TWO NOVEL E-VISAS VERIFICATION SCHEMES BASED ON PUBLIC KEY INFRASTRUCTURE (PKI) AND IDENTITY BASED ENCRYPTION (IBE)

By

NAJLAA ABDULLAH ABUADHMAH

Thesis Submitted In Partial Fulfillment of the Requirements
For The Degree of Master of Science In
Computer Science

JANUARY 2010

PDF created with pdfFactory Pro trial version www.pdffactory.com

DECLARATION

Name: **NAJLAA ABDULLAH ABUADHMAH**
Matric No: **PCOM 0014/08**
Faculty: **SCHOOL OF COMPUTER SCIENCES**
Thesis Title: **TWO NOVEL E-VISAS VERIFICATION SCHEMES BASED ON PUBLIC KEY INFRASTRUCTURE (PKI) AND IDENTITY BASED ENCRYPTION (IBE)**

I hereby declare that this thesis in I have submitted to **SCHOOL OF COMPUTER SCIENCES** on **December 2009** are my own work. I have stated all references used for the completion of my thesis.
I agree to prepare electronic copies of the said thesis to the external examiner or internal examiner for the determination of amount of words used or to check on plagiarism should a request be made.
I make this declaration with the believe that what is stated in this declaration is true and the thesis as forwarded is free from plagiarism as provided under Rule 6 of the Universities and University Colleges (Amendment) Act 2008, University Science Malaysia Rules (Student Discipline) 1999.
I conscientiously believe and agree that the University can take disciplinary actions against me under Rule 48 of the Act should my thesis be found to be the work or ideas of other persons.

Signature: ..... Date: .....

Name: (Najlaa Abdullah AbuAdhmah)

Acknowledgement of receipt by: ……. Date

PDF created with pdfFactory Pro trial version www.pdffactory.com

ACKNOWLEDGMENT

First of all, I would like to take this opportunity to express my deepest gratitude to God for the completion of this dissertation. Many thanks are also due to My King Abdullah bin Abdul Aziz, may Allah bless for my country Saudi Arabia. This thesis has only been made possible with the help of many parties. I would like to express my appreciation to my parents especially my dear father, who never had a chance to join me at this moment, may Allah join me with you in Jannat Al-Na'eem. Thank you, Mom and Dad for all your encouragement and driving me to complete my dissertation. I'd like to thank and send a warm regard to my supervisor Associate Professor Dr. Azman Samsudin for his kindness and patience to take my hand and lead me to a higher level of knowledge, and the Dean of the School of Computer Sciences with all the staff members of the school of computer science of USM. I would like to thank my sister, Azhar for her support and patience in this study and also many thanks to all my family members. To those who had contributed their invaluable assistance and had advises me, either directly or indirectly, yet their names are not cited here, they deserve my greatest gratitude too. Thanks to all of them for everything.

PDF created with pdfFactory Pro trial version www.pdffactory.com

TABLE OF CONTENTS

PDF created with pdfFactory Pro trial version www.pdffactory.com

PDF created with pdfFactory Pro trial version www.pdffactory.com

PDF created with pdfFactory Pro trial version www.pdffactory.com

LIST OF TABLES

PDF created with pdfFactory Pro trial version www.pdffactory.com

LIST OF FIGURES

PDF created with pdfFactory Pro trial version www.pdffactory.com

PDF created with pdfFactory Pro trial version www.pdffactory.com

LIST OF ABBREVIATIONS

AA	Active Authentication
BAC	Basic Access Control
CRL	Certificate Revocation Lists
DS	Document Signer
EAC	Extended Access Control
ENC	Encryption
IBE	Identity Based Encryption
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
IS	Inspection system
ISO	International Organization for Standardization
MRZ	Machine Readable Zone
LDS	Logical Data Structure
PA	Passive Authentication
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
RSA	Name of Public-Key encryption algorithm designed by Ron Rivest, Adi Shamir, and Leonard Adleman
SHA	Secure Hash Algorithm (name of a hash algorithm)
SOD	Security Object Document

PDF created with pdfFactory Pro trial version www.pdffactory.com

DUA SKIM PENGESAHAN E-VISA YANG BARU BERASASKAN INFRASTRUKTUR KUNCI UMUM (PKI) DAN ENKRIPSI BERASASKA IDENTITI (IBE)

ABSTRAK

Visa merupakan dokumen perjalanan yang sangat penting yang membenarkan kita memasuki sesebuah negara yang akan kita lawati. Walau bagaimanapun dokumen penting seperti visa ini masih ditangani secara manual yang mana boleh memberi kesan kepada ketepatan dan kecekapan dalam pemprosesan visa. Perlaksanaan e-visa masih belum meluas. Penyelidikan ini memberikan gambaran yang terperinci tentang cadangan baru prototaip sistem pengesahan e-visa berasaskan teknologi RFID. Teknologi teras bagi sistem pengesahan e-visa yang dicadangkan itu adalah berasaskan Enkripsi Berasaskan Identiti (IBE) dan Infrastruktur Kunci Umum (PKI). Penyelidikan ini juga memberikan perbandingan antara kedua-dua kaedah tersebut dari segi masa pemprosesan dan kebergunaan aplikasi. Hasil penyaelidikan menunjukkan proses sistem pengesahan e-visa mempamerkan kefleksibelan yang tinggi apabila dilaksanakan dengan IBE tetapi menghasilkan kelajuan pemprosesan yang lebih baik apabila dilaksanakan dengan PKI.

PDF created with pdfFactory Pro trial version www.pdffactory.com

TWO NOVEL E-VISAS VERIFICATION SCHEMES BASED ON PUBLIC KEY INFRASTRUCTURE (PKI) AND IDENTITY BASED ENCRYPTION (IBE)

ABSTRACT

Visa is a very important traveling document, which is an essential need at the point of entry of any country we are visiting. However an important document such as visa is still handled manually which affects the accuracy and efficiency of processing the visa. Work on e-visa is almost unexplored. This research provides a detailed description of a newly proposed e-visa verification system prototyped based on RFID technology. The core technology of the proposed e-visa verification system is based on Identity Based Encryption (IBE) and Public Key Infrastructure (PKI). This research provides comparison between both methods in terms of processing time and application usability. The result shows the e-visa verification system process has highly flexible when implemented with IBE and on the other hand produces better processing speed when implemented with PKI.

PDF created with pdfFactory Pro trial version www.pdffactory.com

CHAPTER ONE

RFID TECHNOLOGY FOR E-PASSPORTS AND E-VISAS

1.1 Introduction

In recent years, new electronic e-passports have started to replace conventional paper-based passports around the world. In line with this development, a new protocol for e-visas is proposed in this thesis that can work hand in hand with current e-passport technology. The requirements for this new type of e-visa include a higher level of security, i.e., a higher degree of security inspection must be placed at inspection points at the entry points of countries. The new e-visa reveals the owner's identity and his/her criminal records, if any, using Radio Frequency Identification (RFID) technology.

RFID is a generic term for technology that uses radio waves for automatic identification of entities and individual coffers. RFID technology is the next generation after bar codes in the area of identification technology. The first use of RFID technology was implemented in the 1940s. The British Air Force used RFID technology in World War II to identify whether airplanes were belonged to them. RFID theory was initially introduced by Stockman in 1948 in a conference paper entitled "Communication by Means of Reflected Power". The first patent for RFID was filed by Charles Walton in 1973 (Stockman, 1948).

PDF created with pdfFactory Pro trial version www.pdffactory.com

1.2 The Background of E-visas

The proposed e-visa is relatively similar to the e-passport, in that it is fitted with a microchip. The chip is embedded in the passport and contains the holder's digital photograph, name, gender, nationality, passport number, expiration date, date of issue and place of issue. The same information is also printed on the pages of every visa. In addition, the chip may hold biometric data capable of verifying the identity of the visa holder.

This e-visa can be read very quickly and accurately by readers that retrieve data for immigration systems at borders around the world and/or track foreigners within a given country. The proposed e-visa is based on the cryptography primitive known as Identity-Based Encryption (IBE) or Public-Key Infrastructure (PKI), which can enhance the security of the e-visa itself as well as the e-passport.

1.3 Motivation

E-visas are a very promising technology because of their wide range of applications and the high level enforcement of security measures that can be implemented through them. The present paper-based visa is very easy to clone, especially when it takes the form of an ink stamp. However, e-visas can hold more information on the holder, such as health and criminal records. In addition, the e-visa is issued by the same country as the one that verifies it, and therefore, it should be subject to minimal legal or privacy restrictions because the country that issues the e-visa later uses (i.e., verifies) it.

E-visas can highly increase the security of the e-passport. In addition, the implementation of e-visas could retain the use of a paper passport if some countries have technology to detect an e–passport. The e-visa can be

PDF created with pdfFactory Pro trial version www.pdffactory.com

read easily because the visa is issued by the same country that issues the e-visa. Countries that wish to delay the implementation of e-passports and e-visas can now easily wait until a time of their choosing without affecting the countries that opt for e-visa implementation.

The proposed e-visa uses IBE or PKI, which contains a highly secured mechanism; as such, this technology would pose no inconvenience to any of the parties involved. Lastly, e-visas can also be deployed for other uses, such as criminal detection systems and other related applications involving border-crossings.

There is limited research on e-visas. Therefore, this study helps to show that IBE and/or PKI provide a strong security system in which it is politically safe to implement e-visas. Figure 1.1 shows the usage of e-passports, given that countries may or may not agree on the usage the e-passports, which in turn makes the idea of using e-passports less effective**.** In contrast, Figure 1.2 shows 100% utilisation of the e-visa, assuming the country issuing the e-visa uses the e-visa for its own purposes.

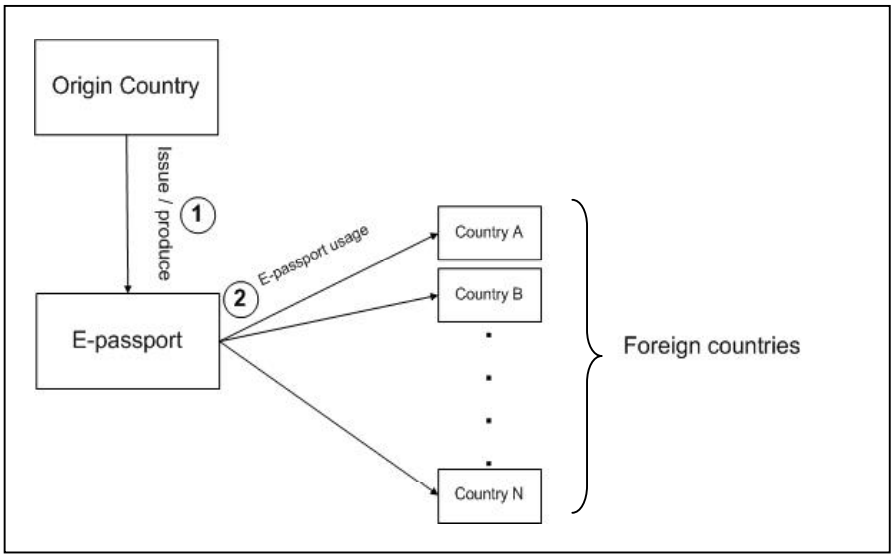

Figure 1.1: E-passport usage

PDF created with pdfFactory Pro trial version www.pdffactory.com

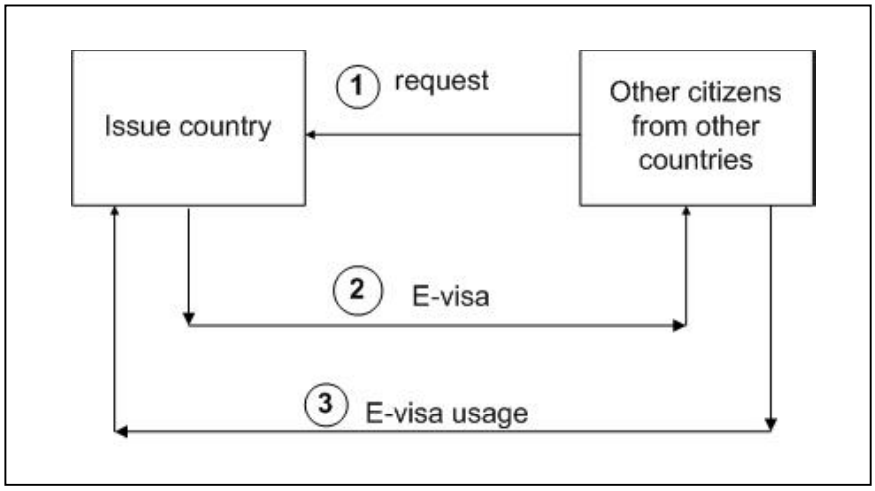

Figure 1.2: E-visa usage

1.4 The Statement of Problem

A visa is a very important travel document, which is normally needed during the inspection process at national borders. Travellers who wish to visit other countries often need visas for entry into destination countries.

The proposed solution is for the embassy of the respective country to issue an e-visa that can be read through the use of an electronic reader. At the main entrance of a country, the e-visa is electronically read to ensure its validity. Access to the data stored in an e-visa can occur at many stages and in many different systems, including for instance, in hotels, through driving licenses, during car rental, in malls and at police stations. Furthermore, the implementation of e-visas speeds up the procedural travel constraints while maintaining high security. Therefore, the implementation of e-visas that integrate RFID with visas is strongly suggested.

Because the proposed e-visa is to be implemented in reality, the data stored in the e-visa chip is subject to change or even being overwritten with

PDF created with pdfFactory Pro trial version www.pdffactory.com

fake data, which leads to the requirement of a verification system that can validate the visa contents and judge the integrity of e-visa information.

1.5 Research Questions

This study seeks to address the following questions.

- What are the problems and issues concerning RFID security and privacy in e-passports that arise in the implementation of e-visas?
- What is an appropriate protocol for e-visa verification?
- How can one verify e-visas using IBE and/or PKI?

1.6 Research Objectives

This research has the following objectives:

1. To review and compare the e-passport security standards based on countries and regions and highlight the main security and privacy contents to study the benefits of implementing e-visas.
2. To propose a secured implementation protocol of e-visa verification using IBE and PKI.
3. To build a prototype e-visa verification system.
4. To compare IBE-based and PKI-based e-visa verification systems.

1.7 Research Scope

This research is limited only to e-visa verification systems as an identification tool for travellers. In this research, a security management solution for an e-visa verification system in addition to the existing passport

PDF created with pdfFactory Pro trial version www.pdffactory.com

system is proposed through the use of IBE and PKI.

1.8 Research Contributions

The new contributions of this research include the following four points:

1. We first evaluate the current state-of-the-art technology. We begin this research with a survey and review of the existing security mechanisms for e-passports, which leads to a greater understanding of how e-passports work and enables an analysis of the main security and privacy concerns as well as the development of new approaches to avoid problems in e-visa implementation.
2. We propose a secured implementation of e-visa verification using IBE and PKI to achieve an optimal security level.
3. We show prototypes of the proposed system to demonstrate the applicability of our proposed method.
4. We conduct a critical security discussion of the proposed e-visa verification system.

1.9 Organisation of Thesis

This thesis is structured as follows (see Figure 1.3):

Chapter 1 presents a brief introduction to the concept of RFID as well as e-visa and e-passport technologies. It also summarises the problem statement, objectives, and research questions and presents a brief overview of this thesis.

Chapter 2 presents relevant background information about e-visa and e-passport technologies and security mechanisms, including articles and reports from specialist departments regarding security and privacy threats. It

PDF created with pdfFactory Pro trial version www.pdffactory.com

also provides more detailed descriptions of security mechanisms and explains several mechanisms used in protecting the privacy and security of e-passports as well as a brief overview of IBE, which is a security mechanism that is proposed for e-visa implementation.

Chapter 3 explains the research procedure and the suitable methods that we could use to verify the e-visa; it also clarifies the theoretical framework and research design.

Chapter 4 presents a security analysis of the new protocol.

Chapter 5 presents the conclusions of this thesis and provides further recommendations for future work.

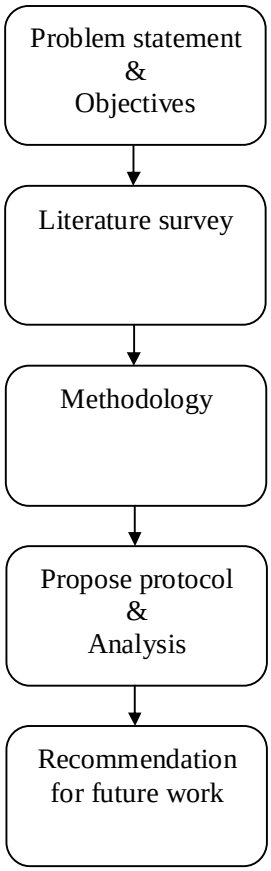

Figure 1.3: Flow of research activates

PDF created with pdfFactory Pro trial version www.pdffactory.com

CHAPTER TWO

REVIEW OF THE E-PASSPORT AND E-VISA SECURITY MECHANISMS

2.1 Introduction

Due to the increasing number of security issues with paper-based passports, their use is slowly but surely fading into oblivion. Despite their increasing shortcomings, paper passports have yet to be phased out as they are still needed for identification and other processing tasks. There is however an increasing need for a new form of electronic travelling document, or e-passport and e-visa, to eventually replace the common paper passports. In general, there arises a serious issue with the usage of e-passports because capable devices are not found in many countries to read the e-passports. Therefore, this research would strive to create a new protocol for e-visa to eventually replace the common paper visas. New implementation of e-visa will be readable around the world and will probably have several other uses, for example, for hotels and car rentals. In order to implement a new suitable technology satisfying the e-visa requirements, the combined use of Radio Frequency Identification (RFID) and biometric identification technologies together in the electronic document (e-passport) would be extremely helpful to produce e-visa sufficiently to serve in the new era of global identification. In this chapter, e-passports will be briefly explained, along with their technology standards, and main privacy and security threats.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Furthermore, a brief overview of e-visa system, Identity Based Encryption (IBE) and Public Key Infrastructures (PKI) will be given in line with the proposal in this thesis to implement e-visa verification system.

2.2 Machine Readable Travel Document (MRTD)

A Machine Readable Travel Document (Gaurav and Paul , 2005) is defined as an official document that is issued by an official party (country or equivalent) which is used by the holder as an identity document for international travel purposes (e.g. passport, visa), containing the mandatory visual (eye readable) data, and a separate mandatory machine-readable electronic data summary. The common international standards for the new passports were set by the International Civil Aviation Organization (ICAO) in 2001 and have been adopted by the waiver countries and the United States of America. (Vaudenay and Vuagnoux, 2007).

The main goals in these standards were to increase the ease of task processing and decrease the duration of tasks, while maintaining a high level of security and accuracy. All the required data would be stored on a RFID microchip that can be accessed from a short distance using radio waves.

2.2.1 E-passport Architecture

In the near future, the use of an e-passport does not spell the abolition of the standard paper-based passport, which will remain necessary until the new technology is used globally. In the meantime, the e-passport would be designed to work in tandem with the paper-based passport, while the paper-based passport can still be used in the absence of the new technology in certain countries. Eventually the use of the paper-based passport will hopefully be phased out when the new technology is used by the whole world

PDF created with pdfFactory Pro trial version www.pdffactory.com

concurrently. Currently, the e-passport makes use of a small contact-less integrated circuit that can be embedded in the back cover of the passport. This chip stores all the data required by immigration departments subject to international standards within an international passport. An additional feature is a digital profile photograph, which could eventually be developed into a 3D image complete with an iris scan, a voice scan, fingerprints, or, when biometric science has developed sufficiently, a DNA pattern, in order to enable high technology biometric comparisons, e.g. through the use of facial recognition technology, at international borders. All these accurate and hard to duplicate features can be stored via RFID, which enables the information to be stored securely in the form of digital information as shown in Figure 2.1. The ICAO has defined a common standard structure.

A standardized Logical Data Structure (LDS) is required to enable global interoperability. The LDS identifies all mandatory and optional data elements and any prescriptive ordering and/or grouping of data elements that must be followed to achieve global interoperability for the reading of details (Data Elements) recorded in a capacity expansion technology (IC Chip).

This structure categorizes the information into mandatory, optional and future information:

1. Mandatory: the information that is also physically present on the passport. At present, face recognition is specified as the only mandatory globally interoperable biometric for the identity verification of travelers.
2. Optional: fingerprint and iris biometric data.

PDF created with pdfFactory Pro trial version www.pdffactory.com

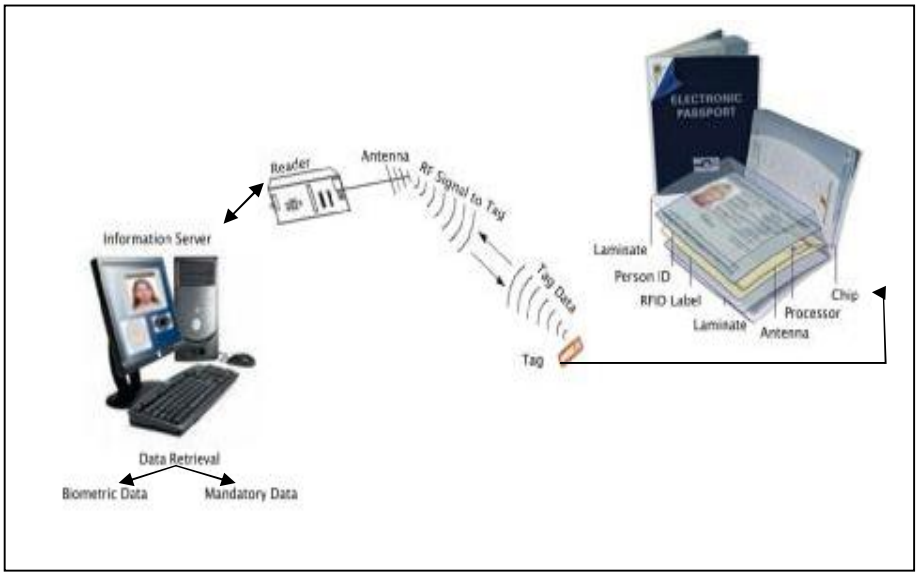

Figure 2.1: How e-passports are processed

According to (Lekkas and Gritzalis, 2007a,2007b), the structure of the data is stored in the passport's chip (the LDS – Logical Data Structure), including the digital signature. Data are separated into two parts:

(a) the user files, in a writable area (Dedicated Files – DF), and

(b) the LDS, providing read-only access.

Sixteen Data Groups, containing the holder's identification and biometric data. According to (Avoine et al., 2008, Kugler) the MRZ (including document number, name of bearer, nationality, date of birth, etc.) is stored in the 1st Data Group, the biometric data, such as facial image and fingerprint and iris scans, are stored respectively in Data Groups 2, 3 and 4. Data Groups 5, Data Groups 6 and Data Groups 7 display identification features. Encoded security features are stored in Data Groups 8, Data Groups 9 and Data Groups 10. The Active Authentication public key is stored in the 15th Data Group. Thus, the public key provides an unambiguous connection

PDF created with pdfFactory Pro trial version www.pdffactory.com

between the whole signed data set and the chip. Similarly, the serial number of the chip may be stored in the LDS Data Group 13, thus providing secure logical and physical binding (but this is optional). The hash values of all the present Data Groups form a new structure, called the LDS Security Object. This is signed, according to the 'Cryptographic Message Syntax', thus producing the Document Security Object (SOD), which is stored in the chip (see Figure 2.2).

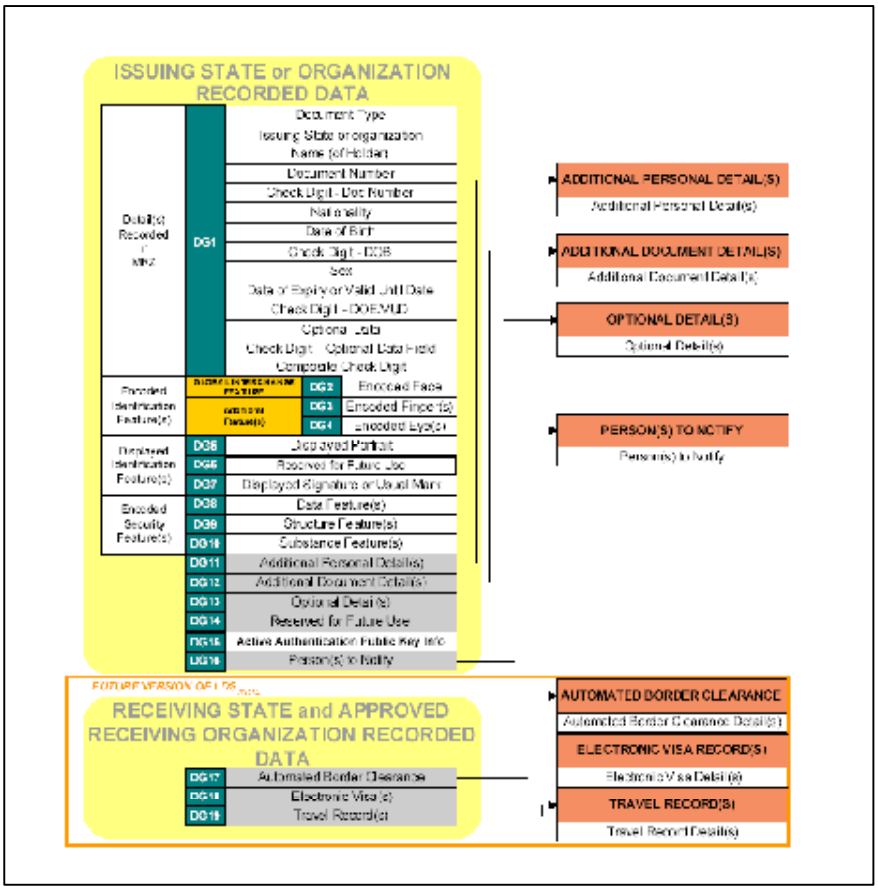

Figure 2.2: Logical Data Structuer cited (MRTD

2.2.2 Biometrics Data

Biometrics data refer to the verification of human identity through the biological characteristics of a person. This biometric authentication is unique

PDF created with pdfFactory Pro trial version www.pdffactory.com

in its ability to differentiate one person from another, and can be very reliable and secure. Many biological features can be used to identify an individual, and the biometric verification systems favored and deployed in e-passports focus on the use of fingerprints, face recognition and irises. The use of fingerprints in e-passports is essentially different from the fingerprint matching system used in criminal investigations (Kosta et al., 2007).

With e-passports, it relies on on-line imaging and is an automated process where fingerprint scanners, such as optical or silicon sensors, would scan an image from the target's fingers and search for a match with the pre-loaded image in the embedded chip in the e-passport. It is rather difficult for the naked eye to recognize a face from a passport picture if the picture is not very recent.

Face recognition involves the photographic imaging of a person's face and searching for a match with the available data in the chip. Another biological feature recognition system is iris recognition, which also uses imaging. The colored annular portion of the eye around the pupil, which is known as the iris, is scanned non-invasively by the biometric systems via a high precision camera, and the image is mapped onto the available data to ascertain the identity of the target individual.

According to (Juels et al., 2005), the processing of biometric data involves a number of critical matters. One of the issues here is whether the person's data have been authenticated. Assuming they have been authenticated, the individual could register the data by setting an initial, high-quality biometric image to the sensor system, which would store the information extracted during the registration process into a data structure

PDF created with pdfFactory Pro trial version www.pdffactory.com

known as a template. This template could then be used as a reference point for the user in future matching processes. Here, the verifying entity compares the biometric information obtained in an on-line manner for authentication with the archived data stored in the template for the user. This 'matching' process is highly valid, in that the template and the authentication image should match effectively. This match is achieved if they are sufficiently similar according to a pre-determined and often complicated and vendor-specified– metric that is acceptable under the law of respective countries.

In order for the verifying entity to be certain that the image is not a prosthetic but a digital one, most manufacturers of biometric sensors try to design them with the ability to resist spoofing via prosthetics, and to employ data security techniques that are supported by trained live-ware to authenticate that the origin of the biometric information is from a trusted sensor. In other words, the privacy of templates is critically important and must be comprehensively guaranteed within the baseline ICAO standards.

2.3 Security and Privacy Issue

The following states an example of a security issue regarding e-passport. When an immigration officer swipes a passport via a reader, the passport's key codes are fed to allow a microchip reader to communicate with the RFID chip. The data contained in this chip, which include the holders picture, is then displayed on the officials screen.

The usual assumption at this stage is that this document is authentic, as it is extremely secure. However, one of the main obstacles in RFID deployment in e-passports are security attacks, which may threaten to manipulate the RFID technology. As it is, privacy and security issues differ

PDF created with pdfFactory Pro trial version www.pdffactory.com

based on the existing mechanisms; hence, the basic threats and attacks need to be explained.

2.3.1 Security Threats

Several researchers have discussed general security threats and privacy issues on the topic of possessing and using e-passports. They have discussed the threats and then evaluated the risks and proposed e-passport types based on them. The focus here is the ICAO standards and the specific deployment choices of some of the nations that have started using the new technology.

- ***Scanning***: RFID tags are subject to concealed scanning. The fundamental ICAO fundamental does not require encrypted or authenticated communication between the passports' tags and readers. As a result, an insecure e-passport chip is subject to short-range (up to a few feet) concealed scanning, which poses the risk of exposing the sensitive personal information of an individual, such as name, place and date of birth, to anyone in possession of a suitable reader (Juels, 2006) .
- ***Tracking***: RFID chips require the production (without authentication) of a chip ID on protocol initiation; this could enable –especially if this ID is different for every passport—the tracking of the passport holders movements by unauthorized parties. Tracking does not require the data on the chip to be read (Meingast et al., 2007a,2007b).
- ***Skimming and cloning***: According Hoepman et al.(2006), Rotter, (2008), Pooters (2008), the data stored in the chip could be read by an

PDF created with pdfFactory Pro trial version www.pdffactory.com

illegitimate reader raising the risk of copying and using data on other chips. As a result, more than one user could be using the same data.

- ***Unauthorized tag reading***: It is possible to build a more powerful reader to eavesdrop and steal information from the original RFID tag. Vaudenay (2007) mentioned that it is relatively cheap to build an extended range reader; and these fake readers could be used by attackers to extend a reading-range by several times that of the standard communication distance to read tag information.
- ***Eavesdropping***: While the RFID tag is being accessed by a legitimate reader, there is a high opportunity of intercepting and capturing the information on the chip. Three major reasons make eavesdropping possible:
    - *Feasibility*: It may be feasible from a longer distance, given that eavesdropping is a passive operation.
    - *Detection difficulty*: As it is purely passive and does not involve powered signal emission, it is difficult to detect.
    - *Function stealth*: Eavesdropping is possible in a variety of circumstances since future applications of e-passports will not only be in airports, but also in new areas like e-commerce (Juels et al., 2005, Hancke, 2005). The threat model consists of a hardware architecture comprising two parts:
        i. The front-end is an RF eavesdropper that can continuously read and record RF-based communication at public places with a high density of e-passports, e.g., near inspection systems at airports. Optionally, a

PDF created with pdfFactory Pro trial version www.pdffactory.com

surveillance camera may snap pictures of the particular passport holder.

ii. The back-end is a cryptanalytic system that is connected to databases as well as to hardware or software modules for the fast cryptanalysis of symmetric ciphers (Carluccio et al., 2007) (see Figure 2.3).

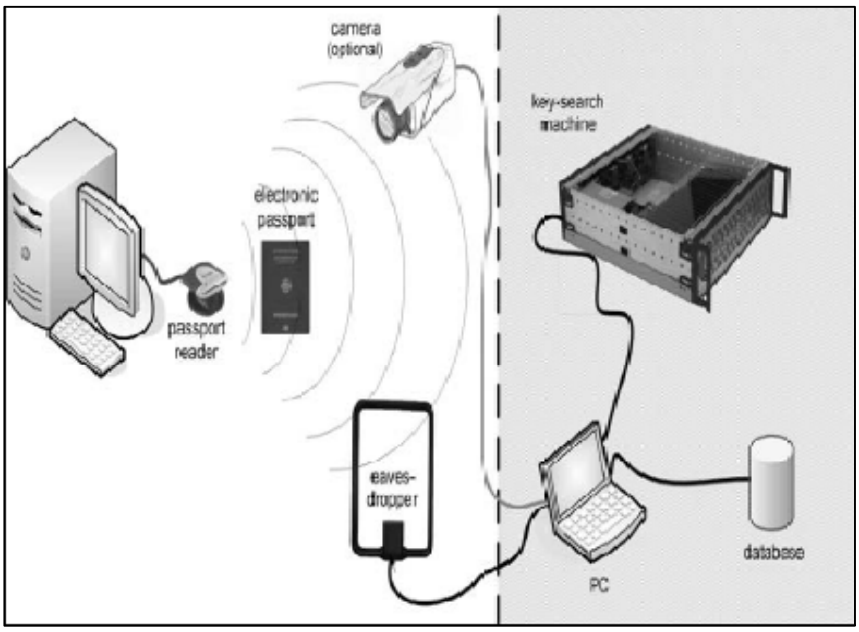

Figure 2.3: Threat model (Carluccio et al., 2007)

- ***Replay attacks***: Attackers can use a clone of a legitimate tag or resend the eavesdropped signal from a PC equipped with an appropriate card and antenna. By doing this, the attackers may hack into authorized tag carriers' identities by repeating their authentication sequences (Hancke, 2005, Hlavac and Rosa, 2007).
- ***Identity theft***: In some tags, information stored on a transponder, including personally identifiable information such as a name or credit

PDF created with pdfFactory Pro trial version www.pdffactory.com

card number might be decrypted; this personal information could then be stolen and used by an unauthorized entity.

- ***Biometric data leakage***: Biometric data stored on e-passports are open to its own security risks. When biometric data, especially facial images, become more popular as standards, it becomes necessary to secure this data so it will not be easy to obtain a person's official biometric identity, particularly if it becomes a standard biometric outside the passport context (Uludag et al., 2004).
- ***Physical Attacks:*** According to Longva (2005), physical attacks involve tags attacked physically in order to gain information stored on the tag. Such physical attacks may include distorting the power supply from the tag, disrupting the circuit, using a laser or an electron beam to read from or write to the tag etc.

2.3.2 Security mechanism

In general, three cryptographic measures are specified to be implemented in e-passports (Vaudenay and Vuagnoux, 2007, Pasupathinathan et al., 2008): Passive Authentication (PA), Basic Access Control (BAC) and Active Authentication (AA). In addition, Extended Access Control (EAC) is the fourth measure currently proposed to be a solution in the next generation of e-passports (Trojani, 2007). The following is the strength and weakness analysis of the existing mechanism which is summarized in a comparison Table 2.1:

PDF created with pdfFactory Pro trial version www.pdffactory.com

Table 2.1: Strengths and weaknesses of existing mechanisms

Mechanism	Strength	Weakness
Passive authentication	§ Verify the authenticity and integrity of e-passports' Logical Data Structures . (Vijayakrishnan et al., 2008).	§ Does not prevent the exact copying of the chip content or chip substitution. § Does not prevent skimming and eavesdropping.
Active authentication	§ Prevents chip duplication or cloning.	§ Cannot prevent illegal reader that reads the electronic data being read; this means that skimming could happen here. § Eavesdropping for unencrypted data is possible. § Does not verify the authenticity and integrity of e-passport LDS.
Basic Access Control	§ Prevents skimming and eavesdropping.	§ Does not verify the authenticity and integrity of e-passport LDS. § Does not prevent the exact copying of the chip content or chip substitution. § Low key entropy could lead to skimming.

2.4 Overview of the E-visa System

So far, there has not been much research in the area of e-visas. Based on the literature, the research on e-visas has been conducted mainly by two researchers, Uzun and Diri (Uzun and Diri, 2005) and the Electronia company. This current research is focused on creating an e-visa method that can strengthen the development of an e-visa system. In the e-visa system, the traditional document visa is replaced by an electronic visa, which is a chip embedded in the passport that contains personal information and digital biometric data on the e-visa holder. When a traveller comes to the

PDF created with pdfFactory Pro trial version www.pdffactory.com

immigration area of an airport, he/she has to insert his/her passport into a reader and place himself/herself in a biometric reading device for identification.

After being confirmed as the correct person, personal information is sent to a central computer server for further verification regarding, e.g., whether the person is on a criminal wanted list or whether the person has any tax liabilities to the government. After this information is validated, the central computer will send a signal to open the gate and let the passenger pass through; otherwise, a signal will be sent to an alarm to alert the security officer. Figure 2.4 below shows a general overview of the e-visa system.

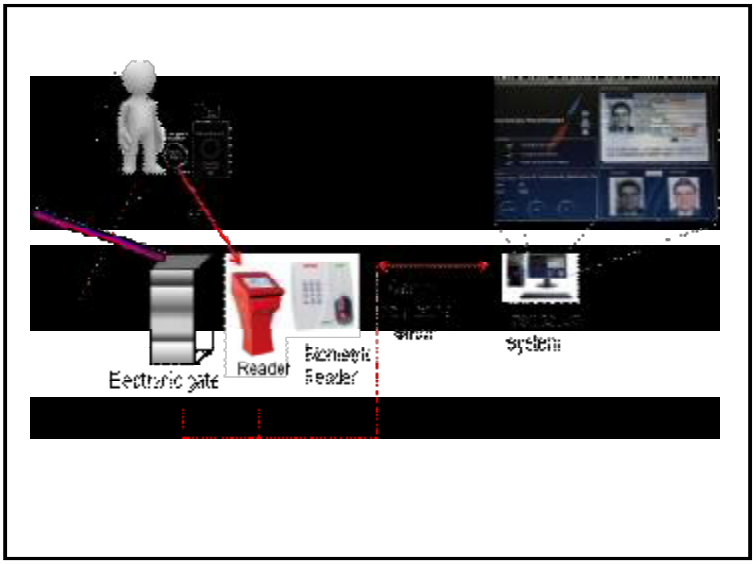

Figure 2.4: General overview of the

2.4.1 E-visa Design

E-visa is used to identify whether the holder is the correct owner of the visa and has approved access to the country. In addition, the e-visa is considered as contactless technology which allows increasing the speed of data transfer up to 424Kb per second. The e-visa can be implemented either

PDF created with pdfFactory Pro trial version www.pdffactory.com

as a smart label of size 50mm x 50mm to be attached to the passport or issued in an ISO ID1 card (Electronia, 2008).

2.4.1.1 Data Store Technology

The requirements and existing infrastructure of each country help in determining the techniques used to transport data. RFID tag and barcode techniques are used to transport information. However, there are important differences between these two technologies which are shown on the following adapted Table 2.2 below from (Finkenzeller, 2003). The table compares them in terms of the level of security, machine readability, cost, reading speed, maximum distance between data carrier and read rate and others.

Table 2.2: Comparison between barcode and RFID

System Parameter	Barcode	RFID
Typical Data Quantity(bytes)	1-100	16-64
Data Density	Low	Low
Machine Read Ability	Good	Good
Readability by People	Limited	Impossible
Influence of Damp/Dirt	very high	No influence
Influence of(opt) covering	Total failure	No influence
Degradation/ wear	Limited	No influence
Purchase cost/reading electronics	Very low	Medium
Operating cost	Low	None
Unauthorized copying/modification	Slight	Impossible
Reading Speed	Low 4 s	Very fast 0.5 s
Maximum Distance Between Data carrier& Read	0-50 cm	0-5 m
Security	Low. Much easier to reproduce or counterfeit	High. Difficult to replicate. Data can be encrypted; password protected, or includes a "kill"

PDF created with pdfFactory Pro trial version www.pdffactory.com

		feature to remove data permanently, so information stored is much more secure.
Read Rate	Very low throughput. Tags can only be read manually, one at a time.	High throughput. Multiple (>100) tags can be read simultaneously.

However contactless chip card technology is seemed to be the optimal solution for providing information of travelers in a reliable method. Physically, there will be some general information used for general inspection purposes only. This information about the visa holder is printed on the surface of the visa, such as photo, name, sex, nationality, date of issue, expiry date, handwriting, signature, etc. On the card, the IC chip stores more details and confidential information. Logically, it is structured in three different layers. Each layer encapsulates and protects more sensitive data that is contained in the deeper layer. A few researches that had been conducted in area of e-visa but only one proposed e-visa structure which is by Uzun and Diri (2005). Figure 2.5 shows the structure of the three layers which was proposed and the logical view of the data stored in the chip. In the later section, the mentioned layers will be discussed individually.

PDF created with pdfFactory Pro trial version www.pdffactory.com

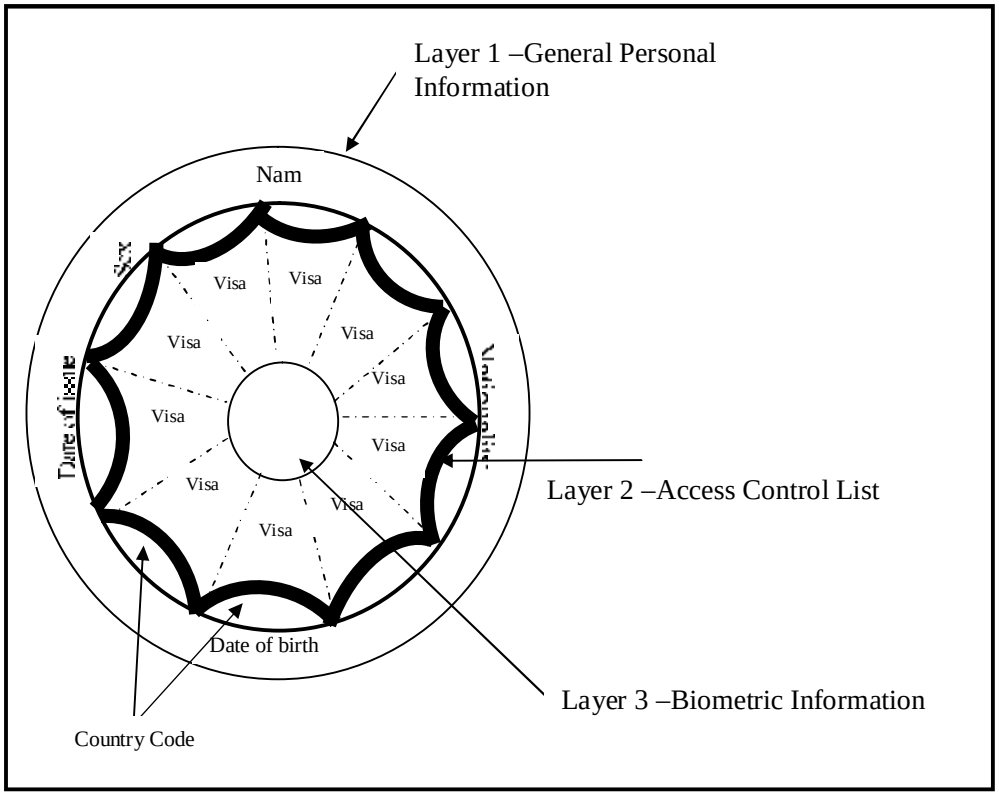

Figure 2.5: E-visa smart card structure (adapted from S. Uzun and B. Diri (2005))

The first layer is General Personal Information. This layer contains general information about the passport holder. This area provides a point to provide information access to be used in a country's civilization area. The second layer is acts as the access control lists / visas. Forms of the visas will be digitalized and stored in this layer. Different visas issued by different countries are stored in sequential records to allow more than one visa at a time. The information stored in each record includes the country code, visa type of class code, issue date, expiry date, terms and conditions, etc. Moreover, each visa should be encrypted independently by the issuer except for the country code.

PDF created with pdfFactory Pro trial version www.pdffactory.com

The third layer is biometric ID information. Incorporation of biometrics will provide a secure and strong authentication for the travelers because this layer should be highly secured as it is used for holder identification. The biometrics systems can be given as examples of deployment in e-visa techniques as voice, fingerprint, and iris recognition. Precisely, the data stored here should be encrypted and read only by authenticated readers.

2.4.1.2 Security Module

There are three different cryptographic secure logical modules which are used to access different layers of the card. The first security module is General Purpose Readings which is used to perform readings on the first layer of the card which contains only general information about the card holder. The second security module is visa approval which is used to read the second layer which contains records of the visas. It should verify whether the card owner carries a valid visa for the respective country.

The third security module is biometric matching and biometric reader. Biometric matching module should be closely designed and identification matching should be completed within the module in order to enable the highest security. For biometric reading technically, it should be constructed with a high reliability, and it should be closely connected with the smart card reader to ensure the biometric data is transferred under a secured channel. In addition to the gate module is the electronic gate.

It is controlled by the central computer which opens or closes upon receiving a signal. The connection between the gate and the computer should be protected in order to avoid wire tapping or interference.

PDF created with pdfFactory Pro trial version www.pdffactory.com