ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
University of St.Gallen

AUTO–ID LABS

Strengthening the Security of Machine-Readable Documents

Combining RFID and Optical Memory Devices

Mikko Lehtonen, Thorsten Staake,
Florian Michahelles, Elgar Fleisch

Auto-ID Labs White Paper WP-HARDWARE-034

Mikko Lehtonen
Senior Researcher
ETH Zurich

Thorsten Staake
Senior Researcher
University of St.Gallen

Florian Michahelles
Associate Director
Auto-ID Labs ETH Zurich

Elgar Fleisch
Research Director
Co-Chair of Auto-ID Labs
University of St.Gallen and ETH Zurich

Contact:

Auto-ID Labs ETH Zurich/St.Gallen
Swiss Federal Institute of Technology (ETH) Zurich
Department of Management, Technology and Economics
Kreuzplatz 5
8032 Zurich
Switzerland

Phone: +41 44 632 86 24
Fax: +41 44 632 10 45

E-Mail: mlehtonen@ethz.ch
Internet: www.autoidlabs.org

Hardware

Abstract

There is an on-going trend towards turning paper documents that store personal information or other valuable data into machine-readable form. An example of this trend is the electronic passport that will become common in the near future. In this paper we show how the security of these machine readable documents could be improved by combining RFID with optical memory devices. We propose integrating an optical memory device into the RFID enabled smart document and present methods how these two storage media can be combined to secure the document against threats like illicit scanning, eavesdropping and forgery. The presented approaches make use of the optical document-to-reader channel which is more secure than the radio-frequency communication interface. To demonstrate the potential of our approaches we show how they could overcome a number of existing security and privacy threats of electronic passports.

1. Introduction

Radio frequency identification (RFID) is an important enabling technique of ambient intelligence. In applications like supply chain management it is used as a mere labelling technique [23], while in anti-counterfeiting its role is for example to implement cryptographic challenge-response authentication protocol [21]. As RFID technology becomes more and more pervasive and closer to our everyday life, also the discussion of the relating security and privacy risks increases. Indeed, addressing the security and privacy threats is of great importance for the acceptance and adoption of RFID [28, 27].

Integration of RFID transponders into physical documents has lead to evolution of machine readable documents. The best known application of this field is the electronic passport, or *e-passport*, where an RFID transponder is used to store biometric data of the passport's holder. Millions of e-passports are already in the circulation today [12] and the number will keep increasing – the U.S. alone will issue more than seven million e-passports each year starting from October 2006 [18, 19].

There are numerous applications where tagging physical documents would be interesting: besides e-passports and other travel documents, also for example customs freight papers, security papers (e.g. gift certificates, jewellery appraisals), driver's licenses and vehicle registration papers would benefit from being machine readable through radio-frequency (RF) communication[1]. A common factor of these documents is that they all relate to a physical entity that is not very well suited to be tagged to become a data carrier itself: integrating RFID chips into an expensive jewellery, for example, might conflict with its classical, non-technical nature. Also, besides some extreme cases[2], tagging of human beings is not likely to happen. Therefore, even though objects are turning into data carriers through integration of ambient

[1] Most passports and driver's licenses of today are machine readable through optical character recognition
[2] http://amal.net/rfid.html

intelligence technologies, there is and will be a need also for separate data carrier documents.

In this paper we propose new ways of combining RFID with optical memory devices to increase the security of machine readable documents. Our goal is to evaluate and show different approaches of the combined use of these devices. It should be noted that throughout this paper we refer to RFID devices in a broad sense that comprises also contactless smart cards. We propose and evaluate four different approaches how this combination could be used to overcome existing security threats of machine readable documents in terms of more secure communication protocols and resistance against forgery and cloning. Instead of establishing security based on sharing secrets between the reader device and document before the communication, we make use of optical memory devices which cannot be read or eavesdropped without a line of sight.

This paper is organized as follows. In section 2 we discuss machine readable documents in general. A general model of the technical infrastructure for RFID enabled machine readable documents is presented in subsection 2.1 and an overview to travel documents in subsection 2.2. The security and privacy of machine readable travel documents is discussed in subsection 2.3. Section 3 presents optical memory devices and four approaches how we combine them with RFID in physical documents to achieve specific security objectives. In section 4 we discuss the security of the proposed communication models and we finish with conclusions.

2. Machine Readable Documents

Physical documents can be made machine readable by integrating RFID transponders into them. This creates a link between the physical world and the virtual world and can extend the role of the documents. Within this paper we denote all physical documents that carry a digital memory device as machine readable documents. The typical instance of these kinds of documents is an RFID tagged paper. Another way to make documents machine readable is to use optical character recognition (OCR) to read data printed on the document.

In existing and proposed applications RFID tags are integrated into documents to enable automated document tracking [20], to increase the security of the documents [22, 11] and in general to improve the document handling processes, like the biometric authentication using e-passports [8]. The possible applications of machine readable documents are as manifold as those of normal documents, and more. This is made possible by the digital storage and, optionally, by the logic of the integrated circuits.

The benefits of having RFID transponders in physical documents come from the simple and fast read processes that does not demand a line of sight connection. Depending on the grade and price of the chip, the contactless memory device can also support for re-writable memory and logical functions like cryptographic primitives. Therefore machine readable documents can also provide high level of security and counterfeit resistance.

The following subsection presents the general technical infrastructure of machine readable documents application. Because travel documents and especially e-passports are the most discussed application of machine readable documents within the scientific community, we concentrate on them in subsection 2.2 and on their security and privacy threats in subsection 2.3.

2.1. Technical Infrastructure

The considered components of an RFID enabled machine readable document application are the document itself, the reader device and the reader's control and crypto unit. These components and their mutual communication channels are illustrated in Figure 1. The document is a physical entity that contains an integrated RFID transponder that serves as a contactless memory device. Typically the transponder stores at least a unique identifier (UID) number. In addition, the transponder can provide logical functionalities like access control (through key comparison), random number generation and data encryption. Thus, the transponder serves as more than a mere barcode label.

The two-way communication in the air interface between the contactless memory device and the reader is indicated as a two directional arrow in Figure 1. Without specific addressing, RFID air interface is not secure and the transponder is vulnerable to clandestine scanning (or *skimming*) and eavesdropping. These two security threats are denoted as dashed lines in the illustration. A commonly used standard for RFID air interface of machine readable documents like e-passports is the ISO 14443 for proximity cards.

The reader device is responsible of the wireless communication. It is connected to the control and crypto unit through a closed, secure channel. Last component in the general infrastructure is the online database that represents data on the network. Though this database is not used in the proposed approaches, it is presented to complete the general view.

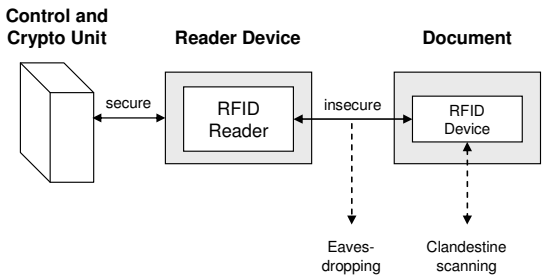

Figure 1. Technical infrastructure and communication channels of RFID enabled machine readable documents. Security threats of eavesdropping and clandestine scanning are illustrated with dashed lines.

2.2. Travel Documents

Machine readable travel documents (MRTD) comprise e-passports, visas and special purpose ID/border-crossing cards [8]. Because of their similar nature, we include also driver's licenses within this group.

Most public discussion around MRTDs has been around the electronic passports. The first e-passports were issued in 1998 by Malaysia, followed by other early adopters [5]. The Malaysian e-passports use an RFID transponder to store a fingerprint image of the passport's holder, which enables automated border checks with less human oversight. E-passports will be a prominent and widespread form of identification within a couple of years [12] as its adaptation is fuelled for example by the U.S. Visa-Waiver Program [3] that involves twenty-seven nations. Not all MRTDs of today use RFID technology. Currently the vast majority of U.S. states use or have plans to use 2-D barcodes to store personal data on driver's licenses [1].

The role of the digital memory devices in the authentication processes of travel documents is twofold: on the one hand they help authenticating the traveller and on the other hand they help proving the authenticity of the document itself. Current e-passport (de-facto) standards are given by the ICAO guidelines [8]. They define only one mandatory security measure that is digital signature. Verifying the integrity of biometric features is of primary importance for passports, but addressing only data integrity leaves the system open to various security and privacy threats. The ICAO guidelines do define other cryptographic features that make use of public-key infrastructure, but these are optional.

E-Passport design has to address needs for individual privacy and national security and thus it poses severe security and privacy requirements. These requirements are discussed in [12] and [9]. First of all, the integrity and authenticity of the data the passport stores has to be guaranteed. Second, the data has to be kept confidential from non-authorized parties. Third, the passport must not pose privacy threats for its carrier and, furthermore, all these have to be fulfilled in a public system during up to 10 year long life-span of the passport.

2.3. Security and Privacy Threats

Most discussion about security and privacy of machine readable documents comes from the field of e-passports. Because of their rigid security requirements listed in subsection 2.2, also we concentrate on e-passports in order to provide a short overview of common security threats of machine readable documents in general.

Juels et al. [12] have discussed the security issues of e-passports and the following four threats, among others, were brought into light: clandestine scanning, clandestine tracking, eavesdropping, and cryptographic weaknesses. Moreover, the authors concluded that the e-passports do not provide sufficient protection for their biometric data. Threats do not only concern the functionality of the system but the security and privacy of its users as well. Also Pattison [17] has listed his concerns about the security of e-passports, concerning the baseline ICAO guidelines. These concerns comprise: unprotected data, unprotected wireless transmission, and missing connection between the chip and the paper. The last of these

concerns is relevant regarding forgery because without this connection, the system can be fooled for example by putting a valid transponder into a fake paper.

The security of e-passports clearly needs careful addressing – compromising the system would threaten individual and national security. The U.S. State Department has already altered its e-passport design due to privacy concerns [10]. Various proposals for addressing the security and privacy issues of RFID do exist, most often based authentication protocols that use public or symmetric key encryption [2, 14, 9]. Scarce resources on the chip limit the use of cryptographic primitives and the goal of the design is often low-cost low-security features.

In the following section we present how optical memory devices can be combined with RFID to overcome some of the security threats of machine readable documents. The addressed security issues comprise:

- No connection between chip and paper
- Data integrity
- Clandestine scanning
- Clandestine tracking
- Eavesdropping

The first two aforementioned issues relate to the security of the overall system and the latter three to the unsecured wireless communication.

3. Combining RFID and Optical Memory Devices

We propose integrating an optical memory device into the RFID enabled machine readable document. What is common to all optical memory devices is that they need a line of sight connection for reading, making them resistant against clandestine reading and eavesdropping. Therefore we can assume that this channel is secure. The optical memory devices we refer to work normally with write-once-read-many (WORM) principle. Figure 2 illustrates how the addition of optical memory device extends the communication channels between machine readable document and reader device.

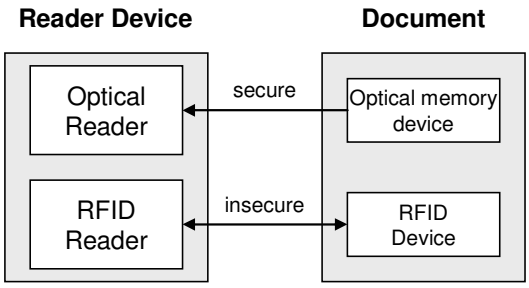

Figure 2. The communication channels between reader device and document using RFID and optical memory

Before we present our approaches, a short introduction to optical memory devices is provided. Even though we do specify what types of memory devices should be used, basic understanding of possible technologies is necessary for the following discussion.

3.1. Optical Memory Devices

Optical memory device refers to numerous technologies, ranging from barcodes to holographic memories with storage capacities on the order of 1 byte to 100 GB, respectively. The optical memory devices are characterized by their data density (e.g. bytes/mm^2) and can support for error correction coding so that data from partially damaged devices can be successfully recovered. The reader or scanner devices of optical memories use photo sensors, laser and charge-coupled devices (CCD). One interesting advantage of optical memory devices, concerning especially printed codes, is that they are easy to integrate in documents in a rather permanent way as the ink that makes the code is inside the paper. Permanent integration of the memory device is important because it contributes to the security of the overall document.

The simplest low capacity optical memory devices are printed one and two dimensional barcodes. Memory capacities of typical barcodes vary from 95 bits of EAN.UCC-12 barcode to maximum data density of about 850 bits per cm^2 of PDF-417 2-D code. In general, the maximum memory capacity of 2-D barcodes is defined by the accuracy of printing and scanning and the redundancy of the code. The printed high-density 2-D codes can provide data capacities up to about 1,250 KB per cm^2 [26].

Holograms and holographic memory form another type of optical memory devices. Since the early seventies, it has been seen as the high capacity storage solution of the future, promising data densities on the order of hundreds of megabytes per square centimetre and remarkable improvements to the data transfer rate [29]. Hologram based optical memory devices are currently being used for example as anti-counterfeiting labels [24]. Also other promising optical memory technologies emerge, for example photoaddressable polymers (PAPs) which offer re-writeable (RW) data storage capabilities [6]. PAPs are promising recording materials for optical data storage applications such as high-capacity DVDs and holographic memory.

In the following subsections we present four approaches how the combination of RFID and optical memory devices can be used to increase the security of machine readable documents. First two approaches address data integrity and bind the chip and the document, while the two other approaches aim at securing the communication. For the sake of simplicity, we use the term reader in the rest of this paper for the combination of optical and RFID reader devices and their control and crypto unit. Because machine readable documents often relate to a physical entity, we assume that data of interest that the document stores relates to this entity. We denote this data as *object specific data* and it can be used for example in authentication. In addition, the documents can store any other application specific data which is merely referred to as *other data*. This other data can be static or dynamic.

3.2. Storing the Object Specific Data in the Optical Memory

In this basic approach, the static object specific data is stored on both the RFID transponder and on the optical memory. This is illustrated in Figure 3. Mirroring the data of interest helps to maintain redundancy and thus increases the reliability of the overall document. Redundancies on other media than contactless memory devices may be important as the electronic devices can be destroyed without visual effect. Moreover, the additional use of optical storage devices may help overcoming problems resulting from limited storage capacities of RFID devices.

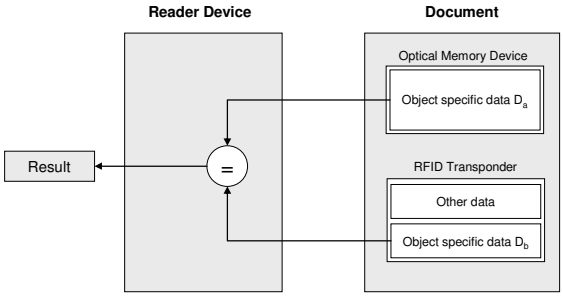

Figure 3. An illustration of storing the object specific data in the optical memory device

The advantage of mirroring the data is to have a mechanism – indicated by the *result* block in Figure 3 – that can tell if one of the two devices has been tampered with. This increases the integrity of the data, though an identical tampering of both devices cannot be detected. In addition, the object or person specific data also interlinks the two devices in an unquestionable way, since this data can be used as a unique identifier of the physical entity. A disadvantage of this approach is that a relatively large size optical memory is needed. Furthermore, the optical memory doesn't provide access control and thus offers another medium where the data is vulnerable to skimming.

3.3. Storing Hash of the Object Specific Data in Optical Memory

The basic step for taking advantage of the additional data integrity and bind between paper and chip of the first approach while guarding the object specific data from optical access is to save only a hash value of the data on the optical device. This comes with the expense of some extra computations and losing the optical backup of the data of interest. The data structures of the memory devices and the data integrity check of the document using this approach are illustrated in Figure 4.

The used hash function needs to be known by the party performing the data integrity check so the specification of the hash function is stored on the chip. Moreover, this gives an additional binding between the two storage devices. Including the transponder UID number in the hash-calculation can also strengthen this linkage. The reader has to calculate the hash value of the object specific data loaded from the contactless device in order to perform the integrity check. Compared to the previous approach, another advantage of storing the hash value is that smaller optical storage space is needed.

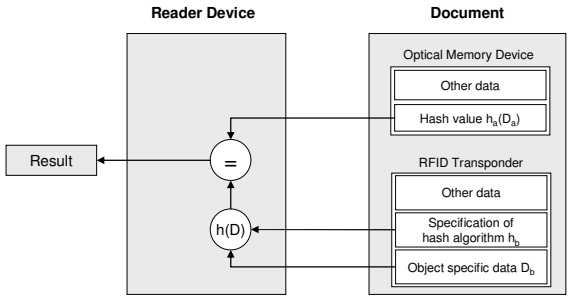

Figure 4. An illustration of storing hash of the object specific data in the optical memory device

3.4. Storing Access Keys in the Optical Memory

While the two previous approaches in subsections 3.2 and 3.3 define data integrity checks, this approach aims at protecting the data. In this approach the RFID transponder does not reveal the object specific data if no correct access key (e.g. a PIN code) has been transmitted in advance, which prevents clandestine reading. Moreover, the data on the electronic tag is read-protected. Also the emission of transponder serial number can be protected in the way described above, protecting the document and its bearer against clandestine tracking. The access key is stored on the optical device and thus can only be read with a line of sight connection. In the context of e-passports, for example, this means that the passport has to be opened for reading and therefore its owner can control who can have access to the contactless memory.

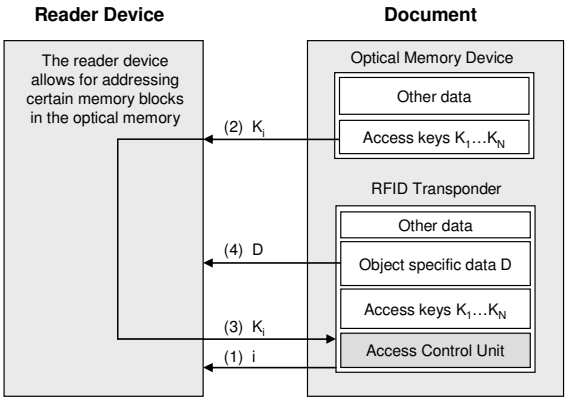

Figure 5. An illustration of storing access keys in the optical memory device

Figure 5 illustrates how the reader can access the object specific data using this approach. Now the requirements of the tag include an access control unit which is capable of generating random indexes and comparing keys. The communication model works as follows: The RFID reader initiates the session by asking the transponder for an index *i* between 1 and *N*, where *N* indicates the number of access keys stored in the document. For the sake of simplicity, this message is not illustrated is Figure 5. After the index value is transmitted by the transponder, the reader can obtain the corresponding key *Ki* from the optical memory and send it to the RFID transponder. We denote the length of K_i as *M* (bits). The transponder access control unit verifies if the received access key matches the one stored in its memory and can grant the access for the reader.

In this approach the link between the paper and transponder is strong and both optical and contactless devices are needed for successful communication. In order to access the object specific data, an attacker has to obtain or successfully guess the access key that matches the requested one. Because single access keys can be still obtained by eavesdropping the radio channel between the reader and the transponder, the number of access keys *N* needs to be large enough to make the malicious use of compromised keys infeasible and spoofing access keys difficult. More precisely, *N* should be chosen in such a way that the probability of getting access with a compromised key in a single random challenge, $\Pr = 1/N$, is not significantly greater than the probability of guessing an access key, $\Pr = 2^{-M}$.

Spoofing access keys can be also countered by temporarily locking the tag when anyone tries to unlock it using a false access key. However, we leave this to be addressed by the more detailed level protocol design.

3.5. Storing Session Keys in the Optical Memory

This fourth approach is similar to the previous one presented in subsection 3.4 where the transponder challenges the reader for a response to be read from the optical device. However, instead of using access keys which can be eavesdropped from the reader-to-tag

radio channel, in this approach the optical memory device stores session keys that are used to encrypt the communication.

How the combination of RFID and optical memory is used for protecting the communication in this approach is illustrated in Figure 6. The access control is established by a challenge response pair which is initiated by the tag by transmitting a pseudo-random challenge *ch* and an index *i* between 1 and *N*. After having received the index, the reader accesses the optical memory of the document to obtain the corresponding session key *Ki*. To authenticate itself to the transponder, the crypto-unit of the reader device calculates and sends the response *resp* which is the challenge encrypted using the session key, denoted by K_i(ch) in Figure 6. Last, the session key *Ki* is used to encrypt the following wireless communication (e.g. transmission of the object specific data) which takes place between the reader and the transponder, to provide protection against eavesdropping.

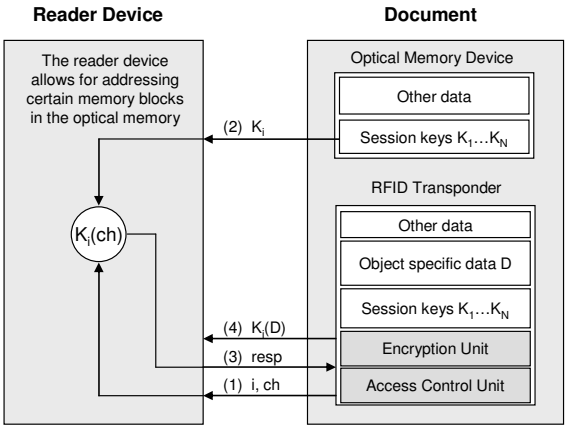

Figure 6. An illustration of storing session keys in the optical memory device

In this approach the successful authentication means that the reader has optical access to the document. Storing session keys in the optical device provides comparable benefits than the approach in subsection 3.4 where access keys are stored on the optical device. Most notably, the passport has to be opened for reading and the two storage media provide strong interlink between the devices. In addition, the use of session keys and encryption provides protection against eavesdropping. Most importantly, the session key is never transmitted in the insecure radio channel as this key is only optically accessible, which overcomes the weakness of the previous approach regarding compromised access keys. On the other hand, this approach requires the transponder to support data encryption.

The presented design has still cryptographic weakness regarding the use of session keys. These keys are not chosen in a truly random manner but taken from a restricted list which makes the authentication protocol more vulnerable for attacks. Nevertheless, even the use of only one session key ($N = 1$) provides good protection for the machine readable document.

4. Discussion

Providing machines with the capability to communicate with documents through RFID could dramatically change the way we see and use them: besides precisely knowing where each document is, data on the tag and on the network could be used to manage the pedigree of the documents, to provide digital signatures etc. However, when the documents are of great value or contain personal information, the upcoming security and privacy threats need to be adequately addressed to protect the systems and their users.

We have proposed four approaches to increase the security of machine readable documents that make use of the different properties of optical and contactless memory devices. For the optical memory device, these properties are resistance to clandestine scanning and eavesdropping. The benefits of RFID are their support of logical functions like cryptographic primitives that can be used for example for authentication protocols. Optical devices, especially printed codes, are easy to integrate in paper documents. Also RFID chips, however, can be integrated inside paper; for example the Hitachi μ-chip [22] is designed to be attached to paper documents. In the future, the development of printable polymer electronics [7] may provide novel and interesting ways to seamlessly integrate transponders in paper.

As discussed in subsection 2.3, the ICAO standards for e-passports may not be secure enough. This does not necessary mean, however, that ISO 14443 based proximity smartcards are inappropriate technology for secure machine-readable documents in general. Because RFID tags are generally cheaper than smartcard chips, we can see a trade-off between the proposed approaches that combine RFID and optical memory devices which always require a line-of-sight, and the more expensive contactless smartcards which don't.

We see the main benefits of combining RFID with optical memory devices in the field of document security. These benefits are discussed in the two following subsections. Besides strengthening the security, also other benefits occur, for example the optical memory device can be used to ease the memory capacity requirements of the RFID transponder. This might become especially interesting in the future with the radical data capacity improvements of emerging optical memory technologies. Furthermore, the optical memory device on the document gives a visual cue of the existence of the tag for the users and holders of the document, which can contribute for the acceptance of RFID technology in general.

4.1. Increased Communication Security

The optical channel can be used to overcome threats relating clandestine scanning and eavesdropping in ways presented in subsections 3.4 and 3.5. These approaches require no pre-distribution of shared secrets between the reader and the document, which favours for

simpler systems; indeed, key distribution is seen as one of the future challenges of RFID security [13]. On the other hand no mutual authentication between the devises is provided. Here the security is established by the assumption that a party who has free visual access to the document is trusted – an assumption that we consider quite feasible regarding for example passports, because, tagged or not, they are to be kept safe and presented to authorized personnel only.

In any case, especially concerning public systems, high level of security needs to be established through secret keys. The presented approaches do not limit the use of public or symmetric key cryptography and so they can be used inside the communication models. Furthermore, the proposed approaches can be combined with each other, namely by selecting one of the first two approaches (subsections 3.2 and 3.3) to guarantee the data integrity and one of the latter two approaches (subsections 3.4 and 3.5) to secure the communication, while taking into account the hardware constraints of reader and memory devices.

With regard to the security and privacy threats of e-passports listed in subsection 2.3, the increased communication security of the approaches presented in subsections 3.4 and 3.5 would help overcome concerns about clandestine scanning, clandestine tracking and eavesdropping.

4.2. Increased Security of the Overall System

Other security contributions of the proposed approaches include increased data integrity, as presented in subsections 3.1 and 3.2. Also a strong bind between the paper and the chip is provided, which answers to the e-passport security concern of missing connection between the paper and the tag, as discussed in subsection 2.3.

The use of two memory devices adds complexity to the system and thus makes the documents harder to be cloned or forged. Even though this conflicts the fundamental security doctrine of Kerckhoffs which says that the security of a system should depend on its key, not on its design obscurity [16], it can provide effective ways to combat counterfeits. For example, the approaches allow for selection of a proprietary optical memory type which cannot be read using devices that are publicly available, if a closed-loop application is preferred.

Also the link between the paper and the tag contributes to cloning resistance: Tags can be made hard to clone by using read protected memories or factory programmed unique transponder ID numbers. An example of how the read protected KILL password of EPCglobal Class-1 Generation-2 tags [4] can be used to strengthen the transponder against cloning can be found in [15]. In addition, special efforts have been made towards anti-clone tags [25]. Consequently, when the seamlessly integrated optical memory device binds the document to an anti-clone tag, cloning and forging the document becomes even harder.

4.3. Related Work

The potential of RFID to secure physical documents is well established. Takaragi et al. [22] have discussed how to prevent forgery of security papers by integrating small RFID tags into the physical documents. The authors compared RFID to barcode and concluded that RFID provides better counterfeit protection due to the fact that it is harder to be copied. However, no link (expect for the physical integration) between the transponder and the document was provided.

The optical channel can be used in RFID also in other ways. Raskar et al. [30] have developed photosensing wireless tags called radio frequency identification and geometry (RFIG) transponders that support for geometric functions. Making use of the photo-sensors, RFIG allows for tags being read only when properly illuminated, which could be used to solve the problem of clandestine scanning of machine readable documents. However, on the contrary to our approaches, no information is transferred in RFIG from the transponder to the reader through this optical channel and, furthermore, no optical memory devices were used. Because of these two facts, our approaches have more potential to increase the security of machine readable documents.

Combining RFID with data printed on the object is not novel in security applications and it has been used for example for privacy protection of tagged banknotes [11]. In this approach the printed serial number (and a signature value) of the banknote is read, namely using OCR, and used to bind the banknote and its RFID chip. Printed data is also being used for the security of travel documents in the advanced security methods defined by optional ICAO e-passport guidelines [9]. In the so called basic access control protocol the e-passport has to be opened and clear-text data like passport number and data of birth of the bearer is used to derive secret cryptographic keys. The purpose of this protocol is to prevent skimming and eavesdropping but according to [12] the scheme fails due to too small entropy of the keys and the fact that only one key is provided for the lifetime of the passport.

This review shows that the previously proposed approaches differ from the contribution of this paper in the way that we make use of the secure optical channel from the document to the reader that cannot be eavesdropped. Furthermore, the existing approaches that use machine readable optical data on documents are normally based on OCR of printed clear-text data, whereas we propose using dedicated optical memory devices which support for much larger storage spaces.

5. Conclusions

In this paper we have shown different approaches to combine RFID and optical memory devices in order to increase the security of machine readable documents. In particular, we

have presented how the proposed approaches could overcome existing security threats of electronic passports concerning eavesdropping and clandestine scanning and tracking. Instead of establishing security based on sharing secrets between the reader device and the document before the communication, we make use of the optical channel between the document and the reader which cannot be read or eavesdropped without a line of sight. Even though strong security in communications always needs secret keys, security of RFID enabled machine readable documents will also depend on a strong connection between the transponder and the paper. We have illustrated how optical memory devices can be used to provide this connection. In conclusion, we believe that the interlinked co-existence of RFID and optical memory devices can play an important role for strengthening the security of smart documents of the future.

References

[1] American Association for Motor Vehicle Administrators (2006). Current and Planned Technologies for U.S. Jurisdictions. Available from http://www.aamva.org/standards/stdUSLicenseTech.asp (22.3.2006)

[2] Dimitriou, T. (2005). A Lightweight RFID Protocol to protect against Traceability and Cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm (to appear), Athens, Greece, September 2005. IEEE.

[3] U.S. Department of State (2006). Visa-Waiver Program (VWP). Available from http://travel.state.gov/visa/temp/without/without_1990.html (20.4.2006)

[4] EPCglobal (2005). Class-1 Generation-2 UHF RFID Conformance Requirements Specification v. 1.0.2. EPCglobal Public Document, February 2005.

[5] RFID Gazette (2005). E-passports. News article, November 8, 2005. Available from http://www.rfidgazette.org/airline/index.html (28.3.2006)

[6] Hagen, R. and Bieringer, T. (2001). Photoaddressable Polymers for Optical Data Storage. Advanced Materials Volume 13, Issue 23, Pages 1805 – 1810, 2001.

[7] Hammerschmidt, C. (2004). Polymer electronics yet to realize promise. EETimes Germany, November 2004.

[8] ICAO (2004). Document 9303, Machine Readable Travel Documents, October 2004. Available from http://www.icao.int/mrtd/publications/doc.cfm (28.3.2006)

[9] ICAO (2004). PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Technical Report, version 1.1, October 2004. Available from http://www.icao.int/mrtd/publications/doc.cfm (28.3.2006)

[10] International Herald Tribune (2005). U.S. to alter passport design because of privacy fears. News Article, April 28, 2005. Available from http://www.iht.com/articles/2005/04/27/news/passport.php (28.3.2006)

[11] Juels, A. and Pappu., R. (2003). Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In Rebecca N. Wright, editor, Financial Cryptography -- FC'03, volume 2742 of LNCS, pages 103--121, Le Gosier, Guadeloupe, French West Indies, January 2003. IFCA, Springer-Verlag.

[12] Juels, A., Molnar, D., and Wagner, D. (2005). Security and Privacy Issues in E-passports. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm (to appear), Athens, Greece, September 2005. IEEE.

[13] Juels, A. (2005). RFID Security and Privacy: A research Survey. Condensed version to appear in 2006 in the IEEE Journal on Selected Areas in Communication.

[14] Juels, A. and Weis, S. (2005). Authenticating pervasive devices with human protocols. In Victor Shoup, editor, Advances in Cryptology – CRYPTO'05, volume 3126 of Lecture Notes in Computer Science, pages 293–308, Santa Barbara, California, USA, August 2005. IACR, Springer-Verlag.

[15] Juels, A. (2005). Strengthening EPC Tags Against Cloning. In M. Jakobsson and R. Poovendran, eds., ACM Workshop on Wireless Security (WiSe), pp.67-76. 2005.

[16] Kerckhoffs, A. (1883). La Cryptographie Militaire. In Journal des Sciences Militaires (Jan 9, 1883), pp 5-38. Available from http://www.petitcolas.net/fabien/kerckhoffs/ (21.4.2006)

[17] Pattison, N. (2004). Securing and Enhancing the Privacy of the E-Passport with Contactless Electronic Chips. Contact: pattison@axalto.com.

[18] RFID Journal (2004). U.S. Tests E-Passports. News Article, November 2, 2004. Available from http://www.rfidjournal.com/article/articleview/1218/1/1/ (19.4.2006)

[19] RFID Journal (2005). United States Sets Date for E-Passports. News Article, October 25, 2005. Available from http://www.rfidjournal.com/article/articleview/1951/1/1/ (19.4.2006)

[20] RFID Journal (2006). Roman Lab to Offer Commercial Services. News Article, March 28, 2006. Available from http://www.rfidjournal.com/article/articleview/2223/1/1/ (19.4.2006)

[21] Staake, T., Thiesse, F., and Fleisch, E. (2005). Extending the EPC Network - The Potential of RFID in Anti-Counterfeiting. In Proceedings of the 2005 ACM symposium on Applied computing (pp. 1607 - 1612). New York (NY): ACM Press.

[22] Takaragi, K., Usami, M., Imura, R., Itsuki, R., and Satoh, T. (2001). An Ultra Small Individual Recognition Security Chip. IEEE Micro, November-December, 2001.

[23] Tellkamp, C., Angerer, A., Fleisch, E., and Corsten, D. (2004). From Pallet to Shelf: Improving Data Quality in Retail Supply Chains using RFID. Cutter IT Journal - The Journal of Information Technology Management, Vol. 17, No. 9, pp. 19-24, 2004.

[24] Tesa AG (2006). Protection system by Tesa Scribos marks spare part packs. Available from http://www.tesa.com/corporate/211628.html (28.3.2006)

[25] Tuyls, P. and Batina, L. (2006). RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, In Topics in Cryptology - CT-RSA - The Cryptographers' Track at the RSA Conference, number 115-131 in lecture Notes in Computer Science, page 3860, San Jose, USA, February 13-17 2006. Springer Verlag.

[26] Veritec Inc (2006). VSCode®. Technology Overview. Available from http://www.veritecinc.com/vs_code.html (28.3.2006)

[27] Weis, S. (2004). RFID Privacy Workshop: Concerns, Consensus, and Questions. IEEE Security and Privacy, vol. 02, no. 2, pp. 48-50, 2004.

[28] Wong, K., Hui, P., and Chan, A. (2006). Cryptography and authentication on RFID passive tags for apparel products. Computers in Industry, May 2006.

[29] M.J. Wickett (2002). Memories of the future. emerging replacements for semiconductor memory, optical and magnetic disks. Multimedia Systems - MMS 2002, South Hampton, UK, January 2002.

[30] R. Raskar, P. Beardsley, J. Baar, Y. Wang, P.H. Dietz, J. Lee, D. Leigh, and T. Willwacher (2004). RFIG lamps: Interacting with a self-describing world via photosensing wireless tags and projectors. ACM Transactions on Graphics (TOG) SIGGRAPH, 23(3):406–415, August 2004.