# CHECK THE DATE:
# Reader Revocation in PKI-Based RFID Systems

Rishab Nithyanand
*Department of Computer Science*
*University of California, Irvine*
*rishabn@ics.uci.edu*

Gene Tsudik
*Department of Computer Science*
*University of California, Irvine*
*gts@ics.uci.edu*

Ersin Uzun
*Department of Computer Science*
*University of California, Irvine*
*euzun@ics.uci.edu*

***Abstract*—One prominent open problem with RFID tags that support public key cryptography is revocation of reader certificates. This is an important issue considering that high-end RFID tags are geared for public key applications such as e-documents and contactless payment instruments. Furthermore, the problem is unique to public key-based RFID systems, since tags have no clock and thus cannot use traditional (time-based) off-line revocation checking methods. Whereas, on-line methods require unrealistic connectivity assumptions.**

**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 our solution via a user study and a discussion of its application feasibility.**

**In our approach, the main extra feature is the requirement for a small passive on-tag display. However, modern low-power display technology is low-cost and appealing for other security purposes such as user-to-tag authentication and transaction verification.**

## I. Introduction

We focus on a class of public key 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. In this context, reader revocation is both imperative and possible. It is imperative, because not doing it prompts some serious threats. A reader may be *lost* or *stolen*, *compromised* (perhaps without its operators knowledge), or *decommissioned*. If such readers cannot be revoked effectively, they can be used to identify and track tags. Further threats are possible depending on the application. For example, ePassports and contactless credit-cards typically store sensitive information, such as biometrics or account numbers, which, in wrong hands, can be used for malicious activities such as identity theft, credit fraud, or forgery.

Our approach to solving the problem of reader revocation status checking is based on several observations:

- In normal operation, 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 (10 digit) displays have been demonstrated by NXP Semiconductors.
- 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.

## II. Protocol and Evaluation

### A. 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.
2) Each tag is equipped with a small (i.e., 6 or more characters) one-line (e.g., ePaper) display unit.
3) Each tag has a mechanism that allows it to become temporarily inaccessible to a reader.
4) 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). This CA issues an updated revocation structure (e.g., a certificate revocation list (CRL)) periodically. Such structures include serial numbers of all revoked reader certificates and their issuance periodicity is known by all the tags.
5) Each tag is equipped with a small non-volatile storage that can store the last verifiable date it encountered. While powered up by a reader, a tag is also capable of starting and running a short timer.
6) [**Optional**] A tag may have *a single button* for user input.

### B. Protocol

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

1) The freshly powered-up tag receives the CRL and the reader certificate. Let $CRL_{iss}$, $CRL_{exp}$, $PKC_{iss}$ and $PKC_{exp}$ denote the issuance and expiration times for purported CRL and PKC, respectively.

2) If either of $CRL_{exp}$ and $PKC_{exp}$ is smaller than the last verified date stored in the tag, or $CRL_{iss} \geq PKC_{exp}$, the tag aborts the protocol.
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) If $CRL_{iss}$ or $PKC_{iss}$ is more recent than the currently stored date, the tag updates it to the more recent of the two.
6) The tag displays the lesser of the $CRL_{exp}$ and $PKC_{exp}$. It then enters into a countdown stage that lasts for a predetermined duration (e.g., 10 seconds).
7) The user views the expiration date on the display unit and makes a decision about its validity. The communication with the reader is either halted or resumed based on the user's decision. Depending on the tag hardware, user can simply press a button (if assumption 6 holds) to signal his/her acceptance or make the tag inaccessible by initiating an escape action (e.g., e-Passports have faraday cages on their cover pages and closing them prevents any communication with the tag). More escape actions are discussed in [1].

### C. Evaluation

We acknowledge that user's awareness of time and ability to abort the protocol (when needed) is essential for our protocol. To this end, we conducted user studies to evaluate the practical security and usability of the protocol. Mock-up implementation on mobile phones are used in the experiment (at the time of this study, actual RFID tags with displays and buttons could not be ordered in modest quantities). 25 subjects were recruited on the campus of University of California – Irvine. The set of dates used in the testing process were: +/-1 day, -3 days, +7 days, -29 days, and -364 days from the actual test date[1].

**Completion Time and Error Rates:** For subjects accepting the displayed date, the average completion time was 3.07 seconds, with sample standard deviation of 1.58 seconds. Among the 25 subjects, the rate of false negatives was quite low. Only one subject rejected the date that was 7 days in the future. The rate of false positives was 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, the error rate spiked up to 40% when subjects were shown a date that was 364 days earlier.

**System Usability Score:** People who tried our mock implementation rated its usability at 77% on the System Usability Scale (SUS) [2]. 84% of the subjects who tested our implementation stated that they would like it to be implemented on their own personal tags, while 12% were neutral to the idea.

**Cost Analysis:** The current 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 when ordered in larger quantities. Although this might seem high, we anticipate that the cost of cutting-edge passive display technologies will sharply decrease in the near future. Moreover, once a display is available, it can be used for other applications, thus amortizing the expense. Such applications include but are not limited to:

- *User-to-Tag Authentication:* In some scenarios, it might be necessary for a user to authenticate to a tag. Currently this can be done only via trusted devices such as readers or phones. However, using a display, it is possible to authenticate users to their tags by having them manipulate a random number displayed on their tag into a known PIN using buttons on the (not necessarily trusted) reader.
- *Transaction Verification:* RFID tags are commonly used as payment and transaction instruments. In such settings, a direct auxiliary channel (such as the display unit on the tag) between the tag and the user is necessary to verify the details of a transaction. A recent online survey [3] we conducted with 98 individuals revealed that 74.2% of the participants would like to have displays on their payment cards for the purpose of transaction verification (17.5% were neutral to the idea).
- *Device Pairing:* A display may be used for secure pairing of tags with other devices that do not share a CA with the tag. Visual channel-based secure device pairing methods that are proposed for personal gadgets can be used with display-equipped RFID tags. 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.

## III. Conclusions

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. We also presented other security applications for the displays on RFID tags, thereby amortizing their cost.

**Acknowledgements:** We would like to thank Thomas Suwald and Arne Reuter for their valuable comments and NXP Semiconductors for providing us the display equipped RFID cards.

## References

[1] R. Nithyanand, G. Tsudik, and E. Uzun. Readers behaving badly: Reader revocation in pki-based rfid systems. Cryptology ePrint Archive, Report 2009/465, 2009.

[2] J. Brooke. Sus - a quick and dirty usability scale. In *Usability Evaluation in Industry*, 1996.

[3] Display enabled identification and payment instruments, November 2009. http://www.ics.uci.edu/~rishabn/survey.html.

[1] Experiments were conducted in the first week of December 2009.