Readers Behaving Badly: Reader Revocation in PKI-Based RFID Systems

Rishab Nithyanand, Gene Tsudik, and Ersin Uzun
Computer Science Department, University of California, Irvine

University of California, Irvine CA 92697, USA
{rishabn,gts,euzun}@ics.uci.edu

Abstract. Recent emergence of relatively inexpensive 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 can not use traditional (time-based) off-line revocation checking methods. Whereas, on-line methods require unrealistic connectivity assumptions.

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 on "high-end" RFID tags. Our approach does not assume any on-line connectivity and involves a very small constant increase in tag-reader bandwidth and tag storage. The main extra feature is the requirement for a small passive on-tag display. However, as discussed in the paper, modern low-power (e.g., e-paper and OLED) display technology is low-cost and appealing for other (e.g., authentication) 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 tags used in e-passports, electronic ID (eID) Cards, eLicenses, and eCredit-cards. 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 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, in turn, can be done off-line, using Certificate Revocation Lists (CRLs) [2] and similar structures, or on-line, using protocols 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. (Recall that an RFID reader is basically a full-blown computing device equipped with usual resources.) 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 identifies itself to a reader (e.g., by encrypting its identity 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, 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. For instance, in case of e-passports, a tag might reveal biometric and other personal information. In case of payment instruments, a tag might disclose its credit card account number.

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

[1] The only exception is Certificate Revocation System (CRS) [1] which is purely implicit.
[2] "Prematurely" means before the expiration of the certificate (PKC).

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:

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

The first step is easy for any pk-enabled tag and has been already incorporated into some reader authentication schemes, e.g., [4] [5]. 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 $O(logn)$ – a non-negligible number for large values of n (where n is the number of readers in the system).

On the other hand, on-line revocation checking (e.g., OCSP) would entail the tag contacting (via the reader) a trusted OCSP Validation Agent (VA). The proof of non-revocation would be short and constant-size, however, the connectivity and the availability requirements would be problematic. If an OCSP VA 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 VAs is problematic. A VA 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, [6] 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 BSI [4] for certificate validation. 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, RFID tags with small (6-8 digit) displays have been demonstrated.
- 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 take an escape action and aborts the interaction with the reader. Otherwise, the interaction proceeds.

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 a case study with the application of the solution to ePassports in section 5. We finalize the paper with our conclusions in section 6.

2 Related Work

There have been many general proposals for dealing with certificate revocation in distributed systems and networks. Of these, the 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) [7] use Merkle's Hash Trees [8] to provide short proofs of (non-)revocation.
- Skip-lists [9] and 2-3 Trees [10] 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 and bandwidth requirements and provides timely revocation status information.
- Certificate Revocation System [1, 11] is the first technique for fully implicit certificate revocation. It takes advantage of hash chains [12] to provide compact proofs of certificate validity.

– Other related results focused on privacy issues in certificate revocation checking, e.g., [13].

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 PK-based RFID systems, e.g., [14, 15] in ePassports, [16] in eCredit-Cards, and [17, 18] in other applications.

As mentioned earlier, the only somewhat viable approach [6] suggested using a monotonically increasing counter (register) as a kind of a loosely synchronized clock. Although, this solution is used in the latest ePassports standard [4], 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. [19].

To the best of our knowledge, the idea of outfitting pk-enabled RFID tags with display units for enhanced security was introduced by Ullman [20]. 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 tag display to solve the problem of revocation checking. Unlike the register-based method [13], 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 more recent than D_{curr} on the tag.
3. If previous steps are completed successfully, the tag accepts the certificate. Moreover, if D_{eff} is more recent 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 protocols, such as Online Certificate Status Protocol (OCSP) [3], help reduce memory constraints on the clients by introducing trusted third parties called Verification Authorities (VAs) 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 VA and receives a signed status of the certificate.

Although it is well-suited for a large and connected infrastructure such as a private network or the Internet, OCSP is problematic in RFID systems. Its use would require a tag to go on-line (through a reader) and connect to a VA every time it is presented with a reader certificate. As passive devices with very limited resources, RFID tags and are not designed to handle long-lasting online communication protocols. More importantly, the assumption of every reader being always connected to the infrastructure is quite unrealistic. Finally, as pointed out above, constant availability of VAs and their high request throughput raise some concerns.

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 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.)

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 ePassports in Section 5.)
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 periodically issues an updated revocation structure (e.g., a CRL) that include all serial numbers of 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. Each tag user/owner knows the periodicity of revocation issuance.
9. While powered up by a reader, a tag is capable of starting and running a short timer.
10. [**Optional**] A tag may store the last valid CRL issuance date it encountered.
11. [**Optional**] A tag may have *a single button* for user input.

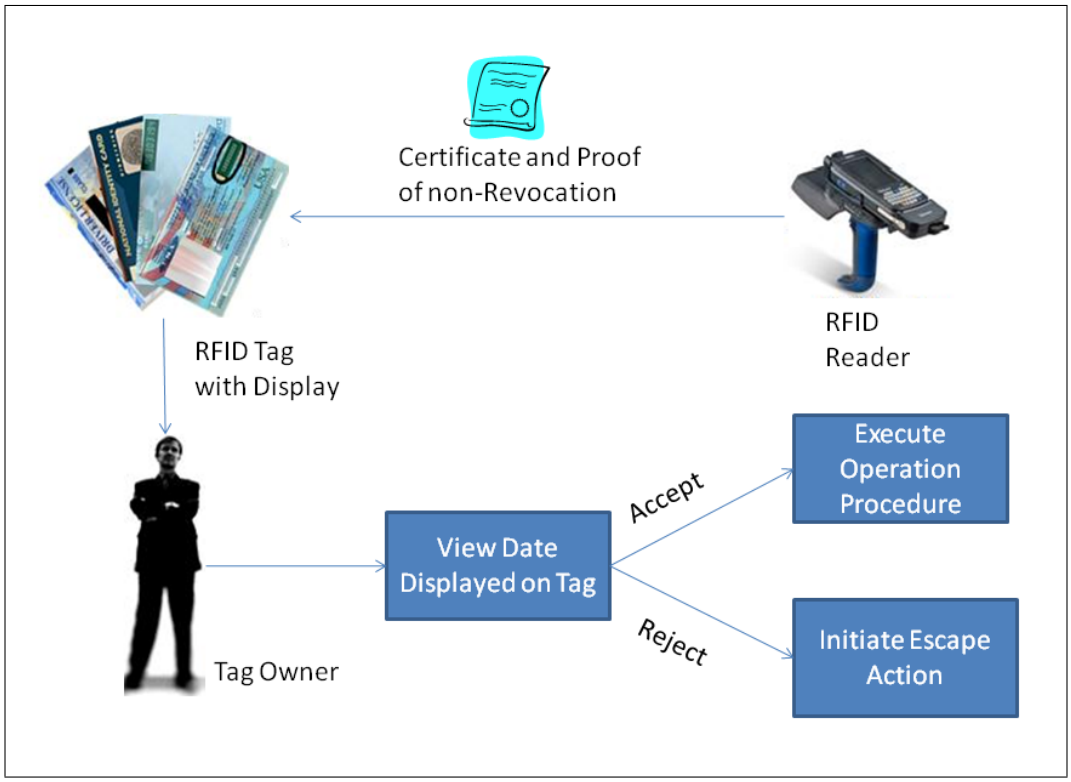

Fig. 1. CRL Validation Protocol for Tags with Display Units

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) the lesser of the two values, i.e. $T_{min} = MIN(T_{crl}, T_{cert})$. It then waits for input and 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:**]
   – If T_{min} is deemed sufficiently current, the user does nothing and communication between the tag and the reader resumes after the countdown stage.
   – Else, if T_{min} 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)
   – If T_{min} is deemed sufficiently current, the user initiates an approval action, e.g, by pressing a button on the tag.
   – Otherwise, either the timer runs out (and no user action is needed) or the user initiates an escape action.

4.3 Escape Actions

As evident from the protocol description above, escape action is required whenever the user decides that the displayed expiration or revocation date (T_{min}) 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.

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[3] 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 ePassports that have one inside the cover pages – the natural escape action is to simply close the passport.

[3] A rump session talk at PETS'09 shed some doubts on today's Faraday Cage-enclosed e-passports.

Disconnecting the Antenna 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.

Halting User Interaction Some RFID protocols and systems (e.g., [4]) require users to enter a PIN or a password into the reader. In such cases, it is natural for a user to terminate a protocol by simply not providing this information. For this approach to be viable, completion of the timer countdown without any user input would be one possible escape action.

4.4 Efficient Revocation Checking

Although we hinted at using CRLs in the description 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 [13].

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 [13] requires the CA[4] 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 according to 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 the 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 revocation information:

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

[4] In practice, a separate entity called a Revocation Authority or RA

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 so, the tag continues with the authentication protocol by displaying the smaller of: T_{exp} and T_{crl}, as in Step 5 in Section 4.2.

Assessment

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 a 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 or stale revocation proof, the security of the proposed reader revocation checking mechanism is evident. However, we readily acknowledge that user's awareness of time and ability to abort the protocol (when needed) are crucial for the overall security.

It is safe to say that, today, awareness of date/time among people is quite universal [21]. Thus, we can assume that people, especially those who might be exposed to this technology, are reasonably aware of current date and time. Although human errors on the order of hours are to be expected, this is not a problem for most RFID systems since CRL update periods are usually measured in (at least) days.

Another critical assumption about, and requirement for, the user is the undivided attention during the reader authentication process and the ability to execute an escape action when a stale expiration 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.

Moreover, taking the *safe default* approach in reader authentication would help eliminate security critical user errors by requiring explicit user approval before disclosing any sensitive information from the tag.[5]

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 $100,000$. The cost goes down appreciably for quantities in the one million range [22]. Although this might seem high, we note that once a display is available, it can be used for other purposes, thus amortizing the expense. We also anticipate that the cost of cutting-edge passive display technologies (i.e., ePaper and OLED) will sharply decrease in the near future. Below, we briefly describe some possible alternative uses for an RFID display.

- **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 [20]. Also, other visual channel-based secure device pairing methods that were proposed for personal gadgets can be used with display-equipped RFID tags. (See [23] and [24] 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.
- **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 the tag would solve this problem by showing the user the transaction amount supplied by the reader and wait for explicit user authorization.
- **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 [25], personal computers and wearable beepers [26]. However, in the future, if a display-equipped RFID tag also has a small input interfaces (e.g., a keypad or a fingerprint scanner) the need for third parties might be obviated.

5 A Case Study: ePassports

In 2004, the International Civil Aviation Organization (ICAO) proposed a set of standards [5] for electronic passport (ePassport) implementations which made use of RFID and Biometric technology in an attempt to improve border security. Since then, there have been

[5] One already-standardized method of user PIN entry (discussed in Section 4.3) is a good example of *safe default* design.

several major revisions to ePassport standards proposed by the ICAO, European Union, and the German Federal Office for Information Security (BSI)[6]. The last proposed set of standards for ePassports was published by the BSI in October 2008 [4]. This specification document effectively mitigates almost all previously criticized security problems on ePassports, except one – certificate revocation checking.

In this section, we take ePassport 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 ePassport tags. We start by describing the basics of the current ePassport PKI system. Then, we explain how ePassport 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 ePassport tags.

5.1 ePassport Public Key Infrastructure

The key elements in the Public Key Infrastructure (PKI) for ePassports 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 ePassports issued by the state.

The Document Verifier is a body that operates between readers (*a.k.a* Inspection Systems) 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 ePassport, 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 [5].

5.2 ePassport Certificate Validation Procedure

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 ePassport 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 ePassport tag:

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 more recent 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 more recent than T_{curr} value stored in the date register, tag also updates T_{curr} to the effective date of the certificate.

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

Fig. 2. Sample ePassport with a Display Unit

After validation phase is successfully completed, ePassport tag-reader interaction continues with access control and passive/active authentication phases as described in the standards [5, 4]. These phases are summarized in the next section of this paper as well.

5.3 Modified ePassport Operation Procedure

In order to integrate our solution, ePassports themselves and their operation procedures have to be modified. The change needed on ePassports is the mere replacement of current tags with ones that have attached displays (Figure 2 shows how an ePassport with display would look like). The modified ePassport operation procedure that integrates our solution is summarized in Figure 3 and explained below. Please note that only the validation phase (step 1 below) is modified to integrate our solution.

1. (a) Validation Phase: The reader sends the ePassport tag its certificate and the non-revocation proof discussed in section 4.4. The ePassport shows the expiration date on its display and enters into a countdown phase. This gives chance to its bearer to react with an escape action if the certificate is expired or the non-revocation proof is not timely. If no escape action is initiated within the countdown period, the communication between the tag and the reader resumes as explained in next steps.
   (b) Escape Action: If the ePassport holder realizes the displayed date is in the past, he is responsible for executing an escape action within the countdown period. Since

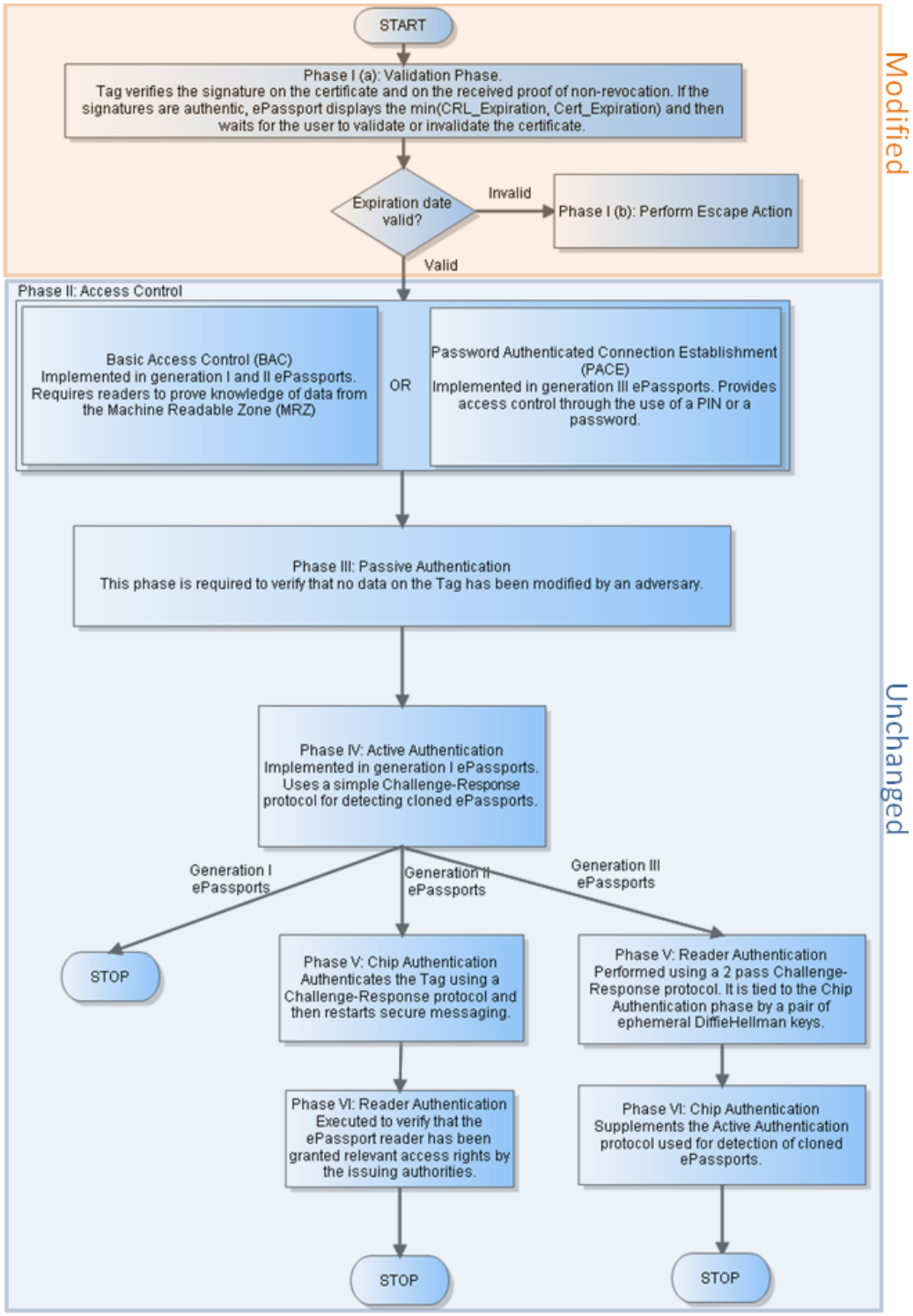

Fig. 3. Modified ePassport Operation procedure

ePassports have a faraday cage in their cover pages, the escape action in this case would be simply closing the passport. As explained in section 4.3, this would abort any ongoing communication and reset the tag state by cutting its power. If an escape action is initiated within the countdown period, none of the following steps would be executed.

2. (a) Basic Access Control Phase: Basic Access Control (BAC) is an optional protocol that attempts to ensure that only readers with physical access to the passport can read tag data.

   (OR)

   (b) Password Authenticated Connection Establishment Phase: PACE replaces the Basic Access Control protocol as a mechanism which enables a tag to verify that the reader has authorized access to the electronic passport.
3. Passive Authentication Phase: Its primary goal is to allow a reader to verify that the data in the ePassport is authentic. This scheme is known as passive authentication since the tag performs no processing and is only passively involved in the protocol.
4. (a) Active Authentication Phase: Using a simple challenge-response mechanism, it aims to detect if a tag has been substituted or cloned.

   (OR)

   (b) Chip Authentication Phase: It was proposed as a part of the Extended Access Control specifications. It aims to replace Active Authentication as a mechanism to detect cloned ePassports.
5. Reader Authentication Phase: The reader Authentication protocol is a protocol that is executed only if access to more sensitive data (secondary biometrics) is required. It is a challenge-response mechanism that allows the tag to validate the reader used in Chip Authentication.

5.4 Feasibility Analysis

Low Power Display Technologies Since ePassport 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 ePassport 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 [27]. 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 [28], SiPix Microcup [29], NemOptic BM100 [30], Kent Displays Incorporated eCards [31]).

Power Analysis ePassport tags such as those supplied by Infineon Technologies, require up to 55mW of power to operate [32] while the display unit requires a maximum power of 100mW to operate. We analyze the power requirements of the proposed system from two aspects:

1. The ePassport tag is on standby when the display unit is updated.
2. The ePassport tag is operating at maximum power when the display unit is updated.

In the first case, the power required by the entire ePassport circuit to operate will be ∼100mW (the power required by the tag during standby is negligible). In the second case, the power required by the ePassport circuit to operate will be ∼155mW (the sum of the power required by the tag and Display). The ePassport tag and reader when placed parallel to each other can be represented as a circuit (see Figure 4), with circuit parameters set in the manner described by Scholz *et al.* [33].

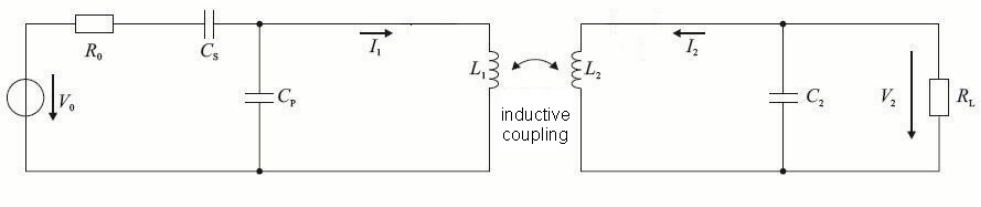

Fig. 4. Circuit Representation of ePassport Tag and Reader

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 [33] 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). The value of R_L is 195.1 Ω in the case that the ePassport tag and display unit operate at maximum power together (case 1). R_L is 302.5 Ω in the case that the ePassport tag is on standby when the display unit is refreshed (case 2). 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 values for x, where x represents the maximum possible operating distance:

– An ePassport tag without a display unit:

$$P_{Tag} = 55\ mW,\ R_L = 550\ \Omega \Longrightarrow x = .097\ m\ (9.7\ \text{cm}) \tag{7}$$

– An ePassport display unit (while the tag is in standby mode):

$$P_{Tag} = 100\ mW,\ R_L = 302.5\ \Omega \Longrightarrow x = .080\ m\ (8\ \text{cm}) \tag{8}$$

– An ePassport with a display unit (Both the tag and the display requiring their maximum power)

$$P_{Tag} = 155\ mW,\ R_L = 195.1\ \Omega \Longrightarrow x = .069\ m\ (6.9\ \text{cm}) \tag{9}$$

From the above results it is clear that 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 ePassport circuit is feasible and doesn't require any changes over the power specifications in the original proposal [4]. If longer operating distances (over 6.9 cm) are needed, it can be achieved with small modifications on the RFID antenna design or by increasing power of a reader.

6 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 his/her 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. We strongly believe that display-equipped RFID tags will soon be in mass production and the method proposed in this paper will be widely applicable to a variety of pk-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. Bundesamt fur Sicherheit in der Informationstechnik: Advanced Security Mechanisms for Machine Readable Travel Documents : Version 2.0. (2008)

5. International Civil Aviation Organization: Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability. (2006)
6. Tsudik, G.: Ya-trap: Yet another trivial rfid authentication protocol. Pervasive Computing and Communications Workshops, IEEE International Conference on **0** (2006) 640–643
7. Kocher, P.C.: On certificate revocation and validation. Lecture Notes in Computer Science **1465** (1998)
8. Merkle, R.C.: Secrecy, authentication, and public key systems. Technical report, Stanford University (June 1979)
9. Goodrich, M., Tamassia, R.: Efficient authenticated dictionaries with skip lists and commutative hashing (January 13 2001)
10. Naor, M., Nissim, K.: Certificate revocation and certificate update. Technical report (March 01 1999)
11. Micali, S.: Efficient certificate revocation. Technical Memo MIT/LCS/TM-542b, Massachusetts Institute of Technology, Laboratory for Computer Science (March 1996)
12. Lamport, L.: Password authentication with insecure communication. (1981)
13. Narasimha, M., Solis, J., Tsudik, G.: Privacy preserving revocation checking. International Journal of Information Security **8**(1) (February 2009) 61 – 75
14. Monnerat, J., Vaudenay, S., Vuagnoux, M.: About Machine-Readable Travel Documents. In: Conference on RFID Security, Malaga, Spain (July 2007)
15. 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
16. 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)
17. 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)
18. 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)
19. 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)
20. 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)
21. Whitrow, G.: Time in history: the evolution of our general awareness of time and temporal perspective. Oxford University Press (1988)
22. Ullman, M. personal communication (Sept 2009)
23. 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
24. 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
25. Saxena, N., Uddin, M.B., Voris, J.: Treat 'em like other devices: user authentication of multiple personal rfid tags. In: SOUPS. (2009)
26. Kaliski, B.: Future directions in user authentication. In: IT-DEFENSE. (2005)
27. Kahn, B., Zervos, H.: Displays and lighting: Oled, epaper, electroluminiscent and beyond. Technical report, IDTechEx (2008)
28. E Ink Corporation: Segment Display Cell: Custom + Standard ePaper Designs. (2008)
29. SIPIX Imaging: SIPIX: Segmented ePaper Displays. (2006)
30. Nemoptic: BM100: BiNem Module - Reflective Display. (2008)
31. 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)
32. Infineon Technologies AG, AIM CC: Preliminary Short Product Information: Chip Card and Security IC's. (2006)
33. Scholz, P., Reihold, C., John, W., Hilleringmann, U.: Analysis of energy transmission for inductive coupled rfid tags. International Conference on RFID (2007)