RFID Based E-Passport System

by

Sharon-Rose Mavengawenyu (R123915N)

Submitted in partial fulfillment for the degree of

BSC (HONS) TELECOMMUNICATIONS

Department of Applied Physics and Telecommunications

in the Faculty of Science and Technology.

Midlands State University

Gweru, Zimbabwe

June 2016

Supervisor: Dr. Nyamhere

[HTEL 438 Dissertation]

Abstract

This dissertation analyses the use of RFID cards as e-passports instead of the conventional paper passport booklet with an embedded chip as the e-passport. Advancement in technology comes with so many possibilities that all information can be stored electronically. The purpose is to limit the use of counterfeit documents. This in turn will prevent illegal entry of the traveller into any specific country at the same time maintaining the privacy and personal security of the e-passport bearers.

To

My Husband Benson Share, my son Stonewall Atidaishe Share, the Mavengawenyu family
and the Share family

DECLARATION

I, **Sharon-Rose Mavengawenyu** hereby declare that I am the sole author of this dissertation entitled “RFID based e-passport system”. I authorize Midlands State University to this dissertation only for purposes of scholarly research.

Signature……………………………………….. Date………………………………………

Approval

This dissertation/thesis entitled "RFID based e-passport system" by **Sharon-Rose Mavengawenyu** meets the regulations governing the award of the degree of *BSc Telecommunications Honours* of the Midlands State University, and is approved for its contribution to knowledge and literal presentation.

Supervisor…………………………….............Date……………………………………….....

Acknowledgements

First and foremost I would like to thank the Almighty God who granted me this opportunity and strength to do this project. Special thanks goes to my husband Benson Share for the love and support financially and morally; the Mavengawenyu family and the Share family for the continuous encouragements throughout this whole period. I would also like to thank my colleagues; their push and motivational support gave me hope during this period. Last but not least special thanks go to my supervisor Dr. Nyamhere for his unreserved and endless support, assistance and patience he rendered to me throughout the whole study.

Table of Contents

List of Figures

List of Tables

CHAPTER 1

1.0 Introduction

Until recently, the travel documents such as a passport where just on paper possessing only the biographic information of the holder. However there has been a shift in technology such that biometric technologies may now be implemented in travel documents. When implemented in travel documents such as passports these are known as electronic passports (e-passports) aiming at strengthening security and reducing forgery. Secure and trusted travel documents are an essential part of international security, as they allow states and international institutions to identify the movement of undesired or dangerous persons. [1]

This project is demonstrating the implementation of an e-passport using Radio Frequency Identity (RFID) cards to store both the biographic and biometric information of the holder, at the same time exasperating to overcome the limitations that come with RFID such as:

i. RFID is susceptible to easy disruption – this is because RFID systems make use of the electromagnetic spectrum thus they are easy to jam if energy is applied at the right frequency. If this is to happen at the border control checkpoints it can be very disastrous and it will inconvenience the travellers because this will mean longer waits at the checkpoints.

ii. RFID reader collision - If this system is to be implemented most probably at the border control check points there will be many readers, then certain techniques must be implemented to overcome this problem. Reader collision takes place when there are two or more signals from different readers that will be overlapping. One of the techniques that may be implemented to overcome this problem is making use of an anti-collision protocol.

iii. Tag collision – If this system is implemented this is a more realistic problem as it is due to the presence of many tags in a small area. At the border controls of a truth there is no point where there will only be one tag to be read, but the reader must be able to differentiate signals from different tags if this is achieved then at the same time the chances of having one's RFID card being read without their knowledge is reduced or even eliminated. Also if this is achieved this will mean that tags will only be read when tapped, swiped or scanned.

iv. Security problems with RFID – If RFID tags are used with a high gain antenna they may be read at a greater distance leading to privacy problems. However this may be overcome by using low gain antennas such that the distance between the tag and the reader is kept very small.

The project is interested in finding out if the integration of RFID into passports will improve the robustness against identity theft by storing the information of the passport bearer electronically on an RFID card in the project prototype and identifying the e-passport holder. The implementation of the RFID e-passports might eventually replace the conventional paper passport and accelerate clearance through passport controls.

1.1 Background

E-passports are already in use in many European countries and the other developed countries but it came to note that in all the countries where these e-passports are in use none of them use RFID cards as passports but instead they are using the conventional passport booklets with contactless chips inserted in them. Electronic passport rollout plans continue to move forward, but some many countries, continue to lag behind. [2] For most African countries and some of the countries which are underdeveloped, the migration from the conventional passport to the e-passport is taking ages because it is expensive for them to acquire the chip let alone manufacturing it. For instance Zimbabwe is a country which is in the process of reviving its economy and hence to produce a passport booklet together with a contactless chip in it is comparable to incurring a double cost. Thus this project aims at providing an affordable solution of overcoming the gap in electronic travel documents which is making most of the underdeveloped countries lag behind by providing an RFID card which will serve as a passport document and maybe in the near future an electronic identity card (e-ID). If this is implemented it is interesting to find out that the cost of manufacturing passports and identity cards might be reduced by double the price it is costing the country now. On eBay the cost of an RFID card and reader kit ranges from at least US$2.50 – US$30 depending on the range in which they operate. In this project low frequency ranges are used and these are not very expensive as their prices range from $2.50 to approximately $15. Currently for a conventional passport booklet it costs US$50 + US$3 for the application form giving a total amount of US$53 in Zimbabwe. This is for the one which the applicant has to collect after six weeks at least. If we are to add the cost of the RFID kit that is considering the high value which is the US$15 together with the application form cost it amounts to a total of $18 which is far much less than the US$53. Hence this will not only lead to a reduction in the cost of manufacturing the passport but will also mean shorter waiting periods which is less than six weeks for the passport to be processed. With the implementation of RFID based e-passports, passports will be issued in a matter of hours as only the cards will have to be configured with the holder's information upon completion of the application form.

1.2 Aims of Study

To design a prototype that will resemble the operation of an e-passport booklet but using an RFID card eliminating the conventional paper passport booklet. The objective is to improve passport security by creating a stronger link between the passport and its holder.

1.3 Purpose of Study

To design a prototype that will reduce forgery, duplication of data entry, look-alike fraud, photo substitution, which may be done by any holder of a conventional passport booklet. To come up with a more efficient travel document with less human intervention eliminating the fraud associated with a paper passport. This system will allow the biographic information such as family name, date of birth, gender, ID number of the bearer to be electronically stored in the system. This can also result in faster movement at the border controls as the bearers just have to tap their RFID cards in front of the card readers and if the fingerprint scanner is present then their fingerprints can be taken there on real time basis to verify if the ones taken presently will match the fingerprints already stored in a template in the database. [2]

1.4 Objectives of Study

Primary Objective

- To develop an e-passport system using RFID cards.

Secondary Objectives

- To provide an affordable solution with the adoption of e-passports in Zimbabwe.
- To enhance imposter detection.
- To make it almost impossible to alter a document for use in gaining admission.
- To guard against multiple passport issuances to the same person.
- To provide protection against identity theft.

- Above all provide a system that protects privacy.

1.5 Hypothesis

The system will electronically store the biographic information of the holder allowing frequent updating of the details of the holder in the system. This system provides a broader overview for the use of e-passports to the holder, the issuing office, border controls and the government as a whole.

1.6 Problem Statement

This research is motivated by the problems that Zimbabwe is facing all over the place when it comes to the issues of conventional paper passport booklets. The problems with paper passports are that they do not provide privacy, identity can be revealed to anyone who can physically access the passport. The paper passport can be used by someone else what is known as identity theft, data can be modified on the passport as everything is accessible and readable and it can be duplicated. [3] This will affect both the user and the border control checkpoints. Having noted the problems that come with paper passports it has also come to note that the use of forged passports by drug couriers and illegal immigrants is increasing and it comes with varying techniques such as photo substitution in combination with data alteration and look-alike fraud which neither requires photo substitution nor data alteration in our traditional paper passports.

Meanwhile, the added security that e-Passports can provide, with the proviso that they are used correctly, will likely mean that fraudulent travellers will move away from falsified passports and instead seek to subvert the border control system either by attempting look-alike fraud using genuine documents, or by trying to subvert the issuance process in order to be fraudulently issued with genuine e-Passports. [1] With the high crime rates that Zimbabwe is facing presently it is very easy for one to commit a crime and escape for countries over the borders before they are caught or brought to justice. Thus the researcher hopes that by adopting e-passports the above problems will be a thing of the past as this system if implemented may also be linked to the Criminal Investigation Department (CID) of the country and an alert can be send to the border controls with the details of the people under investigation, thereby reducing the possibilities of criminals leaving the country.

States decide how long their passports will be valid. Most countries issue passports with a five to ten year validity. [4] In Zimbabwe adult passport booklets when issued are valid for ten years and for the children they are valid for five years. But with the passing of time personal appearances change such that by the time this passport expires there is need for new photographs because the images previously taken for the passport holder no longer resembles them as they will be presently, hence the rationale for wanting to find out the effectiveness of using e-passports as their images may constantly be updated in the systems database without having to worry about issuing another passport booklet to the holder.

The other problem with these conventional passport booklets is that for the business people who travel very often the pages are not sufficient and this requires them to apply for other passports when they have used up their pages before they exhaust the validity of their passports. This brings about the issue of stamping, with the conventional paper passport booklets when the holder is granted access at the border controls their passport booklets are stamped indicating also the duration they have been granted to stay in the foreign land. This project is assuming that the border controls and immigration offices will have a receipting system in place such that for the travellers with e-passports when granted access they are given this receipt which they are supposed to carry with them wherever they are in the foreign land. This receipt should be stating that this traveller is an e-passport holder who has been granted access in the foreign land for such duration.

Then if it so happens that the e-passport holder is required to produce their passport in the foreign land for instance by the police then they should produce that receipt together with their national Identity Card. Warsaw states that:

"The passport serves as an identification document and maybe checked by regular police or in criminal justice chain. Since establishing the identity of the holder is very important in these cases as well as verifying organisations may want to read and verify the chip." [1]

Thus the researcher anticipates that the RFID card will be very useful to the business people as they do not have to worry about using up their pages. Moreover the card is portable, cheaper and requires shorter waiting periods when acquiring them. The card has so many advantages over the paper passport because with the paper passport sophisticated security features apply with them such as high quality papers and adhesives, special or optical variable inks which are expensive, to mention but just a few. [4] In Zimbabwe the paper that makes up the pages of the passport booklet is the same paper that is used for the money notes hence the chances of having one's passport being stolen with fraudsters is very high and these fraudsters may take the pages and use them to print fake money notes.

In addition the other problem is the time it takes to replace a lost or stolen passport in Zimbabwe, but this system will speed up the processing. The process time will be greatly reduced while the tradition inspection requires information to be inputted manually. [5]

1.7 Justification

The project will eliminate forgery as identity will not be revealed to anyone but only to the people authorised to access the system. These RFID cards will be unique and even if they are lost or stolen they cannot be used by someone else. The implementation of this project implies that data can only be modified by the authorised personnel as everything is not accessible or readable to anyone. The issues associated with the duplication of data entry, multiple issuances of the passport to the same person will be done away with. RFID cards are very much portable compared to the conventional passport booklets, simple, reliable and easy to replace if lost with shorter waiting periods than the passport booklet.

1.8 Applications of RFID

Current and proposed uses of RFID span a wide spectrum of application areas which are stated below [6]:

1. Agriculture – animal tracking, crop identification
2. Clothing – Laundry ID
3. Sports and games – tracking golf balls, sport event timing
4. Finance – smart card
5. Human identification – digital ID, facility access
6. Healthcare – pharmaceutics, hospital equipment and personnel
7. Monitoring and tracking – parcels, luggage handling, library inventory
8. Traffic, transportation, ticketing – Toll collection, smart car key, automatic vehicle location
9. Environment – Waste haulage recycling
10. Manufacturing and supply chain management – Resource management

1.9 Literature Review

The e-passport possesses two aspects of technology which are RFID and biometrics all incorporated so as to securely identify and verify the bearer possessing that travel document. In this section of chapter one the writer will site, acknowledge and quote similar works that have been done on the e-passport in brief and also state how this project is going to be different from all these works.

E-passports are already available and in use in several European countries and several researches have been conducted around the world following their deployment in these countries. [7] [8] [9] Kumar et. al discussed the efficient implementation of e-passports scheme using cryptographic security along with multiple biometrics. [2] In this article he states that an e-passport is an identification document which possesses relevant biographic and biometric information of its bearer on paper and also has this information embedded on an RFID chip which is capable of cryptographic functionality. [2] However this project seeks to eliminate the design of having a passport booklet with an RFID chip embedded on it but instead just make use of an RFID card with all the information stored on that card.

In the e-passport design Kumar also talks of the certification whereby the authentication procedure involves two processes which are Registration and Verification whereby during the former phase the applicant registers their biometric under human supervision and the data is stored on the passport tag. However the e-passport designed in this project differs in the sense that instead of having the data stored on the tag to be duplicated on the paper passport, the data should be stored in a centralised system database which is only accessible to the authorised personnel at the border controls. Such that the border official will have to physically check what the system is presenting with the physical appearance in-front of them to see if it matches.

In a thesis written by BC Vollmer in 2006 titled Biometrics, RFID technology and the e-passport he states that the American e-passport will have an RFID chip embedded inside the back cover of the passport booklet and it will store the same information that is printed on the bio-data page of the passport booklet. [10] This project argues that if the passport booklet and the chip are both stored with the same information why then not resort to only one thing – the RFID card which will store all the information because RFID cards are easy to replace if lost or stolen and they are portable (easy to move around with or carry with you all the time) than a passport booklet. Take note that the RFID card and the Chip use the same principle of operation and the same technology. No doubt that this RFID card then must incorporate strong security features to guard against skimming and information altering.

Vollmer also states that the RFID chip found in the e-passport is a passive, write once, read many version of an RFID chip technology. Whereas this project would like to consider the possibilities of writing on the RFID card several times so as to constantly update the photographs of the passport holders in the system after a certain period of time so as to keep them updated as possible. With the American e-passports chips cannot be altered after production. The writer Vollmer mentions also of the read range of this American e-passport which is about 121.92cm and it is the read range when the passport is opened. Now with the RFID tags it will depend with the type which one is using but the ones suitable for this project are the Low frequency RFID tags which have a lower read range than that of the chip. Since both use the RFID technology the Faraday Cage may be used to shield the RFID cards or the chip from transmitting any further than a few centimetres.

With these entire facts one can conclude that with the use of an RFID based e-passport it will be very difficult for sophisticated counterfeiters to steal these RFID based e-passports cards and alter the details to match them. It should prove to be impossible.

1.10 Assumptions

- The RFID cards will only be read when placed in front of the card reader and not when they are still at a distance from the reader because if the people are in a queue then it means that cards will be read before they reach the checkpoints for verification.
- There will always be human supervision at the passport checkpoints.
- An international database of sufficient quality has been developed and all the countries have the same biometric implementations.
- All border controls will have a receipting system in place such that any e-passport holder is granted this receipt which will be stating that this is an e-passport holder who has been granted authority to be in a foreign land for so many days.

- All e-passport holders will have their National Identity cards with them always during their stay in the foreign land.
- The police and other verifying organisations such as the criminal justice chain will also have their inspection systems with the underlying infrastructure which can also read these e-passports in the future and their systems are interlinked with the systems at the border controls.

References

[1] Warsaw, Operational and Technical security of Electronic Passports, Poland: Frontex Agency, 2011.

[2] V. K. Srinivasan and K. Narendira, “DESIGN AND IMPLEMENTATION OF E-PASSPORT SCHEME USING CRYPTOGRAPHIC ALGORITHM ALONG WITH MULTIMODAL BIOMETRICS TECHNOLOGY,” *International Journal of Advanced Information Technology (IJAIT),* vol. 1, no. 6, p. 35, 2011.

[3] H. Meng, S. A. Tandra and V. Agrawal, “ePassport System,” Royal Institute of Technology Sytems Theory and Security, Sweden, 2010.

[4] I. I. O. f. Migration, “Passport and Visa Systems,” *Essentials of Migration Management,* Vols. III-Managing Migration, p. 18, 2011.

[5] B. D. M Semir UZUN, “Developing Electronic Passport And VISA System Using Smart Card Technology,” Turkey, 2011.

[6] Mandeep Kaur, “RFID Technology Principles, Advantages, Limitations & Its Applications,” *InternationalJournal of Computer and Electrical Engineering,* vol. 3, no. 1, 2011.

[7] A. Rana and L. Sportiello, “Implementation of security and privacy in ePassports,” *International journal of critical infrastructure protection,* vol. 7, p. 233–243, 2014.

[8] A. B. Jeng and L.-Y. Chen, “How to enhance the security of ePassport‟,,” *Proceedings of the Eighth International Conference on Machine Learning and Cybernetics,* 2009.

[9] G. Avoine, K. Kalach and J.-J. Quisquarter, ePassport: Securing International Contacts with Contactless Chips, Belgium: Louvain-la-Neuve, 2008.

[10] B. Brianne Christine Vollmer, “BIOMETRICS, RFID TECHNOLOGY, AND THE EPASSPORT,” Washington, DC, 2006.

CHAPTER 2

THEORETICAL ASPECTS

2.1 Introduction

In this chapter the author will describe in detail the various types, operations and applications of the components used in designing this RFID based Electronic passport prototype.

2.1.1 RFID System

Basically RFID (Radio Frequency Identification) is a wireless link to uniquely identify objects or people. RFID enables identification from a distance without requiring line of sight. The RFID system comprises the RFID tag/card, RFID reader, backend database and a control unit. RFID systems have two broad categories passive and active. The RFID reader communicates with the RFID tag through tag interrogation. [1]

2.1.2 RFID Tags/Cards

RFID tags/cards consist of an Integrated circuit attached on an antenna that is printed, etched or stamped onto a base which is often a paper substrate of Polyethylene Terephthalate (PET). The inlay which is the combination of the chip and antenna is then inserted amid the printed label and its adhesive backing or it is either placed in a more durable structure. [2]

The tag consists of the following:

a) A radio frequency chip
b) Encoding and decoding circuitry
c) Antenna unit and
d) A memory unit.[3]

Tags can be classified depending on their power capacity into passive, semi-active and active tags. The distinction of these classifications is illustrated Table 2.1 below. [3]

Table 2-1 Classification of Tags depending on Power Capacity

Passive tags	Semi-active tags	Active tags
These are tags without internal power supply	These are also tags without internal power supply but only use the internal power supply for its internal memory circuitry.	These use their internal power unit to power both the antenna unit and its internal circuitry.

In addition tags can also be categorized basing on their frequency of communication. The energy, read range and in some cases the size of the tag is determined by the communication frequency between the tag and the reader.

Fig. 2-1 below shows an example of the type of RFID cards that are going to be used in this project.

Fig 2-1 Typical RFID card for the project

2.1.3 RFID Reader

The RFID reader is also known as an interrogator, it provides the connection between the tag data and the software that needs the information. [4] The image below is showing an RFID reader.

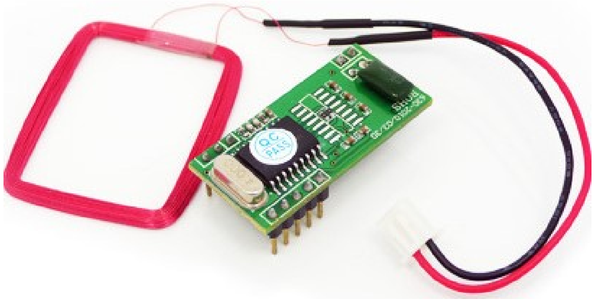


Fig 2-2 RFID Reader

By making use of an attached antenna, the reader extracts the data on the tags and then sends the data to a host computer for further processing.

2.1.3.1 Reader antennas

Their function is to change electrical current to electromagnetic signals that are emitted into space where they are able to be received by the tag antenna and are changed back to electrical current. Two most common reader antenna types are:

i. Linear antennas

- These radiate electric fields that are linear.
- Have long ranges.

- These signals have the ability to enter various diverse materials so as to read tags due to their high levels of power.
- They are very sensitive to tag orientation.
- They can experience a difficult time reading tags depending on the tag angle or placement.

ii. Circular polarized antennas

  - These emit circular fields.
  - They are sensitive to orientation to a lesser extent.
  - Circular polarized antennas deliver less power than linear antennas.

2.1.4 Operating Frequency of RFID Systems

Basing on their operating frequency RFID tags can be classified into three categories which are:

i. Low Frequency (LF)
ii. High Frequency (HF) and
iii. Ultra High Frequency (UHF)

Fig. 2-3 below is showing these categories.

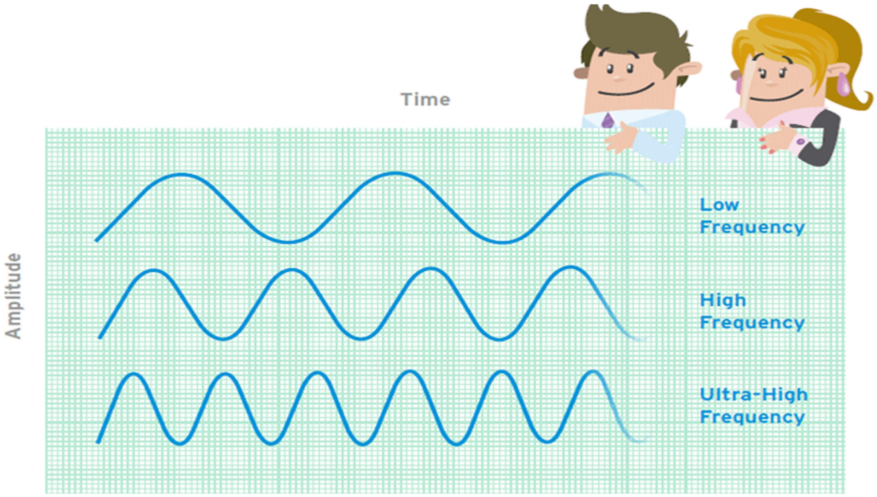


Fig 2-3 Operating Frequency Categories of RFID Tags

Table 2-2 below is showing the difference between these three categories.

Table 2-2 Categories of RFID tags and their differences

	Low Frequency (LF) tags	**High Frequency (HF) tags**	**Ultra High Frequency (UHF) tags**
Operating Frequency	Operate at 125kHz but there are some that operate at 134kHz.	Operates at 13.56MHz.	Frequencies range between 300MHz - 3GHz.
Operating Range	Operate within the range of ≥30kHz and ≤300kHz.	Operates within the range of ≥3MHz and ≤30MHz.	In Gen-2 protocols they operate In ranges of ≥866MHz and ≤960MHz.
Read Range	Has a short read range of 10cm.	Read ranges are between 10cm and 1m.	
Read Speed	Has a slower read speed than High Frequencies		
Sensitivity to Radio Waves Interference	Not very sensitive.	Experience moderate sensitivity to interference.	
Use		It is the most commonly used tag. It is commonly used for ticketing, payment and data transfer applications. [5]	Applicability varies in different countries. [1]

It is these operating frequencies that determine the data rate and the read range of an RFID system. For passive RFID tags they operate at ≥30cm for LF, ≥1m for HF and ≥7m for UHF tags. Yet for an active tag the range can span to 100m because the tag does not require the reader to power its internal circuitry.

2.1.5 Working Principle of an RFID system

Basically the RFID structure comprises of three elements which are:

- An antenna or coil
- Transponder (RF Tag) electronically programmed with unique information.
- Transceiver (with decoder)

These elements communicate by means of radio signals which carry data either unidirectional or bidirectional. When a transponder gets into a read zone, its contents are captured by the reader and can then be transferred through standard interfaces to host devices such as a computer, printer or programmable logic controller (PLC) for storage or action.

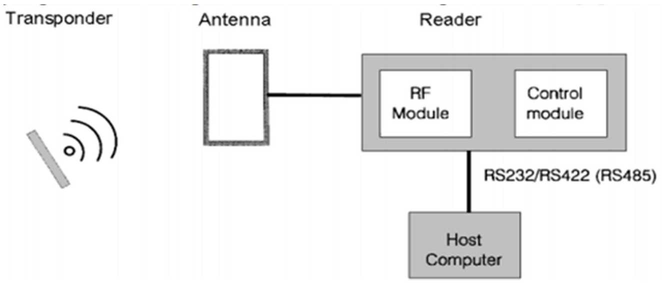


Fig 2-4 Working Principle of an RFID System

2.1.6 Merits of RFID systems

- Tag detection which does not require human intervention eliminates human errors from data collection.
- No line of sight is required hence tag placement is not as much constrained.
- Distinctive item identification is easy to implement with RFID.
- RFID has the ability to identify items individually instead of generically.
- Tags are less affected by adverse conditions such as dust, chemicals, Physical damage, etc. meaning they are able to with-stand harsh environmental conditions.
- RFID tags can be combined with sensors.
- Tracking people, items and equipment in real time.

2.1.7 Demerits

- Faulty manufacture of tags. –Tag manufacturing is not until now 100% failure free currently.
- Standardization – The sparse standards leave much freedom in the choice of communication protocols and the format and amount of information stored in the tag.
- Collision – If several tags are read at a time it may result in signal collision and result in data loss.

2.1.8 Working Principle of an RFID based e-passport

In the e-passport prototype this RFID system will enable details of a passport holder to be stored in a portable device called and RFID card. This RFID card will be read by an RFID reader and processed in order to identify the holder of this e-passport.

2.2 Arduino Uno board

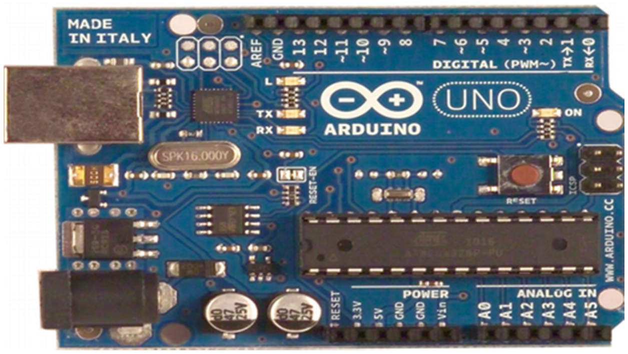


Fig 2-5 Arduino Uno Board

It is a microcontroller board based on the ATmega 328P. It has 14 digital pins, 6 analogue inputs, a 16MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. Fig 2-5 shows a typical Arduino Uno board. One has to simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. [3]

2.2.1 Technical Specifications of the Arduino Uno Board

Table 2-3 Technical Specs of the Arduino board

Microcontroller	ATmega328
Operating Voltage	5V
Input Voltage (recommended)	7V-12V
Input Voltage (limits)	6V-20V
Digital I/O Pins	14 (of which six provide PWM output)
Analogue Input Pins	6
DC Current per I/O pin	40mA
DC Current for 3.3V pin	50mA
Flash Memory	32KB of which 0.5KB is used by bootloader
SRAM	2KB
EEPROM	1KB
Clock Speed	16

Fig. 2-6 is showing the Arduino Uno board with some of its parts labelled.

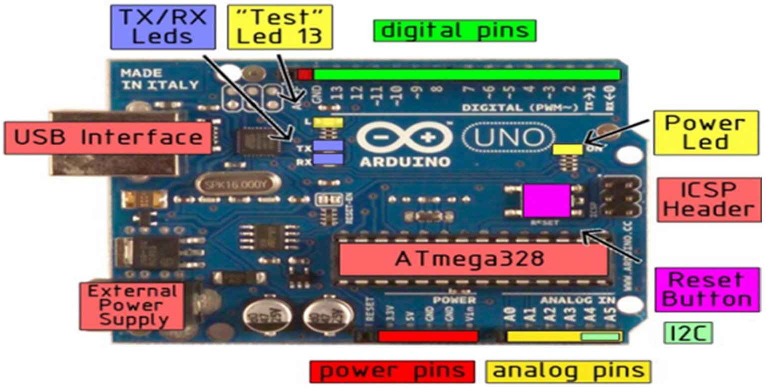


Fig 2-6 Arduino board with parts labelled

This is the type of the Arduino microcontroller board which is going to be used for this e-passport prototype. It can output two levels of power 3V and 5V.

2.3 LEDs

The abbreviation stands for Light Emitting Diodes. The diode is a basic but very important device that has two terminals, the anode and the cathode. [7] An LED is basically a small light producing device that comes under active semiconductor electronic components. [8] When the internal diode junction of the LED gets a forward electric voltage or current, the LED is capable of radiating an equitably constricted bandwidth of either visible or invisible light. [9] Fig. 2-7 is showing some LEDS.

Fig 2-7 Typical LEDs

The visible lights that a LED emits are red, green, orange or yellow. The invisible light comprises infrared light.

2.3.1 Circuit Symbol of a LED

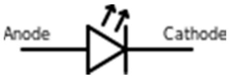
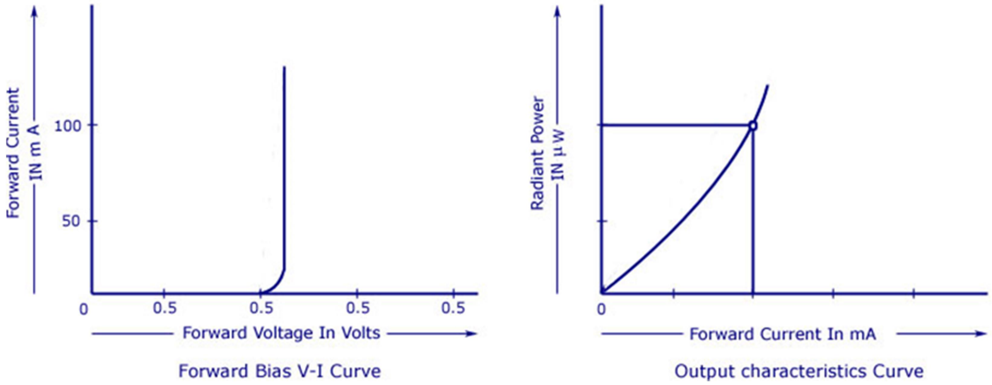


Fig 2-8 LED Circuit Symbol

2.3.2 Characteristics of a LED



Forward Bias V-I Curve

Output characteristics Curve

Fig 2-9 LED Characteristics Curves

Forward bias of just about 1 volt is required to give substantial forward current.

2.3.3 Basic Operation of an LED

When the LED is forward biased, the electrons in the n-type material cross the pn junction and recombine with the holes in the p-type material as illustrated by fig 2-10. These free electrons are in the conduction band and at a higher energy than the holes that are in the valence band.

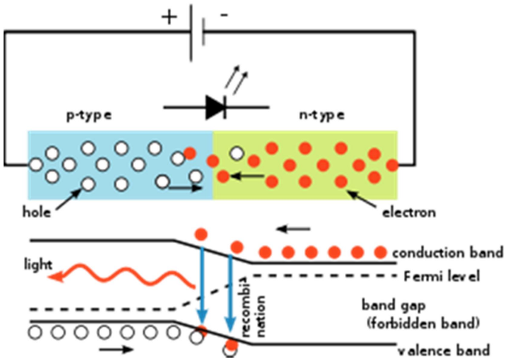


Fig 2-10 Recombination of the holes and electrons in a forward biased LED

Thus the energy level of holes is smaller than that of the electrons. Some part of the energy has to be dissipated so that the electrons and the holes recombine. The minute recombination takes place, energy is released in the form of heat and light. A large exposed surface area on one layer of the semi-conductive material permits the photons to be emitted as visible light. This process is called electroluminescence and is illustrated by Fig. 2-11 below:

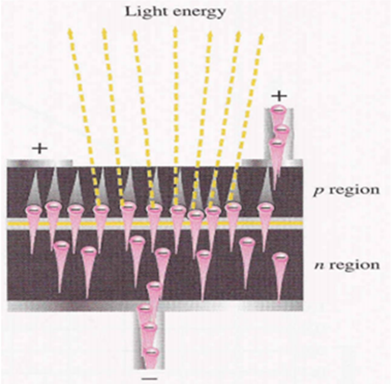


Fig 2-11 Electroluminescence in a forward biased LED

During the doping process various impurities are added so as to establish the wavelength of the emitted light. The wavelength determines the colour of the light whether if it is visible or infrared. [10]

The phenomenon termed electroluminescence may also be defined as the radiation of light from a semi-conductor under the effect of an electric field.

2.3.4 Advantages of LEDs

i. Response time is very fast in the range of 0.1μs.
ii. They have a long life span of more than 20 years.
iii. Small in size hence they are light in weight.
iv. In terms of the voltage and current required to drive the LED, very low voltage and current is sufficient.
v. LEDs do not require any heating and warm up time.
vi. They have a rugged construction thus they can survive shocks and vibrations.

2.3.5 Disadvantages of LEDs

i. An insignificant surplus in voltage or current can destroy the device.
ii. When compared with lasers, LEDs have a much wider bandwidth.
iii. The temperature is determined by the radiant output power or wavelength.

2.4 Resistors

These are electronic components with a specific but never changing electrical resistance. The purpose of the resistor is to slow down the electrical current, as current passes through it thereby limiting the flow of electrons (amount of current) through a circuit. They do not consume power and cannot generate it meaning they are passive components. Generally resistors are used as current limiters, voltage dividers or they are used to pull-up I/O (Input/Output) lines. The electrical resistance of a resistor is measured in ohms and the symbol is denoted by the Greek capital omega **Ω**. The schematic symbols of a resistor are shown in Fig. 2-12:

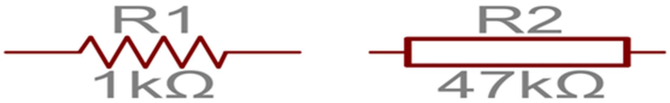


Fig 2-12 Schematic symbols of a Resistor

Resistors can be grouped into three categories which are fixed resistors and these are the ones which are going to be used in this project, variable resistors which are commonly known as potentiometers and variable resistors that are dependent on physical qualities such as the thermistors that are dependent on temperature or the photovoltaic cells that are dependent on light.

2.4.1 Functions of the resistors in the e-passport circuit

I. LED Current limit

LEDs too are very sensitive to high currents. Resistors are the key in ensuring that LEDs do not blow up when power is applied. Thus a resistor when placed in series with the LEDs regulates a proper flow of current through them meaning the current flowing through the LED and the resistor is limited to a safe value. To calculate the value of a series LED resistor, the following formula may be used:

$$R = V_S - (N * V_{F(LED)})/I_F$$

Where R = Series LED resistor

V_S = Supply/Source Voltage

N = number of LEDs in series

V_F (LED) = forward voltage of the LED used, and

I_F = current through the LEDs (10mA optimum).

Fig. 2-13 below is demonstrating how a resistor can be used to limit current to an LED.

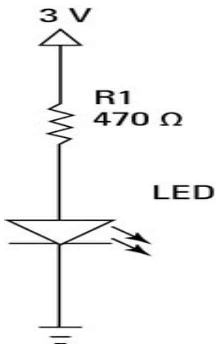


Fig 2-13 Current Limiting Resistors on an LED

The Table 2-4 is showing the resistor values that can be used to limit the current flowing in different LEDs depending on the voltage supplied, the number of the LEDs connected in series and the LED forward voltage.

Table 2-4 Resistor values for different LEDs

Power Supply Voltage (V)	Color of the LED	LED forward voltage V_f	Series LEDs	Desired Current (mA)	Calculated Resistor values in Ω	Rounded Resistor values in Ω
3	Red, Yellow or Yellow-Green	1.8	1	25	48	51
4.5	Red, Yellow or Yellow-Green	1.8	2	25	36	39
4.5	Blue, Green, White or UV	3.3	1	25	48	51
5	Blue, Green, White or UV	3.3	1	25	68	68
5	Red, Yellow or Yellow-Green	1.8	1	25	128	150
5	Red, Yellow or Yellow-Green	1.8	2	25	56	56
9	Red, Yellow or Yellow-Green	1.8	4	25	72	75
9	Blue, Green, White or UV	3.3	2	25	96	100

II. Pull down or Pull up resistor

These are often used when interfacing with a button or a switch input. When one needs to bias a microcontroller's input pin to a known state a pull up resistor is used. The resistor's one end is connected to the microcontroller unit's pin and the other end is connected to a high voltage. Without a pull up resistor the inputs on the microcontroller unit could be left floating and there remains no guarantee that a floating pin is either high or low. Pull up resistors are often used when interfacing with a button or switch input. In this project a pull up resistor is going to be used with the status button on the Arduino microcontroller board.

The value of a pull up resistor does not have to be anything specific but at least it should be high enough such that not too much power is lost if a certain voltage is applied across it. Generally resistor values around 10kΩ work well.

2.5 LCD

The abbreviation LCD stands for Liquid Crystal Display. A LCD is a flat-panel electronic visual display that makes use of the light modulating properties of liquid crystals. It can be defined as the combination of two states of matter – liquid and solid. LCDs have both solid and liquid properties. They maintain their corresponding states with regard to another. Liquid crystals they do not radiate light directly. [11]

LCDs display arbitrary or fixed images with low information content, which can be displayed or hidden for example digits, 7-segment displays as in a digital clock and pre-set words. [12]

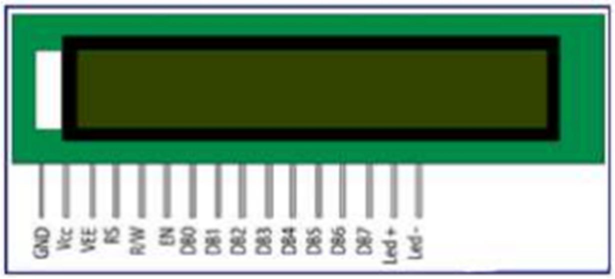


Fig 2-14 LCD Display

2.5.1 How LCDs work

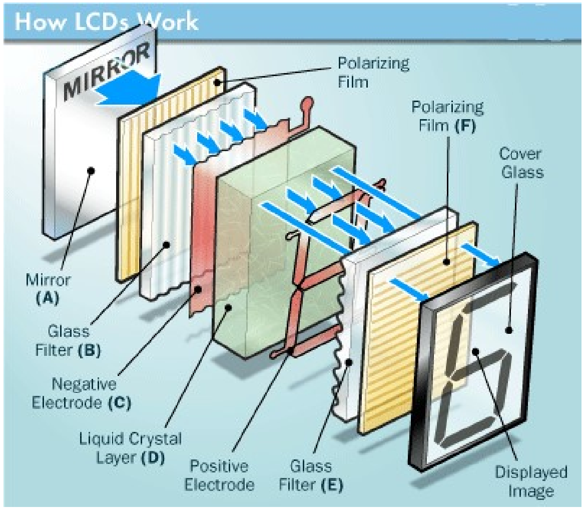


Fig 2-15 How LCDs Work

The main principle behind is that electric current is applied to the liquid crystal molecules. The minute this electric current is applied the liquid crystal molecules tend to untwist. As a result the angle of the top polarizing filter changes with regard to the liquid crystal molecule. Thus little light is then permitted to go via that particular LCD area and that area when compared to the others becomes darker. [13]

To make up an LCD screen, in the back a reflective mirror is setup. In addition to that an electrode plane is set on the top. The electrode plane is made up of indium-tin oxide. On the bottom side there is a glass with a polarizing film. The whole area of the LCD is enclosed by a common electrode and there is the liquid crystal substance on top of it. It is then followed by another piece of glass with a rectangle shaped electrode on the bottom and another polarizing film on the top. Both of them are kept at right angles. This is shown in Fig. 2-15 above. The mirror reflects the light that passes through the front of the LCD when there is no current and it is bounced back. Connected to a temporary battery is the electrode and the current from it will cause the liquid crystals in the middle of the common plane electrode and the electrode shaped like a rectangle to untwist. Hence light is blocked such that it is not able to pass through and that particular rectangular area looks blank. [13]

References

[1] I. R. A. a. N. B. Ithnin, Users Authenticationand Privacy control of RFID Card.

[2] 2. B.Divya, "LOW POWER RFID WIRELESS SENSOR FOR SMART," *International Journal of Infinite Innovations in Engineering and Technology,* vol. II, no. 1, 2015.

[3] I. R. A. N. B. Ithnin, Users Authentication and Privacy control of RFID Card, Universiti Teknologi Malaysia..

[4] T. G. a. H. L. Qinghan Xiao, "RFID Technology, Security Vulnerabilities,," in *Supply Chain, The Way to Flat Organisation* , Vienna, Austria, I-Tech, 2008, p. 404.

[5] V. S. A. B. V. H. Aadesh Kamble, "Automatic Toll Collection Systems using WSN (RFID)," *IJSRD - International Journal for Scientific Research & Development,* vol. III, no. 04, p. 6, 2015 |.

[6] M. S. N. M. a. P. S. S. Mandeep Kaur, "RFID Technology Principles, Advantages,," *International Journal of Computer and Electrical Engineering,* vol. III, no. 1, 2011.

[7] A. R. Humbley, Electrical Engineering Principles and Application, Prentice Hall.

[8] "Internal Functioning of Light Emitting Diodes (LEDs) Explained," brighthubengineering.com, 2012. [Online]. [Accessed 14 March 2016].

[9] "How a LED works – Light Emitting Diode working," 2015 CircuitsToday, 2015. [Online]. Available: www.CircuitsToday.com. [Accessed 17 March 2016].

[10] T. L. Floyd, Electronic Devices, New Jersey: Pearson Prentice Hall, 2005.

[11] [Online]. Available: http://www.merriam-webster.com/dictionary/lcd.

[12] [. e. al., "LCD display," *INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT,* vol. III, no. 02, p. 52, 2016.

[13] "Liquid Crystal Displays (LCD) - Working," [Online]. Available: www.circuitstoday.com/liquid-crystal-displays-lcd-working. [Accessed 24 March 2016].

[14] [Online]. Available: www.electronicdefinitions.com/definition.php?defid=2474. [Accessed 20 March 2016].

[15] "Fingerprint recognition," [Online]. Available:

https://en.m.wikipedia.org/wiki/Fingerprint_recognition. [Accessed 20 March 2016].

[16] "Know about Fingerprint Authentication based identification for Operating Loads," EDGEFX.IN, [Online]. Available: www.edgefx.in/fingerprint_authentication-and-controlling-system-using-microcontroller/. [Accessed 20 March 2016].

[17] D. B. &. S. Kale, Industrial Automation (IAU) 12149, 2012.

[18] M. P. e. al, "A Beam Technology on the Pen," *International Journal of Advance research, Ideas and Innovations in Technology,* vol. I, no. 02, 2014.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter covers in detail the methodology used in designing this prototype. It discusses the different methods that were used in collecting data for this project. It focuses on the prototype design, information gathering techniques and the system requirement analysis and specifications.

3.2 Information Gathering Techniques

3.2.1 Interviews

A worker who works at the Harare passport offices was consulted on several aspects of our Zimbabwean passport today. The following types of questions were asked at the Zimbabwe Passport Office:

1. Zimbabwe today's unique passport features.
2. How Zimbabwe's current passport system works.
3. What type of system is Zimbabwe using?
4. Does Zimbabwe follow the ICAO (International Civil Aviation Organisation) Standards?

3.2.2 Online Material

In order to come up with this prototype design several online books and journals were consulted for guideline, the overall goal being to design a proper system that demonstrates the researcher's findings in the most appropriate way.

3.2.3 Participatory Method

Field visits were conducted by the author to the passport offices and information was collected on the procedure being done now on the issuance of passports to individuals. At some point the writer was also a participant when they crossed the borders visiting in the neighbouring countries. Thus the author also had first-hand information of the sequence of events that take place at the border checkpoints using the conventional passport booklet.

3.3 Structure of the System

The overall system consists of the following hardware components.

- RFID Reader
- RFID Cards
- LEDs
- LCD display
- Resistors

3.4 The Arduino Uno board and its Pins.

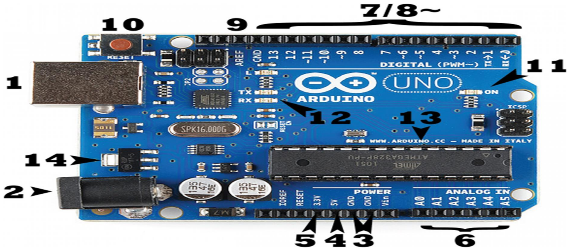


Fig 3-1 The Pins on the Arduino Uno board

The Arduino board has pins where one connects wires to construct a circuit in conjunction with a breadboard and some wires. [1]

Table 3-1 Pins on the Arduino board and their functions

Pin Number	Function
1	Power (USB Connection). This is the USB connection which can be used to power the Arduino Uno from the computer. This USB connection will also be used to load the code onto the Arduino board.
2	It is the barrel jack and it can also be used to power the Arduino board from a wall power supply.
3	With reference to fig 3-1 these are the pins labelled GND (ground) on the Arduino board and they can be used to ground one's circuit.
4	This is the pin labelled 5V and it supplies 5V of power.
5	This is the pin labelled 3.3V and it supplies 3.3V of power.
6	These are the analogue input pins labelled A0-A5 on the Arduino board. These are the pins which read analogue signals from analogue devices and convert them to digital form values that human beings can read.
7	These are the digital pins labelled 0-13 just across the analogue pins. These pins can be used for digital input and digital output.
8	On the 0-13 digital pins, pins 3, 5, 6 and 9, 10, 11 have a ~ (tilde) beside them meaning that these pins are normal digital pins but can also be used for PWM (Pulse Width Modulation).
9	Pin 9 labelled AREF it stands for Analog Reference. It is used sometimes to set an external reference voltage between 0V and 5V as the upper limit for the analogue input pins.
10	This is the reset button – pushing it will temporarily connect the reset pin to ground and restart any code that is loaded on the Arduino.
11	It is a tiny power LED indicator. It should light whenever the Arduino is plugged into a power source. If it does not turn on then the circuit needs to be rechecked.
12	These are transmit and receive LEDs which give some indications when the Arduino is receiving or transmitting data.
13	This is the main IC on the Arduino. It can be called the brains of the Arduino and it is usually from the ATmega line.
14	This is the voltage regulator that controls the amount of the voltage that goes into the Arduino board; it blocks any extra voltage that can damage the circuit.

3.5 Interfacing the RDM 6300 RFID Reader with the Arduino Uno board

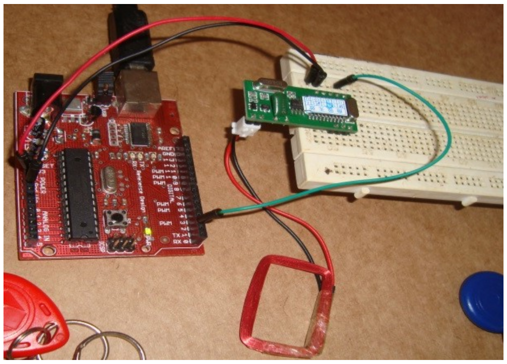


Fig 3-2 interfacing the RFID reader with the Arduino board

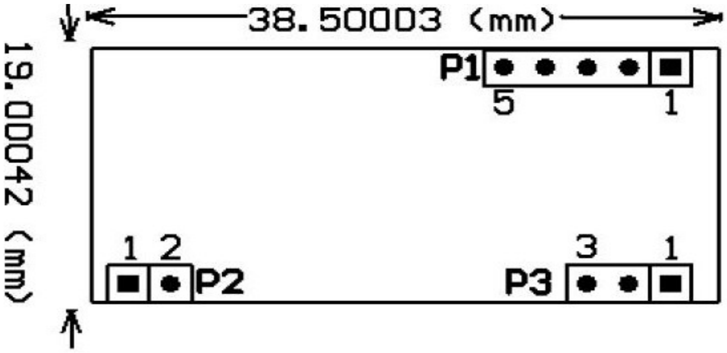


Fig 3-3 RFID Reader Pins

Pin Definition:

P1:

PIN1	TX
PIN2	RX
PIN3	
PIN4	GND
PIN5	+5V (DC)

P2:

PIN1	ANT1
PIN2	ANT2

P3:

PIN1	LED
PIN2	+5V (DC)
PIN3	GND

The RFID reader main board was inserted onto the solderless breadboard as follows:

1. Using the jumper wires, the 2nd pin on **P3** of the RFID board labelled on fig 3-3 above was connected to the Arduino's 5V supply and the 3rd pin on **P3** was connected to Ground.
2. The RFID coil (reader antenna) was connected to **P2's** Pin1 and Pin2 shown on fig 3-3 above.
3. Lastly, on **P1** of the RFID board a jumper wire was connected from **P1's** Pin 1 to Arduino digital pin 2 as the receiver and **P1's** Pin 4 was connected to ground.

3.6 Interfacing the LCD display with the Arduino board

Fig. 3-4 is showing the pins on the LCD display unit. [2]

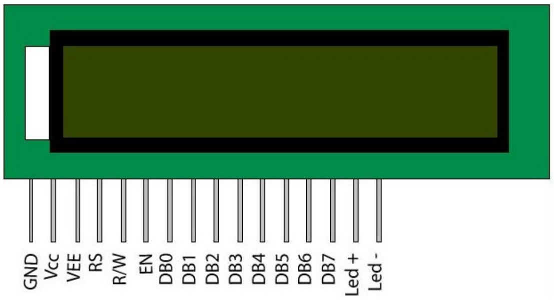


Fig 3-4 Pins on the LCD display unit

The connections which were done for the LCD are given below:

- Pin 1 or V_{SS} to Ground (GND)
- Pin 2 or V_{DD}/V_{CC} to 5V Power
- Pin 3 or V_{EE} to GND
- Pin 4 or R_S (Register selection) to Pin 11 of Arduino Uno
- Pin 5 or RW (Read/Write) to GND
- Pin 6 or EN (Enable) to Pin 10 of Arduino Uno
- Pin 11 or DB4 to Pin 5 of the Arduino Uno
- Pin 12 or DB5 to Pin 4 of the Arduino Uno
- Pin 13 or DB6 to Pin 3 of the Arduino Uno

- Pin 14 or DB7 to Pin 6 of the Arduino Uno

Six (6) pins of the LCD are connected to the controller in which 4 pins are data pins and 2 pins for control. Fig. 3-5 is showing how the LCD is interfaced with the Arduino Uno board.

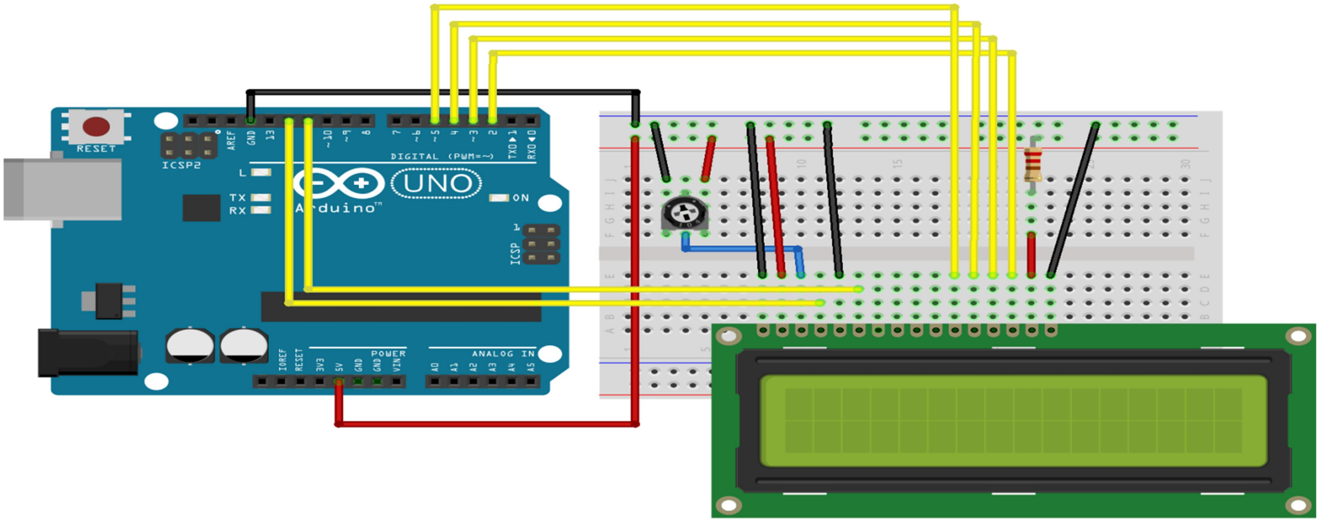


Fig 3-5 Interface connections of the LCD display with the Arduino Uno board

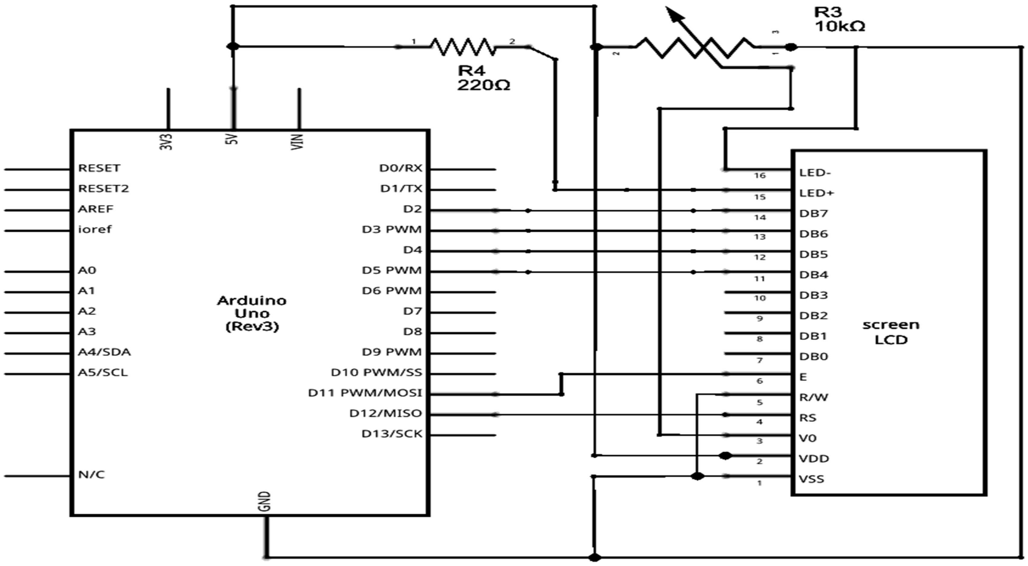


Fig 3-6 Schematic of the LCD connections

3.7 Software Descriptions

To program the whole e-passport system the embedded C programming language was used on the Arduino Uno microcontroller board such that when the system has been interfaced with the PC the LCD display, displays that it is an e-passport system, user is welcome and indicates the instruction swipe card to the RFID e-passport card holder.

3.8 Block diagram of the System

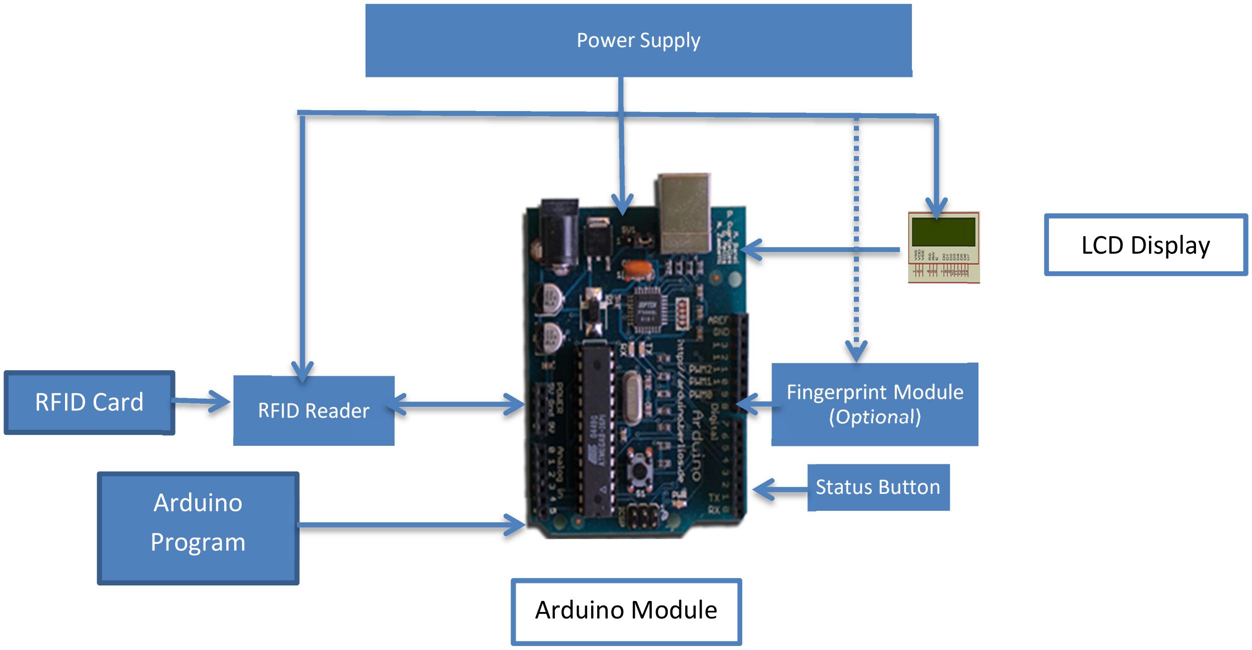


Fig 3-7 Block Diagram of the System

The block diagram in Fig. 3-7 shows the overall e-passport architecture. When an individual arrives at the border control check point they produce their RFID card to the border official who then scans the RFID card on the RFID reader. The RFID reader in-turn detects the e-passport RFID card and it decodes the information embedded on the card. If there is no match the LCD displays invalid, and alarm is signified by a red led and the user is denied access.

3.9 Data Flow Diagram of events at the border checkpoint.

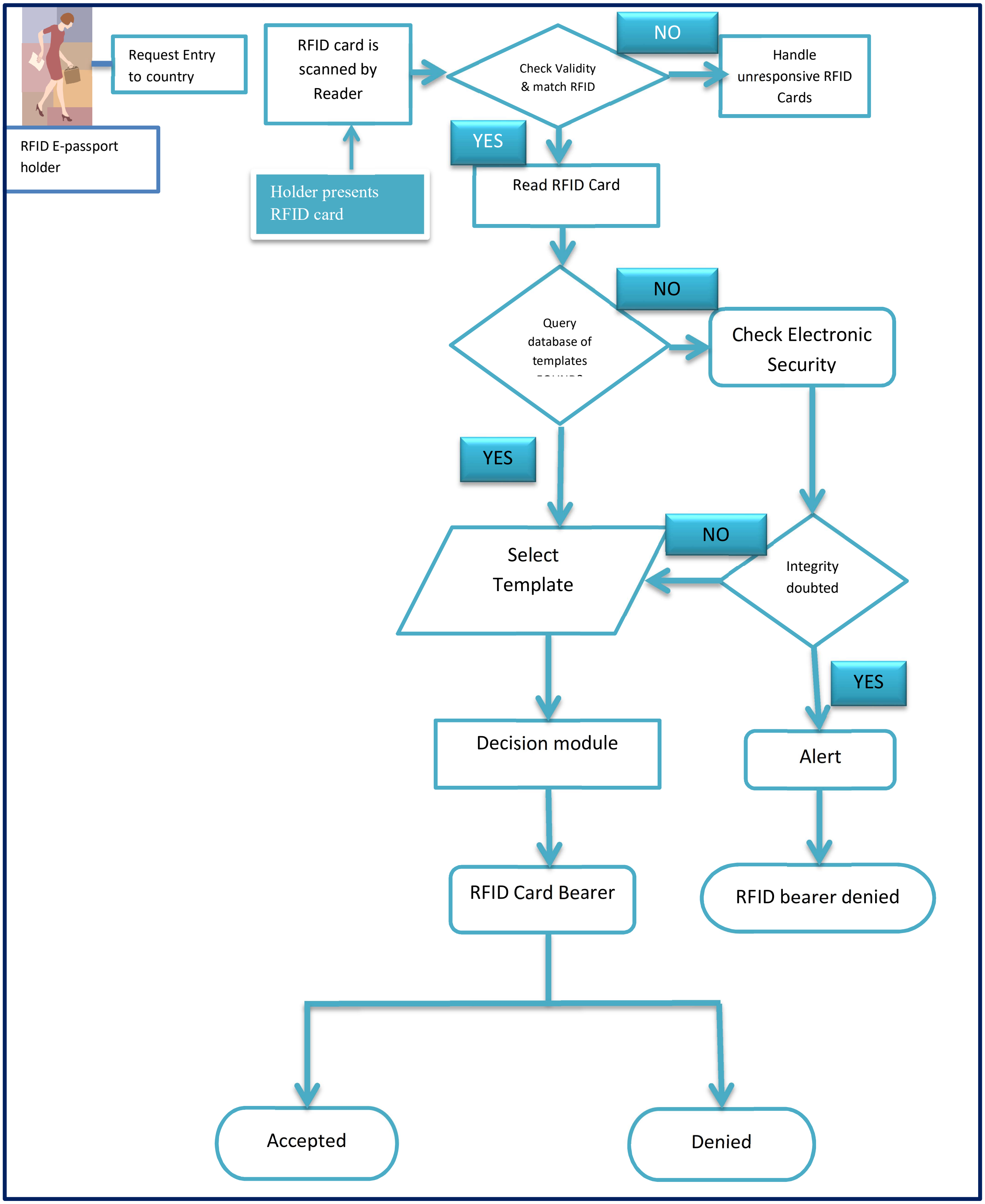


Fig 3-8 Data flow of the sequence of events at the border checkpoint

The flow chart shown in Fig. 3-8 is showing the procedure at the border checkpoint. The RFID e-passport holder presents their RFID card. The RFID card is scanned and checked for validity. If it is valid the contents of the card are retrieved and the database is queried to search for a matching template. If the template is found it is selected and the information is sent to the decision module and the user is either accepted or denied pass.

References

[1] "Starting Electronics," 31 July 2012. [Online]. Available: http://startingelectronics.org/beginners/start-electronics-now/tut3-starting-with-arduino/. [Accessed April 2016].

[2] "Circuits Today," 12 March 2016. [Online]. Available: www.circuits.com/interfacing-lcd-to-arduino. [Accessed 15 April 2016].

Chapter 4

Results and Discussions

4.1 Introduction

This is going to present the analysis of the data obtained through the use of the prototype system designed in comparison with the system that is currently in use in Zimbabwe. The results obtained during the circuit test operation will be presented in the form of a schematic, tabular form and pictorials showing the results obtained.

4.2 Schematic Design and Operation

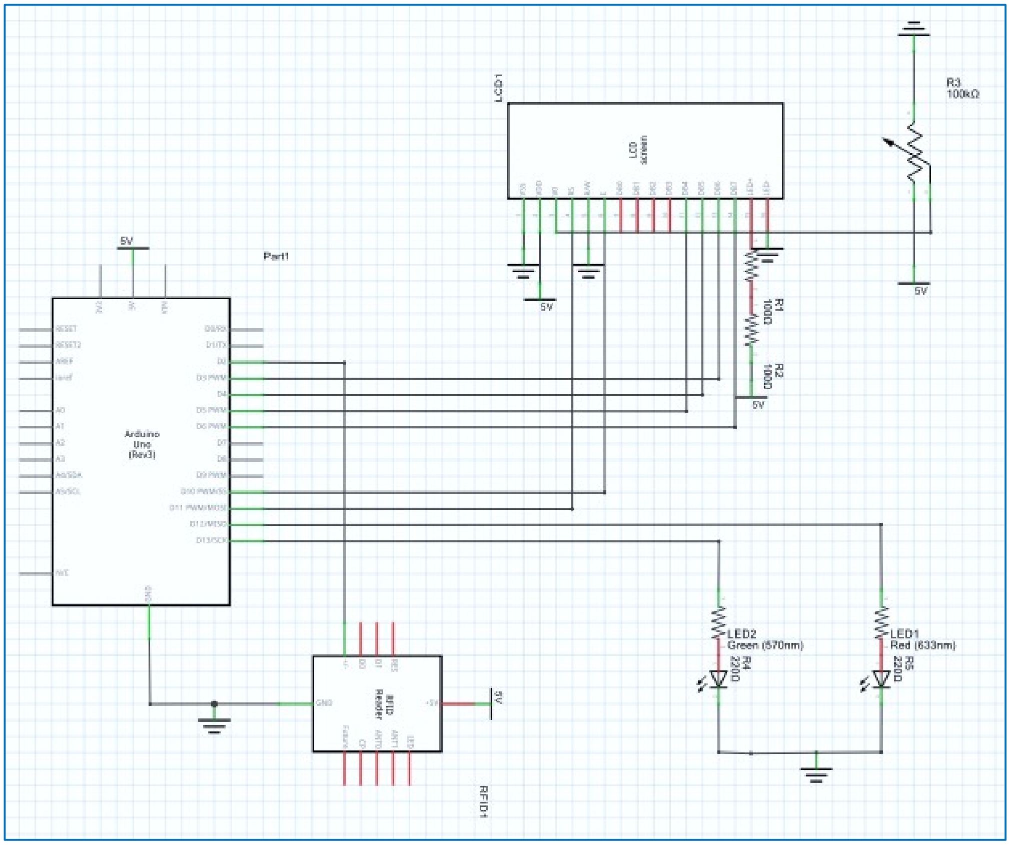
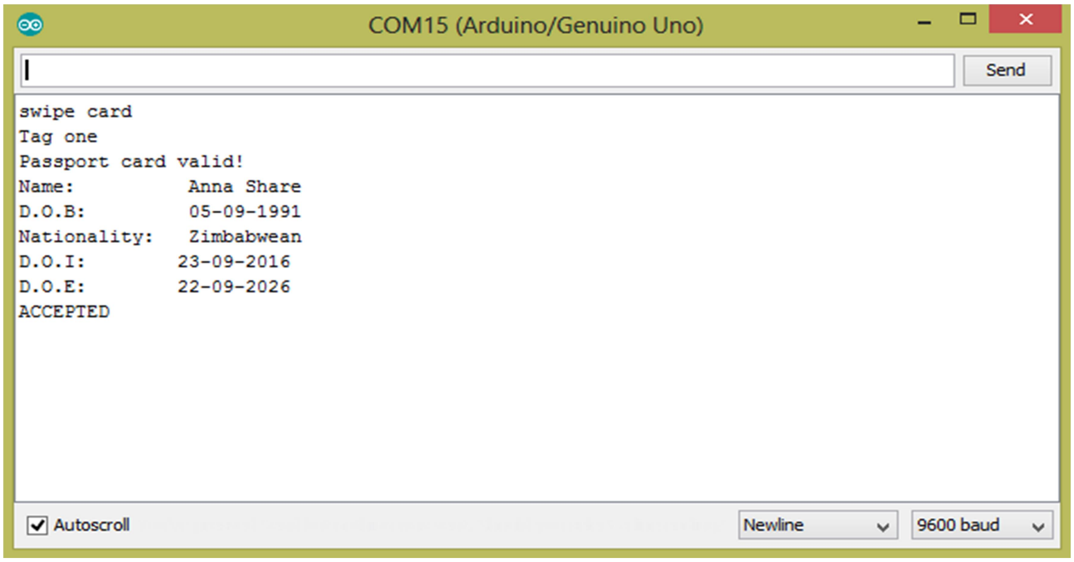


Fig 4-1 RFID based e-passport schematic

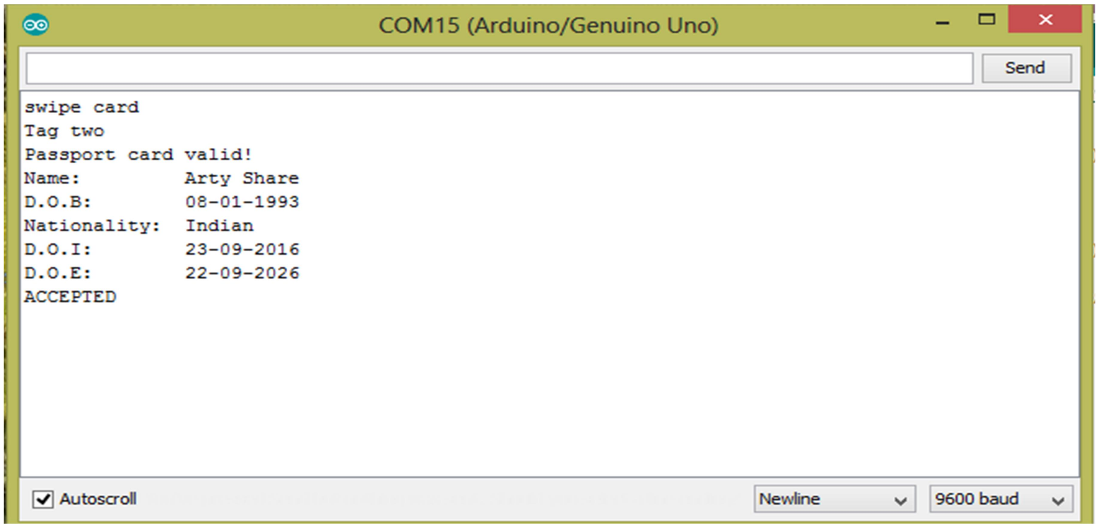
Fig. 4-1 is showing the schematic of the RFID based e-passport prototype. The RFID reader is interfaced with the reader antenna on the pins labelled ANT0 and ANT1 where the e-passport RFID card is tapped.



```
swipe card
Tag one
Passport card valid!
Name:          Anna Share
D.O.B:         05-09-1991
Nationality:   Zimbabwean
D.O.I:        23-09-2016
D.O.E:        22-09-2026
ACCEPTED
```

Fig 4-2 Results for Tag 1

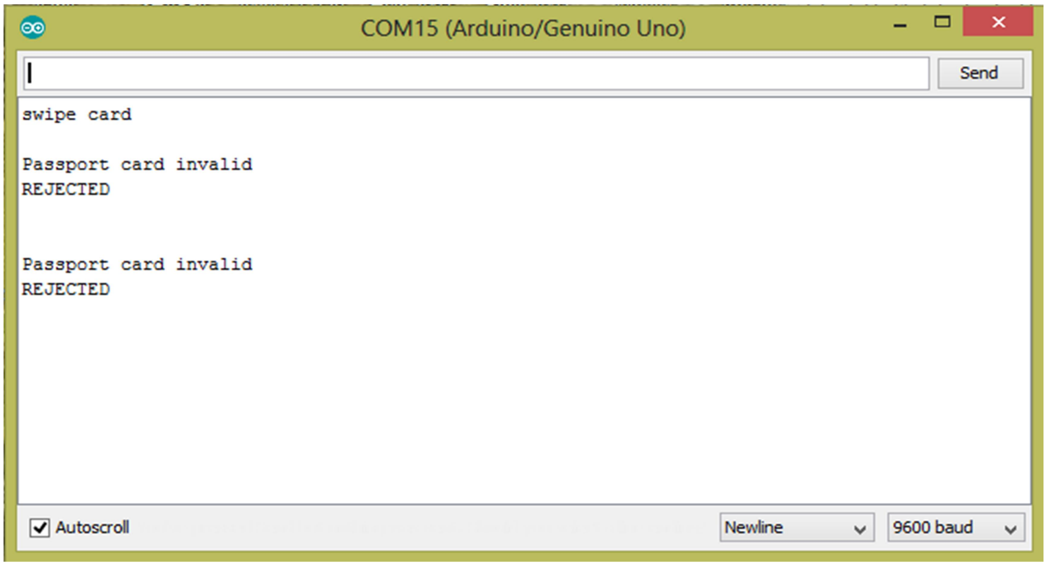
Having tapped the card, if it is a valid card, the details shown on Fig. 4-2 are displayed on the Arduino serial monitor and the LCD. These results were signified by a green LED on the circuit of the prototype available.



```
swipe card
Tag two
Passport card valid!
Name:          Arty Share
D.O.B:         08-01-1993
Nationality:   Indian
D.O.I:         23-09-2016
D.O.E:         22-09-2026
ACCEPTED
```

Fig 4-3 Results for Tag 2

From the results shown on Fig. 4-3 above it can be observed that tag two is also valid, meaning that it is recognized by the system and has its details stored in the system which are then displayed after the card has been swiped.



```
swipe card

Passport card invalid
REJECTED


Passport card invalid
REJECTED
```

Fig 4-4 Results for Tag Three

Fig. 4-4 is showing the results for tag three. The results are for an invalid card which is not recognized by the system and this is signified by a red led on the circuit of the available prototype. This is the result that should be obtained for any card that would not have had its details previously stored in the system.

4.3 Optimization of the LCD display

As shown on the schematic on Fig. 4-1 of the available prototype it can be seen that the LCD is hook up with a potentiometer. The potentiometer is used to vary the contrast of the LCD. While varying the potentiometer readings the following evaluations shown in Table 4-1 can be said about the display contrast of the LCD:

Table 4-1 LCD Optimization Results

Resistance Value k Ω	LCD Contrast Observation
19.15	No display
16.65	More dimmer but no display
14.35	Less dimmer but still no display
12.72	Dim with no display
8.35	Visible Display
5.12	Good (Contrast Not Very Bright)
3.20	Good
2.48	Good
1.09	Better
0.05	Best (Contrast Very Bright)

The meter used to measure the values of these resistor values shown in Table 4-1 was placed between the wiper and the ground leg of the potentiometer such that the resistance values that result in the display contrast are the ones obtained. Basing on these results the conclusion that was drawn is that with very high resistances the LCD cannot show anything but it has certain resistor values ranging from 0.05kΩ – 5.12kΩ at which its display contrast is good.

4.4 RFID Reader Response

A total of three RFID cards were administered and out of these three, all the three were successfully read by the RFID reader giving a 100% RFID reader response. Of these three cards two were valid and one was not valid. The two valid ones when swiped they were signified by a green LED indicating their validity, and the invalid one was signified by a red LED. This response rate is high enough to warranty that the RDM 6300 RFID reader used in the prototype design is reliable and efficient.

4.5 Analysis

This system clearly shows that all the passport details will be electronically stored there by reducing the risk of forgery, duplication of identity or identity theft, major problems which come with the conventional paper passport booklet.

The system also proves that it is possible to constantly update the details of the card holder in the system without any problems.

The RFID cards as soon as they enter the electromagnetic field zone of the reader they are read without any hassles and in a split of a second the details of the card are displayed on the system monitor. Thus the system saves time and provides enriched border control.

For any RFID cards which will not have been stored in the system's database these were not recognized by the system. In the event that there are some who will present any RFID cards to the system there is guarantee that they will not be recognized by the system.

The e-passport as observed from the prototype demonstration (available) is a user-friendly system which one can easily adapt to.

The system is a little bit compatible with the current passport system that is now being used in Zimbabwe in the sense that the current system now relies on a central electronic database at the Registry's department. Thus if the e-passport system is implemented there is guarantee of ease of penetration into the already existing system.

The LCD clearly displayed the welcome information visibly and it was well read. The passport card details were also displayed successfully despite the fact that the reader type used in this system (the RDM 6300) does not have the enable pin to switch it on and off. The looping effect problem was simply handled by adding a delay function such that when the cards are quickly swiped they are only read once. Of course the cards were swiped quickly but one has to pose the card for a second to ensure that it is read by the antenna.

The project showed positive results as the passport details could be viewed on the system monitor without any problems.

4.6 Views on the e-passport prototype

The following issues were of concern to the e-passport prototype (available) operation:

- If these RFID cards are implemented how then can one distinguish these cards from each other? Upon implementation these cards may have the image of the holder printed on the cards for distinction purposes.
- How efficient is it? Will one not travel several kilometers to another country only to be told at the border checkpoint that your card could not be read? Basing on the results obtained on this project, I the writer suppose not, that such is likely to happen because there was a 100% response of the RFID cards used for testing the functionality of this project.
- Is it secure? As demonstrated by this prototype this system will be secure because the details of the holder will be electronically stored.
- Others really criticized the issue of a receipting system which indicates that one is in a foreign country legally. Their arguments were that we are in a digital age and thus the paper system should be removed completely. Their suggestions were that even the other departments such as the police should have their e-passports checkpoints which can retrieve the information on these cards. However this will compromise the security of the e-passports and privacy of the holders as their biometric information will be accessible to anyone.

4.7 Technical issues observed of the e-passport prototype

- Upon implementation of this project there is need for expert analysis on the verification part.
- Data integrity has to be enhanced by a verification system.
- The risk of unauthorized remote accessibility of the RFID cards. This should also be taken into consideration and studied further before implementation. Maybe contact-based technologies may also be considered.

4.8 Chapter Summary

This chapter presented the prototype results compared with the current system of the conventional passport booklets. The chapter provides the basis on which conclusions and recommendations of the study are made. The next chapter provides conclusions, recommendations of the study and area of future study.

References

[1] M. Attaran, “Catch the wave of e-procurement,” *Industrial Management,* vol. III, no. 11, pp. 33-40, 2001.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter is going to give the recommendations that can be drawn from this project and the conclusions drawn from the demonstration of the working principle behind this e-passport prototype.

5.2 A Summary of the Results

This RFID based e-passport prototype was successful. The biographic information of the e-passport holder was able to be electronically stored and retrieved without any difficulties. This project ensures that privacy is ensured as the holder's identity will not be revealed to anyone as these details are stored electronically but will only be revealed to the authorized personnel who can access the serial monitor. Problems such as photo substitution and forgery are inevitable and problems like look-alike fraud and data duplication are eliminated. These results show that security is highly ensured. The fast response of the RFID cards means that movement at the border checkpoints will be fast.

5.3 Current Passport Issuance System in Zimbabwe

In an article published in the Chronicle Newspaper article on April, 09 2016 it stated that the President commissioned an e-passport production center machine which prints 16 000 conventional paper passport booklets per day. All this was done to alleviate standards of the travel documents and international security at the same time improving the relationship between the government and the people. The machine is also capable of producing the e-passport to be introduced as soon as government approves this new trend in passports. [1] The already existing Zimbabwean passport booklet is issued with a machine readable code.

Table 4-2 depicts the factors that the Zimbabwe's passport office complies with for the success of the e-passport system.

Table 5-1 Factors considered by the Passport office

Factor	Yes	No
State of the art travel document	*	
International Security features	*	
High Quality	*	
Quantity	*	
Production time	*	
International Compatibility	*	

The Registrar General spoke about the introduction of ICT in passport processing and this project enhances that. Making a comparison of the current issuance system and this project the conclusion that it will be easy to change the current passport IT infrastructure for the implementation of this project can be drawn. This is so because already now Zimbabwe has an e-passport system although it is not yet in use.

In addition to that Zimbabwe already has machine readable biometric identity cards with security features. Thus if these ID cards could be enhanced to be RFID based as this project is demonstrating, these IDs could serve as e-IDs and e-passports and the citizens will only apply for these national documents once. This will improve production costs and save time for the government, the people, the business and the stakeholders. This will be a positive contribution to the ZIM ASSET program of uplifting the socio-economic status of the ZIM people.

5.4 Challenges Anticipated in the adoption of the Electronic Passport System

5.4.1 Security

Attaran pointed out that with the opening up of connectivity, a lowering in the security of data has also occurred and concern over security is a factor limiting the implementation of e-commerce systems. [1]

5.4.2 Poor IT Infrastructure

To implement the whole system within the Passport issuing offices in Zimbabwe, an approach which requires enormous investment in software, hardware, altering the already existing LAN infrastructure, consultancy, installation and integration and re-organization is required and co-coordination of the system technologies the world over is an essential necessity. Slow and unstable connections may also be faced at first after this system has been implemented because a small sample of the RFID cards was used with the system. Whereas if this system is implemented it will be dealing with thousands of RFID cards per day, a risk which has to be taken into consideration prior to the installation and implementation of the system.

5.4.3 Lack of readiness from the people

Naturally the human mind always has fear of the unknown, the what ifs statements will always hover in their minds, such as what if the system does not function as expected and this can be a major setback on the adoption of the e-passport system. In addition to that, people, that is the staff at the passport offices and at the border controls and the users may also be resistant to change, a fact which may also pose a problem in the adoption of the e-passport system. Cultural indifferences are also another reason which may result in the failure of the adoption of the e-passport system.

5.5 Recommendations

A Faraday cage together with the Basic Access control should be implemented when these e-passports are deployed such that unauthorised remote reading of the e-passports is prevented.

This project could also be enhanced by a finger-print module which can be used for verification on a real time basis, whereby the border official requests for a fresh presentation of a fingerprint scan from the individual. The fingerprint module then sends this information to the microcontroller and comparison of the freshly presented fingerprint with the one already stored in the template of the user is done. If it matches with the template on the card then the LCD displays valid and the user is granted access. In an article published by the Chronicle on April 09, 2016 it stated that the President said an approach should be used to bring to fruition the other key components such as the automated fingerprint identification system and the computerised border management system.

In addition this system may also be used as a secure access system which can be used at secured buildings such as the president’s office, mobile network sites, etc. where only authorised personnel are allowed to enter.

Other technologies which can be used in the development of this e-passport which does not compromise the information of the intended user besides RFID may also be looked further into.

5.6 Areas of Future Study

As anticipated in the ICAO guidelines, e-passports will likely see use not just in airports but in new areas like e-commerce and they may also provide valuable experience in how to build more secure and more private identification platforms in the years to come. [2] Thus another area of study might be to look into the future use of the e-passports.

The issue of e-passports serving as e-IDs must also be taken into consideration. In an article in the Newsday on July 23, 2014 the Registrar General Tobaiwa Mudede wanted the already existing plastic IDs as passports thus if this system can be implemented such that these RFID cards will also be serving as the e-ID then they can serve multiple purposes.

The issuance of Visas on the e-passport must also be considered. How visas can be implemented in-conjunction with these e-passports is also another area which can be studied in the future.

5.7 Conclusions

The main objective of the Registrar General's Department which includes the passport office is to effectively serve the people of Zimbabwe and security is paramount. This project endorses these major objectives of this department by providing a fast and more efficient way to issue out passports to the general public. Although now the process of passport issuances has greatly improved than in the previous years, a more faster and efficient way will be provided in the sense that passports will be applied for and issued on the very same day and the waiting period will have been reduced to a few hours rather than the normal 4-6 weeks of the conventional passport booklet.

References

[1] M. Attaran, “Catch the wave of e-procurement,” *Industrial Management,* vol. III, no. 11, pp. 33-40, 2001.

[2] A. Juels, D. Molnar and D. Wagner, *Security and Privacy Issues in E-passports.*

APPENDIX A

Software Algorithm

```
#include <SoftwareSerial.h>

#include <LiquidCrystal.h>

LiquidCrystal lcd(11, 10, 5, 4, 3, 6);

SoftwareSerial RFID(2, 3); // RX and TX

int data1 = 0;

int ok = -1;

int yes = 13;

int no = 12;

// use first sketch in http://wp.me/p3LK05-3Gk to get your tag numbers

int tag1[14] = {2,55,52,48,48,49,50,54,52,69,56,69,65,3};

int tag2[14] = {2,55,52,48,48,49,50,51,69,57,55,67,70,3};

int newtag[14] = { 0,0,0,0,0,0,0,0,0,0,0,0,0,0}; // used for read comparisons

void setup()

{

// set up the LCD's number of columns and rows:

  lcd.begin(16, 2);

 // Print a message to the LCD.


  lcd.setCursor (0,0);

  lcd.print("e-PassportSystem");

  delay (1000);
 lcd.setCursor (1,1);

lcd.print("Welcome!");

delay (1000);

lcd.clear ();

lcd.setCursor (0,0);

lcd.print("swipe card");

delay (2000);

lcd.clear ();

RFID.begin(9600); // start serial to RFID reader

Serial.begin(9600); // start serial to PC

Serial.print("swipe card");

Serial.println();

pinMode(yes, OUTPUT); // for status LEDs

pinMode(no, OUTPUT);

}

boolean comparetag(int aa[14], int bb[14])

{

boolean ff = false;

int fg = 0;

for (int cc = 0 ; cc < 14 ; cc++)

{

if (aa[cc] == bb[cc])

{
```

```
fg++;
}
}
if (fg == 14)
{
ff = true;
}
return ff;
}
void checkmytags() // compares each tag against the tag just read
{
ok = 0; // this variable helps decision-making,
// if it is 1 we have a match, zero is a read but no match,
// -1 is no read attempt made
if (comparetag(newtag, tag1) == true)
{
Serial.println("Tag one ");
lcd.setCursor (0,0);
lcd.print("Tag one ");
  delay (1000);
Serial.println("Passport card valid!");
lcd.setCursor (0,1);
lcd.print("Card Valid!");
```

```
 delay (1000);
lcd.clear();
Serial.println("Name:          Anna Share ");
lcd.setCursor (0,0);
lcd.print("Name: Ann Share");
 delay (1000);
Serial.println("D.O.B:         05-09-1991 ");
lcd.setCursor (0,1);
lcd.print("DOB: 05-09-91");
 delay (1000);
 lcd.clear();
Serial.println("Nationality:   Zimbabwean ");
lcd.setCursor (0,0);
lcd.print("Nationality: ZIM");
 delay (1000);
Serial.println("D.O.I:        23-09-2016 ");
lcd.setCursor (0,1);
lcd.print("DOI: 23-09-16");
 delay (1000);
lcd.clear();
Serial.println("D.O.E:        22-09-2026 ");
lcd.setCursor (0,0);
lcd.print("DOE: 22-09-26");
```

```
  delay (1000);

lcd.setCursor (0,1);

lcd.print ("Swipe next card");

delay (1000);

lcd.clear();

ok++;

}

if (comparetag(newtag, tag2) == true)

{

Serial.println("Tag two ");

lcd.setCursor (0,0);

lcd.print("Tag two ");

  delay (1000);

Serial.println("Passport card valid! ");

lcd.setCursor (0,1);

lcd.print("Card Valid! ");

  delay (1000);

lcd.clear();

Serial.println("Name:         Arty Share ");

lcd.setCursor (0,0);

lcd.print("Name: Arty Share ");

  delay (1000);

Serial.println("D.O.B:        08-01-1993 ");
```

```
lcd.setCursor (0,1);

lcd.print("DOB: 08-01-93");

  delay (1000);

lcd.clear();

Serial.println("Nationality:  Indian ");

lcd.setCursor (0,0);

lcd.print("Nationality: ZIM ");

  delay (1000);

Serial.println("D.O.I:        23-09-2016 ");

lcd.setCursor (0,1);

lcd.print("DOI: 23-09-16 ");

  delay (1000);

lcd.clear();

Serial.println("D.O.E:        22-09-2026 ");

lcd.setCursor (0,0);

lcd.print("D.O.E 22-09-26 ");

  delay (1000);

lcd.setCursor (0,1);

lcd.print("Swipe Next Card ");

  delay (1000);

lcd.clear();

ok++;

}
```

```
}

void readTags()

{

for(int e=0;e<2;e++){

ok = -1;

if (RFID.available() > 0)

{

// read tag numbers

delay(100); // needed to allow time for the data to come in from the serial buffer.

for (int z = 0 ; z < 14 ; z++) // read the rest of the tag

{

data1 = RFID.read();

newtag[z] = data1;

}

RFID.flush(); // stops multiple reads

// do the tags match up?

checkmytags();

}

// now do something based on tag type

if (ok > 0) // if we had a match

{

Serial.println("ACCEPTED");

digitalWrite(yes, HIGH);
```

```
delay(1000);

digitalWrite(yes, LOW);

RFID.flush();

ok = -1;

}

else if (ok == 0) // if we didn't have a match

{

Serial.println ("");

Serial.println("Passport card invalid ");

lcd.setCursor (0,0);

lcd.print("Card Invalid! ");

  delay (1000);

Serial.println("REJECTED");

lcd.setCursor (0,1);

lcd.print("REJECTED ");

  delay (1000);

lcd.clear();

Serial.println();

digitalWrite(no, HIGH);

delay(1000);

digitalWrite(no, LOW);

RFID.flush();

ok = -1;
```

```
}
}
}
void loop()
{
readTags();
RFID.flush();
}
```

APPENDIX B

List of Abbreviations

EEPROM	Erasable Electronically Programmed Read Only Memory
E-IDs	Electronic Identity Cards
E-Passport	Electronic Passport
HF	High Frequency
I/O	Input/output
ICAO	International Civil Aviation Organisation
ICT	Information Communications Technology
ID	Identity
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LF	Low Frequency
PC	Personal Computer

RFID	Radio Frequency Identification
SRAM	Static Random Access Memory
UHF	Ultra-High Frequency

APPENDIX C

List of Components

Component	**Value**	**Quantity**
	Voltage(V)	
Arduino Uno	5	1
RFID Reader	5	1
RFID Antenna	5	1
16*2 LCD	5	1
	Ohms	
Resistors	220Ω & 100Ω	4
LEDs	Red & Green	2
RFID cards	----------------	3
Total		**13**