UNIVERSITY OF CALIFORNIA,
IRVINE

Securing Personal RFID Tags and Infrastructures

THESIS

submitted in partial satisfaction of the requirements
for the degree of

MASTER OF SCIENCE

in Computer Science

by

Rishab Nithyanand

Thesis Committee:
Professor Gene Tsudik, Chair
Professor Alfred Kobsa
Professor Alice Silverberg

2010
DEDICATION

To my amazing family, friends, and marky – my 19 year old dog who recently passed away.
# TABLE OF CONTENTS

| LIST OF FIGURES | iv |
| LIST OF TABLES | v |
| ACKNOWLEDGMENTS | vi |
| ABSTRACT OF THE THESIS | vii |

## 1 Introduction
  1.1 Introduction to RFID Technology ........................................ 1
  1.2 Current and Emerging RFID Applications ................................. 4
  1.3 Security and Privacy in RFID Infrastructures ......................... 8
  1.4 Personal RFID Tags .................................................. 11
  1.5 Thesis Organization .................................................. 13

## 2 A Typical Personal RFID Tag – The ePassport
  2.1 Introduction ......................................................... 14
  2.2 The ePassport Logical Data Structure ................................ 16
  2.3 The ePassport Public Key Infrastructure .............................. 17
  2.4 Security Protocols in ePassports .................................... 18
     2.4.1 Basic Access Control ........................................... 18
     2.4.2 Password Authenticated Connection Establishment ............. 21
     2.4.3 Passive Authentication ......................................... 22
     2.4.4 Active Authentication .......................................... 22
     2.4.5 Chip Authentication Version 1 ................................ 23
     2.4.6 Reader Authentication Version 1 ................................ 24
     2.4.7 Reader Authentication Version 2 ................................ 25
     2.4.8 Chip Authentication Version 2 ................................ 26
  2.5 Weaknesses of ePassport Security Protocols and Specifications .... 27
     2.5.1 Optional Status of BAC, PACE and Active Authentication ...... 27
     2.5.2 Low Entropy of the BAC Seed Key ................................. 29
     2.5.3 Lack of Access Rules ............................................. 29
     2.5.4 Poor Detection of Expired or Revoked Readers ................. 30
3 Addressing Reader Revocation in Personal RFID Based PKIs 32
   3.1 Introduction ............................................. 32
   3.2 Motivation ............................................... 33
      3.2.1 Why Is reader Revocation Hard? .................. 35
   3.3 Related Work ........................................... 36
   3.4 Trivial Solutions ....................................... 38
      3.4.1 Date Register ...................................... 38
      3.4.2 On-line Revocation Checking ...................... 39
      3.4.3 Internal Clocks .................................... 40
   3.5 Proposed Solution ...................................... 41
      3.5.1 Assumptions ........................................ 41
      3.5.2 Protocol ............................................ 42
      3.5.3 Escape Actions ..................................... 43
   3.6 Efficient Revocation Checking ......................... 46
      3.6.1 Assessment ......................................... 48
   3.7 Security Considerations ................................ 48
   3.8 Usability Analysis ...................................... 49
      3.8.1 On-line Survey ..................................... 50
      3.8.2 Usability Testing ................................... 52
      3.8.3 Discussion .......................................... 55
   3.9 Feasibility Analysis .................................... 56
      3.9.1 Low Power Display Technologies ................. 56
      3.9.2 Power Analysis .................................... 58

4 Transaction Verification in Personal RFID Payment Instruments 62
   4.1 Introduction ............................................. 62
   4.2 Proposed Solution ...................................... 64
      4.2.1 Assumptions ........................................ 64
      4.2.2 Protocol ............................................ 66
   4.3 Usability Analysis ...................................... 67
      4.3.1 On-line Survey ..................................... 68
      4.3.2 Survey Results .................................... 69

5 Future Work and Conclusions 71
   5.1 Future Work ............................................. 71
   5.2 Conclusions ............................................. 72

Bibliography 74

Appendices 79
   A Questionnaire: Usability Analysis for Reader Revocation and Transaction Verification .................. 79
   A.1 Demographics ........................................... 79
   A.2 Project Background Information and Description ................. 80
   A.3 Reader Revocation in ePassports ....................... 81
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>RFID Tag Embedded in an ePassport</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>Examples of Objects Containing Personal RFID tags</td>
<td>12</td>
</tr>
<tr>
<td>2.1</td>
<td>ePassport Public Key Infrastructure</td>
<td>18</td>
</tr>
<tr>
<td>2.2</td>
<td>ePassport Protocol Stack</td>
<td>19</td>
</tr>
<tr>
<td>2.3</td>
<td>Basic Access Control challenge-response protocol</td>
<td>20</td>
</tr>
<tr>
<td>2.4</td>
<td>Password Authenticated Connection Establishment</td>
<td>21</td>
</tr>
<tr>
<td>2.5</td>
<td>Active Authentication protocol</td>
<td>23</td>
</tr>
<tr>
<td>2.6</td>
<td>Chip Authentication (Version 1) protocol</td>
<td>24</td>
</tr>
<tr>
<td>2.7</td>
<td>Reader Authentication (Version 1) protocol</td>
<td>25</td>
</tr>
<tr>
<td>2.8</td>
<td>Reader Authentication (Version 2) protocol</td>
<td>26</td>
</tr>
<tr>
<td>2.9</td>
<td>Chip Authentication (Version 2) protocol</td>
<td>27</td>
</tr>
<tr>
<td>3.1</td>
<td>Online Certificate Status Protocol (OCSP)</td>
<td>39</td>
</tr>
<tr>
<td>3.2</td>
<td>Sketch of Revocation Status Checking Protocol</td>
<td>44</td>
</tr>
<tr>
<td>3.3</td>
<td>Shielding Effect of a Faraday Cage</td>
<td>45</td>
</tr>
<tr>
<td>3.4</td>
<td>Modified ePassport protocol with revocation status checking</td>
<td>57</td>
</tr>
<tr>
<td>3.5</td>
<td>Circuit representation of a coupled ePassport tag and reader</td>
<td>58</td>
</tr>
<tr>
<td>4.1</td>
<td>Typical POS Transaction Procedure</td>
<td>65</td>
</tr>
<tr>
<td>4.2</td>
<td>Modified POS Transaction Procedure with Transaction Verification for RFID Enabled Payment Instruments</td>
<td>65</td>
</tr>
<tr>
<td>4.3</td>
<td>Sketch of Transaction Verification Operation Procedure</td>
<td>68</td>
</tr>
<tr>
<td>A.1</td>
<td>ePassport revocation checking procedure description</td>
<td>82</td>
</tr>
<tr>
<td>A.2</td>
<td>Credit card transaction verification procedure</td>
<td>84</td>
</tr>
</tbody>
</table>
## LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Evolution of RFID Applications</td>
<td>11</td>
</tr>
<tr>
<td>2.1</td>
<td>ePassport Logical Data Structure</td>
<td>16</td>
</tr>
<tr>
<td>2.2</td>
<td>Security Protocols in ePassports</td>
<td>28</td>
</tr>
<tr>
<td>2.3</td>
<td>Vulnerabilities of ePassports</td>
<td>28</td>
</tr>
<tr>
<td>2.4</td>
<td>ePassport Security Protocols Notation</td>
<td>31</td>
</tr>
</tbody>
</table>
ACKNOWLEDGMENTS

I am sincerely thankful to the many people who contributed directly and indirectly to this thesis. My wonderful experience as a graduate student at UCI would not have been the same without the below mentioned mentors and friends.

It is difficult to express the amount of gratitude and respect I have for my advisor, Prof. Gene Tsudik. His advice, guidance, incredible sense of humour, and (most importantly) patience have made my period of study at the University of California in Irvine extremely enjoyable and fruitful. I will always be thankful to Gene for giving me the opportunity to work with him.

I am thankful to Prof. Alfred Kobsa for his help and comments on this thesis. My gratitude also goes to Prof. Alice Silverberg for helping me better my presentation and writing styles through very useful feedback after each presentation at the mathematics of cryptography series, and for her invaluable support and help during the time I was planning my graduate school applications. I am also thankful to Prof. Stanislaw Jarecki for his useful feedback on this thesis.

I would like to thank everyone in the SPROUT Lab – Mishari Almishari, Emiliano De Cristofaro, Karim El Defrawy, Yanbin Lu, Dr. Ivan Martinovic, Gabriele Oligeri, John Solis, Ersin Uzun, and Shuichiro. It has been a great experience and a lot of fun to work with this group. Many thanks to Gina Anzivino and Kris Bolcer for always kindly guiding me through the administrative procedures at UCI ICS.

Above all, I have to mention that I have been blessed with a great family. I am forever grateful to my parents for giving me the perfect childhood, unaltering encouragement, love, and support. I want to thank my loving sister for putting up with me in spite of all the (silly) fights and arguments we’ve had. Many thanks must go to my wonderful friends in India, UCI, and everywhere else.

This thesis is the result of my work with Prof. Gene Tsudik and Ersin Uzun.
The recent emergence of RFID tags that are capable of performing high level cryptographic operations (including public key operations) motivates new RFID applications, including electronic travel documents, identification cards, and payment instruments. This has introduced a new class of RFID tags which store sensitive owner specific data (e.g., biometrics) – i.e., personal RFID tags. The primary task of these tags is to identify and authenticate their authorized holders to authorized RFID readers. In such settings, we observe an important feature that distinguishes these tags from the more traditional RFID tags used in supply chain and inventory management is the involvement of a human user and the sensitive nature of data contained in the tags.

We take advantage of the user’s awareness and presence to construct simple, efficient, secure, feasible, and (most importantly) usable solutions for important, yet largely ignored problems in such RFID systems. These include RFID reader revocation status checking in RFID public key infrastructures and transaction verification in RFID enabled payment instruments.

We also evaluate the usability and practical security of each of our solutions via usability studies which include online surveys and actual tests using prototypes. Our
approach to solving the above mentioned problems takes advantage of new low-power
technologies such as OLED, ePaper, and other more recent advances in hardware
integration on RFID tags. We use these technologies to improve security by applying
them to establish secure I/O channels for communication between the tag owner, the
personal tag, and the reader.
Chapter 1

Introduction

1.1 Introduction to RFID Technology

Radio Frequency Identification (RFID) is a wireless technology mainly used for identification of various types of objects, e.g., merchandise. Usually, 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.

The first known application of RFID was the “friend or foe” identification system used in fighter planes in World War II [3]. After a few decades, interest in RFID technology resurfaced as it was envisaged as a replacement for bar codes in supply chain and inventory management [32]. Today, 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 dollars [20]. These tags are powerful enough to perform hefty public key operations, e.g., encryption and signature verification. At the opposite end, are tags used for supply chain and inventory management (as Electronic Product Codes). Such applications involve tags that are typically very cheap, each costing a few cents [52]. These tags have extremely low computational power and struggle to perform even simple hashing and symmetric key cryptographic operations.

RFID constitutes three subsystems: tags (transponders), readers (transceivers), and antennas.

**RFID Tags:** These are tiny chips which consist of an antenna and IC for data storage, signal modulation, and signal demodulation. Depending on the type of tag, they may also contain a battery. RFID tags may be one of three types – active,
passive, or semi-active. Active tags are those which contain a battery from which they draw power for computation and for communication to readers (and even other tags). Passive tags do not contain any sort of on-board power. They draw power from the RF signals sent by the readers. As a result, they do not have the ability to communicate or compute (and are essentially dead) in the absence of a reader that supplies appropriate signals. The third type (semi-active), is a combination of active and passive RFID technology. These tags contain an on-board battery that is exclusively utilized as a computation resource (and not for communication). They draw power for communication and initialization from the RF signals transmitted by the reader. Therefore, semi-active tags do not require the presence of a reader until they have to power-up, transmit, or receive data.

**RFID Readers:** These are devices that are used to communicate and extract meaningful data from RFID tags. This data could be anything from a serial number to the biometric information of an individual. An RFID reader transmits a low-power radio wave which is used to power up the tag so that the tag may relay the required data back to the reader. The frequency of this radio wave may be anywhere between 3MHz and 5GHz, depending on the read range required (and the application). Readers are typically connected to full blown computing devices which have high computation capabilities and may also have access to back-end databases which are used to correlate data obtained from the tag with other information regarding the individual or object with which the tag is associated.

**RFID Antennas:** The antennas are built around the IC on the RFID tag and into the RFID reader. Inductive coupling is used to power up passive RFID tags – i.e., the reader induces a current on the tag through the antenna. The current on the tag charges a capacitor which acts as a power source in the tag. The antennas used in RFID tags and readers are made out of highly conducting materials such as copper
and aluminum. The capacitor connected to the tag antenna is made of mica or any ceramic material. Loop antennas are used in the reader circuit as they are most suitable for generating the magnetic field that is required to transfer energy to the tag [59].

1.2 Current and Emerging RFID Applications

Retail, Inventory Management, and Supply Chain: The RFID revolution began as soon as its potential as a replacement for bar codes was realized. Statistics reveal that in 2003, over 555.4 million RFID tags were sold for the purpose of inventory, retail, and supply chain management [53]. One can only imagine that this number is far higher today.

While RFID tags are more expensive than bar codes, they have the advantage that they do not require line-of-sight or valuable package real-estate. Tags used for this purpose cost in the order of a few cents and are incapable of any complex computation.

The tag typically contains a 96 bit number that uniquely identifies the product it is attached to. They are capable of communication with readers up to a distance of a few meters. Readers (connected to back end databases) are placed at strategic locations – such as warehouse shelves, transport trucks, store checkout counters, and exit points – enabling them to maintain a detailed history of products through the manufacturing and retail cycle until (or maybe even after) it reaches the consumer of the product. RFIDs in such scenarios are also useful for preventing theft or product loss.

Access Control and Physical Security: RFID readers can be used for user authentication at building and room entry points. Authorized personnel are provided
with RFID tags which are queried by the readers. Once a challenge is issued, only an authorized tag is (or, should be) capable of responding correctly to it. Once the correctness of the response is verified, the electronic strike on the door retracts and the door may be pushed open.

Further, such systems remove the need for handling many keys – they require the tag to simply be within the range of the reader. The cost of RFID access control systems is comparable with regular locks and access control systems. RFID access control systems not only allow better security, but are also extremely useful in emergency evacuations since they allow accountability of individuals that enter and leave a room.

**Human Identification:** The fusion of biometrics and RFID tags has resulted in the development and deployment of the new generation of ID cards. Currently, over 30 million ePassports have been issued across the world (this is the single largest deployment of RFID enabled ID cards). In addition to ePassports, RFID has also been deployed in licenses, visas, insurance cards, and even voter IDs.

The implementation of Biometric and RFID technologies in human identification documents such as those mentioned above, aim to reduce fraud by negating forgery and establishing without doubt the identity of the documents’ bearer. However, when used for such purposes, security and privacy of the sensitive data stored on the tag is a fundamental concern and should not be ignored.

**Cashless Payment at Point of Sale:** RFID enabled credit cards were introduced in the United States by American Express (ExpressPay), Mastercard (paypass), and Visa(payWave) in 2006. Since then there has been a lot of opposition to the technology by the public and the press. While some of the concerns regarding the implementation of RFID have been well founded, a large amount of it has been based of near-facts and half truths (examples of these may be found in many on line forums discussing
We describe briefly the operation procedure of these cards below.

1. The customer holds his card within a distance of 10-15 centimeters from the POS RFID reader.
2. The tag in the card is activated by the RF signals sent by the reader.
3. The transaction is authorized without a PIN for transactions under $25. Otherwise, the customer needs to enter a PIN at the POS terminal.
4. Once the PIN is entered, a cryptographic matching algorithm verifies the correctness of the entered PIN.
5. The card sends via an RF signal, the information that would normally be obtained from the magnetic strip of the card - i.e. card number, expiry date, and card holders name. This information is sent in plain text for some banks, other banks use pseudonyms, transaction counters, or cryptography to conceal some of this very sensitive information.
6. The RFID reader transfers this information to the back end processing system along with other transaction related information such as destination account, transaction time, and transaction amount. The charges are made and the amount is transferred to the merchant from the card holders account.

Medical Industry: In 2004, the use of Surgichip [21] on surgery-bound patients was approved by the U.S Food and Drug Administration (FDA). Surgichip tags are external adhesive RFID tags which aim to reduce the possibility of wrong patient, wrong procedure, wrong site (the 3W’s [25]) operations. On admittance and post diagnosis, the tag is labeled and stores information including the patients name,
age, diagnosis, operation procedure required, etc. This allows surgeons to verify critical information pre and post surgery. The tag also logs data such as time elapsed, operating surgeon, etc.

Another RFID enabled device used in the industry is Verichip [64] – an implantable RFID tag that is used for patient identification and access to medical history. The Verichip tag does not store any patient related data on itself, instead, it stores only a 16 bit unique identifier which can be used to identify patients and their medical history through a centralized database (now available thanks to the recent push for digitization of medical records). This is especially useful in emergencies, where time is valuable, the patients condition is critical, and the medical history of the patient is unknown.

The application of RFID has also been extended to use in implantable pacemakers and implantable cardiac defibrillator’s (ICD’s). The main benefit of combining these technologies (medical devices, RFIDs, and the Internet) is the ability for physicians to remotely monitor patients [16]. Further, RFID tags are also used to prevent drug counterfeiting.

Note: Both Surgichip and Verichip tags use write only registers. This makes it impossible to overwrite or modify data stored on the tag – a very important feature.

**Sports Industry:** RFID technology has also been welcomed in the sporting world (for applications other than ticketing) – particularly in athletics and motor sports.

In athletics, adhesive RFID tags are pasted on athletes to provide accurate timing information. The use of such tags in marathons also allows participant tracking throughout the race thereby rooting out any possibility of cheating. This was first introduced in the 2009 Seattle Rock-n-Roll marathon.
In motor sports (Nascar and more recently Formula 1), RFID tags (enhanced with devices such as accelerometers, thermometers, etc.) are attached to parts of the car including the nose, tires, etc. This not only allows easy identification and inventorying of car parts, but also provides teams with extremely accurate and useful data such as tire temperatures, tire wear, aerodynamic conditions, etc. The tags used here are usually active (i.e., battery powered).

1.3 Security and Privacy in RFID Infrastructures

Security and privacy of data (and of consumers) is one of the major concerns that has hindered the adoption of RFID technology for many applications. The absence of protocols for privacy and security introduce concerns such as clandestine scanning and tracking, cloning, eavesdropping, and cross contamination attacks. However, a major problem is – the lack of computational resources on RFID tags. This prohibits the use of common cryptographic operations to enhance privacy and security in RFID infrastructures, creating a challenge of finding new lightweight alternatives.

**Privacy:** RFID tags have the problem that they always (when no user input is required to initiate communication) respond to queries by readers without their owners knowledge or consent. This makes achieving privacy more challenging. The solution to the privacy problem in RFID infrastructures essentially boils down to establishing methods to prevent illegal readers from interacting with RFID tags (and as a result, maintaining data confidentiality). In cases where public key infrastructures are available, this problem can be solved by reader authentication mechanisms (in addition to the protocols described in chapter 3). This is not so easy in symmetric key setups since reader revocation is impossible. The main privacy concerns for RFID infrastructures are attacks which involve *clandestine scanning, tracking, and*
eavesdropping.

- Clandestine Scanning: As mentioned above, since RFID tags respond to queries from readers without the need for user input, it is possible for illegitimate readers to covertly interrogate tags. Such attacks are easy to launch since they can go undetected and from a distance. It is possible to prevent such attacks using Faraday cages. Faraday cages shield tags that are concealed in them from any electromagnetic waves, thus preventing reader queries from reaching them.

- Clandestine Tracking: When tag responses to reader queries are unique (but the same on each iteration), it is possible for an unauthorized party in possession of a reader to constantly track the movement of the tag owner. Tracking is possible even if the data on the tag is encrypted. As with clandestine scanning, Faraday cages can be used to prevent such attacks.

- Eavesdropping: Eavesdropping attacks are carried out by having an adversarial reader record the data stream between the tag on the card and another (legitimate) reader. The adversary now has data that was intended only for the legitimate reader. These attacks cannot be prevented by using a Faraday cage since the tag is already taking part in a legitimate transaction while the adversary is simply recording its data stream. These attacks are easy to carry out since they can be carried out from a distance, do not involve data transmission from the adversarial reader to the tag, and do not alert the owner of the tag of any wrongdoing.

**Security:** RFID security concerns the problem of fake (cloned) or manipulated tags feeding false information to legitimate readers. It is important to verify tag authenticity (using tag authentication protocols) before harvesting data obtained from the
tag. The main security concerns for RFID infrastructures arise out of attacks which compromise data integrity and allow forgery via tag cloning.

Note: User authentication is also important in the case of personal tags to ensure that the tag is a trustworthy source of information about its carrier.

- Data Integrity: An adversary that is able to modify data on an RFID tag can be very dangerous. Consider the following example – a known terrorist modifies the biographic data (name, address, etc.) on his ePassport tag and is able to cross borders into any country since his modified data does not appear on any existing watch list. A simple way to prevent such attacks is to sign all data on the tag with the private key of the tag issuer (for eg., the passport office that supplied the ePassport). However, with such an approach, it is critical that all document verifiers are aware of every tag issuers public key (for signature verification purposes). An alternate approach is for tags to have write only registers which make it impossible to write over any data. However, it is easy to see that this approach has several obvious disadvantages – they make data corrections, updates, and appends impossible.

- Tag Cloning: While digital signatures make it easy to verify the data integrity of tags, they are useless against attacks that involve tag cloning (they prevent forgery, not copying). Cloning of tags can be prevented by using techniques such as unique numbering with tag inventoring or authentication (requiring the tag to prove knowledge of a secret stored in read only registers that are signed by the tag issuer).

- Denial of Service: DoS attacks are a major cause for concern in RFID environments. Not only are such attacks possible, they are also very easy, unsophisticated, and cheap to carry out. It is possible to ‘fry’ tags (rendering
them useless) in adverse conditions (e.g., exposure to very high temperatures, very strong electromagnetic pulses (these attacks can be curbed using Faraday cages)). Tags can crash by having malicious readers overload them with more data than they can handle (these attacks can be curbed by using the reader revocation technique described in this thesis).

1.4 Personal RFID Tags

<table>
<thead>
<tr>
<th>Application Domain</th>
<th>Year</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military</td>
<td>1941</td>
<td>Friend or Foe Craft Identification</td>
</tr>
<tr>
<td>Warehousing</td>
<td>1969</td>
<td>Inventorying, Tracking, Security</td>
</tr>
<tr>
<td>Border Security</td>
<td>1998</td>
<td>Human Identification – ePassports</td>
</tr>
<tr>
<td>Medical Industry</td>
<td>2004</td>
<td>Human Identification – Implantable Tags</td>
</tr>
<tr>
<td>Banking Industry</td>
<td>2006</td>
<td>Human Identification – Payment Instruments</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>2006</td>
<td>Human Identification – Driving Licenses</td>
</tr>
<tr>
<td>Athletics</td>
<td>2008</td>
<td>Athlete Tracking and Timing</td>
</tr>
<tr>
<td>Voting Security</td>
<td>2008</td>
<td>Human Identification – Voter Id Cards and Tokens</td>
</tr>
<tr>
<td>Motor Sports</td>
<td>2009</td>
<td>Timing, Environmental Data Collection</td>
</tr>
</tbody>
</table>

From Table 1.1, it is interesting to note that since 1998, five of the seven new applications of RFID have been for human identification. This has introduced a new class of RFID tags which store sensitive owner specific data (e.g., biometrics) i.e., personal RFID tags. The primary task of these tags is to identify and authenticate their holders to the correct authorities.

Personal tags have several properties that distinguish them from regular tags that are used for inventorying, vehicle identification, etc. These are:

- The tag is carried by a human (rather than a vehicle or a package).
- The tag stores very sensitive data, that if in the wrong hands could be used to
harm the owner.

- These tags have higher computational capabilities, and as a result are more expensive.

- The owner of the tag is (or, at least should be) aware of the tags participation in a conversation with a reader.

- Usually, the owner does something to initiate the conversation between the tag and the reader.

It must be noted that all personal RFID tags use passive natured RFID tags. Henceforth, any reference to a tag or personal tag should be understood as a passive tag unless mentioned otherwise.
1.5 Thesis Organization

- In chapter 2, we introduce the most commonly used RFID personal tags – ePassports. We provide a brief description of the cryptographic protocols implemented for the purpose of security, and then point out the weaknesses of current deployments.

- In chapter 3, we address the problem of reader revocation in RFID based public key infrastructures – a weakness in all personal RFID deployments (including ePassports). First, we explain why this problem is harder in the case of RFID PKI’s. Next, we describe some trivial approaches to solve the problem and point out their shortcomings. We then go on to present our protocol for efficient reader revocation. Finally, we analyse the results of our usability study.

- In chapter 4, we address the problem of transaction verification in RFID enabled payment instruments. First, we present our protocol for transaction verification by using the integrated display unit. Finally, we show the results of our usability study.

- In chapter 5, we make our conclusions and describe our future work in the area of securing personal RFID tags.

- The appendix contains the questionnaires and project descriptions that were used on subjects and survey participants while conducting the user studies of the protocols for reader revocation and transaction verification.
Chapter 2

A Typical Personal RFID Tag –
The ePassport

2.1 Introduction

An electronic passport (ePassport) is an identification document which possesses relevant biographic and biometric information of its bearer. It also has embedded in it a Radio Frequency Identification (RFID) tag which is capable of cryptographic functionality. The successful implementation of Biometric and RFID technologies in documents such as ePassports aim to strengthen border security by reducing forgery and establishing without doubt the identity of the documents’ bearer.

RFID enabled passports were first adopted by Malaysia in 1998 [23]. However, until 2002, these passports failed to maintain basic security requirements since the passport holder information was not encrypted. The only security measure that was implemented was a digital signature on all the data to ensure that information could not be modified by adversaries. This was largely inadequate since it did not prevent
passports from being cloned, or illegal data gathering through passport skimming.

Later in 2004, as a guideline, the International Civil Aviation Organization issued a set of design guidelines and protocol specifications for nations that wished to implement RFID enabled passports. This was done in an attempt to standardize passport design while making them more secure. The security goals of the ICAOs ePassport specifications were identified as: Data Confidentiality, Data Integrity, Data Origin Authentication, Non Repudiation, Mutual Authentication, and Key Integrity.

Soon after the ICAO released their ePassport specifications, the first major initiative towards the global implementation of ePassports for increased border security was taken by the United States in 2006. It mandated the adoption of the ICAO specification by the twenty-seven nations in its Visa Waiver Program (VWP) [63]. As the US government pushed for the global adoption of ICAO’s ePassport standards, evidence of inadequate data protection aroused media attention and public concern [55]. As a result of these concerns, a new specification which included a set of protocols called Extended Access Control (EAC) that mitigated some of the privacy issues in the first generation of ePassports was proposed in 2006 [42]. The EAC protocol stack introduced the concept of mutual authentication which allowed the authentication of a tag and reader to each other. After its release, there were several proposals for the third generation ePassport scheme which included authentication protocols such as OSEP (Online Secure ePassport Protocol [50]) and an on line authentication mechanism based on the Elliptic Curve Diffie-Hellman key agreement [5].

Finally, in October 2008 a new protocol stack was released by the Bundesamt fur Sicherheit in der Informationstechnik (BSI) - Germany called EAC v2.01. This stack introduced a new version of tag and reader authentication which fixed some issues present in the original EAC proposal. In addition, a new protocol called Password Authenticated Connection Establishment (PACE) was added to the EAC protocol
stack. This protocol aimed to further improve security through stronger user authen-
tication.

2.2 The ePassport Logical Data Structure

<table>
<thead>
<tr>
<th>Data Group</th>
<th>Data Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>DG 1</td>
<td>Document Details</td>
</tr>
<tr>
<td>DG 2</td>
<td>Encoded Headshot</td>
</tr>
<tr>
<td>DG 3</td>
<td>Encoded Fingerprint</td>
</tr>
<tr>
<td>DG 4</td>
<td>Encoded Iris</td>
</tr>
<tr>
<td>DG 5</td>
<td>Displayed Portrait</td>
</tr>
<tr>
<td>DG 6</td>
<td>Reserved for Future Use</td>
</tr>
<tr>
<td>DG 7</td>
<td>Signature</td>
</tr>
<tr>
<td>DG 8 - DG 10</td>
<td>Data Features</td>
</tr>
<tr>
<td>DG 11- DG 13</td>
<td>Additional Data</td>
</tr>
<tr>
<td>DG 14</td>
<td>Chip Authentication Public Key</td>
</tr>
<tr>
<td>DG 15</td>
<td>Active Authentication Public Key</td>
</tr>
<tr>
<td>DG 16</td>
<td>Persons to Notify</td>
</tr>
<tr>
<td>SDE</td>
<td>Security Data Element</td>
</tr>
</tbody>
</table>

The ICAO issued a standardized data structure called Logical Data Structure (LDS) for the storage of data elements (the same LDS is used in all three generations of ePassports). This was to ensure that global interoperability for ePassport tags and readers could be maintained. The specifications state that all the 16 data groups are write protected and can be written only at the time of issue of the ePassport by the issuing state. A hash of the elements stored in data groups 1-16 are stored in the security data element (SDE), each of these hashes are signed by the ePassport issuing state.
2.3 The ePassport Public Key Infrastructure

A Public Key Infrastructure is required to aid the process of public key distribution and authentication. The Public Key Infrastructure for ePassports has remained unchanged over the last five years. The key elements in the ePassport PKI are the Country Verifying Certificate Authorities (CVCA) a.k.a Country Signing Certificate Authorities (CSCA), Document Verifiers (DV), and Inspection Systems (IS). The Public Key Infrastructure usually has a hierarchical structure.

The highest level body in each nation acts as the CSCA. The CSCA generates and stores a key-pair \((K{Pu}_{CSCA}, K{Pr}_{CSCA})\). The private key of the CSCA \((K{Pr}_{CSCA})\) is used to sign each Document Verifier (DV) certificate (from its own and from other countries). There are usually many Document Verifiers in each nation. Each of these Document Verifiers generates and stores a key-pair \((K{Pu}_{DV}, K{Pr}_{DV})\). The private key \((K{Pr}_{DV})\) of the DV is used to sign each Inspection System (reader) (IS) certificate in its domain and also the security data element (SDE) of every passport it issues.

In order to efficiently share DV certificates from all nations, the ICAO provides a Public Key Directory (PKD). The PKD will store only the certificates of all registered DV’s. This repository of certificates is available to every nation and is not read protected. Certificate Revocation Lists (CRL) may also be stored in the same PKD. Every nation is responsible for updating its own repository of public certificates and CRL’s by downloading them from the PKD, once this is done, each nation distributes the newly downloaded information to every DV and IS in its jurisdiction.
2.4 Security Protocols in ePassports

Please refer to Table 2.4 for explanations of the notation used in this section and Figures 2.3 - 2.9.

2.4.1 Basic Access Control

Basic Access Control is an optional protocol that attempts to ensure that only readers with physical access to the passport can read tag data. When a reader attempts to scan the BAC enabled ePassport, it engages in a protocol which requires the reader to prove knowledge of a pair of secret keys (called ‘access keys’) that are derived from data on the Machine Readable Zone (MRZ) of the passport. From these keys, a session key which is used for secure messaging is obtained.

- **Generating Access Keys:** The Access Keys \((K_{ENC}, K_{MAC})\) are derived from the following data available on the MRZ – the passport number (Doc No), date
Figure 2.2: ePassport Protocol Stack
of birth of the passport holder (DOB), expiration date of the passport (DOE), and 3 check digits (C).

\[
K_{\text{seed}} = 128\text{msb}(h(\text{DocNo}||\text{DOB}||\text{DOE}||\text{C}))
\]

\[
K_{\text{ENC}} = 128\text{msb}(h(K_{\text{seed}}||1))
\]

\[
K_{\text{MAC}} = 128\text{msb}(h(K_{\text{seed}}||2))
\]

\(h\) is the SHA-1 hashing algorithm and 128msb denotes the 128 most significant bits.

- **Challenge Response Protocol and Session Key Generation:** The challenge response protocol used to generate the session keys are illustrated in Figure 2.3.
2.4.2 Password Authenticated Connection Establishment

Password Authenticated Connection Establishment (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. The tag and the reader share a common password ($\pi$) which is used in conjunction with the Diffie-Hellman key agreement protocol to provide a strong session key. This password is called a CAN (Card Access Number). The CAN may be a short static or dynamic password. If the CAN is static, it is simply printed on the ePassport. If it is dynamic, the tag randomly selects it and displays it on the ePassport using low power display technologies such as OLED or ePaper. This password is then entered into the reader by the ePassport owner. The primary benefit of PACE is that it is less vulnerable to guessing and brute force attacks than BAC (owing to its much higher entropy).
2.4.3 Passive Authentication

Passive Authentication is the only mandatory cryptographic protocol in the three generations of ePassport protocols. 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. One must note that Passive Authentication does not tie the tag to a passport i.e., we can only establish that the data on the tag is correct, not the authenticity of the tag itself (i.e., it cannot detect cloning).

The Inspection System retrieves the certificate of the issuing document verifier, using the public key from the certificate it verifies the digital signature used to sign the data in the LDS. Once the validity of the signature is established, the reader computes the hash of each of these data elements and compares them with the hashed values stored in the SDE. If there is a match, it can be established that the data on the tag was not manipulated.

2.4.4 Active Authentication

Active Authentication is an optional protocol in all three generations of ePassports. Using a simple challenge-response mechanism, it aims to detect if a tag has been substituted or cloned.

If Active Authentication is supported, the tag on the ePassport stores a public key ($K_{Pu_{AA}}$) in Data Group 15 and its hash representation in the SDE. The corresponding private key ($K_{Pr_{AA}}$) is stored in the secure section of tag memory. In order for the tag to establish its authenticity, it must prove to the reader that it possesses this private key. The protocol is illustrated in Figure 2.5.
Note: The private key ($KPr_{AA}$) must be tied to the ePassport and biometrics of the owner in order to prevent man-in-the-middle attacks against Active Authentication.

### 2.4.5 Chip Authentication Version 1

The Chip Authentication (version 1) protocol is a mandatory protocol in the BSI v1.0 specifications. It was put in place to replace Active Authentication as a mechanism to detect cloned ePassports. It does this by having the tag prove possession of a private key that is stored in the secure section of tag memory.

If Chip Authentication is performed successfully it establishes a new pair of encryption and MAC keys to replace BAC derived session keys and restarts secure messaging with these new keys. It does this using the static Diffie-Hellman key agreement.
protocol. Note that the ePassport Tag already has a Chip Authentication public key – $TKPu_{CA}$ (in Data Group 14) and private key – $TKPr_{CA}$ (in the secure section of tag memory). The process of Chip Authentication is illustrated in Figure 2.6.

Note: As in Active Authentication, the private key of the tag must be tied to the ePassport and the biometrics of the owner to prevent man-in-the-middle attacks.

### 2.4.6 Reader Authentication Version 1

The Reader Authentication (version 1) protocol is optional and 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 the previously executed Chip Authentication protocol. The reader proves to the tag using digital certificates...
that it has been authorized by the home and visiting nation to read ePassport Tags. The process of authentication is illustrated in Figure 2.7.

2.4.7 Reader Authentication Version 2

In the new specifications (EAC v2), Reader Authentication must be performed before Chip Authentication. The purpose of this authentication protocol is to allow the tag to validate the reader before granting it access to sensitive biometric information or even authenticating itself. It works on a two pass challenge-response scheme. The reader proves to the tag using digital certificates that it has been authorized by the home and visiting nation to read ePassport Tags. The process of authentication is illustrated in Figure 2.8.
2.4.8 Chip Authentication Version 2

The Chip Authentication protocol in the EAC v2 specifications, is executed only after the Reader Authentication protocol is executed. This is a necessity since the Chip Authentication protocol requires the ephemeral Diffie-Hellman key pair that was generated in the Reader Authentication phase.

If Chip Authentication is performed successfully it establishes a new pair of encryption and MAC keys to replace BAC derived session keys and restarts secure messaging with these new keys. It does this using the static Diffie-Hellman key agreement protocol. Note that the ePassport Tag already has a Chip Authentication public key – $TKPu_{CA}$ (in Data Group 14) and private key – $TKPr_{CA}$ (in the secure section of tag memory). The process of Chip Authentication is illustrated in Figure 2.9.
2.5 Weaknesses of ePassport Security Protocols and Specifications

The primary causes for concern with ePassports are their vulnerability to clandestine scanning, skimming, tracking, and cloning. These concerns arise out of the following flaws in their specifications.

2.5.1 Optional Status of BAC, PACE and Active Authentication

The BAC (or PACE in EAC v2.01) and Active Authentication schemes are only optional – it is not mandatory for all nations to incorporate them into their ePassports.
If these protocols are not implemented in conjunction with RFID technology, ePassport holders become much more vulnerable to adversaries (than regular passport holders).

This argument is easy to justify – the lack of tag authentication and access control techniques allow an adversary to skim data from the tag without the holders knowledge (this is possible because of lack of access control), clone the ePassport, and use this cloned ePassport successfully (this is possible because of lack of tag authentication). In comparison, in regular passports, accessing and cloning the passport is not possible unless the adversary has physical access to it.

Note: In the EAC v1.0 and EAC v2.01 specifications, the presence and mandatory status of the Chip Authentication protocols mitigate the latter part of the above problem by providing a means to detect cloned tags.
2.5.2 Low Entropy of the BAC Seed Key

The BAC is the only protocol designed for the purpose of access control to protect ePassport holders from skimming and eavesdropping attacks in the ICAO and EAC v1.0 specifications. Unfortunately, the security of the entire protocol is based on the entropy of the seed key (which generates the two access keys) which is derived from data items on the MRZ of the ePassport.

While the entropy of the seed key is claimed to be 56 bits, most of these bits are easily guessable (for example, the entropy of the date of birth field can be reduced to null for diplomats and dignitaries – since their date of birth is public information). Several attacks on Dutch and German ePassport seed keys have shown that the entropy of BAC seed key can be reduced to the range of 25-35 bits \[7, 24\] by cleverly guessing other bits that correspond to the ePassports number and the expiry date of the ePassport.

The predictability of the bits of the seed key is a serious flaw – an adversary who correctly guesses the entire key will be able to read and track the tag throughout the lifetime of the ePassport.

Note: This problem does not exist with PACE, since the CAN is a randomly generated number that is not associated with any data from the ePassport.

2.5.3 Lack of Access Rules

The ICAO first generation ePassport specifications do not have special access rules for secondary biometrics such as fingerprints and iris images which are considered to be more sensitive than other accessible information. This lack of access rules makes it easily possible for parties to obtain access to information that is very private and
they clearly do not require. For example, it is easy for hotel receptionists, car rental agencies, and other organizations, to access and store a client’s biometric information.

Further, when combined with the above two vulnerabilities, it is possible for any individual with a 12.56MHz reader to access this highly sensitive data. At this point, an adversary may be able to use the stolen information to commit identity theft – a growing problem in today’s world.

Note: This problem does not exist in either of the EAC specifications – only readers which go through the Reader Authentication phase are granted access to biometric and other sensitive data.

2.5.4 Poor Detection of Expired or Revoked Readers

Since even a high-end tag is a passive device, there is no way for it to maintain a clock. Thus, the 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.

ePassports use a simple monotonically increasing time-stamp which is updated after every successful tag-reader interaction with the reader’s certificate issuance date. Whenever the 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 e-Passports. In the case of ePassport tags which store sensitive data such as biometrics and other personal data, it is possible for an adversary to easily obtain this information and use it in malicious activities such as identity theft or forgery.

Note: This vulnerability is solved by implementing our protocol for reader revocation checking described in chapter 3.

<table>
<thead>
<tr>
<th>Description</th>
<th>Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1 hash function</td>
<td>$h$</td>
</tr>
<tr>
<td>Most significant bits</td>
<td>$msb$</td>
</tr>
<tr>
<td>Random number</td>
<td>$R$</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>$K_{ENC}$</td>
</tr>
<tr>
<td>MAC Key</td>
<td>$K_{MAC}$</td>
</tr>
<tr>
<td>3-DES Encryption Algorithm under key $K_{ENC}$</td>
<td>$E_{K_{ENC}}$</td>
</tr>
<tr>
<td>3-DES Decryption Algorithm under key $K_{ENC}$</td>
<td>$D_{K_{ENC}}$</td>
</tr>
<tr>
<td>ANSI MAC under key $K_{MAC}$</td>
<td>$M_{K_{MAC}}$</td>
</tr>
<tr>
<td>Digital Signature on $X$ with key $K$</td>
<td>$Sign(X,K)$</td>
</tr>
<tr>
<td>Active Authentication public key</td>
<td>$KP_{uAA}$</td>
</tr>
<tr>
<td>Active Authentication private key</td>
<td>$KP_{rAA}$</td>
</tr>
<tr>
<td>PACE - Tag public key</td>
<td>$TKP_{uPACE}$</td>
</tr>
<tr>
<td>PACE - Tag private key</td>
<td>$TKP_{rPACE}$</td>
</tr>
<tr>
<td>PACE - Reader public key</td>
<td>$RPK_{uPACE}$</td>
</tr>
<tr>
<td>PACE - Reader private key</td>
<td>$RPK_{rPACE}$</td>
</tr>
<tr>
<td>Chip Authentication - Tag public key</td>
<td>$TKP_{uCA}$</td>
</tr>
<tr>
<td>Chip Authentication - Tag private key</td>
<td>$TKP_{rCA}$</td>
</tr>
<tr>
<td>Chip Authentication - Reader public key</td>
<td>$RPK_{uCA}$</td>
</tr>
<tr>
<td>Chip Authentication - Reader private key</td>
<td>$RPK_{rCA}$</td>
</tr>
<tr>
<td>Diffie Hellman key generation parameters</td>
<td>$D$</td>
</tr>
<tr>
<td>Reader (Inspection System) certificate - Issued by local DV</td>
<td>$CERT_{IS}$</td>
</tr>
<tr>
<td>Issuing DV certificate - Issued by local CVCA</td>
<td>$CERT_{DV}$</td>
</tr>
<tr>
<td>Reader public key</td>
<td>$RP_{u}$</td>
</tr>
<tr>
<td>Reader private key</td>
<td>$RP_{r}$</td>
</tr>
<tr>
<td>Reader (Terminal) Authentication - Tag public key</td>
<td>$TKP_{uTA}$</td>
</tr>
<tr>
<td>Reader (Terminal) Authentication - Tag private key</td>
<td>$TKP_{rTA}$</td>
</tr>
<tr>
<td>Reader (Terminal) Authentication - Reader public key</td>
<td>$RPK_{uTA}$</td>
</tr>
<tr>
<td>Reader (Terminal) Authentication - Reader private key</td>
<td>$RPK_{rTA}$</td>
</tr>
</tbody>
</table>
Chapter 3

Addressing Reader Revocation in Personal RFID Based PKIs

3.1 Introduction

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) [19] and similar structures, or on-line, using protocols such as Open Certificate Status Protocol (OCSP) [43]. 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

\(^1\)The only exception is Certificate Revocation System (CRS) [40] which is purely implicit.
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.

### 3.2 Motivation

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., ePassports and eLicenses), 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 [66].

Thus far, it might seem that our motivation is based solely on the need to detect prematurely revoked reader certificates. 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.

2“Prematurely” means before the expiration of the PKC.
3.2.1 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 public key enabled (pk-enabled) tag and has been already incorporated into some reader authentication schemes, e.g., [10], [22]. 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, on line revocation checking protocols (e.g., OCSP used with nonces [43]) 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, [60] 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 [10]. 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.

3.3 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 [19]. Other techniques that improve the efficiency of revocation checking are:

- Certificate Revocation Trees (CRTs) [31] use Merkle’s Hash Trees [38] to communicate relatively shorter proofs of (non-)revocation.

- Skip-lists [14] and 2-3 Trees [44] improve on the CRT update procedure through the use of dynamic data structures, offering asymptotically shorter proofs.

- Online Certificate Status Protocol(OCSP) [43] is an on-line verification ap-
proach that reduces storage requirements and provides timely revocation status information.


- Other related results focused on privacy issues in certificate revocation checking, e.g., [45].

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., [41, 18] in e-Passports, [17] in eCredit-Cards, and [11, 49] in other applications.

The only seemingly viable approach [60] 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 [10], 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. [8].

To the best of our knowledge, the idea of outfitting pk-enabled RFID tags with display units for enhanced security was introduced by Ullman [61]. 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 [60], 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.

3.4 Trivial Solutions

As discussed in earlier, 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.

3.4.1 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.

### 3.4.2 On-line Revocation Checking

Online revocation-checking approaches, such as the Online Certificate Status Protocol (OCSP) [43], 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 are not designed to be good random number generators or handle long-lasting on-line communication protocols. More importantly, the assumption of every reader being always connected to the infrastructure is quite unrealistic. Further, the implementation of OCSP 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 requiring a signed reply can result in congested responders and increase overall transaction delays.

### 3.4.3 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.

### 3.5 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.

#### 3.5.1 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.
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.
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”.
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.

### 3.5.2 Protocol

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 $CRL_{iss}$ and $CRL_{exp}$ denote the purported CRL issuance and expiration times, respectively. Let $PKC_{iss}$ and $PKC_{exp}$ be the purported Public Key Certificate (PKC) issuance and expiration times, respectively.

2. If $CRL_{iss} \geq PKC_{exp}$, 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 $CRL_{exp}$ and $PKC_{exp}$. 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 the displayed date 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 displayed date is stale, the user terminates the protocol by initiating an escape action while the tag is still in countdown stage.

[OPTION B:] (If Assumption 10 holds)

(a) If the displayed date 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 displayed date is stale, the timer runs out and the tag automatically aborts the protocol (with no user action is needed).

3.5.3 Escape Actions

As evident from the protocol description above, escape action is required whenever the user decides that the displayed date 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.
Recent developments in low power hardware integration on contactless cards have led to deployment of buttons on RFID tags [33, 62]. 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 [28]. A drawback of such techniques is that physical damage to the tag

---

3 A rump session talk at PETS’09 shed some doubts on today’s Faraday Cage-enclosed e-passports.
is a possibility if the switch is handled roughly.

3.6 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 [45].

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 [45] requires the CA\textsuperscript{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 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:

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

\textsuperscript{4}In practice, a separate entity called a Revocation Authority (RA)
where, $CRL_{iss}$ 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.

\[
Sign(1) = \{ h(CRL_{iss}||SN_i||-\infty) \}_{SK_{RA}} \tag{3.2}
\]

\[
Sign(n + 1) = \{ h(CRL_{iss}||+\infty||SN_n) \}_{SK_{RA}} \tag{3.3}
\]

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:

\[
SN_j, \ SN_{j-1}, \ CRL_{iss}, \ Sign(j) \tag{3.4}
\]

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 $CRL_{exp}$, as in step 5 of our protocol.
3.6.1 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 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: CRL’s impose linear overhead, whereas, the modified CRL method is bandwidth-optimal, requiring only the transmission of two serial numbers, issuance date and a signature.

3.7 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.

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 the next section, 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 [65]. 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.

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.

3.8 Usability Analysis

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 proto-
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: on line 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?

### 3.8.1 On-line Survey

We created a comprehensive on line survey [48] 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) [9]. They also answered 4 additional questions, as discussed later in this section.

**Subject Background**

98 individuals completed the (anonymous) on line 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:
Gender distribution was 78% male and 22% female. The subjects were generally well-educated with 97% having a bachelor’s or higher degree. A small minority of the 95 subjects had handicaps which interfered with their visual perception (11.83%) or their handling of devices with small keypads (1.08%).

**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% [37]. 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.
3.8.2 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 [2] (simulating the tag) and a Nokia E51 [1] (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\textsuperscript{5}. 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.

\textsuperscript{5}“+/-” indicates future/past dates, respectively.
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 3.8.3 below.

User Opinion: People who tried our mock-up implementation on cell-phones rated its usability at 77% on the System Usability Scale (SUS) [9], 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.
3.8.3 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.

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 eg., displaying a date in YYYYMMDD (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.

3.9 Feasibility Analysis

3.9.1 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
Figure 3.4: Modified ePassport protocol with revocation status checking
3.9.2 Power Analysis

ePassport tags such as those supplied by Infineon Technologies, require up to 55mW of power to operate [20] 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 approximately 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 3.5), with circuit parameters set in the manner described by Scholz et al. [56].

First, we establish a relationship between the mutual inductance (M) and the distance (x) between the antenna of the tag and the reader.

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

(3.5)

Where \( \mu \) 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

\[
M = \frac{1.57 \times 10^{-12}}{x^3}
\]

(3.6)

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.

\[
P_{tag} = I_1^2 R_T
\]

(3.7)

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

\[
R_T = \frac{M^2 R_L}{L_2^2}
\]

(3.8)

Where \( L_2 \) is assigned a value of 168nH [56] and \( R_L \) is the load resistance given by (5).

\[
R_L = \frac{V_T^2}{P_{tag}}
\]

(3.9)
$V_T$ is the voltage required in the tag circuit (5.5 Volts). The value of $R_L$ is 195.1 $\Omega$ in the case that the ePassport tag and display unit operate at maximum power together (case 1). $R_L$ is 302.5 $\Omega$ 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 $P_{tag}$.

$$x^6 = \frac{(1.57 \times 10^{-12})^2 \times (I_1)^2 \times (R_L)}{P_{tag} \times (L_2)^2}$$ \hspace{1cm} (3.10)

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:

  $$P_{tag} = 55 \text{ mW}, \ R_L = 550 \text{ $\Omega$} \implies x = .097 \text{ m (9.7 cm)}$$ \hspace{1cm} (3.11)

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

  $$P_{tag} = 100 \text{ mW}, \ R_L = 302.5 \text{ $\Omega$} \implies x = .080 \text{ m (8 cm)}$$ \hspace{1cm} (3.12)

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

  $$P_{tag} = 155 \text{ mW}, \ R_L = 195.1 \text{ $\Omega$} \implies x = .069 \text{ m (6.9 cm)}$$ \hspace{1cm} (3.13)

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 [10]. 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.
Chapter 4

Transaction Verification in Personal RFID Payment Instruments

4.1 Introduction

Credit and debit cards have long been accepted as a convenient alternative to carrying wads of cash in a wallet. However, while it has been accepted by the public, credit card fraud has been a rather expensive problem that has plagued societies around the world for more than a decade. There has been some significant effort over the last few years by the EMV to quell this problem. One such effort led to the introduction of RFID enabled credit cards in 2006 [57]. RFID enabled credit cards were introduced in the United States by American Express (ExpressPay), Mastercard (Pay Pass), and Visa (Pay Wave) in 2006. Following this, RFID tags have been deployed for use in other environments to make transactions (e.g., as insurance IDs and voting cards).
In such settings, an auxiliary channel between the tag and the user is needed 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 tags owner 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 RFID enabled payment card would solve this problem by showing the transaction amount (with other information such as credited account, etc.) requested by the reader on its display and waiting for explicit user approval before authorizing it. This display resolves one of the weaknesses in current deployments of payment instruments – the lack of trusted interfaces [47].

Statistics from the United Kingdom alone indicate losses of over £609 million in 2008 due to card fraud – 17% of this loss results from disputes regarding incorrect charges at retail (Point-of-Sale) locations [6]. This not only causes trouble for the credit card companies that have to process these disputes, but also for customers who unfortunately sometimes lose points on their credit score as a result of these disputes [4].

Out of band (OOB) communication (SMS, Telephone calls, etc.) is the best way to handle transaction verification in card not present (CNP) environments and we do not intend to replace it for such transactions. However, we argue that OOB verification is not just time inefficient, but also a rather inconvenient procedure for customers to undergo on a regular basis, as they would if it were implemented for POS transactions. Our proposal aims to solve the problem of (on the fly) transaction verification in POS environments only.
4.2 Proposed Solution

Our approach is designed for any RFID enabled transaction instrument. It’s primary goal is to provide simple, efficient, and usable transaction verification at a POS. In the rest of this section, we discuss our assumptions and details of the proposed solution.

4.2.1 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 aware of the transaction amount.

2. Each tag is equipped with a small one-line character display capable of showing a 4-8 digit number in a reasonably legible format.

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”.

4. A tag can not be activated without the consent of the user. For example, in case of credit cards, the tag is physically inside a wallet which may have a Faraday Cage in it. The user normally keeps the wallet closed thus preventing any contact with the tag.

5. While powered up by a reader, a tag is capable of starting and running a short timer.

6. [Optional] A tag may have a single button for user input to initiate an escape action.
Figure 4.1: Typical POS Transaction Procedure

Figure 4.2: Modified POS Transaction Procedure with Transaction Verification for RFID Enabled Payment Instruments
4.2.2 Protocol

Before a tag participates and performs any transaction, it must allow the owner to validate and verify the transaction. 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 payment tag receives the transaction details from the reader after both the reader and the tag have been authenticated, but before the details have been passed on to the payment gateway (i.e., before step 1 in Figure 4.1).

2. The tag verifies that the details (such as issuing bank, account number, etc.) on the transaction statement match the data that was presented on the readers certificate during the reader authentication phase. The transaction is aborted if there is a mismatch. This is to prevent man-in-the-middle attacks.

3. The tag extracts critical user verifiable data such as the amount charges, account holder credited, etc., and displays it on the integrated display unit. It then enters into a countdown stage that lasts for a predetermined duration (e.g., 10 seconds).

4. The user views the transaction information on the display unit.

[OPTION A:]

(a) If the transaction amount and other details are deemed correct by the user, he does nothing for the duration of the countdown. After the countdown is complete, the tag signs the time stamped transaction statement and returns it back to the reader. This signed statement is then sent through the various stages depicted in Figure 4.1.

(b) Else, if the details are noted to be incorrect, the user terminates the protocol by initiating an escape action (as in section ??) while the tag is still in
countdown stage. The tag does not send back the signed statement, thus preventing the reader from proceeding with the transaction.

[OPTION B:] (If Assumption 6 holds)

(a) If the transaction amount and other details are deemed correct by the user, he presses the button on the tag before the timer runs out. At this point, the tag signs the time stamped transaction statement and returns it back to the reader. This signed statement is then sent through the various stages depicted in Figure 4.1.

(b) Else, if the details are noted to be incorrect, the timer runs out and the tag automatically aborts the protocol (with no user action needed). The tag does not send back the signed statement, thus preventing the reader from proceeding with the transaction.

The effect of the proposed transaction verification protocol for RFID enabled payment instruments on the typical POS transaction procedure is illustrated in Figure 4.2.

4.3 Usability Analysis

Since our technique requires active user involvement, its usability is one of the key factors influencing its potential acceptance. Thus, we conducted a usability study consisting of an on line survey. The goal of the survey was to answer the following questions:

1. Do everyday users worry about being charged incorrectly at a POS?

2. How do prospective users rate the usability of our solution?
Although no tests with prototypes and real users were carried out, we would like to point out that the security and usability tests conducted by Uzun et al. in [29, 34] for various device pairing techniques (including the compare-and-confirm method) indicated that users rarely made errors or took a very long time while comparing numbers on two displays. This, in addition to the high SUS score that was received by the compare-and-confirm method leads us to believe that our solution will be usable and unlikely to result in significant error rates from users.

4.3.1 On-line Survey

We created a comprehensive on line survey [48] 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 transaction verifica-
tion 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) [9]. They also answered 4 additional questions, as discussed later in this section.

**Subject Background**

98 individuals completed the (anonymous) on line 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. A small minority of the 95 subjects had handicaps which interfered with their visual perception (11.83%) or their handling of devices with small keypads (1.08%).

**4.3.2 Survey Results**

Based on the data collected from the results of the conducted survey, we address the questions raised in the beginning of this section:
Are people worried about being charged incorrectly at a POS?

From the 98 survey participants, 89% indicated that they were worried about completely unauthorized charges to their accounts and 80.4% were also worried about authorized parties making incorrect charges to their account. These questions received scores of 4.34 (with a standard deviation of 0.87) and 4.05 (with a standard deviation of 1.04) respectively on a 5-point Likert scale. Further, 67% of the participants indicated that they were more concerned about unauthorized charges to their accounts while using RFID enabled payment instruments. We attribute some of this increased concern to misinformation that is propagated on the internet and by the media about the threats of RFID.

How do people rate the usability of our solution?

Given the detailed description of the method and the required interaction, 98 participants rated its usability at 75.75% on the SUS questionnaire. This score is significantly higher than the industry average of 62.1% and indicates good usability and acceptability characteristics. Further, 74.2% of the participants stated that they would like to see this solution implemented on their creditcards for regular use, while 17.5% were neutral to the idea and the average score on 5-point Likert scale was 3.97 (with a standard deviation of 1.03).
Chapter 5

Future Work and Conclusions

5.1 Future Work

The 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 and button 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 [62]. Although this might seem high, we note that once a display is available, it can be used for purposes other than revocation status checking and transaction verification, 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.

Due to the sensitive nature of data stored in personal RFID tags, it might be necessary for a user to authenticate to a tag (e.g., credit card or passport). It is important
that such a mechanism is implemented in order to prevent personal tags from revealing data to (not-necessarily revoked) readers when they (i.e., the tags) are lost or stolen. Currently this can be done only via trusted third party devices such as mobile phones [54], personal computers and wearable beepers [27] – which may also be stolen (it is likely that users store all these devices in a single location while traveling). However, in the future, if a display-equipped RFID tag also has a small (known to be feasible) input interfaces (e.g., buttons) the need for third parties can be obviated. Further, we argue that the assumptions made in previous work [54, 12] are less realistic since they work only on WISP [51] tags which are equipped with accelerometers to detect motion or vibrations. Such tags are also known to operate with UHF waves which are not used by most personal RFID tags.

A display may also 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 [61]. Also, other visual channel-based secure device pairing methods that were proposed for personal gadgets can be used with display-equipped RFID tags. (See [35] and [30] 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.

5.2 Conclusions

In this thesis, we presented a simple and effective method for dealing with reader revocation checking on personal RFID tags. Our solution requires a tag to be equipped
with a small display unit and be attended by a human user during certificate validation. As long as the user (tag owner) plays their part correctly, our solution eliminates the period of vulnerability with respect to revoked readers. We also proposed a protocol for transaction verification in personal tags used as payment instruments. This protocol also makes use of the integrated display unit (thus amortizing its cost).

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 both the solutions for both – reader revocation and transaction verification – 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 methods proposed in this thesis will be applicable to a wide variety of personal RFID tags.
Bibliography


Appendices

A Questionnaire: Usability Analysis for Reader Revocation and Transaction Verification

A.1 Demographics

1. Age
   - 18-24
   - 25-29
   - 30-34
   - 35-39
   - 40+

2. Gender
   - Male
   - Female

3. Highest Educational Degree Completed
• High School
• Bachelors
• Masters
• Doctoral

4. Do you experience any difficulties with your visual perception? (Do not select 'Yes' if you can recover full visual abilities by using glasses, contact lenses, etc.)

• Yes
• No

5. Do you have any physical condition that may interfere with holding objects steady or typing on small keypads?

• Yes
• No

A.2 Project Background Information and Description

Currently, many passports have small radio chips embedded inside them. Such chips digitally store passport owner’s biometric and personal data to prevent counterfeiting and unauthorized use. However, currently the information stored in these chips can be read from a distance without the owner’s explicit authorization. Thus, it is important to give owner the control of when his information can be read. Moreover, the current systems don’t provide a mechanism to assure the interacted readers are currently authorized to handle this kind of sensitive information. For better security, it is essential to verify the reader’s authorization has not expired or revoked.
Contactless payment cards (e.g. Mastercard Paypass or Visa Payware) also suffer from similar vulnerabilities, e.g., a payment card can be charged from a distance without the card owner’s consent. Even in the scenarios where the card owner authorizes his credit card to be charged, it is not possible to know the charged amount before seeing the card statement (Note that a malicious merchant can easily tamper with a cash register to make it print misleading receipts or show incorrect amounts on its screen, so the actual amount charged on the card can be different than the one shown on the register receipt).

In this study, we want to get your opinion on a solution that addresses the above mentioned problems. The solution uses a thin and flexible display and a button on ePassport and contactless payment cards. These additions are perfectly feasible using today’s technology and we ask you to assume such ePassports and contactless payment cards are already available.

In the next pages, you will be given a use case followed by several questions. Please read the use cases before starting to answer questions.

A.3 Reader Revocation in ePassports

Please answer the following the questions based on the ePassport use case described above.

1. I think that I would like to use this method frequently.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

2. I found the method unnecessarily complex.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree
When you use your ePassport for identification (at control points, travel agencies, rental counters, etc.), check to see if the displayed date (i.e., expiration date of the reader’s license) is sometime in the future. If it is, the reader can be trusted and pressing the OK button (within 10 seconds) on your passport will allow it to be read. However, if the displayed date is in the past, the reader is not authorized to handle sensitive information anymore and NOT pressing the OK button will automatically cancel the communication without revealing any information to the reader.
3. I thought that the method was easy to use.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

4. I think that I would need the support of a technical person to be able to use this method.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

5. I found the various functions in this method were well integrated.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

6. I thought there was too much inconsistency in this method.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

7. I would imagine that most people would learn to use this method very quickly.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

8. I think the method is very cumbersome to use.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

9. I feel very confident about using the method.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

10. I need to learn a lot of things before I can get going with this method.
    Strongly disagree, Disagree, Neutral, Agree, Strongly agree

11. I would like to see my ePassport equipped with the above solution.
    Strongly disagree, Disagree, Neutral, Agree, Strongly agree

12. I am worried about revealing my personal information to unauthorized parties.
    Strongly disagree, Disagree, Neutral, Agree, Strongly agree
Whenever you use your contactless payment card, check to see if your card is being charged the correct amount. The display on your card shows the amount you will be billed and pressing the button (within 10 seconds) on your card allows the transaction to go through. On the other hand, if the displayed amount is NOT correct, you can cancel the transaction by NOT pressing the button. And if a transaction is canceled, your card will not reveal any of your account information to the merchant.

Figure A.2: Credit card transaction verification procedure

13. I am worried about identity theft.

   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

14. In a normal day, I would know the date with...

   - No error
   - Error of at most +/- 1 day
   - Error of at most +/- 3 day
   - Error of at most +/- 7 days
   - Error of more than +/- 1 week
A.4 Transaction Verification in Credit Cards

Please answer the following the questions based on the Credit Card use case described above.

1. I think that I would like to use this method frequently.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

2. I found the method unnecessarily complex.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

3. I thought that the method was easy to use.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

4. I think that I would need the support of a technical person to be able to use this method.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

5. I found the various functions in this method were well integrated.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

6. I thought there was too much inconsistency in this method.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

7. I would imagine that most people would learn to use this method very quickly.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

8. I think the method is very cumbersome to use.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree
9. I feel very confident about using the method.
   Strongly disagree, Disagree, Neutral, Agree, Strongly agree

10. I need to learn a lot of things before I can get going with this method.
    Strongly disagree, Disagree, Neutral, Agree, Strongly agree

11. I would like to see my contactless credit cards to be equipped with the described system.
    Strongly disagree, Disagree, Neutral, Agree, Strongly agree

12. When using my credit card(s), I am concerned about being charged for an incorrect amount.
    Strongly disagree, Disagree, Neutral, Agree, Strongly agree

13. In general, I am concerned about unauthorized charges on my credit card(s).
    Strongly disagree, Disagree, Neutral, Agree, Strongly agree

14. If I had a contactless credit card (without a button and a display), I would be more concerned about unauthorized charges.
    Strongly disagree, Disagree, Neutral, Agree, Strongly agree