Readers Behaving Badly
Reader Revocation in PKI-Based RFID Systems

Rishab Nithyanand, Gene Tsudik, and Ersin Uzun
{rishabn,gts,euzun}@ics.uci.edu

Department of Computer Science
University of California - Irvine
Irvine, CA 92697

Abstract. Recent emergence of RFID tags capable of performing public key operations motivates new RFID applications, including electronic travel documents, identification cards and payment instruments. In such settings, public key certificates form the cornerstone of the overall system security. In this paper, we argue that one of the prominent -and still woefully unaddressed- challenges is how to handle revocation checking of RFID reader certificates. This is an important issue considering that these high-end RFID tags are geared for applications such as e-documents and contactless payment instruments. Furthermore, the problem is unique to public key-based RFID systems, since tags (even those capable of complex cryptographic operations) have no clock and thus cannot use traditional (time-based) off-line revocation checking methods. Whereas, on-line methods require unrealistic connectivity assumptions.
In this paper, we address the problem of reader revocation in PKI-Based RFID systems. We begin by observing an important distinguishing feature of *personal* RFID tags used in authentication, access control or payment applications -the involvement of a human user. We then take advantage of the user's awareness and presence to construct a simple, efficient, secure and (most importantly) feasible solution for reader revocation checking. And finally, we evaluate the usability and practical security our solution via usability studies and discuss its feasibility in a case study of e-Passports.
In our approach, the main extra feature is the requirement for a small passive on-tag display. However, as discussed in the paper, modern low-power display technology (e.g., e-paper) is low-cost and appealing for other (e.g., authentication and verification) purposes.

1 Introduction

Radio Frequency Identification (RFID) is a wireless technology mainly used for identification of various types of objects, e.g, merchandise. An RFID tag is a passive device, i.e., it has no power source of its own. Information stored on an RFID tag can be read by special devices called RFID readers, from some distance away and without requiring line-of-sight. Although RFID technology was initially envisaged as a replacement for barcodes in supply chain and inventory management, its low cost and ease of use has opened up many other possibilities. Current and emerging applications range from visible and personal (e.g., toll transponders, passports, credit and access cards, livestock/pet tracking devices) to stealthy tags in merchandise (e.g., clothes, pharmaceuticals and library books). The cost and capabilities of an RFID tag vary widely depending on the target application. At the high end of the spectrum are the tags used in e-Passports, electronic ID (e-ID) Cards, e-Licenses, and contactless payment instruments. Such applications involve relatively sophisticated tags each costing a few (usually < 10) dollars or euros. These tags are powerful enough to perform hefty public key operations, e.g., encryption and signature verification.

In the "real world", one of the main security problems in using public key cryptography is certificate revocation. Any certificate-based public key infrastructure (PKI) needs an effective revocation mechanism. Traditionally, revocation is handled implicitly, via certificate expiration, and/or explicitly, via revocation status checking. Most PKI-s use a combination of implicit and explicit methods[1].The latter can be done off-line, using Certificate Revocation Lists (CRLs) [2] and similar structures, or on-line, using protocols

[1] The only exception is Certificate Revocation System (CRS) [1] which is purely implicit.

such as Open Certificate Status Protocol (OCSP) [3]. However, as discussed below, these approaches are untenable in public key-enabled RFID systems.

Intuitively, certificate revocation in RFID systems should concern two entities: RFID tags and RFID readers. The former only becomes relevant if each tag has a "public key identity", i.e., if each tag has its own public/private key-pair and (optionally) a public key certificate (PKC) binding its identifier to a public key. We claim that revocation of RFID tags is a non-issue, since, once a tag identifies itself to a reader, the latter (as the entity performing a revocation check) can use any current revocation method (except perhaps OCSP which requires continuous network connectivity). This is possible due to the fact that an RFID reader is a full-blown computing device with internal storage, clock and opportunistic communication (e.g., USB, Wi-Fi) to receive periodic CRL updates. Moreover, tags do not engage in communication with other tags.

In contrast, revocation of readers is a problem in any public key-enabled RFID system. While a tag may or may not have a public key identity, a reader must have one (otherwise, the use of public key cryptography becomes non-sensical). Therefore, before a tag discloses any information to a reader (e.g., by encrypting it using the reader's public key), it must make sure that the reader's PKC is not revoked.

1.1 Why Bother?

We now discuss further justification for revocation checking of RFID readers by tags. One common and central purpose of all RFID tags and systems is to enable tag identification (at various levels of granularity) by readers. With that in mind, many protocols have been proposed to protect the identification process (i.e., the tag-reader dialog) from a number of threats and attacks. In systems where tags can not perform cryptographic operations or where they are limited to symmetric cryptography, reader revocation is not an issue, since it is essentially impossible. Whereas, in the context of public key-enabled tags, reader revocation is both imperative and possible, as we show later in this paper. It is imperative, because not doing it prompts some serious threats. For example, consider the following events:

- A reader is lost or stolen
- A reader is compromised (perhaps without knowledge of its operator/owner)
- A reader is decommissioned

In all of these cases, if it cannot be revoked effectively, a reader that has fallen into the wrong hands can be used to identify and track tags. Further threats are possible depending on the application. In the case of tags which store sensitive data such as biometrics and other personal data (e.g., e-Passports and e-Licenses), it is possible for an adversary to easily obtain this information and use it in malicious activities such as identity theft or forgery. In the case of tags used in payment instruments, an adversary may obtain financially valuable information, such as credit-card account information, which can later be sold for money or used in credit card fraud [4].

Thus far, it might seem that our motivation is based solely on the need to detect *prematurely revoked* reader certificates[2]. However, what if a reader certificate naturally expires? In that case, a well-behaved reader would not be operated further and a new certificate would be obtained by its owner. However, if a reader (or rather its owner) is not well-behaved, it might continue operation with an expired certificate. Without checking for certificate expiration, an unsuspecting tag would be tricked into identifying itself and possibly divulging other sensitive information.

In the remainder of this paper, we make no distinction between certificate revocation and certificate expiration checking. The reason is that both tasks require current time, which, as we discuss below, is unavailable on passive devices.

1.2 Why Is Reader Revocation Hard?

When presented with a PKC of a reader, a tag needs to check three things:

[2] "Prematurely" means before the expiration of the PKC.

1. Signature by the issuing certification authority (CA)
2. Expiration
3. Revocation status

The first step is easy for any public key enabled (pk-enabled) tag and has been already incorporated into some reader authentication schemes, e.g., [5], [6]. Unfortunately, the last two steps are problematic. Since even a high-end tag is a passive device, there is no way for it to maintain a clock. Thus, a tag, by itself, has no means of deciding whether a presented certificate is expired.

Revocation checking is even more challenging. First, similar to expiration, off-line revocation checking (e.g., CRL-based) requires current time, i.e., a clock. This is because the tag needs to check the timeliness of the presented proof of non-revocation. Also, communicating a proof of non-revocation entails extra bandwidth from the reader to the tag. For CRLs, the bandwidth is $O(n)$ and even for more efficient CRTs, the bandwidth is $O(log\ n)$ – a non-negligible number for large values of n (where n is the number of readers in the system).

On the other hand, online revocation checking protocols (e.g., OCSP used with nonces [3]) would entail the tag contacting (via the reader) a trusted OCSP responder. The proof of non-revocation would be constant-size, but the connectivity and the availability requirements would be problematic. If an OCSP responder is accessed over the Internet, the readers must always have a high-speed and low-delay connection to the Internet or to some other network infrastructure. Moreover, constant availability of OCSP responders is problematic. A responder represents a single point of failure, as far as crashes, request overload as well as denial-of-service attacks.

There have been revocation handling proposals that attempted to compensate for lack of a clock on a tag. For example, [7] suggested using a simple monotonically increasing time-stamp which is updated after every successful tag-reader interaction to the reader's PKC issuance date. This method is adopted by the German Federal Office for Information Security (BSI) for certificate validation in e-Passports [5]. Whenever a tag is presented with a signed certificate or a CRL, it compares the date of expiry with the stored time-stamp and accepts it only if the certificate's expiration date exceeds the time-stamp. However, this approach does not solve the problem, since it leaves a large window of vulnerability between time-stamp updates. This is especially problematic in case of infrequently used tags, such as e-Passports.

1.3 Our Approach: Roadmap

We focus on a class of pk-enabled RFID systems where tags are both personal and attended. This class includes e-Passports, e-Licenses and contactless credit cards. *Personal* means that a tag belongs to a human user and *attended* means that a tag is supposed to be activated only with that user's (owner's) consent. Our approach to reader revocation is based on several observations:

- User/owner presence and (implicit) consent are already required for the tag to be activated.
- Low-cost and low-power flexible display technology is a reality, e.g., e-paper and OLED. In fact, passive RFID tags with small (6-8 digit) displays have been demonstrated and are shown to be feasible.
- Since certificate revocation and expiration granularity is usually relatively coarse-grained (i.e., days or weeks but not seconds or minutes), human users can distinguish between timely and stale date/time values.

The rest is rather straight-forward: a display-equipped tag receives from a reader a PKC along with a signed and time-stamped proof of non-revocation (details discussed later in the paper). After verifying the respective signatures on the reader's PKC and the non-revocation proof, the tag displays the lesser of: (1) PKC expiration time and (2) non-revocation proof time-stamp. The user, who is reasonably aware of the current time, validates the timeliness of the displayed time-stamp. If the time-stamp is deemed to be stale, the user aborts the interaction with the reader. Otherwise, user allows the interaction to proceed.

The rest of this paper is organized as follows: We go over the related work in section 2. In Section 3, we overview some trivial solutions to reader revocation checking and discuss their shortcomings. We describe our solution in section 4; followed by the results from our preliminary usability study in section 5. In section 6, we present a case study with the application of our solution to e-Passports and finalize the paper with our conclusions in section 7.

2 Related Work

There have been many general proposals for dealing with certificate revocation in distributed systems and networks. Of these, Certificate Revocation Lists (CRLs) are the most commonly used mechanism. CRLs form a part of the X.509 Public Key Infrastructure for the Internet [2]. Other techniques that improve the efficiency of revocation checking are:

- Certificate Revocation Trees (CRTs) [8] use Merkle's Hash Trees [9] to communicate relatively shorter proofs of (non-)revocation.
- Skip-lists [10] and 2-3 Trees [11] improve on the CRT update procedure through the use of dynamic data structures, offering asymptotically shorter proofs.
- Online Certificate Status Protocol(OCSP) [3] is an on-line verification approach that reduces storage requirements and provides timely revocation status information.
- Certificate Revocation System [1, 12] is the first technique for fully implicit certificate revocation. It utilizes hash chains [13] to provide compact proofs of certificate validity.
- Other related results focused on privacy issues in certificate revocation checking, e.g., [14].

In spite of substantial prior work, very little has been done in terms of finding practical methods for revocation checking in RFID systems. However, the problem has been recognized and concerns were raised regarding the lack of reader revocation checking mechanisms in current PKI-based RFID systems, e.g., [15, 16] in e-Passports,[17] in eCredit-Cards, and [18, 19] in other applications.

The only seemingly viable approach [7] suggested using a monotonically increasing counter (register) as a kind of a loosely synchronized clock. Although, this solution is used in the latest e-Passports standard [5], it suffers from a potentially large window of vulnerability between register updates. The problem of the high communication cost of CRL-s in current solutions has been also noted by Blundo, et al. [20].

To the best of our knowledge, the idea of outfitting pk-enabled RFID tags with display units for enhanced security was introduced by Ullman [21]. It suggests using a display unit to establish secure and authenticated wireless channels using short passwords. The display is used as a means of transmitting a freshly generated one-time password in an attempt to prevent clandestine scanning and eavesdropping.

In this paper, we propose using a small display on tags to solve the problem of revocation checking. Unlike the register-based method [7], our approach does not have a large window of vulnerability (beyond that already inherent to any off-line revocation method). Furthermore, it is very efficient in terms of reader-tag bandwidth and tag storage.

3 Trivial Solutions

As discussed in Section 1, due to their passive nature, RFID tags are highly vulnerable to attacks by revoked readers. Lack of an internal clock and impracticality of using on-line revocation checking protocols constitute the main challenge in reader revocation checking. In this section, we describe some trivial approaches and discuss their shortcomings.

3.1 Date Register

Every PKC has a validity period which defined by its effective date (D_{eff}) and expiration date (D_{exp}). During the certificate verification process, a tag uses the date stored in its register (D_{curr}) to determine whether a certificate has expired or not. The verification steps are as follows:

1. Tag verifies the CA signature of the reader's certificate.
2. Tag checks that D_{exp} in the certificate is greater than D_{curr} on the tag.
3. If previous steps are completed successfully, the tag accepts the certificate. Moreover, if D_{eff} is greater than D_{curr}, the tag also updates D_{curr} to D_{eff}.

(*) If reader authentication involves explicit revocation check, the timeliness of the non-revocation proof is verified in a similar way using the D_{curr} value.

In this approach, it is easy to see that the estimate of the current date – D_{curr} – stored by the tag is not guaranteed to be accurate and does not always help to protect it from readers with expired or revoked certificates. This is especially the case for a tag that has not been used for some time. The value of D_{curr} could reflect a date far in the past, exposing the tag to attacks from readers revoked (implicitly or explicitly) at any point after D_{curr}. Even for frequently used tags, a recently revoked reader would always pose a danger.

3.2 On-line Revocation Checking

Online revocation-checking approaches, such as the Online Certificate Status Protocol (OCSP) [3], alleviate storage requirements on clients by introducing trusted third parties called responders that provide on-demand and up-to-date certificate status information. To validate a certificate, a client sends an OCSP status request to the appropriate responder and receives a signed status of the certificate. In its basic form, OCSP requires a clock on the client as it uses time-stamps to assure freshness. However, with an optional extension, OCSP supports use of nonces (20-byte random values) as an alternative to time stamps.

Although suitable for a large and well-connected infrastructure such as a private network or the Internet, OCSP is problematic in RFID systems. Its use would require a tag to generate a 20-byte random value and run an on-line (through a reader) challenge-response protocol with a responder every time it is presented with a reader certificate. As passive devices with very limited resources, RFID tags and are not designed to be good random number generators or handle long-lasting online communication protocols. More importantly, the assumption of every reader being always connected to the infrastructure is quite unrealistic. Further, the implementation of OSCP will require drastic changes in already well established PKI structures the RFID systems are currently employing.

Furthermore, depending on the application setting (e.g., e-Passports or rfid-enabled credit cards) the load on responders can become an issue. For example, millions of nearly simultaneous credit card transactions, each requiting a signed reply can result in congested responders and increase overall transaction delays.

3.3 Internal Clocks

Another trivial solution is to simply add an internal clock to an RFID tag. This would allow tags to accurately determine whether a certificate is expired and whether a non-revocation proof is current. However, a typical RFID tag is a passive device powered by radio waves emitted from a nearby reader. As such, it has no power source when a reader is not nearby. Since a clock needs uninterrupted power to work properly, it cannot be sustained by passive RFID tags. One might consider equipping RFID tags with batteries, however, this would raise a myriad of new problems, such as clock synchronization, battery replacement, maintenance costs and other robustness issues.

4 Proposed Solution

Our approach is designed for pk-based RFID systems. It has one simple goal: secure and reliable revocation checking on RFID tags. In the rest of this section, we discuss our assumptions and details of the proposed solution.

4.1 Assumptions

Our design entails the following assumptions:

1. Each tag is physically attended and owned by a human user who understands the operation procedure of the tag and is reasonably aware of the current date. (We elaborate on this in Section 4.5.)

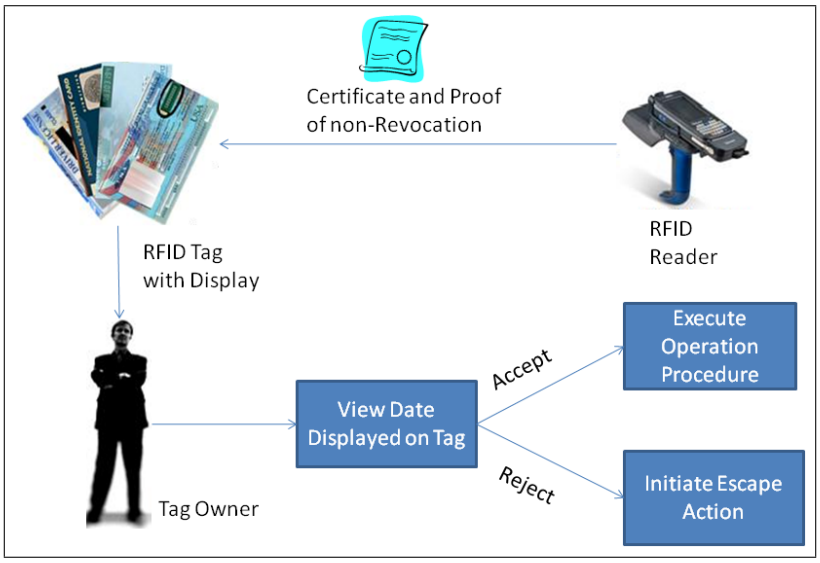

Fig. 1. CRL Validation Protocol for Tags with Display Units

2. Each tag is equipped with a small one-line character display capable of showing a 6-8 digit date in a reasonably legible format. (We describe the appropriate display technology and its feasibility in the context of e-Passports in Section 6.)
3. Each tag has a mechanism that allows it to become temporarily inaccessible to the reader, or that allows the user to explicitly "turn it off". (We address this assumption in more detail in section 4.3).
4. A tag can not be activated without the consent of the user. For example, in case of e-Passports, the tag is physically inside the passport which has a Faraday Cage in its cover pages. The user normally keeps the passport closed thus preventing any contact with the tag.
5. Each tag is aware of the name and the public key of a globally (in terms of the entire RFID system) trusted certification authority (CA).
6. The CA issues an updated revocation structure (e.g., a CRL) periodically. It includes serial numbers of all revoked reader certificates.
7. The CA is assumed to be infallible and correct: anything signed by the CA is guaranteed to be genuine and error-free, including, of course, all time-stamps.
8. While powered up by a reader, a tag is capable of starting and running a short timer.
9. A tag can store the last valid CRL issuance date it encountered.
10. [**Optional**] A tag may have *a single button* for user input.

4.2 Basic Idea

Before providing any information to the reader, a tag has to validate the reader's certificate. Recall our assumption that the user is physically near (e.g., holds) his tag during the entire process. Verification is done as follows:

1. The freshly powered-up tag receives the CRL and the reader certificate. Let T_{crl} and T_{cert} denote the purported CRL issuance and reader certificate expiration times, respectively.
2. If $T_{crl} \geq T_{cert}$, the tag aborts the protocol. Regardless of the validity of the CA signature on the certificate, this indicates an error, at best.
3. The tag checks whether the CRL includes the serial number of the reader certificate. If so, it aborts the protocol.
4. The tag checks CA signatures of the certificate and the CRL. If either check fails, the tag aborts the protocol.

5. The tag displays (to the user) T_{crl}, which is the lesser of the two values T_{crl} and T_{cert} (see step 2). It then enters into a countdown stage that lasts for a predetermined duration (e.g., 10 seconds).
6. The user views the date information on the display unit.
   [**OPTION A:**]
   (a) If T_{crl} is deemed sufficiently current (*i.e.,* sometime in the near future), the user does nothing and interaction between the tag and the reader resumes after the countdown stage.
   (b) Else, if T_{crl} is stale, the user terminates the protocol by initiating an escape action while the tag is still in countdown stage.
   [**OPTION B:**] (If Assumption 11 holds)
   (a) If T_{crl} is deemed sufficiently current (*i.e.,* sometime in the near future), user presses the button on the tag before the timer runs out, and communication with the reader continues normally.
   (b) Else, if T_{crl} is stale, the timer runs out and the tag automatically aborts the protocol (with no user action is needed).

4.3 Escape Actions

As evident from the protocol description above, escape action is required whenever the user decides that the displayed date (T_{crl}) is stale. Escape actions prevent malicious readers from gaining access to sensitive information stored on a tag. Although the choice of an escape action is likely to be application-dependent, we sketch out several simple and practical examples.

Using a Button Recent developments in low power hardware integration on contactless cards have led to deployment of buttons on RFID tags [22, 23]. On a button-equipped RFID tag, the user can be asked to press a button (within a fixed interval of time) as a signal of acceptance. If the button is not pressed within that interval, the protocol is terminated automatically by the tag. Thus, the escape action in this case is: user doing nothing. We recommend this implementation over the alternatives discussed below since it complies with *safe defaults* design principle. (*i.e.*, if no explicit approval is received from the user, a tag would automatically reject talking with a reader).

Faraday Cages A Faraday Cage is a jacket made of highly conductive material which blocks external electric fields from reaching the device it encloses. Since tags are powered by the electric field emitted from a reader, it is theoretically possible to isolate them from any reader access by simply enclosing them in a Faraday cage. Thus, in the context of tags that have an enclosing Faraday Cage – such as e-Passports that have one inside the cover pages – the natural escape action is to simply closing the passport.

Disconnecting Antennas An RFID tag communicates and receives power through the coil antenna attached to the chip. Disconnecting the antenna from a tag circuit would immediately halt any communication and shut down the tag. If a simple switch (even a mechanical one, e.g, a slide-switch operated by a finger) is placed between a tag and its antenna, a user can use it as the escape action. More such mechanical actions which result in the lack of communication between a tag and a reader (but are still reversible) are described in [24]. A drawback of such techniques is that physical damage to the tag is a possibility if the switch is handled roughly.

4.4 Efficient Revocation Checking

Although we hinted at using CRLs in the description of the basic idea, our approach would work with CRTs or any other off-line revocation scheme. However, both CRLs and even CRTs may wind up being quite inefficient as the number of revoked readers increase. The better of two, CRTs, would impose $O(log(n))$ bandwidth cost, where n is the number of revoked readers. With CRLs, the cost becomes $O(n)$.

Our goal is to minimize the bandwidth cost due to the transmission of revocation information by making it constant, i.e, $O(1)$. To achieve this, we take advantage of a previously proposed modified CRL technique that was originally intended to provide privacy-preserving revocation checking [14].

In traditional CRLs, the only signature is computed over the hash of the entire list. Consequently, the entire list must be communicated to the verifier. To make CRLs bandwidth-optimal, the technique in [14] requires the CA[3] to sign each (sorted) entry in a CRL individually, but binds it with the previous entry.

In more detail, the modified CRL technique works as follows: we assume that the CRL is sorted in ascending order by the revoked certificate serial numbers.

For a CRL with n entries, the CA generates a signature for the i-th entry ($1 < i \leq n$) as follows:

$$Sign(i) = \{h(T_{crl}||SN_i||SN_{i-1})\}_{SK_{RA}}$$

where, T_{crl} is the issuance time of this current CRL, SN_i is the i-th certificate serial number on the ordered CRL, SN_{i-1} is the immediately preceding revoked serial number, SK_{RA} is the secret key of the CA and h is a suitable cryptographic hash function. To mark the beginning and the end of a CRL, CA uses two well-known sentinel values: $+\infty$ and $-\infty$. The CA signs the beginning and the end of a CRL as follows.

$$Sign(1) = \{h(T_{crl}||SN_1|| - \infty)\}_{SK_{RA}}$$
$$Sign(n+1) = \{h(T_{crl}|| + \infty||SN_n)\}_{SK_{RA}}$$

Assuming it is not revoked, when authenticating to a tag, a reader provides its own certificate as well as the following constant-size non-revocation proof:

$$SN_j,\ SN_{j-1},\ T_{crl},\ Sign(j)$$

where reader certificate serial number SN_{rdr} is such that $SN_{j-1} < SN_{rdr} < SN_j$

The reader certificate along with the above information allows the tag to easily check that: (1) the range between adjacent revoked certificate serial numbers contains the serial number of the reader's certificate, and (2) the signature $Sign(j)$ is valid. If both are true, the tag continues with the authentication protocol by displaying T_{crl}, as in step 5 in Section 4.2.

Storage Overhead: with traditional CRLs, readers must store entire lists of revoked certificate numbers. This can cause significant storage overhead. In the above method, storage overhead for both readers and tags is negligible since only one signature, two certificate serial numbers and the issuance date are needed for effective revocation checking.

Computational Overhead: the modified CRL method calls for the CA to separately sign each CRL entry, whereas, only one signature is needed for a traditional CRL. Although this translates into significantly higher computational overhead for the CA, we note that CAs are powerful entities running on high-end resource-rich systems and new CRLs are issued periodically, i.e., typically not every minute of every hour. Computation overhead for tags is minimal in the modified CRL scheme. Verifying traditional CRLs requires hashing $O(n)$ serial numbers, in contrast to hashing a constant-length tuple in modified CRLs. On the other hand, both methods require one signature verification which usually overshadows the cost of hashing.

Communication Overhead: CRLs impose linear communication overhead, whereas, the modified CRL method is bandwidth-optimal, requiring only the transmission of two serial numbers, issuance date and a signature.

4.5 Security and Cost

Security Considerations: Assuming that all cryptographic primitives used in the system are secure and the user executes necessary escape actions in case of expired (or revoked) reader certificate, the security of the proposed reader revocation checking mechanism is evident.

[3] In practice, a separate entity called a Revocation Authority (RA)

We acknowledge that user's awareness of time and ability to abort the protocol (when needed) are crucial for the overall security. To this end, we conducted some usability studies, including both surveys and experiments with a mock-up implementation. As discussed in section 5, our studies showed that people are reasonably aware of date and also able to execute the protocol with low error rates.

At the same time, awareness of date/time among general population is quite universal [25]. Thus, we can assume that people, especially those who might be exposed to this technology, are reasonably aware of current date and time (especially in the case of e-Passport reader revocation checking, since people are more likely to remember the date with much better accuracy while traveling). Although human errors on the order of hours are to be expected, this is not a problem for most RFID systems since revocation update periods are usually measured at least in days, or more commonly in weeks or months.

Another critical assumption about, and requirement for, the user is the undivided attention during the reader authentication process and the ability to react whenever a stale expiration or revocation date is observed. However, we believe that users can be educated – e.g., via manuals and warning labels – about the meaning of their participation in the protocol and operation procedure of their tags.

Cost Assessment: Recent technological advances have enabled mass production of small inexpensive displays that can be easily powered by high-end RFID tags aided by nearby readers. Notable examples are ePaper and OLED. The current (total) cost of an ePaper display-equipped and public key-enabled RFID tag is about 17 Euros in quantities of $100,000$ and the cost goes down appreciably for quantities in the one million range [23]. Although this might seem high, we anticipate that the cost of cutting-edge passive display technologies (i.e., ePaper and OLED) will sharply decrease in the near future. Moreover, once a display is available, it can be used for other purposes, thus amortizing the expense. Below, we briefly describe some possible alternative uses for an RFID display:

- **Transaction Verification:** RFID tags are commonly used as payment and transaction instruments (e.g., credit cards, insurance IDs and voting cards). In such settings, a direct auxiliary channel between the tag and the user is necessary to verify the details of a transaction. This problem becomes especially apparent with payment applications. A malicious (but not necessarily revoked) reader can easily fool the tag into signing or authorizing a transaction for an amount different from that communicated to the user (e.g., via a paper receipt printed by the reader). A display on a contactless payment card would solve this problem by showing the transaction amount requested by the reader on its display and waiting for explicit user approval before authorizing it.
- **Device Pairing:** A display may be used for secure pairing of tags with other devices (such as laptops, mobile phones, etc.) that do not share a CA with the tag. For example, Ullman proposes a technique for secure connection establishment with RFID tags using an attached display [21]. Also, other visual channel-based secure device pairing methods that are proposed for personal gadgets can be used with display-equipped RFID tags (See [26] and [27] for an extensive survey of such methods). The ability to establish a secure ad hoc connection with arbitrary devices is a new concept for RFID tags that might open doors for new applications, e.g., the use of NFC-capable personal devices (PDAs or cell-phones) to change and control settings on personal RFID tags.
- **User/Owner Authentication:** In some scenarios, it might be necessary for a user to authenticate to a tag (e.g., credit card or passport). Currently this can be done only via trusted third party devices such as mobile phones [28], personal computers and wearable beepers [29]. However, in the future, if a display-equipped RFID tag also has a small input interface (e.g., a keypad), the need for third parties might be obviated.

5 Usability

Since our technique requires active user involvement, its usability is one of the key factors influencing its potential acceptance. Moreover, due to the nature of the protocol, certain type of user errors (i.e., accepting an incorrect or stale date) can result in a loss of security. Thus, we conducted two separate usability studies: online surveys and hands-on usability experiments. The goal of these studies was to answer the following questions:

1. Do everyday users worry about the reader revocation problem?
2. How do prospective users rate the usability of our solution?
3. Are average users reasonably aware of current date? And, what are the expected error rates?

5.1 On-line Survey

We created a comprehensive online survey [30] which was used to anonymously sample 98 individuals. After collecting some basic demographic data (with only five questions), survey participants were given an explanation of the reader revocation problem in plain English. Then, they were presented with our approach where all necessary user interaction (using text and images) and the sequence of required actions were explained in detail. Next, participants rated the proposed technique via the 10-question System Usability Scale (SUS) [31]. They also answered 4 additional questions, as discussed later in this section.

Subject Background 98 individuals completed the (anonymous) online survey. The subjects were typically students, working professionals, and faculty who were recruited through social network postings and mailing lists. The survey-takers tended to be on the younger side, with ages distributed as follows:
(1) 58% – 18-24, (2) 29% – 25-29 range, and (3) 13% over 30
Gender distribution was 78% male and 22% female. The subjects were generally well-educated with 97% having a bachelor's or higher degree.

Survey Results The proposed reader revocation technique received a score of 68/100 on the system usability scale (SUS). This is almost 10% higher than the industry mean SUS score of 62.1% [32]. 66% of the participants stated that they would like to see this solution implemented on their passports, while 26% were neutral and the average score on 5-point Likert scale was 3.67 with standard deviation of 0.87.

On the other hand, 84% of the participants were worried about identity theft and 88% stated that they are concerned about revealing personal information to unauthorized parties in general.

When participants were asked about their general awareness of the current date, 40% indicated that they are usually aware of the exact date, 35% were confident to know it with at most one-day error margin, while 22% claimed to be within the +/- 3-day range. The remaining 3% indicated that 7 or more days error would be possible as far as their current date awareness.

5.2 Usability Testing

In order to assess the usability of our method vis-a-vis real users, 25 subjects were recruited to take part in the usability study. Tests were conducted at a variety of campus venues, depending mainly on the subjects' preferences. They included: cafés, student housing, classrooms, offices and outdoor settings.

Apparatus and Implementation Our mock-up was implemented using two mobile phones: a Nokia N95 [33] (simulating the tag) and a Nokia E51 [34] (simulating the reader). These devices were chosen since, at the time of this study, actual RFID tags with displays and buttons could not be ordered in modest quantities. We used *Bluetooth* as the wireless communication medium between the N95 and E51. All implementation code was written in Java Mobile Edition. On the N95, the smallest button next to the display was programmed to act as the accept button and the time period for automatic reject was set to 10 seconds.

Subject Background Our study participants were mainly students at the University of California, Irvine. Participants' age was quite well distributed and fell into three groups:
(1) 36% – 18-24, (2) 32% – 25-29 range, and (3) 32% over 30
Gender distribution was controlled for and participants' were thus almost evenly split between male and females (52% and 48%, respectively). Of the 25 subjects, 48% were physical/natural science majors,

28% – engineering majors, and the remaining 24% – social science majors. Due to the specifics of the venue (university campus), the average participant was quite well-educated with 80% having at least a bachelor's degree.

Testing Procedure Participants were first given a brief overview of our method, this usability study and its goals. Then, they were presented with the mock-up implementation. After testing it six times in succession, each participant was asked to fill out a post-test questionnaire. Participants were encouraged to ask questions before – but not during – the usability tests were carried out. They were also advised not to consult any source of current data/time before and during the tests. Specifically, they were asked not to look at their watches or phones.

The set of dates used in the testing process was: +/-1 day, -3 days, +7 days, -29 days, and -364 days from the actual test date[4]. All experiments were conducted during the first week of December 2009, and choices of -29 days and -364 days were deliberate to make the staleness of these dates more deceiving to the subjects. For example, for a test date of 12/03/09, such cases resulted in 11/04/09 and 12/04/08 being displayed, respectively.

Test cases were presented to each participant in a random order. The test administrator was holding the phone simulating the reader and was sending a date to the device held by the subject, which simulated the e-Passport. After a date was displayed on the "e-Passport", the test subject was asked to decide whether to: (1) accept it by pressing the button within ten seconds, or (2) reject it by doing nothing. The process was repeated for all six test-cases.

Test Results Completion Time and Error Rates: For subjects accepting the displayed date, the study yielded the average completion time of 3.07 second, with sample standard deviation of 1.58 seconds. This shows that the subjects were quite fast in reacting whenever they considered the date to be current. This also shows that our choice of a 10-second time-out period was appropriate.

Among the 25 subjects, the rate of false negatives (rejecting a date that was not stale) was quite low. No one rejected a date that was one day in future, and only one subject (4% of the sample population) rejected the date that was seven days in the future.

The rate of false positives, i.e., accepting a stale date, were also low in all cases, except one. When subjects were shown dates that were: 1, 3 and 29 days earlier, the error rates were 0%, 0% and 4% respectively. However, surprisingly, the error rate spiked up to 40% when subjects were shown a date that was 364 days earlier. We discuss the possible reasons for this high error rate as well as how it can be addressed in Section 5.3 below.

User Opinion: People who tried our mock-up implementation on cell-phones rated its usability at 77% on the System Usability Scale (SUS) [31], a score that is about 13% higher than that obtained from the on-line survey. 84% of the subjects who tested our implementation stated that they would like this system to be implemented on their own e-Passports, while 12% were neutral to the idea. The average score on a 5-point Likert scale was 4.1 with standard deviation of 0.75.

5.3 Discussion

Based on the results of the usability studies, we can now attempt to address the questions raised in the beginning of this section:

Are people worried about the problem we aim to solve? Among the total of 123 participants (98+25, in both studies) 88% are worried about revealing information to unauthorized parties. Moreover, 70% said that they wanted to see the proposed technique implemented on their e-Passports.

[4] "+/-" indicates future/past dates, respectively.

How do people rate the usability of our approach? Given the detailed description of the method and the required interaction, 98 participants rated its usability at 68% on the SUS questionnaire. The usability rating was even higher, at 77%, for the 25 subjects who experimented with our mock-up implementation. Both scores are well above respective industry averages and indicate good usability and acceptability characteristics.

Are users reasonably aware of current date? As results show, our method very rarely results in false negatives: users are quite capable of not claiming valid (future) dates as being in the past.

As far as false positives, however, the results are split. Stale days and months are, for the most part, easily recognized as such by the users. However, with the stale (past) year, the observed error rate is quite high (40%). This deserves a closer examination. While we do not claim to know the exact reason(s), some conjectures can be made.

When confronted with a date, most people are conditioned to first check day and month, e.g., current dates on documents and expiration dates on perishable products. At the same time, users do not tend to pay as much attention to more gross or blatant errors (such as a stale/past year) perhaps because they consider it to be an unlikely event. Also, we note that among 6 test-cases for each user, just one had a date with the wrong year. This may have inadvertently conditioned the participants to pay more attention to the month/day fields of the dates.

We anticipate that, in practice, year mismatches will be rare since the tags will record *valid* dates (authorized by the user), including the year. Therefore, wrong year values will be mostly detected by the tags themselves, before any user interaction. Of course, this is not a comprehensive solution, especially, for tags that are used very infrequently.

On the other hand, more comprehensive user-studies are needed to evaluate whether certain changes in date representation and formatting would help to lower the observed error rates. For example, displaying a date in YYYYMMMDD (e.g., 2009Dec03) format, instead of MM/DD/YY (e.g., 12/03/09), may help users to pay more attention to the year field.

6 Sample Application: e-Passports

Fig. 2. Sample e-Passport with a Display Unit

In 2004, the International Civil Aviation Organization (ICAO) proposed a set of standards [6] for electronic passport (e-Passport) implementations which made use of RFID and Biometric technology in an attempt to improve border security. Since then, there have been several major revisions to e-Passport standards proposed by the ICAO, European Union, and the German Federal Office for Information Security (BSI)[5]. The last proposed set of standards for e-Passports was published by the BSI in October 2008 [5]. This specification document effectively mitigates almost all previously criticized security problems on e-Passports, except one – certificate revocation checking.

In this section, we take e-Passport system as a case study and discuss how our solution can be integrated into the current standards to address the problem of revocation check on e-Passport tags. We start by describing the basics of the current e-Passport PKI system. Then, we explain how e-Passport operation procedure can be modified to include our solution and finalize our case study with feasibility and power analysis of embedding a functional display onto e-Passport tags.

6.1 e-Passport Public Key Infrastructure

The key elements in the Public Key Infrastructure (PKI) for e-Passports are the Country Verifying Certificate Authority (CVCA), the Document Verifiers (DV), and Inspection Systems (*a.k.a* readers). The primary role of the CVCA of a state is to issue certificates to Document Verifiers (national and international) and determine their access rights to e-Passports issued by the state.

The Document Verifier is a body that operates between readers and the CVCA. It is authorized by the CVCA to issue certificates to readers in its domain. The certificates issued by the Document Verifier to the readers contain information such as their access rights and validity period. The access rights and validity period of readers are restricted by the values issued to their Document Verifier by the CVCA. In order to access data on an individuals e-Passport, the reader must have the Document Verifier certificate issued to it by the individuals' home state. To achieve this, the Document Verifier distributes all Document Verifier certificates (it received from other CVCA's) to every reader it is responsible for. For easy distribution, the ICAO (International Civil Aviation Organization) provides a Public Key Directory (PKD) which contains the public keys of all participating Document Verifiers [6].

6.2 Certificate Validation in e-Passports

Every Certificate (issued by a CVCA or a Document Verifier) has a validity period which is defined by its effective date (T_{eff}) and expiration date (T_{exp}). During the certificate validation process, the e-Passport tag uses its *(estimated)* current date (T_{curr}) stored in a non-volatile register to determine whether a certificate has expired or not. When presented with a reader certificate and a CRL, an e-Passport tag does the following:

1. verifies the signatures (of the CVCA / DV) on the presented certificate and the CRL.
2. verifies that the presented certificate is not listed in the CRL.
3. confirms that T_{exp} is greater than T_{curr}.
4. If all the above steps are completed successfully, the certificate is deemed valid. If the effective date of a valid certificate is greater than T_{curr} value stored in the date register, tag also updates T_{curr} to the effective date of the certificate.

After the validation phase is successfully completed, e-Passport tag-reader interaction continues with access control and the two (passive and active) authentication phases as described in the standards [6, 5].

6.3 Modified e-Passport Operation Procedure

In order to integrate our solution, e-Passports themselves and their operation procedures have to be modified. The change needed on e-Passports is the mere replacement of current tags with ones that have attached displays. Figure 2 shows how such e-Passports may look like. The modified e-Passport operation procedure that integrates our solution is summarized in Figure 3. Please note that only the validation phase is modified to integrate our solution.

[5] BSI stands for Bundesamt fur Sicherheit in der Informationstechnik.

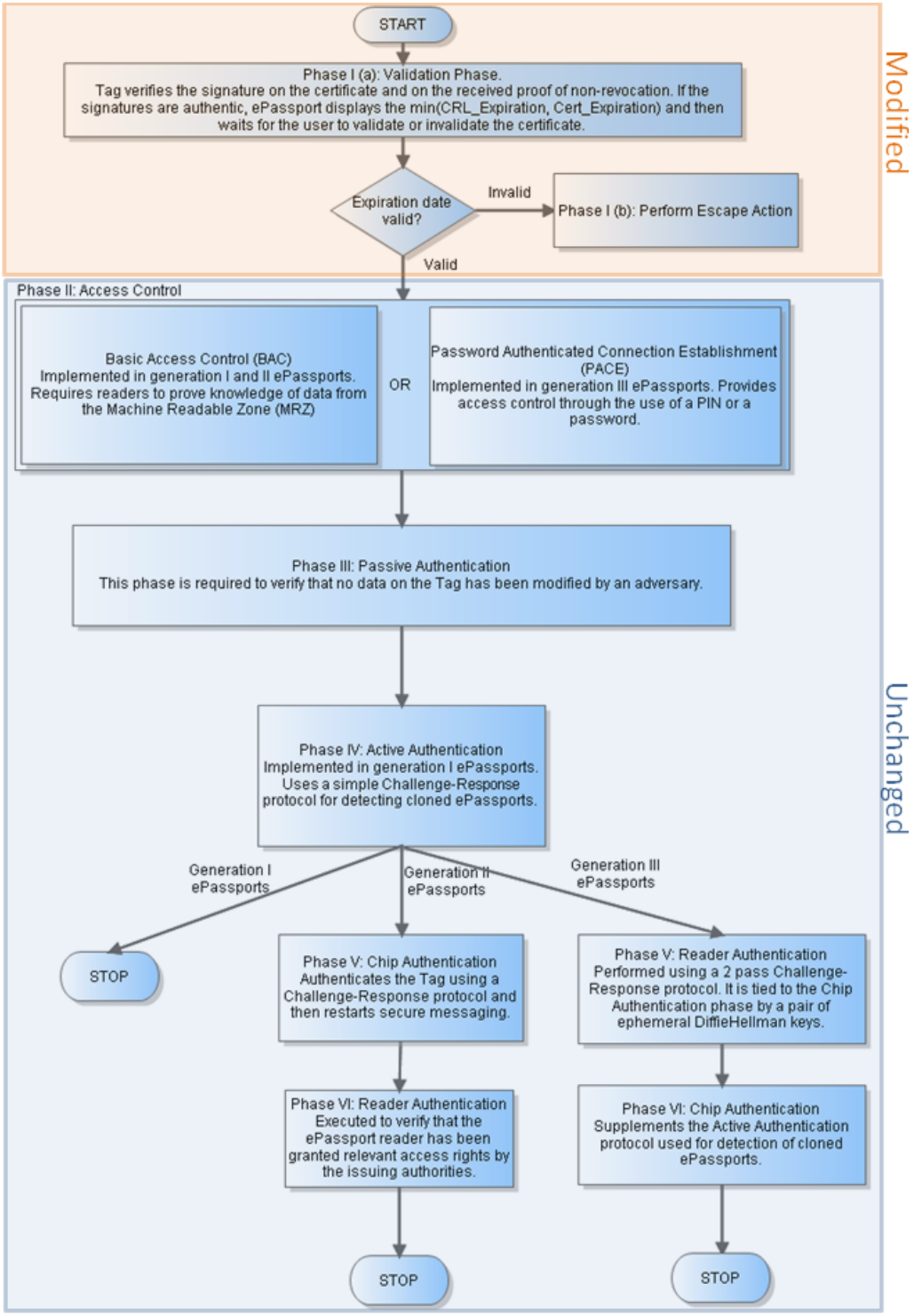

Fig. 3. Modified e-Passport Operation procedure

6.4 Feasibility Analysis

Low Power Display Technologies Since e-Passport tags are passive in nature and cannot supply continuous power to attached peripherals, we require that the eight or ten digit display unit used in the e-Passport is operating with minimal power consumption. For this, we propose the use of display technologies such as ePaper, OLED, and other such low-power bistable displays [35]. These displays require power of the order of 100mW (for a 2" display unit) during display updates and 1mW of power during standby. There are several suitable low power display technologies available in the market today (eInk Segmented Displays [36], SiPix Microcup [37], NemOptic BM [38], Kent Displays Incorporated eCards [39]).

Power Analysis e-Passport tags such as those supplied by Infineon Technologies, require up to 55mW of power to operate [40] while the display unit requires a maximum power of 100mW to operate. We analyze the maximum power requirements of the proposed system and its effect on the maximum working distance on current readers.

The power required by the e-Passport circuit to operate will be ∼155mW (the sum of the power required by the tag and Display), with circuit parameters set in the manner described by Scholz *et al.* [41]. First, we establish a relationship between the mutual inductance (M) and the distance (x) between the antenna of the tag and the reader.

$$M = \frac{\mu\pi N_1 N_2 (r_1 r_2)^2}{2\sqrt{(r_1^2 + x^2)^3}} \tag{1}$$

Where μ is the Permeability $[H/m]$; N_1 and N_2 are the number of turns in the antennas of the tag and reader; r_1 and r_2 are the radii $[mm]$ of each of these turns. Substituting default values we get the relation

$$M = \frac{1.57 \times 10^{-12}}{x^3} \tag{2}$$

Now we establish a relationship between the power required by the tag (P_{Tag}) and distance (x). This is done through the series of equations below.

$$P_{Tag} = I_1^2 R_T \tag{3}$$

Where I_1 is the current running in the reader circuit $[mA]$ and R_T represents the tag impedance which is given by (4).

$$R_T = \frac{M^2 R_L}{L_2^2} \tag{4}$$

Where L_2 is assigned a value of 168nH [41] and R_L is the load resistance given by (5).

$$R_L = \frac{V_T^2}{P_{Tag}} \tag{5}$$

V_T is the voltage required in the tag circuit (5.5 Volts). And the value of R_L is 195.1 Ω. Finally, by combining equations 2 through 5, we can get a relationship between x and P_{Tag}.

$$x^6 = \frac{(1.57 \times 10^{-12})^2 \times (I_1)^2 \times (R_L)}{P_{Tag} \times (L_2)^2} \tag{6}$$

Making the necessary substitutions, we get the following value for x, where x represents the maximum possible operating distance:

$$P_{Tag} = 155\ mW,\ R_L = 195.1\ \Omega \Longrightarrow x = .069\ m\ (6.9\ \text{cm}) \tag{7}$$

Compared to the working distance of 9.7cm for an e-Passport tag without a display unit, even with the current reader and antenna specification, adding a display reduces the maximum operating distance between the tag and reader only by 2.8 cm. Therefore, adding a display unit to the current e-Passport circuit is feasible and does not require any changes for the power specifications in the original proposal [5]. Longer operating distances can also be achieved with small modifications of the RFID antenna design or by increasing the power of a reader.

7 Conclusions

In this paper, we presented a simple and effective method for dealing with reader revocation checking on pk-enabled RFID tags. Our solution requires a tag to be equipped with a small display and be attended by a human user during certificate validation. As long as the user (tag owner) plays its part correctly, our solution eliminates the period of vulnerability with respect to revoked readers.

Recent advances in display technology, such as ePaper and OLED, have already yielded inexpensive display-equipped RFID tags. The low cost of these displays combined with the better security properties and potential new application domains make displays on RFID tags a near reality. Moreover, our usability studies suggest that users find this solution usable and they are capable of performing their roles within reasonable error rates.

We believe that display-equipped RFID tags will soon be in mass production and the method proposed in this paper will be applicable to a wide variety of public key-enabled tags.

References

1. Micali, S.: Certificate revocation system. United States Patent (September 1997) US Patent 5,666,416.
2. Housley, R., Ford, W., Polk, W., Solo, D.: RFC 2459: Internet X.509 public key infrastructure certificate and CRL profile (January 1999) Status: PROPOSED STANDARD.
3. Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: Internet public key infrastructure online certificate status protocol- ocsp (1999)
4. Zeller, T.: Black market in stolen credit card data thrives on internet. The New York Times (June 2005)
5. Bundesamt fur Sicherheit in der Informationstechnik: Advanced Security Mechanisms for Machine Readable Travel Documents : Version 2.0. (2008)
6. International Civil Aviation Organization: Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability. (2006)
7. Tsudik, G.: Ya-trap: Yet another trivial rfid authentication protocol. Pervasive Computing and Communications Workshops, IEEE International Conference on **0** (2006) 640–643
8. Kocher, P.C.: On certificate revocation and validation. Lecture Notes in Computer Science **1465** (1998)
9. Merkle, R.C.: Secrecy, authentication, and public key systems. Technical report, Stanford University (June 1979)
10. Goodrich, M., Tamassia, R.: Efficient authenticated dictionaries with skip lists and commutative hashing (January 13 2001)
11. Naor, M., Nissim, K.: Certificate revocation and certificate update. Technical report (March 01 1999)
12. Micali, S.: Efficient certificate revocation. Technical Memo MIT/LCS/TM-542b, Massachusetts Institute of Technology, Laboratory for Computer Science (March 1996)
13. Lamport, L.: Password authentication with insecure communication. (1981)
14. Narasimha, M., Solis, J., Tsudik, G.: Privacy preserving revocation checking. International Journal of Information Security **8**(1) (February 2009) 61 – 75
15. Monnerat, J., Vaudenay, S., Vuagnoux, M.: About Machine-Readable Travel Documents. In: Conference on RFID Security, Malaga, Spain (July 2007)
16. Hoepman, J.H., Hubbers, E., Jacobs, B., Oostdijk, M., Wichers Schreur, R.: Crossing Borders: Security and Privacy Issues of the European e-Passport. In Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S.i., eds.: Advances in Information and Computer Security, First International Workshop on Security – IWSEC. Volume 4266 of Lecture Notes in Computer Science., Kyoto, Japan, Springer-Verlag (October 2006) 152–167
17. Heydt-Benjamin, T.S., Bailey, D.V., Fu, K., Juels, A., O'Hare, T.: Vulnerabilities in First-Generation RFID-Enabled Credit Cards. Manuscript (October 2006)
18. Cheon, J.H., Hong, J., Tsudik, G.: Reducing RFID Reader Load with the Meet-in-the-Middle Strategy. Cryptology ePrint Archive, Report 2009/092 (2009)
19. Oren, Y., Feldhofer, M.: A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes. In: Proceedings of the second ACM Conference on Wireless Network Security – WiSec'09, Zurich, Switzerland, ACM (March 2009)
20. Blundo, C., Persiano, G., Sadeghi, A.R., Visconti, I.: Resettable and Non-Transferable Chip Authentication for ePassports. In: Conference on RFID Security, Budapest, Hungary (July 2008)

21. Ullman, M.: Flexible visual display units as security enforcing component for contactless smart card systems. In: The First International EURASIP Workshop on RFID Technology, Vienna, Austria (September 2007)
22. Kugler, D., Ullman, M.: Contactless security tokens - enhanced security by using new hardware features in cryptographic based security mechanisms. In: Dagstuhl Seminar Proceedings of Foundations for Forgery - Resilient Cryptographic Hardware. (July 2009)
23. Ullman, M. personal communication (Sept 2009)
24. Karjoth, G., Moskowitz, P.A.: Disabling rfid tags with visible confirmation: clipped tags are silenced. In: WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, New York, NY, USA, ACM (2005) 27–30
25. Whitrow, G.: Time in history: the evolution of our general awareness of time and temporal perspective. Oxford University Press (1988)
26. Kumar, A., Saxena, N., Tsudik, G., Uzun, E.: Caveat eptor: A comparative study of secure device pairing methods. Pervasive Computing and Communications, IEEE International Conference on **0** (2009) 1–10
27. Kobsa, A., Sonawalla, R., Tsudik, G., Uzun, E., Wang, Y.: Serial hook-ups: a comparative usability study of secure device pairing methods. In: SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security, New York, NY, USA, ACM (2009) 1–12
28. Saxena, N., Uddin, M.B., Voris, J.: Treat 'em like other devices: user authentication of multiple personal rfid tags. In: SOUPS. (2009)
29. Kaliski, B.: Future directions in user authentication. In: IT-DEFENSE. (2005)
30. : Display enabled identification and payment instruments. `http://www.ics.uci.edu/~rishabn/survey.html` (November 2009)
31. Brooke, J.: Sus - a quick and dirty usability scale. In: Usability Evaluation in Industry. (1996)
32. Lewis, J., Sauro, J.: The factor structure of the system usability scale. In: Proceedings of the Human Computer Interaction International Conference (HCII 2009), San Diego CA, USA. (2009)
33. : Nokia n95 specifications. `http://www.nokiausa.com/find-products/phones/nokia-n95-8gb/specifications`
34. : Nokia e51 specifications. `http://europe.nokia.com/find-products/devices/nokia-e51/specifications`
35. Kahn, B., Zervos, H.: Displays and lighting: Oled, epaper, electroluminiscent and beyond. Technical report, IDTechEx (2008)
36. E Ink Corporation: Segment Display Cell: Custom + Standard ePaper Designs. (2008)
37. SIPIX Imaging: SIPIX: Segmented ePaper Displays. (2006)
38. Nemoptic: BM100: BiNem Module - Reflective Display. (2008)
39. Green, A., Montbach, E., Miller, N., Davis, D., Khan, A., Schneider, T., Doane, W.: Energy efficient flexible reflex displays. Technical report, Kent Displays, Inc. (2008)
40. Infineon Technologies AG, AIM CC: Preliminary Short Product Information: Chip Card and Security IC's. (2006)
41. Scholz, P., Reihold, C., John, W., Hilleringmann, U.: Analysis of energy transmission for inductive coupled rfid tags. International Conference on RFID (2007)