8 percent of the 500 billion USD in *medicines* sold worldwide are counterfeit, as estimated by the Word Health Organisation (WHO) [6]. In some developing countries, the counterfeiting of drugs is endemic, with patients having a better chance of getting a fake medicine than a real one [7]. Counterfeit drugs have farreaching health implications, attracting considerable attention from public bodies such as the WHO or the U.S. Food and Drug Administration (FDA).

In all segments, the share of counterfeit goods has increased within the last years. Especially affected are markets in Asia and Eastern Europe. The aforementioned data give rise to the magnitude of the problem resulting from counterfeiting.

2.2 Impact on Affected Parties

Counterfeiting has an impact on the rights holder, the country where counterfeiting takes place, and it causes social costs.

The rights holder, i.e. the party whose goods are faked, suffers from reduced sales and profits as he or she competes against counterfeiters. Additionally, hidden costs exist: inferior products associated with a company are likely to have a negative impact on future sales as they compromise the corporate image and create a loss of goodwill. Moreover, consumers may blame the rightsowner if a faked product causes monetary losses or even physical injuries. Expensive lawsuits or reparations may be the result. Countries where counterfeiting takes place deter producers of reputable products from investing within the national economy since their intellectual property is at risk. Moreover, the prevalence of counterfeiting in a market discourages innovativeness. Another consequence is loss of taxes since mostly unregistered organizations manufacture faked products. On the long run, counterfeiting discourages investment in research and development: the advantages resulting from F&E are diminished when stolen by counterfeiters.

Social implications result from the abovementioned costs: consumers pay for the distorted competition, finally leading to less innovative products, higher taxes and unemployment. Moreover, consumers take health and safety risks resulting from inferior product quality.

3. Existing Approaches to Combat Counterfeiting

Companies, as well as enforcement agencies, are becoming increasingly aware of the problems resulting from counterfeiting. Safeguards against counterfeits constitute of four major ingredients: legislation, legal enforcement, anti-counterfeiting policy, and technological measures [4].

National governments, including those in the US, UK, China, as well as intergovernmental organizations such as the EU, have recently established new programs and procedures to foster cooperation, policymaking and training with respect to intellectual property enforcement.

During the last few years, companies have formulated systematic anti-counterfeiting policies. Investors regard anti-counterfeiting work as goodwill raising, and more and more enterprises see the advantages of publishing their efforts.

Legal issues and anti-counterfeiting policies are very important topics, but a detailed discussion is far beyond the scope of this paper. In the following, the focus is on technological measures.

Companies increasingly employ technologies to protect their products. In the past, this area was somewhat neglected, partly because of the limited availability of suitable technologies as well as the perception that technologic measures were not cost-effective. However, this trend has changed with more victims of counterfeiting becoming aware of the potentials and the falling costs of anti-counterfeiting technologies [4].

3.1 Current Technological Principles

The available technologies are broadly divided into optical, biological & chemical, and electronic technologies.

Optical anti-counterfeiting technologies are widely in use. Prominent examples are holograms. In the past, the use of holograms as security devices has been successful for a number of reasons: holograms have a strong visual appeal, and replicating them was possible only with a high investment. However, today equipment to manufacture holograms is cheap, and holograms constitute no great barrier for counterfeiters. Moreover, due to their extensive use, customers pay less attention to holograms than in the past. There is a large range of other optical anti-counterfeiting devices, including optically variable thin films, retro-reflective material, and micro printing technologies.

Biotechnology is becoming increasingly attractive as anti-counterfeiting measure, mostly due to the improved understanding of the unique characteristics of proteins, enzymes and DNA. One method, for example, uses specific antibodies to detect antigens or marker chemicals. Engineers add the marker chemicals in low concentrations to products such as pharmaceuticals or liquor. Specific antibodies contained in test kits detect the markers in the original products.

Microelectronics receive growing acceptance as anti-counterfeiting devices. Solutions range from identification technologies based on a simple, unique number to sophisticated digital signatures providing a very high degree of security. Devices can be implemented covert or overt, may or may not be accessible to the user, are nondestructive and suited for automated checks. A drawback is the high price, but experts expect less expensive devices in the near future.

A number of technologies, such as holograms, smart cards, biometric markers, and inks can be used in combination in order to protect and authenticate products. Comprehensive knowledge is essential when implementing these technologies. The International Anti-Counterfeiting Directory 2003, published by the ICC Counterfeiting Intelligence Bureau [8], provides general information on organizations that offer services in this area.

It is important to realize that in the past no anti-counterfeiting mechanism has been secure over a long time. Holograms, for example, lost a significant level of their impact in recent years. An overt, secure and user-friendly solution is not yet in place. Today, few people would argue that an anti-counterfeiting mechanism is secure perennially. However, the use of anti-counterfeiting technologies can significantly reduce the risk or scale of counterfeiting. The goal is to develop a technology, which, over the lifespan of a product, makes counterfeiting financially unattractive. The next section details a promising approach, the use of Radio Frequency Identification augmented with extensible electronic security features.

4. The Potential of RFID in Anti-Counterfeiting

A drawback of existing anti-counterfeiting measures is the low achievable degree of automation when checking the originality of a product. With existing schemes, large-scale checks, for example required in pharmaceutical warehouses, are not feasible. Radio Frequency Identification, or RFID, helps to address this problem, and provides the possibility to implement extensible, secure protection mechanisms.

4.1 RFID - Tags and Infrastructure

RFID is a generic term for technologies that use radio waves to automatically identify objects. In the most basic form, a serial number that identifies an object is stored on a microchip attached to an antenna (the chip and the antenna together are called *RFID transponder or RFID tag*).

Passive and active tags are distinguished. The former have no battery, but draw power from the reader, which sends out electromagnetic waves that induce a current in the tag‘s antenna. Transponders transmit information to the reader by reflecting the electromagnetic field. Passive tags have a short read range of typically less then 20 feet and can only perform computational non-intense tasks. Today, the price for simple passive tags is in the region of 20 US cents, but leading research institutes predict a further drop in price when the RFID market evolves. This effect could drive prices for passive labels well below 10 cents in the mid term [9].

Active RFID tags have a battery, which powers the microchip‘s circuitry and the RF transmitter. They are suited for computational intense tasks as required for complex cryptography algorithms. The price for sophisticated active tags including the battery may be as high as 3 to 10 USD, but experts expect prices to drop below one USD with the evolving market and the advancing technology [9].

The Electronic Product Code (EPC), a globally unique object ID tailored to RFID solutions [3], is suited for global object identification.

To enable the seamless sharing of RFID-related data, the Auto-ID Labs proposed an infrastructure referred to as EPC Network, whose deployment is now advanced by EPCglobal. Figure 2 illustrates the EPC infrastructure.

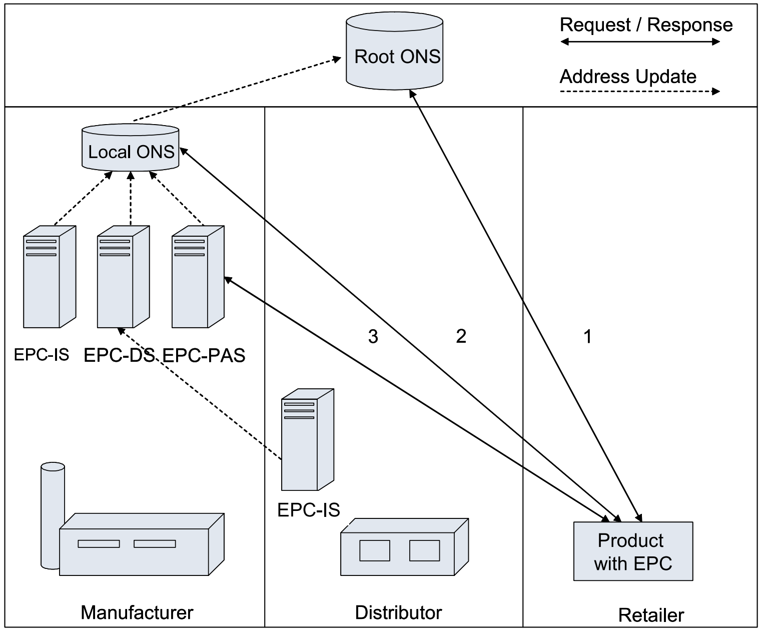

Fig. 2. The EPC infrastructure - overview

Main components of the infrastructure are the Object Name Service (ONS), the EPC Discovery Service (EPC-DS) and the EPC Information Service (EPC-IS). The proposed EPC Product Authentication Service (EPC-PAS) is outlined in Section 4.3.
The *Object Name Service* is a directory service that routes requests similar to the Internet's Domain Name Service (DNS). Two layers constitute the ONS: The first is called Root ONS, which is the authoritative directory of manufacturers offering information about their products on the EPC Network. The second layer is referred to Local ONS and serves as directory for individual products of a specific manufacturer. It contains the addresses of other EPC information resources.

The *EPC Information Service* stores and provides access to product information. While only manufacturers deploy Object Name Services, all trading partners may offer EPC Information Services.

The *EPC Discovery Service* records the addresses of EPC-IS servers, which provide information on the manufacturer's products. Thereby, it enables track & trace.

Note that the EPC Network relies on the EPC tags that only store a serial number in plaintext. Therefore, common tags are easy to duplicate and do not provide measures to securely authenticate products.

4.2 Track & Trace – A Plausibility Check

Radio Frequency Identification tagging of products by manufacturers, wholesalers and retailers appears to be the most promising approach to reliable product tracking and tracing. Inexpensive passive transponders store only a unique identification number, the EPC. The EPC is associated with a database entry via an ONS. This mapping is performed in two steps: first, the Root ONS resolves the EPC to determine the address of the associated Local ONS at the manufacturer. Then, the Local ONS is queried to look up the address of the requested service. This service may be the

EPC-IS of the manufacturer offering information about the product, or the address of the EPC-DS. The EPC-DS contains access information to services at other supply chain partners and enables tracking and tracing of individual products.

The EPC Network can provide benefits in areas such as inventory control, while also providing the ability to track & trace the movement of goods from production to consumption. This capability provides pedigree information about goods.

Pedigree information enables the buyer to perform plausibility checks: a drug, for example, having a serial number associated with a product currently stored in a warehouse in the UK is likely to be a counterfeit when offered in Nigeria at the same time. For the specific example of the pharmaceutical supply chain, Koh et al. discuss the value of RFID in [2].

This solution is adequate for some products. However, taking into account that an RFID tag with an EPC is easy to copy, the following scenario is possible: a manufacturer sells a product to a retailer via a number of shipping agencies. So far, every party, including the retailer, correctly updates the track & trace database. Then, the retailer copies the tag and attaches it to counterfeits. When selling the product, the customers may query the database, receiving a plausible history. This assumes that the counterfeiter does not update the database, nor does the costumer registers the deal. The latter is reasonable as the customer has no incentive to do so. Furthermore, he or she may have privacy concerns. This enables the retailer to sell counterfeits, as long as no customer updates the PML Server. Figure 3 illustrates the example. A simple track & trace solution does not avert this kind of defraud.

Problems also occur when intermediate owners do not update the database. This may happen when parties have no access to the database, when they act neglectful or when they are unwilling to record the transaction. If a consistent history of products is mandatory, incomplete pedigrees cause high costs. Employees then have to record track & trace information manually, or, if not possible, products may become unsaleable.

The abovementioned example shows that solely relying on track &trace may not be sufficient. Secure authentication of RFID tags constitutes a possible solution: if an RFID tag not only contained a unique serial number, but also implemented a feature making it possible to securely authenticate the tag - i.e. making it infeasible to copy it — this problem were solved.

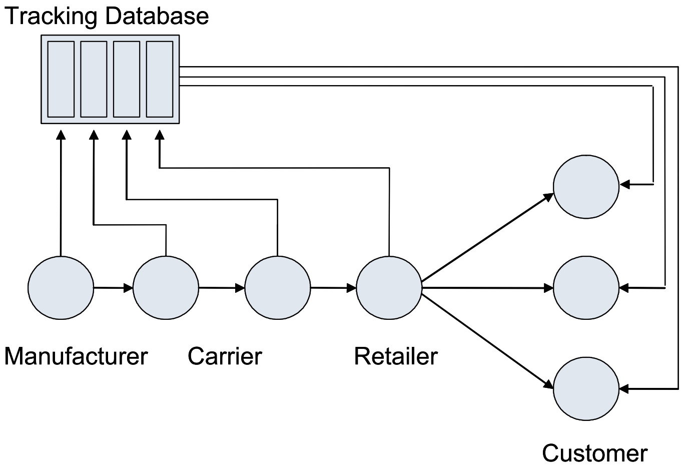

Fig. 3. Counterfeit despite track & trace

4.3 RFID and Advanced Cryptography

Providing the stated security goals requires implementing product authentication. This necessitates hardware support for cryptographic algorithms on RFID tags. Unfortunately, as stated by Sanjay Sarma et al., supporting strong cryptography is beyond the resources of low cost (0.05 - 0.10 USD) tags [10]. However, a number of applications do require strong protection mechanisms in order to prevent cloning attacks of tags and so justify higher tag prices.

The principle technical solution to provide secure authentication in a database-reader-tag environment is illustrated in Figure 4. The tag contains a unique identification number, a secret key, and a cryptographic unit. A database stores the according key; in the EPC Network, the EPC Information Service may include the cryptographic unit, or a separate cryptographic service may be offered. Research indicates that a separate cryptographic service function is to prefer for higher flexibility and a more secure design. Introducing secure authentication does not necessarily affect the reader device.

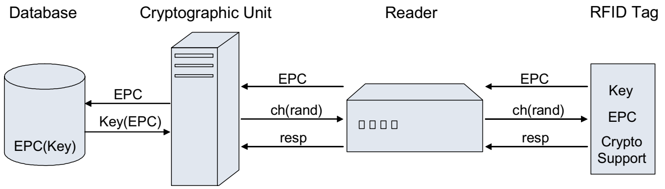

Fig. 4. Secure authentication in a database-reader-tag environment

Authentication is performed as follows: the tag communicates its identity number with the cryptographic unit (CU) at the manufacturer. Then, the CU generates a random message (challenge) which is sent to the tag. The tag encrypts the message with its secret key and transfers the response back to the CU. The CU looks up the according key in a database and verifies the response. Note that the authentication process is transparent to the reader.

Technical solutions of varying complexity range from lightweight hash-based challenge-response type authentication, proposed for example in [11] and [12], to public key based digital signatures such as RSA (as specified in ANSI X9.31). Several papers propose lightweight cryptographic primitives for resource constrained applications like smart cards and sensor networks. Examples include resource efficient public key schemes such as NTRU [13]. A hardware RFID implementation of the less complex symmetric encryption algorithm Advanced Encryption Standard (AES) [14] is shown in [15]; the AES core, tailored to implementations in RFID tags, together with program ROM, controller and analogue RF front-end lead to chip areas of 1.5 mm^2 in a 0.35µ CMOS process, corresponding to 0.8 mm^2 in up-to-date 0.18µ technology. A promising design, named Tiny Encryption Algorithm [16], uses a large number of iterations rather than complex operations and may be feasible for implementation in low cost RFID tags in the near future. Standard cryptographic hash functions such as SHA-1 [17] are still costly, but may be implemented for processes that require a higher level of security.

Analysing available RFID tags [18, 19] that support secure authentication showed that existing devices were designed for a variety of applications. The cryptographic units mostly support more than one encryption and decryption algorithm and are built as add-on to general-purpose processors. Moreover, a large part of the chip area is comprised by memory cells. When such a device exclusively has to provide secure authentication, only a small fraction of the chip's functionality is used, leading to unnecessarily expensive devices.

However, a large number of companies need solutions to protect expensive parts or highly security-relevant processes from counterfeit based on secure authentication. Therefore, further research should address the design of efficient, dedicated authentication devices.

In order to ensure the interoperability of authentication solutions, it is necessary to define standards for the information system infrastructure, i.e. an EPC-Authentication Service, as well as for authentication tags, constituting another area of future work.

5. Conclusion and Outlook

This paper discusses anti-counterfeiting technologies currently used to protect a wide variety of products. The technologies lack the possibility of automating counterfeit checks or, for certain applications, do not provide the desired level of security. RFID is likely to eliminate these shortcomings, providing an extensible, flexible and secure measure against counterfeiting.

The central conclusion is that a track & trace approach using inexpensive, passive tags storing a unique Electronic Product Code (EPC) is sufficient for many applications. A large number of products, however, do require secure protection mechanisms, with the cost of a counterfeit justifying more expensive tags. Therefore, the evolving EPC Network should comprehend the functionality required to handle tags with a secure authentication mechanism.

We suggest extending the upcoming EPC Network infrastructure with an EPC Product Authentication Service to provide secure authentication functionalities. Future research will address the design of this service. Moreover, the development of cost-effective, dedicated authentication devices as well as the belonging standardization constitutes important areas of future work.

Acknowledgements

The presented work was supported by the M-Lab – The Mobile and Ubiquitous Computing Lab alongside with its partner companies. The M-Lab is a joint project at the University of St.Gallen and the ETH Zurich, and member of the international Auto-ID Lab Network.

References

[1] ICC Policy Statement (2003) The fight against piracy and counterfeiting of intellectual property. Submitted to the 35th World Congress, Marrakech, Document no 450/986 www.iccwbo.org/home/intellectual_property/ fight_against_piracy.pdf

[2] Robin Koh, Edmund W. Schuster, Indy Chackrabarti, Attilio Bellman (2003) Securing the Pharmaceutical Supply Chain. White Paper, Auto-ID Labs, Massachusetts Institute of Technology, www.autoidlabs.com/whitepapers/mit-autoid-wh021.pdf

[3] David L. Brock (2001) The Electronic Product Code (EPC) - A Naming Scheme for Physical Objects. White Paper, Auto-ID Labs, Massachusetts Institute of Technology, www.autoidlabs.com/whitepapers/MIT-AUTOID-WH-002.pdf

[4] Organization for Economic Co-operation and Development (OECD) (1998) The Economic Impact of Counterfeiting. www.oecd.org/dataoecd/11/11/2090589.pdf

[5] Kommission der Europäischen Gemeinschaft (1998, 2000) Grünbuch zur Bekämpfung von Nachahmungen und Produkt- und Dienstleistungspiraterie im Binnenmarkt. europa.eu.int/comm/internal_market/en/indprop/piracy/ com789de.pdf

[6] World Health Organization (2003) Counterfeit medicines, Frequently Asked Questions. www.who.int/medicines/ organization/qsm/activities/qualityassurance/cft/counterfeir _faq.htm

[7] U. S. Department of Health and Human Services, Food and Drug Administration (2004) Combating Counterfeit Drugs, A Report of the Food and Drug Administration. http://www. fda.gov/oc/initiatives/counterfeit/report02_ 04.pdf

[8] ICC Counterfeiting Intelligence Bureau (2003) The International Anti-Counterfeiting Directory 2003. www.iccwbo.org/ccs/cib_bureau/CIBDirectory.pdf

[9] RFID Journal (2004) Frequently Asked Questions, http://www.rfidjournal.com/article/articleview/207

[10] Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels (2002) RFID Systems, Security & Privacy Implications. White Paper, Auto-ID Labs, Massachusetts Institute of Technology, www.autoidlabs.org/ whitepapers/MIT-AUTOID-WH-014.pdf

[11] Dirk Henrici, Paul Müller (2004) Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifier. Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04)

[12] Istvan Vajda, Levente Buttyan (2003) Lightweight authentication protocols for low-cost RFID tags. Second Workshop on Security in Ubiquitous Computing — Ubicomp 2003, Seattle, WA, USA.

[13] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman (1998) NTRU: A Ring-Based Public Key Cryptosystem. Lecture Notes in Computer Science 1423, 267-288, Springer-Verlag, Berlin

[14] Federal Information Processing Standards Publication 197 (2003) Specification for the Advanced Encryption Standard (AES)

[15] Martin Feldhofer (2004) A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags.
IEEE Proceedings of MELECON 2004, Vol. 2, pp. 759–762

[16] David J. Wheeler, Robert M. Needham (1995) TEA, a Tiny Encryption Algorithm. Technical report, Computer Laboratory, University of Cambridge,
www.ftp.cl.cam. ac.uk/ftp/papers/djw-rmn/djw-rmn-tea.html

[17] Federal Information Processing Standards Publication 180-1 (1995) Secure Hash Standard

[18] Infineon Technologies (2001) Security and Chip Card ICs, SLE 55R01 Short Product Information. www.infineon.com/cgi/ecrm.dll/ecrm/scripts/public_download.jsp?oid=29991&parent_oid=14537

[19] Infineon Technologies (2004) Secure Mobile Solutions - Security, SLE 66CL80P Short Product Information.
www.infineon.com/cmc_upload/documents/036/428/SPI_SLE66 CL80P_0102.pdf

[20] Press Release from the World Customs Organization (2003)
www.wcoomd.org/ie/en/ press/ Counterfeiting_E.htm

[21] World Trade Organization (1986-1994) Agreement Establishing the World Trade Organization, Annex 1C, Agreement on Trade-Related Aspects of Intellectual Property Rights.
www.wto.org/english/docs_e/legal_e/27-trips.pdf