World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:3, No:12, 2009

Implementation of an Improved Secure System Detection for E-passport by using EPC RFID Tags

A. Baith Mohamed Ayman Abdel-Hamid Kareem Youssri Mohamed

Open Science Index, Computer and Information Engineering Vol:3, No:12, 2009 publications.waset.org/15750/pdf

Abstract**—**Current proposals for E-passport or ID-Card is similar to a regular passport with the addition of tiny contactless integrated circuit (computer chip) inserted in the back cover, which will act as a secure storage device of the same data visually displayed on the photo page of the passport. In addition, it will include a digital photograph that will enable biometric comparison, through the use of facial recognition technology at international borders. Moreover, the e-passport will have a new interface, incorporating additional anti-fraud and security features. However, its problems are reliability, security and privacy. Privacy is a serious issue since there is no encryption between the readers and the E-passport. However, security issues such as authentication, data protection and control techniques cannot be embedded in one process. In this paper, design and prototype implementation of an improved E-passport reader is presented. The passport holder is authenticated online by using GSM network. The GSM network is the main interface between identification center and the e-passport reader. The communication data is protected between server and e-passport reader by using AES to encrypt data for protection will transferring through GSM network. Performance measurements indicate a 19% improvement in encryption cycles versus previously reported results.

Keywords**—**RFID "Radio Frequency Identification", EPC "Electronic Product Code", ICAO "International Civil Aviation Organization", IFF "Identify Friend or Foe"

I. Introduction

THE aim of all governments is to fuse Radio Frequency Identification (RFID) and biometric technologies in a new generation of identity cards which promise to be more secure for the entire world, ease identity checks, and enhance security but this technologies raise new risks. Some of the threats that need to be addressed when implementing RFID technology in sensitive fields such as international security are scanning, tracking, eavesdropping, and cloning. We try to implement a portable secure reader to allow checking the authority of the passport holder in any place at any time worldwide. Many works in the research community have tried to cover the privacy issue [1].

In Malaysia there was the first passport that includes a chip containing an image of a thumbprint of the passport holder in 1998. The second generation of e-passports rolled out in 2003 that contains extracted fingerprint information only. The Malaysian citizen in Kuala Lumpur International Airport passes through an automated gate that reads the thumb print from the chip and compares it to the thumb pressed on a scanner. The specification of these E-passports were based on the guidelines issued by the International Civil Aviation Organization (ICAO) in ICAO Document 9303[3] but the first Malaysian e-passport was pre-dating the ICAO standard. When the ICAO implemented the standards for the e-passports there were several security issues that were improperly addressed in ICAO's first generation E-passport specifications [4, 6]. Therefore there were a new specification which included a set of protocols called Extended Access Control (EAC) which improved the privacy issue that was a lake in the first generation of ICAO [8]. The goal of the ICAO is to implement a strong authentication through documents that unequivocally identify their bearers. Data integrity and physical integrity are vital to the security of ID cards as authenticators.

In this paper, design and prototype implementation of an embedded reader system which is secured and portable to read the biometric data from the passport is presented. The ICAO defines the biometric file formats, organization and communication protocols used in the passports as it will be discussed in section II. The comparison of biometric features is performed outside the passport chip to overcome the overhead of the processing inside the chip controller. To store biometric data on the contactless chip, it includes Electrically Erasable Programmable Read-Only Memory (EEPROM) storage memory, and runs according to the interface used ISO/IEC 14443 international standard or any other protocol [15]. Then, the information of passport holder will be checked through a GSM network and the authentication for that person will be received. The data will be encrypted by using AES before sending to the identification center and before being transmitted to the e-passport reader.

The rest of this paper is organized as follows Section II discusses biometric authentication, RFID introduction, and e-passport standards. Section III shows the design and prototype implementation of the e-passport reader. Section IV concludes the paper and outlines future work.

* Authors are with the Arab Academy for Science, Technology, and Maritime Transport, Egypt. e-mail: baithmm@hotmail.com

Open Science Index, Computer and Information Engineering Vol:3, No:12, 2009 publications.waset.org/15750/pdf

II. Technical Background

A. Introduction to Biometrics

The Biometric authentication is the verification of human identity through measurement of biological characteristics. Human beings authenticate one another by the use of biometric authentication. Computers are also able to perform authentication to the biological characteristics with more efficiency than humans, and biometric authentication is gaining currency as a means for people to authenticate themselves to computing systems (Fig. 1) shows the system authentication. The biometrics includes head shots, fingerprints, thermograms, iris images, hand geometry, retinal scans, DNA, and voice. E-passports use the head shots, fingerprints, and iris images.

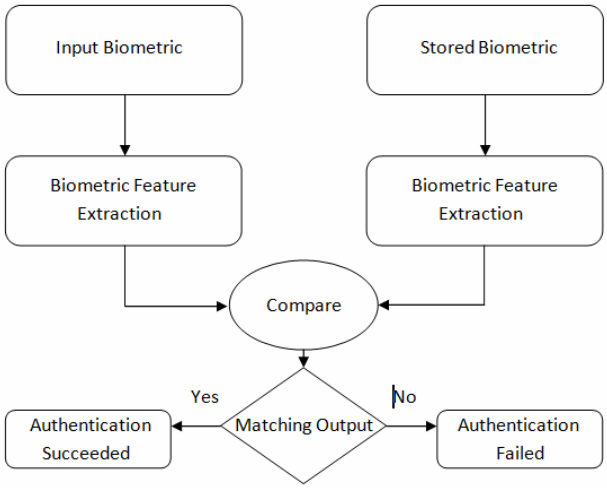


Fig. 1 Biometric Authentication

B. History & Introduction to RFID

The term Radio Frequency Identification (RFID) has come to stand for a family of technologies that communicate data wirelessly from a small chip, often called a "tag," to an inspection system called a Reader. First the RFID technology were discovered in the world war II to overcome the problems of the radar which. The problem was there was no way to identify which plane belongs to the enemy and which were a country's own pilots returning from a mission. The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back. This crude method alerted the radar crew on the ground that these were German planes and not Allied aircraft.

Under Watson-Watt, who headed a secret project, the British developed the first active Identify Friend or Foe (IFF) system. They put a transmitter on each British plane. When it received signals from radar stations on the ground, it began broadcasting a signal back that identified the aircraft as friendly. RFID works on this same basic concept. A signal is sent to a transponder, which wakes up and either reflects back a signal (passive system) or broadcasts a signal (active system) [11].

C. RFID System Components

RFID consists of Tags, Readers, and antennas as shown in (Fig. 2). RFID Tags can be one of three types: active, semi-active or passive. Active tags are those which are run by a battery, while passive tags do not have batteries. So they supply their own power by using the power obtained from radio signals emitted by the RFID Readers to operate. Because these tags do not supply their own power, communication with them needs to be short and usually does not transmit much data usually just an ID code. The range for transmission is from about 10mm to about 5 meters. There are four different kinds of tags in use, categorized by their radio frequency: low frequency (between 125 to 134 KHz), high frequency (13.56 MHz), UHF (868 to 956 MHz), and microwave (2.45 GHz) [4].

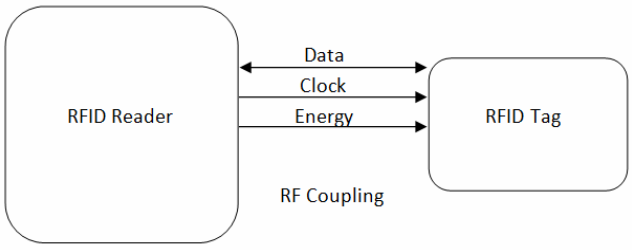


Fig. 2 RFID Main System Components

The second Component is the RFID Readers which operates at a range of frequencies, power, and reading ranges which are defined by the application. Finally, The RFID Antennas which are usually built into the RFID Reader and the RFID Tag to improve signal.

D. E-passport Standards

The e-passport standard was defined by the International Civil Aviation Organization (ICAO). The ICAO specification for e-passports relies on the International Organization for Standardization (ISO) 14443 standards that define RFID in passports as "Integrated contact-less chip" and specify a radio frequency of 13.56MHz and must has a logo to be defined by. The physical features of the e-passport tags are defined by the ISO 7810 standard which specifies the Tag dimensions of size 125mm x 88mm and These RFID Tags must have a built-in antenna.

Tags in the ISO 14443 standard are Passive tags which mean that they have the power source by reflecting the signal back to the reader instead of using active tags which needs battery to get its power to transmit signal to the reader. The passive tags are also chosen because of their low cost, high fidelity, and short read ranges.

E-passport Tags contains a built-in EEPROM memory which is between 32 to 144 kilobytes. This memory stores 16 data groups from DG1 to DG16 as in Table I and hash of data groups 1-15 stored in the security object data (SOD) which is known by security data element.

Open Science Index, Computer and Information Engineering Vol:3, No:12, 2009 publications.waset.org/15750/pdf

TABLE I
ICAO standard data structure Logical Data Structure (LDS)

Data Group 1	Contains the same data as printed on the passport
Data Group 2	Encoded facial image and corresponding biometric data
Data Group 3	Encoded biometric fingerprint data
Data Group 4	Encoded biometric iris data
Data Group 5	Displayed Portrait
Data Group 6	Reserved for Future Use
Data Group 7	Signature
Data Group 8-10	Data Features
Data Group 11	Additional Personal Details
Data Group 12	Additional Document Details
Data Group 13	Other Details
Data Group 14	CA Public Key
Data Group 15	AA Public Key
Data Group 16	Persons to Notify

III. Proposed E-Passport Reader Architecture

A. Design and Components

Our technology used microcontroller which is connected to RFID reader to read the EPC data and connected to a wireless GSM network which will send identification data and receive authentication from an identification center. In addition, a database server in the identification center is used to store the data of the passport as shown in Fig. 3.

The AVR microcontroller is used to interface with the reader. The AVR has many advantages than any other 8-bit microcontroller. From these advantages it is high performance coupled with low power consumption, Reduced Instruction Set Computer (RISC) with Harvard Architecture, Most of the instructions are single-cycle instruction execution, architecture designed for the Assembly and C-language programming and it has a very powerful in system programming, debugging and verification. The AVR has other features as On-chip 2-cycle Multiplier, for communication it uses Serial Peripheral Interface (SPI), Two-Wire Interface (TWI) and Universal Synchronous and Asynchronous serial Receiver and Transmitter (USART), Up to 16 MIPS Throughput at 16 MHz and Packaging which makes you upgrade your system without any problems.

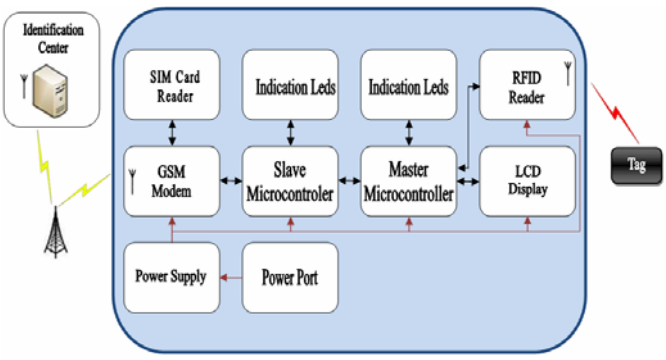


Fig. 3 Reader and System Configuration

This implementation is designed and developed from drawing schematics of circuit board and development of Gerber files then Printed Circuit Boards (PCBs) fabrications, assembly of electronics components and then finally writing the software and integration for microcontroller using embedded C programming language in the implementation of the interface with Reader and Assembly Programming in the implementation of Advanced Encryption Standard (AES) to secure the data transfer.

B. System Threats

There are many threats may affect that system. Some of these threats are between reader and passport as skimming, eavesdropper and cloning. Also there are threats between reader and server which will authenticate the information of the passport holder. In the proposed prototype Chip Authentication and Terminal Authentication are implemented to avoid threats between reader and e-passport, also AES is developed to defend system threats in between the server and reader.

C. RFID Threats

RFID threats are the threats between E-passport and reader. In the first and second generation of the e-passport the ICAO made standers to ensure the privacy and data correctness. In the first generation the ICAO provides the Passive Authentication (PA), Active Authentication (AA) and Basic Access Control (BAC). The second generation has provided Chip Authentication and Terminal Authentication which improved the authentication lack in the first generation.

1. **Passive Authentication (PA):** This scheme is known as passive authentication since the Tag performs no processing and is only passively involved in the protocol. This authentication checks the digital signature that the reader calculated is equal to the digital signature stored in the RFID embedded inside the passport. It uses the public key from the certificate it verifies the digital signature used to sign the data in the groups 1-15 and the SOD. Once the validity of the signature is established, the reader computes the hash of each of these data elements and compares them with the hashed values stored in the SOD. If there is a match, it can be established that the data on the Tag was not manipulated. This authentication can't detect cloning.

2. **Active Authentication (AA):** Active Authentication is an optional protocol in the ICAO first generation specification. It aims to detect if a Tag has been substituted or cloned. If Active Authentication is supported then the Tag on the e-passport stores a public key in Data Group 15 and its hash representation in the SOD. The corresponding private key is stored in the secure section of Tag memory. In order for the Tag to establish its authenticity, it must prove to the Reader that it has this private key [16].
3. **Basic Access Control (BAC)**: Is an optional protocol designed to prevent skimming and eavesdropping. Since RFID communication occurs over the air so it is easy to monitor transmitted personal data and capture, record and

Open Science Index, Computer and Information Engineering Vol:3, No:12, 2009 publications.waset.org/15750/pdf

analyze it for the attacker. So BAC is used to ensure that only Readers with physical access to the passport can read Tag data [5].

4. **Chip Authentication (CA)**: Is a mandatory protocol which aims to replace Active Authentication. This protocol is designed to avoid e-passport cloning. This attack is capable of defeating access control [2]. If the attacker analyze personal information data and by using reverse engineering to the captured data, then the E-passport could be cloned.

5. **Terminal Authentication (TA):** Main goal to make even the reader identified to the passport (the Basic Access Control and Chip Authentication can only identify the passport to the reader), thus preventing unauthorized readings. The identification is made by using the digital signature protocol with a public key on the reader side. This passport generates the challenge that is a random string and sends it to the reader. The reader signs the challenge with the private key using the public key of its own digital certificate and sends the signature to the passport. The passport verifies the signature correctness.

D. Server Threats

Server security is as important as network security because servers will hold most or all of the identification information. If a server is hacked, all of its contents may become available for the cracker to steal or manipulate at will. The network between server and reader is also important for data privacy and security. So server threats must to be covered to avoid loss of data or system hacking. In our implementation we have encrypted the data that will be sent or received between the reader and the server by using AES encryption technique on an 8-bit microcontroller. In a future work we could check the authority of the server if it is the server requested or it a clone server.

E. Implementation

1) Reader Implementation

The reader works as follows, at first, the RFID Reader searches for presence of an ID. Then the RFID Reader reads out data from memory of a microchip which can be built in the e-passport or in the ID card. Identification data of a microchip will be displayed on the LCD attached to the microcontroller which reads out from the reader. After data read-out from a master microcontroller it will be sent to a slave microcontroller which encrypt and transfers identification data in GSM modem network, data will be transferred to the identification (ID) center. Identification of data is made in a mode of real time for a greater distance by means of GSM is shown to a network and our Reader. The reader as a 3D view is shown in (Fig. 4).

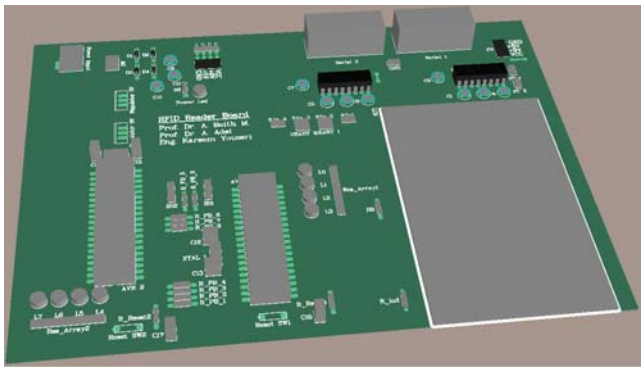


Fig. 4 System Implementation 3D Board

First the data is read for the RFID memory by the reader then we have communicated with the reader through serial communication "RS232" by building the circuit that converts signals from an RS-232 serial port to signals suitable for use in TTL compatible digital logic circuits.

Before the data is sent through the GSM network, it will be encrypted by using an encryption technique (AES, RSA, 3DES) [9] to authenticate the data between reader and server, we have implemented AES Rijndael encryption technique on an 8-bit microcontroller AVR [10]. The Rijndael have been implemented very efficiently on a wide range of processors and in hardware. Rafael R. Sevilla implemented by 80186 assembly and Geoffrey keating's Motorola 6805 implementation is also available on Rijndael site [12]. After Encrypting the identity data it will be send over GSM network to database server which will check for the identification data of the e-passport holder and will send the acceptance or discard of this data after encrypting the message and then send back to the microcontroller system to perform the reader.

Then to send the identity data from the master controller to the server or from the server to the master controller we have used SPI interface between Master controller and slave controller to send and receive data. Then the server will get the identity data and check for it by using a database engine then it will replay to Master controller through GSM Network and then passing by the slave controller. In (Fig. 5) we display the system overview for the sequence of the system implementation.

2) AES Implementation

AES is an efficient implementation on 8-bit and 32 bit platforms because most of the transformations are performed by the shift, rotation, substitution which are easy to be implemented on an 8-bit microcontroller. If we used 32-bit microcontroller we could implement lookup tables to improve performance [13]. To overcome the problem of using the registers to be accessed in the best access we have used the assembly language for AVR by using AVR Studio as a compiler. AES have been implemented on an 8-bit microcontroller previously as shown in table II, [14]. We have used Rijndael 128-bit Key length and 128-bit block length on an 8-bit AVR microcontroller and we have improved the speed of encryption on the microcontroller to 3,268 cycles but the code length has been increased. This represents an improvement of around 19% versus AVR platform reported in 2006 [14].

TABLE II
AES/RIJNDAEL PERFORMANCE ON 8-BIT PLATFORMS

Platform	Year	Encryption/Decryption Cycles
68HC08	1998	8,390 / N/A
68HC05	1999	14,945 / N/A
Z80	2000	25,494 / N/A
8051	1998	3,168 / N/A
8051	2001	7,542 / N/A
8051	2006	3,905 / 5,876
AVR	2003	7,498 / 11,548
AVR	2006	4,009 / 6,073

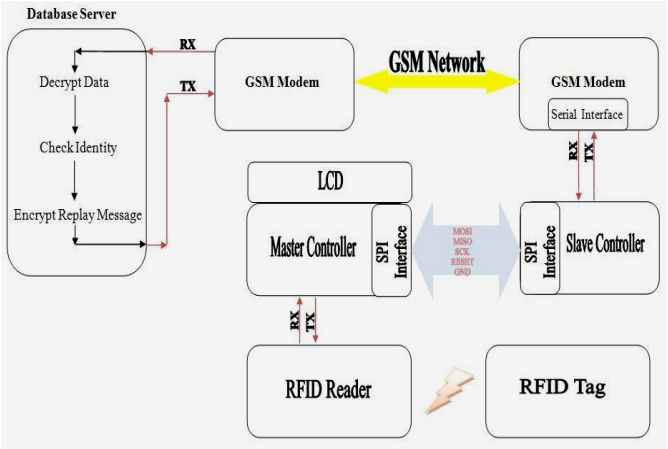


Fig. 5 System Overview

IV. CONCLUSION AND FUTURE WORK

This paper presents the design and prototype implementation of an e-passport reader on an 8-bit AVR microcontroller. Performance evaluation results indicate the enhancement of AES encryption execution cycles on an 8-bit microcontroller to 19%. Furthermore, our design incorporates the first use of a GSM network in identification for e-passport to the best of our knowledge. The availability of such readers presents an opportunity in a mode of real time identification which can be built in e-passport or other document. Data on huge distances from ID center are allowed to approve to us, therefore, this paper solved the problem of protection and identification. This system provides a comprehensive system to create, manage and monitor the identity data online. The system generates the relationships between the physical layer hardware, their process interaction and the ultimate backend applications.

Future work includes the use of a 32-bit microcontroller instead of 8-bit microcontroller which will improve the performance of AES implementation.

REFERENCES

[1] Juels. RFID security and privacy: a research survey. *Selected Areas in Communications, IEEE Journal on*, 24(2):381–394, 2006.
[2] J. Mandel, A. Roach, and K. Winstein, "MIT proximity card vulnerabilities," Tech. Rep., Massachusetts Institute of Technology, March 2004.
[3] ICAO. Document 9303, machine readable travel documents, October 2004.
[4] Juels, A., Molnar, D., Wagner, D.: Security and privacy issues in E-passports. Report, Cryptology ePrint Archive (March 2005).
[5] ICAO, Machine readable travel documents, Part-1, Machine Readable Passport Volume 2, Specifications for Electronically Enabled Passports with Biometric Identification Capability, Doc. 9303, 2005.
[6] Lekkas, D., Gritzalis, D.: E-passports as a means towards the first world-wide public key infrastructure.
In Lopez, J., Samarati, P., Ferrer, J.L., eds.: *Public Key Infrastructure, 4th European PKI Workshop: Theory and Practice*, EuroPKI 2007, Palma de Mallorca, Spain, June 28-30, 2007, Proceedings. Volume 4582 of Lecture Notes in Computer Science, Springer (2007) 34–48.
[7] Yan, Lu, et al. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Cambridge, UK : Cambridge, ; Beijing, China : Beijing University of Aeronautics & Astronautics, 2008.
[8] ICAO: Doc 9303: Machine Readable Travel Documents - Part 1, Volume 2. (2006).
[9] J. Daernen and V. Rijmen. Aes proposal: Rijndael, 1998.
[10] Sungha Kim, Ingrid Verbauwhede AES implementation on 8-bit microcontroller, Los Angeles, CA-90024.
[11] "The History of RFID Technology." RFID Journal.2002-2009 < http://www.rfidjournal.com/article/view/1338/1/129 >.
[12] Rijndael home site http://www.esat.kuleuven.ac.be/~rijmen/rijndael/
[13] J. Daemen and V. Rijmen. The Design of Rijndal. Information Security and Cryptography. Springer 2002. ISBN 3-540-42580-2.
[14] Lopez, Javier, Zhou, Jianying. Wireless Sensor Network Security. Netherlands : IOS Press, 2008.
[15] Cerede, G.: Understanding the antenna design challenge. RFIDesign (2006) 10–13.
[16] ISO: Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms, ISO/IEC 9796-2, Second edition (2002).

AUTHOR BIOGRAPHY



A. Baith Mohamed, Professor at the Arab Academy for Science and Technology (AAST MT), College of Engineering and Technology, Computer Engineering Department. IEEE Senior Member. Board member in Computer Scientific Society, Egypt.
Email: baithmm@hotmail.com



Ayman Abdel-Hamid, Associate professor in the College of Computing and Information Technology, Arab Academy for Science, Technology, and Maritime Transport (AASTMT), Egypt. In addition, he holds the position of Manager of AASTMT's Computer Networks and Data Center. His research interests include mobile computing, network-layer mobility support, computer and network security, distributed systems, and networking and group communication aspects of interactive remote instruction. He is a member of IEEE, IEEE Computer Society, ACM, and ACM SIGCOMM.
Email: hamid@aast.edu



Kareem Youssri Mohamed, Engineer at the Arab Academy for Science and Technology, Industrial Service Center, Mechatronics and Embedded Systems Department
Email: Kareem_youssri_2002@msn.com

Open Science Index, Computer and Information Engineering Vol:3, No:12, 2009 publications.waset.org/15750/pdf