International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 5, ISSN No. 2455-2143, Pages 377-383
Published Online September 2019 in IJEAST (http://www.ijeast.com)

ELECTRONIC PASSPORT USING RFID TECHNOLOGY

Kumud Kumar
Department of Electronics and Communication Engineering
IFTM University Moradabad
Shahabad, Rampur, India

Rasmi Singh,
Assistant Professor in Department of Eletronics and Communication Engineering
IFTM University Moradabad

***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 travellers into any specific country at the same time maintaining the privacy and personal security of the e-passport bearers and track the person in which country.**

I. INTRODUCTION

An e-passport is a passport which features microchip technology. An integrated circuit (chip) within its pages contains the data that are essential in verifying the identity of the passport holder. These data include the personal data found on the data page of the passport, the biometrics of the passport holder, and the unique chip identification number. Electronic passports have an integrated chip, generally embedded in the cover page of the document that contains personal information of the document owner. a contactless (or RFID) technology has been chosen for the inspection process. An e-passport, or a digital passport, is a combined paper and electronic passport that contains biometric information that can be used to authenticate the identity of travellers. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or canter page, of the passport. Electronic passports include contactless chip which stores personal data of the passport holder, information about the passport and the issuing institution. In its simplest form, an electronic passport contains just a collection of read-only files. The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented. The specific choice of each country as to biometric security features to include makes a major difference in the level of security and privacy protection.

In this, the details of the person would be fed into the RFID cards (passports in RFID form). The RFID reader reads the details of the RFID passport and sends the data wirelessly with the help of RF transceiver. On the other side, the other RF receiver receives the details and sends to the microcontroller. Here, the controllers compares with the data already there. If it matches than the person is allowed, less he would be termed as a criminal by giving an alarm/buzzing signal. The e-passport with wireless contact on border control requires that any information is available without the holder's consent. It can be realized based on the access control procedure. The microchip is activated only by a code that is delivered from the machine-readable zone – MRZ. Hence, only the holders permit to access to the data stored inside of the chip. While inclusion of the MRZ sped up passport processing, it did little to improve the document‘s inherent security. The practice of removing a passport holder‘s picture and replacing it with another, however, has garnered much attention as a potentially simple means of committing passport fraud.

II. RELATED WORK

2.1 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.

2.2 Purpose of Study

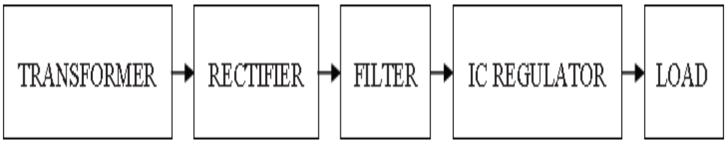
To design a prototype that will reduce forgery, duplication of data entry, look-alike fraud, photo substitution, which may be done by any holder of a conventional passport booklet. To come up with a more efficient travel document with less human intervention eliminating the fraud associated with a paper 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 thereon real-time basis to verify if the ones taken presently will match the fingerprints already stored in a template in the database.

2.3 Objectives of Study

1. **Primary Objective**
   - To develop an e-passport system using RFID cards.
2. **Secondary Objectives**

- 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 protect against identity theft.
- Above all provide a system that protects privacy.

III. POWER SUPPLY



Typically a 220V AC RMS voltage is connected to a transformer to step the AC voltage down to the level of the desired DC output. A full-wave rectified voltage is then provided by a diode rectifier which is initially filtered by a simple capacitor filter to produce a DC voltage. There are some ripples in the resulting DC voltage. A regulator IC will remove this ripples and will retain the same DC value even if there are variations in the DC voltage.

IV. RFID SYSTEM

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.

V. RFID TAGS/CARDS

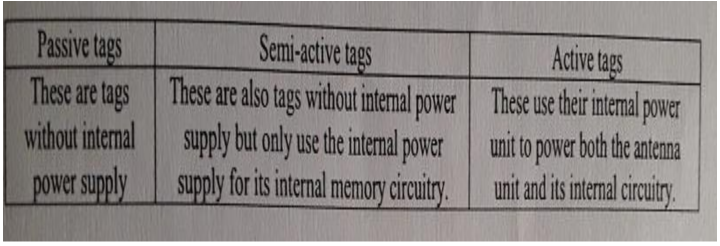
RFID tags/cards consist of an Integrated circuit attached on an antenna that is printed, etched or stamped onto a base which is often a paper substrate of Polyethylene Terephthalate (PET). The inlay which is the combination of the chip and antenna is then inserted amid the printed label and its adhesive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

The tag consists of the following:

- A radio frequency chip
- Encoding and decoding circuitry
- Antenna unit and
- 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 5-1 below.

Table 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.

Besides, tags can also be categorized based 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.1below shows an example of the type of RFID cards that are going to be used in this project.

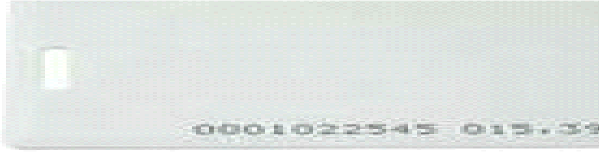


Fig 1 Typical RFID card for the project

VI. 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. The image below is showing an RFID reader.

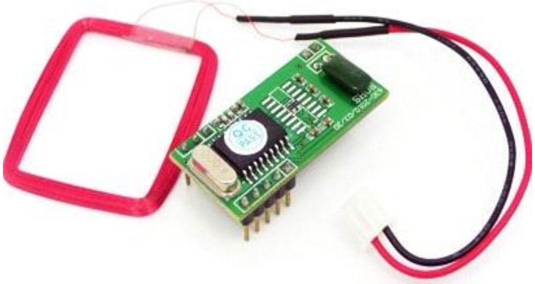


Fig 2 RFID Reader

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.

VII. 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 using radio signals which carry data either unidirectional or bidirectional. When a transponder gets into a red 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.

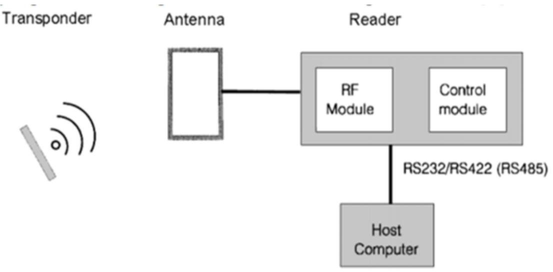


Fig 3 Working Principle of an RFID System

VIII. ARDUINO UNO BOARD

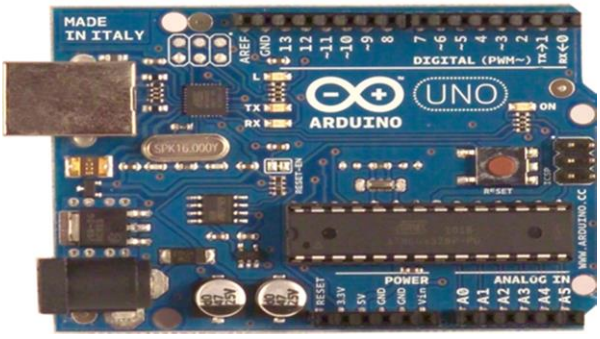


Fig 4 Arduino Uno Board

It is a microcontroller board based on the AT mega 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 8-1 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.

IX. BLOCK DIAGRAM OF THE SYSTEM

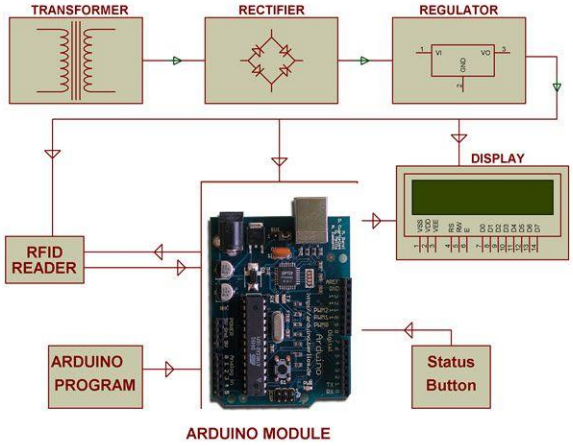


Fig 5 Block Diagram of the System

The block diagram in Fig. 3-7 shows the overall e-passport architecture. When an individual arrives at the border control checkpoint 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 passport RFID card and it decodes the information embedded on the card. If there is no match the LCDs invalid, and alarm is signified by a red led and the user is denied access.

X. 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:

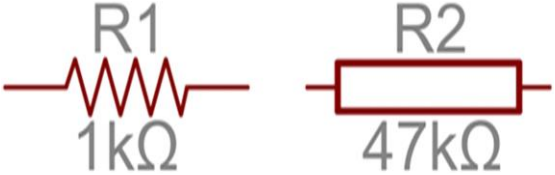


Fig 6 Schematic symbols of a Resistor

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 thermostats that are dependent on temperature or the photovoltaic cells that are dependent light.

XI. FUNCTIONS OF THE RESISTOR IN THE E-PASSPORT CIRCUIT

A. LED Current limit

LEDs too are very sensitive to high curren Resistors are the key in ensuring that LEDs not blow up when power is applied. Thus resistor when placed in series with the LEI regulates a proper flow of current throu them meaning the current flowing through t LED and the resistor is limited to a safe valu To calculate the value of a series LED resisto 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. 7 below is demonstrating how a resistor can be used to limit current to an LED.

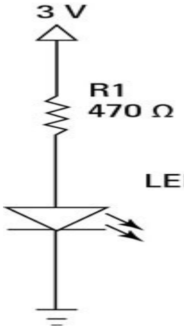
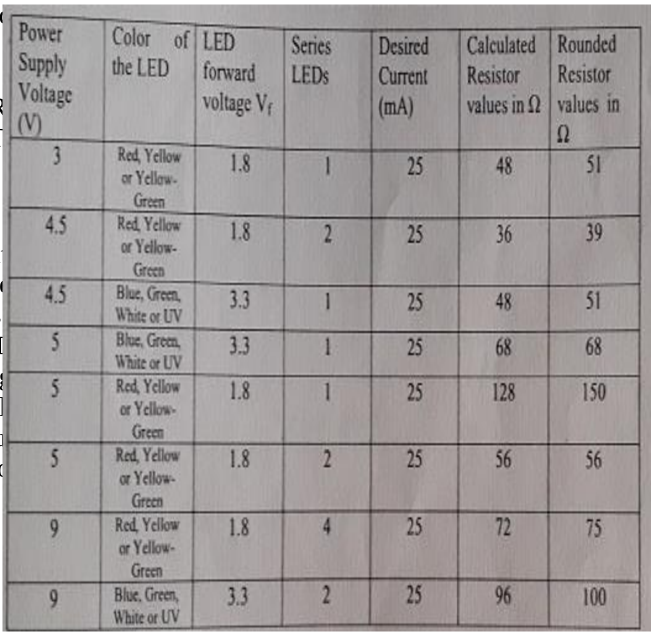


Fig 7 Current Limiting Resistors on an LED

The Table 2 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 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

B. 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.

XII. SCHEMATIC DESIGN AND OPERATION

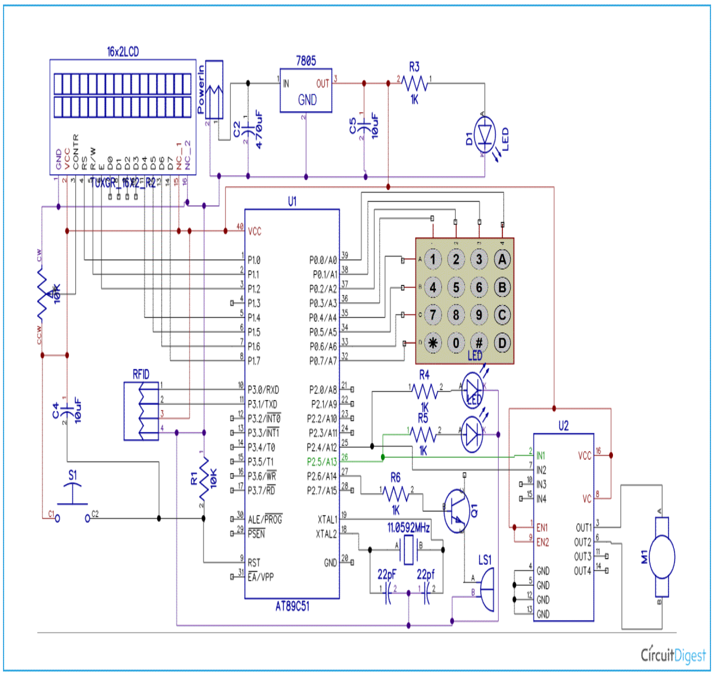
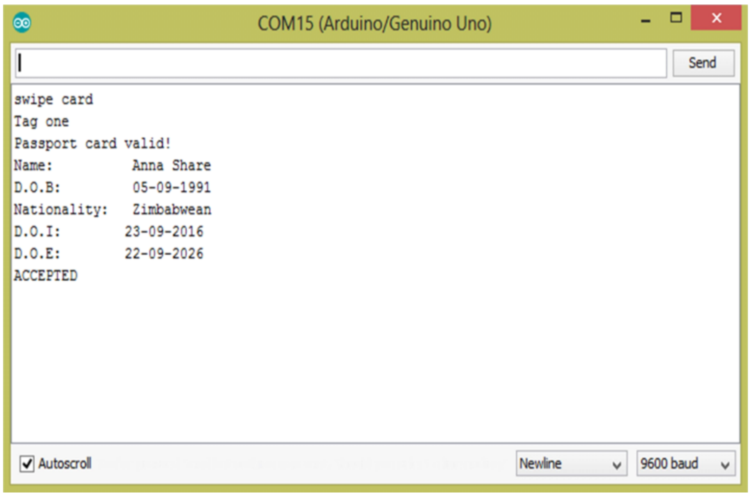


Fig 8 RFID based e-passport schematic

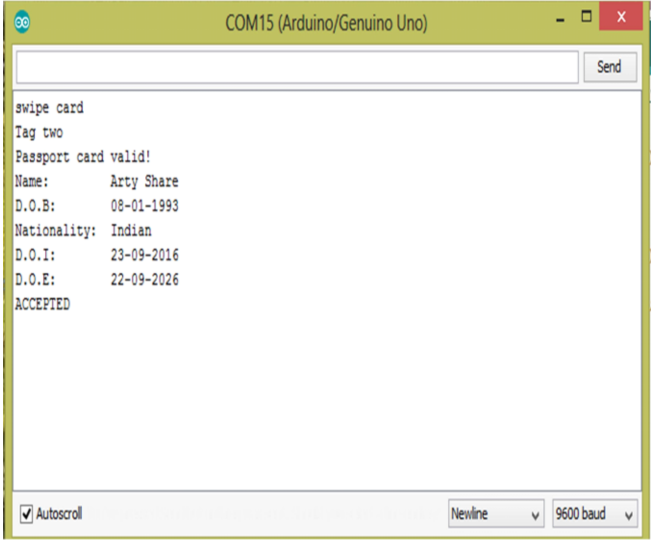
Fig. 8 is showing the schematic of the RFID based e-passport prototype. The RFID reader is interfaced with the reader antenna on the pins labeled ANT0 and ANT1 where the e-passport RFID card is tapped.



```
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 9 Results for Tag 1

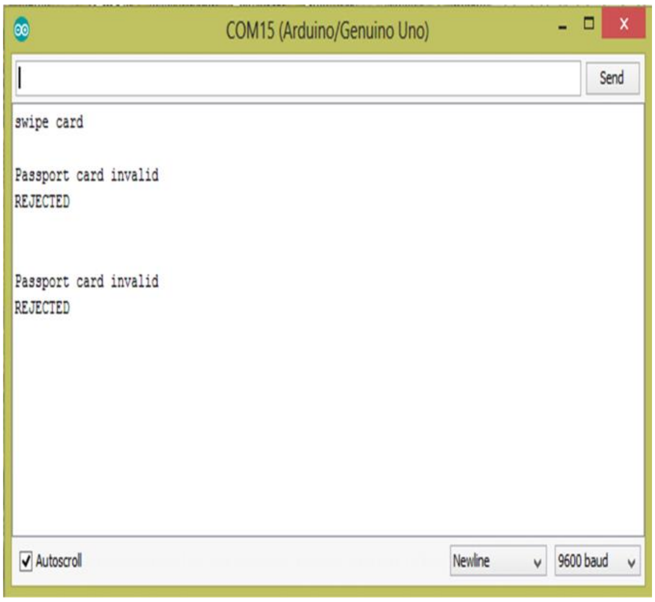
Having tapped the card, if it is a valid card, the details shown on Fig. 9 are displayed on the Arduino serial monitor and the LCD. These results were signified by a green LED on the circuit of the prototype available.



```
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 10 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 11 Results for Tag Three

Fig. 12-4 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.

XIII. CONCLUSIONS

This system clearly shows that all the passport details will be electronically stored thereby 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 cardholder 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. If some will present any RFID cards to the system there is a guarantee that they will not be recognized by the system.

XIV. ACKNOWLEDGEMENT

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

The LCD displayed the welcome information visibly and it was well-read. The passport card details were also displayed successfully although 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.

XV. REFERENCES

1. G. Matthew Ezovski, Steve E. Watkins, ―The Electronic Passport and the Future of Government Issued RFID-Based Identification‖ 2007 IEEE International Conference on RFID Gaylord Texan Resort, Grapevine, TX, USA March 26-28, 2007.

2. Marci Meingast, Jennifer King, and Deirdre K. Mulligan, "Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond," Journal of Communications, vol. 2, no. 7, pp. 36-48, 2007.

3. K. Ouafi and R. C.-W. Phan, "Privacy of recent RFID authentication protocols," 4th International Conference on Information Security Practice and Experience – ISPEC 2008, ser. Lecture Notes in Computer Science, vol. 4991. Sydney, Australia: Springer, April 2008, pp. 263–277.

4. M. Arapinis, T. Chothia, E. Ritter, and M. Ryan, "Untraceability in the applied pi-calculus," in Proceedings of the 1st Int. Workshop on RFID Security and Cryptography., 2009, to appear.

5. S. Delaine, S. Kremer, and M. Ryan, "Verifying privacy type properties of

electronic voting protocols," Journal of Computer Security, vol. 17, no. 4, pp. 435–487, 2009.

6. M. Arapinis, T. Chothia, E. Ritter, and M. Ryan, "Untraceability in the applied pi-calculus," in Proceedings of the 1st Int. Workshop on RFID Security and Cryptography., 2009, to appear.
7. Piotr Porwik, "The Biometric Passport: The Technical Requirements and Possibilities of Using", Biometrics and Kansei Engineering, International Conference - *ICBAKE* on 2009, pp. 65.
8. Dr Albert B. Jeng, Elizabeth Hsu, And Chia-Hung Lin Sponsor: "Should and How CC be used to evaluate RFID based Passports‖
9. K. Nohl and D. Evans, "Privacy through noise: a design space for private identification," in Annual Computer Security Applications Conference (ACSAC 2009), 2009.
10. "The new Polish passport with fingerprint". Polska Wytwórnia Papierów Wartościowych S.A. 22 June 2009. *Retrieved 5 June 2010.*
11. "Electronic Passport System". Archived from the original on August 29, 2010. Retrieved March 28, 2010.
12. *"e-Passport emulator". Dexlab.nl. Archived from the original on 12 April 2010. Retrieved 8 September 2010.*
13. *"The e-Passport". Passport Canada. 6 December 2012. Archived from the original on 28 July 2011. Retrieved 10 August 2011.*
14. *"E-Passports set to be on roll in June". The Independent. 19 March 2019. Archived from the original on 11 April 2019.*