

Biometric Passport Validation Scheme using Radio Frequency Identification

V.K. Narendira Kumar¹

¹Assistant Professor, Department of Information Technology, Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
kumarmcagobi@yahoo.com

Dr. B. Srinivasan²

²Associate Professor, PG & Research Department of Computer Science, Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
srinivasan_gasc@yahoo.com

Abstract — Biometric passports issued nowadays have an embedded RFID chip that carries digitally signed biometric information. This RFID chip is integrated into the cover of a passport, called a biometric passport. Electronic passports as it is sometimes called, represents a bold initiative in the deployment of two new technologies: RFID and biometrics such as face, fingerprints, palm prints and iris. The electronic passport is the privacy and security risks that arise by embedding RFID technology. The goal of the adoption of the biometric passport is not only to expedite processing at border crossings, but also to increase security. Policymakers have put their faith in the technological promise of biometric identification because absolute identification could eliminate mismatched computer records and stolen identities.

Index Terms — Biometrics, Passport, Face, Fingerprint, Palmprint, Iris, Radio Frequency Identification

I. INTRODUCTION

An electronic passport (e-Passport) is an identification document which possesses relevant biographic and biometric information of its bearer. It also has embedded in it a Radio Frequency Identification (RFID) Tag which is capable of cryptographic functionality. The successful implementation of biometric technologies in documents such as e-Passports aims to strengthen border security by reducing forgery and establishing without doubt the identity of the documents' bearer [9].

Typically, Radio Frequency Identification (RFID) systems are composed of three main components: tags, readers, and a database. An RFID tag is a small device that can be attached to products and allow for unique item Identification and product description. RFID tags can be battery powered (active) or powerless (passive). Passive RFID tags (which are the main emphasis of this paper) are very cheap devices with limited memory and limited computational capabilities. An RFID reader, on the other hand, is a computationally powerful device with

ability to interrogate tags and access the database, where information about individual tags and their corresponding items is stored [5].

When an RFID tag is within communication range of an RFID reader, the reader interrogates that tag (and powers it if it is passive). Upon interrogation, the tag responds with a quantity that allows legitimate readers to access the database and carry out the Identification process. If things work as planned, the reader should be able to uniquely identify the interrogated tag.

The International Civil Aviation Organization has adopted a global, harmonized blueprint for the integration of biometric identification information into machine readable passports. This study aims to find out to what extent the integration of biometric identification information into passports will improve their robustness against identity theft. The integration of biometrics can provide better verification performance than the individual biometrics. Biometrics will also increase robustness of the biometric systems against the spoofing attacks and solve the problem of non-universality. Since the facial image is the mandatory biometric identifier to be included in the future passports, researcher study focus on the use of the facial image and finger prints for the identity verification of passport holders. In order of least secure and least convenient to most secure and most convenient, they are:

- Something you **have** - card, token, key.
- Something you **know**- PIN, password.
- Something you **are** - biometric [1].

The remaining sections are organized as follows: Brief outline of biometric passport systems is presented in section 2. System methodology steps are mentioned in Section 3. The other phases of the biometric passport security, logical data structure and implementation of the system are briefly explained in section 4, 5 and 6. Experimental results are given in Section 7. Finally, Section 8 describes the concluding remarks.

II. LITERATURE SURVEY

Jules *et al* (2005) discussed security and privacy issues that apply to e-passports. They expressed concerns that, the contact-less chip embedded in an e-passport allows the e-passport contents to be read without direct contact with an IS and, more importantly, with the e-passport booklet closed. They argued that data stored in the RFID chip could be covertly collected by means of “skimming” or “eavesdropping”. Because of low entropy, secret keys stored would be vulnerable to brute force attacks as demonstrated by Laurie (2007). Kc and Karger (2005) suggested that an e-passport may be susceptible to “splicing attack”, “fake finger attack” and other related attacks that can be carried out when an e-passport bearer presents the e-passport to hotel clerks. There has been considerable press coverage (Johnson, 2006; Knight, 2006; Reid, 2006) on security weaknesses in e-passports. These reports indicated that it might be possible to “clone” an e-passport [12].

A. Purpose of the Study

The primary objective of the study is to produce new knowledge with respect to security of biometric techniques and RFID in an e-passport setting. The results of the work should be useful for those making e-passport design decisions with respect to RFID security and biometric technologies in an e-passport setting.

B. Statement of the Problem

The purpose of biometric passports is to prevent the illegal entry of travelers into a specific country and to limit the use of fraudulent documents by more accurate identification of individuals. It is interesting to find out to what extent the integration of RFID and biometric identification information into passports will improve their robustness against identity theft.

C. RFID Tags

RFID tags come in three general varieties: *passive*, *active*, or *semi-passive* (also known as *battery assisted*). Passive tags require no internal power source, thus being pure passive devices (they are only active when a reader is nearby to power them), whereas semi-passive and active tags require a power source, usually a small battery. To communicate, tags respond to queries generating signals that must not create interference with the readers, as arriving signals can be very weak and must be told apart. Besides backscattering, load modulation techniques can be used to manipulate the reader's field. Typically, backscatter is used in the far field, whereas load modulation applies in the near field, within a few wavelengths from the reader [3].

Passive: Passive RFID tags have no internal power supply. The minute electrical current is induced in the antenna by the incoming radio frequency signal; it provides just enough power for the CMOS integrated circuit in the tag to power up and transmits a response. Most passive tags signal by backscattering the carrier wave from the reader. This means that the antenna has to be designed to both collect powers from the incoming signal and also to transmit the outbound backscatter signal. The response of a passive RFID tag is not

necessarily just an ID number; the tag chip can contain non-volatile, possibly writable EEPROM for storing data.

Active: Unlike passive RFID tags, active RFID tags have their own internal power source, which is used to power the integrated circuits and broadcast the signal to the reader. Active tags are typically much more reliable (i.e. fewer errors) than passive tags due to the ability for active tags to conduct a “session” with a reader. Active tags, due to their onboard power supply, also transmit at higher power levels than passive tags, allowing them to be more effective in “RF challenged” environments like water (including humans/cattle, which are mostly water), metal (shipping containers, vehicles), or at longer distances, generating strong responses from weak requests (as opposed to passive tags, which work the other way around). In turn, they are generally bigger and more expensive to manufacture, and their potential shelf life is much shorter.

Semi-Passive: Semi-Passive tags are similar to active tags in that they have their own power source, but the battery only powers the microchip and does not broadcast a signal. The RF energy is reflected back to the reader like a passive tag. An alternative use for the battery is to store energy from the reader to emit a response in the future, usually by means of backscattering. The battery-assisted receive circuitry of semi-passive tags lead to greater sensitivity than passive tags, typically 100 times more. The enhanced sensitivity can be leveraged as increased range (by a factor 10) and/or as enhanced read reliability (by one standard deviation).

III. BIOMETRICS IN E-PASSPORTS

Biometrics in e-passports complying with the ICAO standard consists of a mandatory facial image and fingerprints. While the former are used by a significant number of countries and thus information on them is widely available, the latter is currently used seldom. Therefore, this section only covers the vulnerabilities of facial images, fingerprints, palmprint and iris images.

A. Face Image

Facial images are the most common biometric characteristic used by humans to make a personal recognition, hence the idea to use this biometric in technology. This is a nonintrusive method and is suitable for covert recognition applications. The applications of facial recognition range from static (“mug shots”) to dynamic, uncontrolled face identification in a cluttered background (subway, airport). Face verification involves extracting a feature set from a two-dimensional image of the user's face and matching it with the template stored in a database. The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. It is questionable if a face itself is a sufficient basis for recognizing a person from a large number of

identities with an extremely high level of confidence. Facial recognition system should be able to automatically detect a face in an image, extract its features and then recognize it from a general viewpoint (i.e., from any pose) which is a rather difficult task. Another problem is the fact that the face is a changeable social organ displaying a variety of expressions [4].

B. Fingerprint

A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. In real-time verification systems, images acquired by sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources.

C. Palmprint

The palmprint recognition module is designed to carry out the person identification process for the unknown person. The palmprint image is the only input data for the recognition process. The person identification details are the expected output value. The input image feature is compared with the database image features. The relevancy is estimated with reference to the threshold value. The most relevant image is selected for the person's identification. If the comparison result does not match with the input image then the recognition process is declared as unknown person. The recognition module is divided into four sub modules. They are palmprint selection, result details, ordinal list and ordinal measurement. The palmprint image selection sub module is designed to select the palmprint input image. The file open dialog is used to select the input image file. The result details produce the list of relevant palmprint with their similarity ratio details. The ordinal list shows the ordinal feature based comparisons. The ordinal measurement sub module shows the ordinal values for each region.

D. Iris Recognition

Iris recognition technology is based on the distinctly colored ring surrounding the pupil of the eye. Made from elastic connective tissue, the iris is a very rich source of biometric data, having approximately 266 distinctive characteristics. These include the trabecular meshwork, a tissue that gives the appearance of dividing the iris radically, with striations, rings, furrows, a corona, and

freckles. Iris recognition technology uses about 173 of these distinctive characteristics. Iris recognition can be used in both verification and identification systems. Iris recognition systems use a small, high-quality camera to capture a black and white, high-resolution image of the iris. The systems then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system [11].

E. Biometric System Modules

Enrollment Unit: The enrollment module registers individuals into the biometric system database. During the phase, a biometric reader scans the individual's biometric characteristic to produce its digital representation.

Feature Extraction Unit: The module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual [1].

Matching Unit: The module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user's master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one too many matching).

Decision Maker: The module accepts or rejects the user based on a security threshold and matching score.

IV. SYSTEM METHODOLOGY

An e-passport bearer presents his/her document to a border security officer who scans the MRZ information in the e-passport through a MRZ reader and then places the e-passport near an e-passport reader to fetch data from the microchip. The current implementation consists of three protocols:

- *Basic Access Control (BAC) protocol (optional):* It provides encrypted communication between the RFID chip and the Inspection System (IS).
- *Passive Authentication (PA) protocol (mandatory):* A border security officer reads and verifies the authenticity of e-passport content stored in the RFID chip.
- *Active Authentication (AA) protocol (optional):* It provides integrity verification of e-passport's data.

The two new protocols that intend to replace active authentication and thus now consists of the following four protocols:

- *Basic Access Control (BAC) protocol (mandatory):* It facilitates the e-passport and the IS to establish an encrypted communication channel.
- *Chip Authentication (CA) protocol (mandatory):* A mechanism to detect cloned e-Passports
- *Passive Authentication (PA) protocol (mandatory):* As in first generation passport standard.
- *Terminal authentication (TA):* Only if all protocols are completed successfully, the e-passport releases sensitive information like secondary biometric

identifiers. The e-passport performs the collection of protocols as specified in the first generation e-passports, therefore providing backward compatibility [6].

A. Logical Data Structure

The ICAO issued a standardized data structure called Logical Data Structure (LDS) for the storage of data elements. This was to ensure that global interoperability for e-Passport Tags and Readers could be maintained. The specifications state that all the 16 data groups are write protected and can be written only at the time of issue of the e-Passport by the issuing state shown in table I. A hash of data groups 1-15 are stored in the security data element, each of these hashes should be signed by the issuing state.

TABLE I. PASSPORT LOGICAL DATA STRUCTURE

Data Group	Data Element
DG 1	Document Details
DG 2	Encoded Headshot
DG 3	Encoded Face biometrics
DG 4	Encoded Fingerprint biometrics
DG 5	Encoded Palmprint biometrics
DG 6	Encoded Iris biometrics
DG 7	Displayed Portrait
DG 8	Reserved for Future Use
DG 9	Signature
DG 10	Data features
DG 11-13	Additional Details
DG 14	CA Public Key
DG 15	AA Public Key
DG 16	Persons to Notify
SDE	Security Data Element

V. BIOMETRIC PASSPORT SECURITY GOALS

Researcher analyzes e-passport protocols by first identifying their security goals. Researcher assumes that a country implements the highest level of Cryptographic security and multiple biometrics for e-passports.

A. Data Confidentiality

Data confidentiality ensures the privacy of e-passport details and encryption is the common technique that provides confidentiality. In the case of e-passport, encryption is used to create a secure channel between the e-passport reader and the microchip. Note that the cryptographic keys used for encryption have to be guarded against unauthorized access.

B. Data Integrity

Data integrity prevents against illegal modifications of information exchanged between the e-passport reader and the microchip. Also the DF, SOD and LDS should be secure against any unauthorized modifications, i.e., any data tampering should be easily detectable by the border security centre.

C. Data Authentication

Data origin authentication ensure that the source of the transmission in a protocol is authentic, i.e., the data on the RFID chip should be bound to information on MRZ and to the data that appears in the e-passport bio-data page currently being examined by a border security officer.

D. Certificate Manipulation

Certificates acts as an off-line assurance from a trusted authority that the certified public key really does belong to the principal who is in possession of corresponding secret key. The responsibility of the protocol to validate that the corresponding secret key is actually held by the principal claiming ownership of the public key. The e-passport reader should have a guarantee that certificates presented by the e-passport are valid and match the data on the e-passport. ICAO has implemented a PKI which would store signature certificates from issuing state and organizations [6].

E. Security and Privacy Solutions

Cryptography can be applied to RFID to provide security and privacy. The problem of applying cryptography to RFID tags is that computation is required for encryption and decryption. This is a problem of low-cost RFID tags because it cannot run standard functions of cryptography [1]. Even symmetric key encryption cannot be executed in low-cost RFID. The research of Jules [2] suggests minimalist cryptography so that cryptography can be applied to low-cost RFID tags. Public key-based Basic Access Control for electronic passport is one of the first examples, which is deployed using RFID authentication. Figure 1 shows biometric passport with RFID chip embedded.

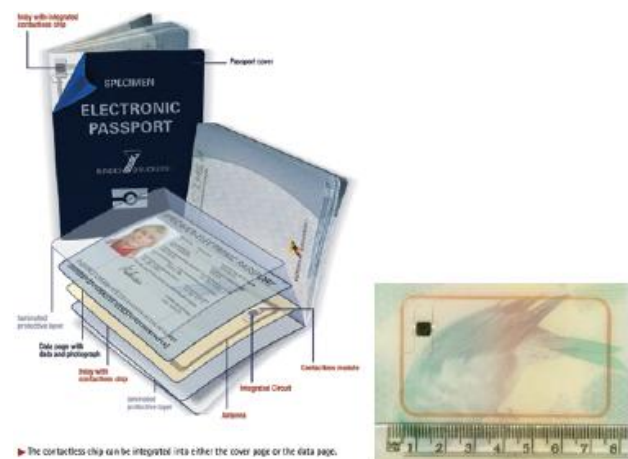


Figure. 1 The Biometric Passport Using RFID Chip.

Skimming: By using an embedded metallic element in the passports, it provides RF signal blocking. The RF blocking material covers the passport so that it only can be physically opened when it should be read [7].

Eavesdropping: Basic Access Control (BAC) minimizes the chance of skimming and eavesdropping. Initial interaction should be necessary between the RFID chip in the passport and the control reader which contain protocols that are for the secure communication channel.

Once authentication is done successfully, the data from passport will be issued. If not, the passport declines the access of data content.

Tracking: Unique Identifier (UID) is still possible to be tracked even though BAC is used. The solution of tracking is using a random UID (RUID). Embedded random number generator (RNG) generates a RUID.

Cloning: RFID chip can be copied, so it can be used for another electronic passport. By comparing the RFID chip data and the data on electronic passports data page, it is possible to diminish of cloning. Using Public Key Infrastructure (PKI) is one of the ways to prevent cloning. PKI can be applied to the travel document, so that comparing the data between the RFID chip and travel document. If the data is stored by authority, the data is not changed.

Temporary Deactivation: There is another way to protect personal privacy. By making RFID tags deactivate, privacy can be protected. One of the ways to deactivate is using Faraday cage which can block out external electrical fields. EPC global tags make enables to deactivate tags forever by using password-protected deactivate function [4, 5]. The tags which have temporary deactivation functions can be found in more expensive RFID tags [13].

VI. RADIO FREQUENCY IDENTIFICATION

A RFID chip is activated by a magnetic field from a reader and subsequently broadcasts the data that is stored in its memory. The fact that this personal information is being broadcast raises many questions about the use of this technology in such sensitive areas such as passports. It seems that contact chip technology would be preferable. However, the International Civil Aviation Organization (ICAO), the organization that developed the standards for electronic passports, analyzed these options and excluded contact chips from use in electronic passports. It was argued that contact chip technology, which is primarily used in card formats, would be difficult to put in a passport style document. Also, because contact chip technology requires exposed areas that require precise contact points with a reader, it was postulated that a contact chip document would not be able to function for the entire ten-year lifespan of a passport [14]. Therefore, a contactless chip technology, such as RFID is used in the electronic passports.

The two security concerns with the use of a RFID chip in an electronic passport are skimming and eavesdropping. Skimming is the act of reading the data on a chip without the holder's permission. Eavesdropping is when a party monitors the information in the communication between a chip and an authorized reader.

Due to the standardization of the RFID chips, the chip in an electronic passport can be read by commercially available readers. While this standardization is essential for international customs agents to be able to read any passport [12], it also makes it possible for anyone to potentially obtain a reader and "skim" the information from an electronic passport. The State Department

proposes to address this problem by placing an "anti-skimming" material in the cover and spine of the passport. This material will shield the RFID chip when the passport is closed, mitigating the threat of skimming [14]. Therefore, a person must physically open the passport booklet for it to be read.

Although the ICAO technical specifications for the use of contactless chips in passports claims that it is not possible to read an RFID chip from a distance greater than ten centimeters [10], critics argue that eavesdropping is possible from as much as 60 feet away [13]. To protect against eavesdropping, the Department of State proposes to shield the reader area in customs checkpoints, so no transmissions will be detected by anyone nearby. Also, the proposed system involves a unique identifier to implement Basic Access Control (BAC) in order to keep passport information from being revealed to an unauthorized party.

VII. IMPLEMENTATION OF THE SYSTEM

In order to implement this electronic passport system using cryptographic security and multiple biometrics technology efficiently, ASP.NET program is used. This program could speed up the development of this system because it has facilities to draw forms and to add library easily. There are three ways of doing authentication and authorization in ASP.NET:

Windows Authentication: In this methodology ASP.NET web pages will use local windows users and groups to authenticate and authorize resources.

Forms Authentication: This is a cookie based authentication where username and password are stored on client machines as cookie files or they are sent through URL for every request. Form-based authentication presents the user with an HTML-based Web page that prompts the user for credentials.

Passport Authentication: Passport authentication is based on the passport website provided by the asp.net. So when user logs in with credentials it will be reached to the passport website where authentication will happen. If Authentication is successful it will return a token to your website.

Anonymous Access: If you do not want any kind of authentication then you will go for Anonymous access.

Researcher model the flow of e-passport protocol according to the following stages: When an e-passport is presented at a border security checkpoint, the RFID chip and the e-passport reader execute the BAC protocol, in order to establish a secure (encrypted) communication channel between them. On successful completion of PA the RFID chip and the e-passport reader execute the AA protocol [8].

A. On-line Secure E-Passport Protocol

To resolve the security issues identified in both the first- and second-generation of e-Passports, in this section, we present an on-line secure e-Passport protocol (OSEP protocol). The proposed protocol leverages the infrastructure available for the standard non-electronic

passports to provide mutual authentication between an e-Passport and an IS. Currently, most security organizations are involved in passive monitoring of the border security checkpoints. When a passport bearer is validated at a border security checkpoint, the bearer's details are collected and entered into a database. The security organization compares this database against the database of known offenders (for instance, terrorists and wanted criminals) [10].

The on-line secure e-Passport protocol provides the following security features: An e-Passport discloses its information stored on the e-Passport RIFD chip only after a successful authentication of the IS (Inspection System). This prevents revealing the e-Passports identity to a third party that is not authorized or cannot be authenticated. This prevents the covert collection of e-Passport data from 'skimming' or 'eavesdropping' attacks that were very effective against both the first- and the second-generation e-Passports [14].

- The OSEP protocol uses the existing ICAO PKI implementation (as in first generation e-Passports) and eliminates the need for cross-certification among the participating countries, as required by the EAC (second-generation e-Passports).
- The OSEP protocol eliminates the need for certificate chain verification by an e-Passport. Only the top level certificate ($CERT_{CVCA}()$) is required to be stored in an e-Passport, thus reducing the memory requirements and preventing a malicious reader from performing a DOS attack on an e-Passport.
- The OSEP protocol also requires an IS to provide proof-of-correctness for public key parameters to an e-Passport. This allows an e-Passport to verify that an IS is using the correct domain parameters and to prevent related attacks.

B. Biometric Passport Initial Setup

All entities involved in the protocol share the public quantities p , q , and g where:

- p is the modulus, a prime number of the order 1024 bits or more.
- q is a prime number in the range of 159 -160 bits.
- g is a generator of order q , where $Ai < q$, $g^i \neq 1 \pmod p$.
- Each entity has its own public key and private key pair (PK_i, SK_i) where $PK_i = g^{(SK_i)} \pmod p$
- Entity i 's public key (PK_i) is certified by its root certification authority (j), and is represented as $CERT_j(PK_i, i)$.
- The public parameters p , q , g used by an e-Passport are also certified by its root certification authority.

C. Phase One – Inspection System Authentication

Step 1 (IS) When an e-Passport is presented to an IS, the IS reads the MRZ information on the e-Passport using an MRZ reader and issues the command GET CHALLENGE to the e-Passport RIFD chip.

Step 2 (P) The e-Passport RIFD chip then generates a random $eP \ \xi_R \ 1 \leq eP \leq q - 1$ and computes $K_{eP} = g^{eP} \pmod p$, playing its part in the key

agreement process to establish a session key. The e-Passport replies to the GET CHALLENGE command by sending K_{eP} and its domain parameters p , q , g .

$eP \rightarrow IS: K_{eP}, p, q, \text{ and } g$

Step 3 (IS) On receiving the response from the e-Passport, the IS generates a random $IS \ \xi_R \ 1 \leq IS \leq q - 1$ and computes its part of the session key as $K_{IS} = g^{IS} \pmod p$. The IS digitally signs the message containing MRZ value of the e-Passport and K_{eP} .

$S_{IS} = SIGN_{SK_{IS}}(MRZ \parallel K_{eP})$

It then contacts the nearest DV of the e-Passports issuing country and obtains its public key. The IS encrypts and sends its signature S_{IS} along with the e-Passport's MRZ information and K_{eP} using the DV's public key PK_{DV} .

$IS \rightarrow DV: ENC_{PK_{DV}}(S_{IS}, MRZ, \text{ and } KeP),$
 $CERT_{CVCA}(PK_{IS}, IS)$

Step 4 (DV) The DV decrypts the message received from the IS and verifies the $CERT_{CVCA}(PK_{IS}, IS)$ and the signature S_{IS} . If the verification holds, the DV knows that the IS is genuine, and creates a digitally-signed message S_{DV} to prove the IS's authenticity to the e-Passport.

$SDV = SIGN_{SK_{DV}}(MRZ \parallel K_{eP} \parallel PK_{IS}),$
 $CERT_{CVCA}(PK_{DV}, DV)$

The DV encrypts and sends the signature S_{DV} using the public key PK_{IS} of IS.

$DV \rightarrow IS: ENC_{PK_{IS}}(S_{DV}, [PK_{eP}])$

The DV may choose to send the public key of the e-Passport if required. This has an obvious advantage, because the IS system now trusts the DV to be genuine. It can obtain a copy of e-Passport's PK to verify during e-Passport authentication.

Step 5 (IS) After decrypting the message received, the IS computes the session key $K_{ePIS} = (K_{IS})^{eP}$ and encrypts the signature received from the DV, the e-Passport MRZ information and K_{eP} using K_{ePIS} . It also digitally signs its part of the session key K_{IS} .

$IS \rightarrow eP: K_{IS}, SIGN_{SK_{IS}}(K_{IS}, p, q, g), ENCK_{ePIS}$
 (S_{DV}, MRZ, KeP)

Step 6 (C) On receiving the message from the IS, the e-Passport computes the session key $K_{ePIS} = (K_{IS})^{eP}$. It decrypts the message received using the session key and verifies the signature SDV and $VERIFY_{PK_{IS}}(SIGN_{SK_{IS}}(K_{IS}, p, q, \text{ and } g))$. On successful verification, the e-Passport is convinced that the IS system is genuine and can proceed further in releasing its details. All further communications between an e-Passport and IS are encrypted using the session key K_{ePIS} .

D. Phase Two - e-Passport Authentication

Step 1 (C) The IS issues an INTERNAL AUTHENTICATE command to the e-Passport. The e-Passport on receiving the command, the e-Passport creates a signature $S_{eP} = SIGN_{SK_{eP}}(MRZ \parallel K_{ePIS})$ and sends its domain parameter

certificate to the IS. The entire message is encrypted using the session key K_{ePIS} .

$eP \rightarrow IS: ENCK_{ePIS}(S_{eP}, CERT_{DV}(PK_{eP}), CERT_{DV}(p, q, \text{ and } g))$

Step 2 (IS) The IS decrypts the message and verifies $CERT_{DV}(p, q, g)$, $CERT_{DV}(PK_{eP})$ and S_{eP} . If all three verifications hold then the IS is convinced that the e-Passport is genuine and authentic.

During the IS authentication phase, and IS sends the e-Passport's MRZ information to the nearest e-Passport's DV, which could be an e-Passport country's embassy. Embassies are DV's because they are allowed to issue e-Passports to their citizens and because most embassies are located within an IS's home country, any network connection issues will be minimal. Because the embassy now has a list of all its citizens that have passed through a visiting country's border security checkpoint. We do not see any privacy implications, because, in most cases, countries require their citizens to register at embassies when they are visiting a foreign country.

VIII. EXPERIMENTAL RESULTS

A successful design, deployment and operation of biometric passport systems depend highly on the results for existing biometrical technologies and components. These existing technologies as well as new solutions need to be evaluated on their passport system performance. An RFID chip will be embedded into the back cover of the passport. However it is often forgotten that the biometric face, finger, iris, and palm prints is only one part of a fully deployed application. As biometric (sub) systems are often not designed with security and or privacy in mind, system integrators will need to address the requirements of the deployed application in this light. The fears and concerns of a significant segment of the user population need to be addressed as early as possible in the design process, to ensure that appropriate mechanisms are in place to reassure such users. These concerns may relate to privacy or to safety issues, which may be addressed in part through legal and regulatory measures. This article discusses the requirements, design and application scenarios of biometrical systems in general and the introduction of a new biometrical passport in particular. The e-passport authentication system is divided into enrollment module and authentication module. The passport users who are included in the enrollment module are e-passport holder, Immigration administrator. Figure 2 shows the enrollment module in the e-passport authentication architecture design.

The RFID chip in the e-Passport will be a proximity contactless chip that must be held within ten centimeters of a reader in order to be read. Moreover, the data on the RFID chip cannot be accessed unless the machine-readable zone on read, which means that the passport book must be open. Border authorities equipped with e-Passport readers will insert the traveler's e-Passport into a scanner, which will read the machine-readable zone, thereby opening the RFID chip so that it can be read as

well. The machine also checks other security features, such as the country's signature. Border authorities who are not equipped with e-Passport readers will continue to examine travelers' passports as they do now. Table II shows the description of each of the passport user in the e-passport authentication system.

The e-passport holder registers to the system by providing the personal data and some important documentation to the immigration officer. After that, Immigration Administrator will make the enrollment for the e-passport holder by filling the data into the enrollment system. After enrollment process, the data of the e-passport holder will be encrypted by proposed cryptography technique and stored into immigration database and RFID tag inside the e-passport. Besides that, Enrollment module also includes the modifying process and deleting process. Modifying process will be carried out if there was a special request from e-passport holder to change the information of the e-passport, the e-passport spoil, or finished pages. Deleting process will be carried out if the previous e-passport validation date was expired or the e-passport holder lost their passport. They have to register a new e-passport in order to get an e-passport again.

The passport user involve in the authentication module are e-passport holder and check point officer. When e-passport holder arrives to check point, e-passport holder will put the e-passport onto RFID reader, and a signature required key in by e-passport holder so that authentication process can be performed to verify an e-passport holder. After authentication process authenticated the e-passport holder, RFID reader will read the encrypted data which was stored inside the RFID tag in e-passport. The encrypted data will be sent to the system to match with the encrypted data in the database system. If the encrypted data in the e-passport match with the encrypted data which is stored inside the database during enrollment process, the encrypted data in the e-passport will be decrypted by a certain key. Then the check point officer has to check and verify the identity of the e-passport holder. Figure 3 shows the authentication module in the e-passport authentication architecture design.

The attributes inherent in the e-Passport provide a here to fore unavailable means of improving the security of the international travel system. These are described below under three general categories: preventing the use of multiple identities; linking the bearer to the document in a traditional border operations environment; and serving as a strong token to drive a biometric identification process. After these uses have been explored in some detail, the paper will examine why the e-Passport may not be universally accepted by states as the sole device used to fully automate the border clearance process for registered participants as envisioned by the process flow.

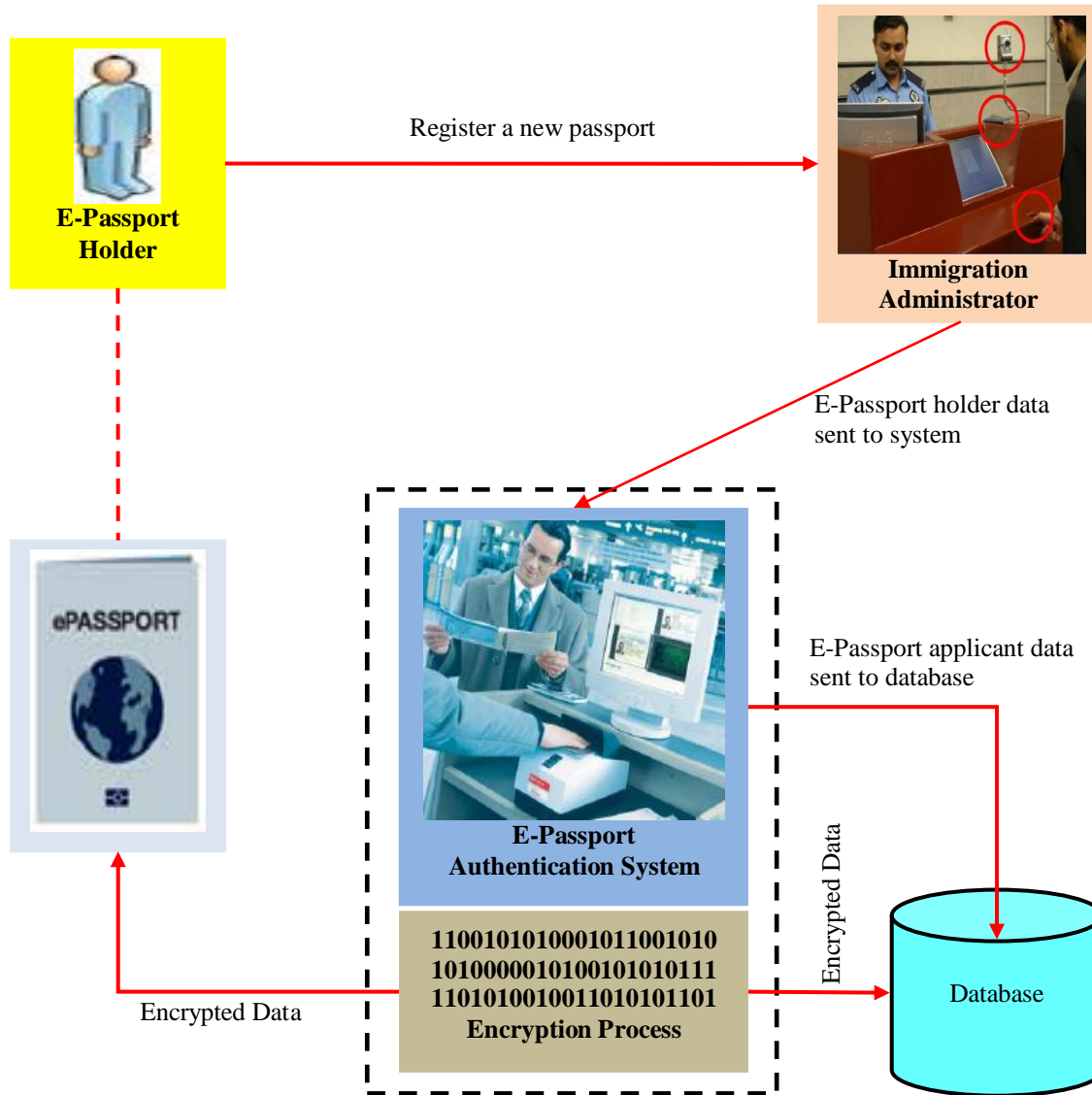


Figure. 2 Enrollment Module of E-Passport Authentication Architecture

Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint, palm print or iris biometrics on the MRTD as per LDS standards (or on a database accessible to the Receiving State). Given an ICAO standardized biometric

image and/or template, receiving States must select their own biometric verification software, and determine their own biometric scoring thresholds for identity verification acceptance rates – and referral of imposters.

TABLE II: DESCRIPTION OF PASSPORT USER IN THE E-PASSPORT AUTHENTICATION SYSTEM

Passport Users	Description
E-passport holder	E-passport holder is the main user in the e-passport authentication system where the e-passport holder must register to the system so that all the data will be store into the database system and some important data can be encrypted into RFID tag.
Check Point officer	Check point officer will retrieve the decrypted data through RFID reader and displayed in the check point officer’s computer. After that, the verification and identification process will be done by check point officer to the e-passport holder.
Administrator	Administrator provides the service of enrollment to e-passport holder. The data will be store to the database and administrator can delete and modify the e-passport holder data when it is needed. Besides that, administrator will store the decrypted data of e-passport holder inside RFID tag in e-passport.

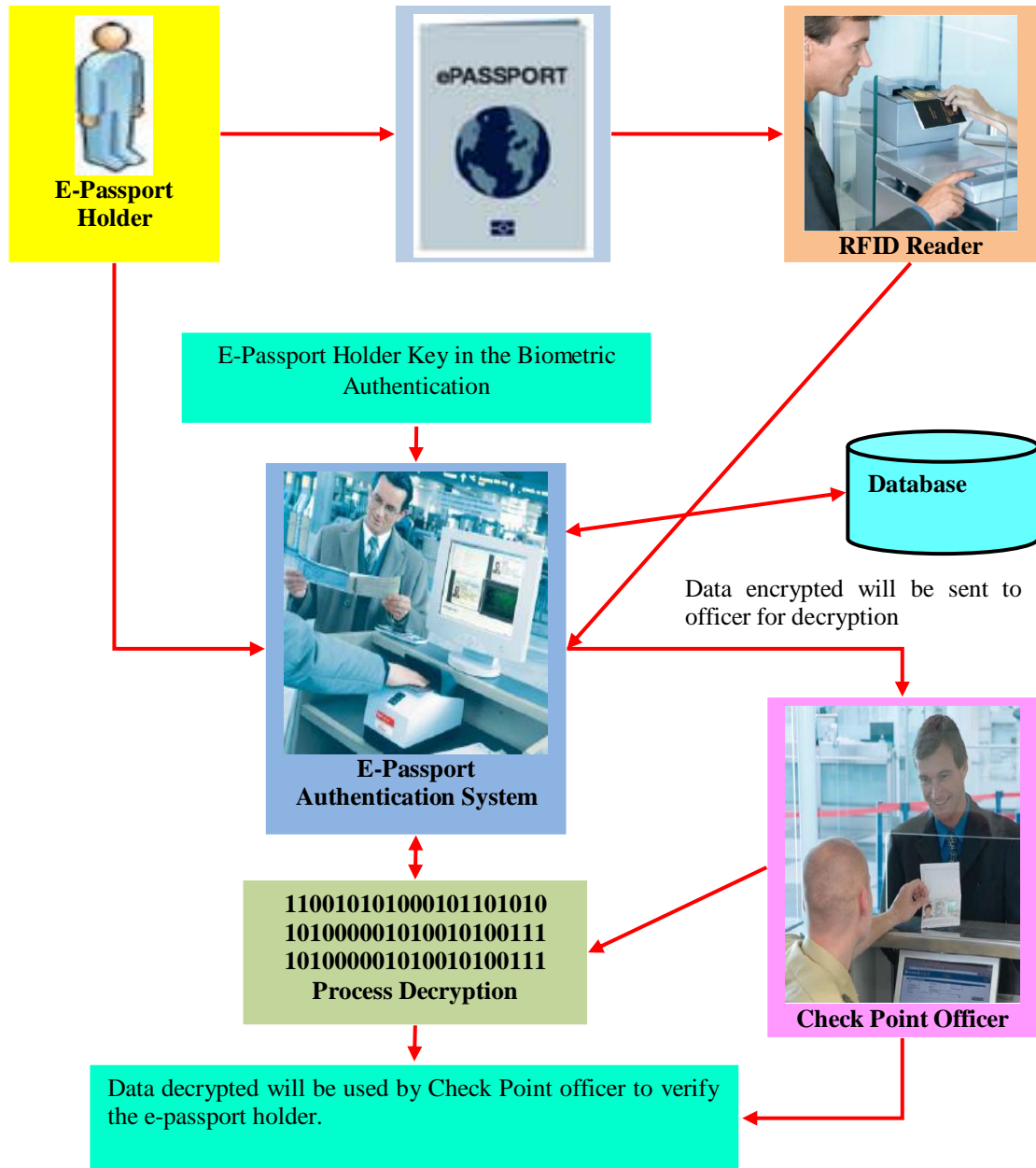


Figure. 3 Authentication Module of E-Passport Authentication Architecture

IX. CONCLUSIONS

The work represents an attempt to acknowledge and account for the presence on e-passport using biometrics recognition towards their improved identification. The application of facial, fingerprint, palm print and iris recognition in passports requires high accuracy rates; secure data storage, secure transfer of data and reliable generation of biometric data. An RFID chip will be embedded into the back cover of the passport. Border guards will be able to compare the face of the person standing in front of them with the image of the person stored onto the RFID chip. This image will also have to match the image printed into the passport page. Policymakers have put their faith in the technological promise of biometric identification because absolute identification could eliminate mismatched computer

records and stolen identities. The discrepancy in privacy laws between different countries is a barrier for global implementation and acceptance of biometric passports. A possible solution to un-encrypted wireless access to passport data is to store a unique cryptographic key in printed form that is also obtained upon validation. The key is then used to decrypt passport data and forces thieves to physically obtain passports to steal personal information. The inclusion of biometric identification information into machine readable passports will improve their robustness against identity theft if additional security measures are implemented in order to compensate for the limitations of the biometric technologies. It enables countries to digitize their security at border control and provides faster and safer processing of an e-passport bearer. E-passports may provide valuable

experience in how to build more secure and biometric identification platforms in the years to come.

REFERENCES

- [1] Ari Jules, Paul Syverson, and Dan Bailey, "High-power proxies for enhancing RFID privacy and utility", Workshop on Privacy Enhancing Technologies (PET 2005), May 2005.
- [2] G. Avoine. Cryptography in Radio Frequency Identification and Fair Exchange Protocols. PhD thesis, EPFL, Lausanne, Switzerland, December 2005.
- [3] G. Tsudik, "YA-TRAP: Yet Another Trivial RFID Authentication Protocol", In International Conference on Pervasive Computing and Communications, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press, 2006.
- [4] C.Hesher, A.Srivastava, G.Erlebacher, "*A novel technique for face recognition using range images*" in the Proceedings of Seventh International Symposium on Signal Processing and Its Application, 2003.
- [5] G. Tsudik, "A family of dunces: Trivial RFID identification and authentication protocols", In Privacy Enhancing Technologies 7th International Symposium, PET 2007, Ottawa, Canada, June 20-22, 2007: Revised Selected Papers, volume 4776, page 45. Springer, 2007.
- [6] D. Monar, A. Juels, and D. Wagner, "*Security and privacy issues in e-passports*", Cryptology ePrint Archive, Report 2005/095, 2005.
- [7] HOME AFFAIRS JUSTICE, "*EU standard specifications for security features and biometrics in passports and travel documents*", Technical report, European Union, 2006.
- [8] J. Wu and D. R. Stinson, "A Highly Scalable RFID Authentication Protocol", In Proceedings of the 14th Australia Conference on Information Security and Privacy, Brisbane, Australia, July 2009.
- [9] Inoue, S. and Yasuura, H., "RFID Privacy using user-controllable uniqueness", In Proceedings of RFID Privacy Workshop, MIT, MA, USA. 2003
- [10] Klaus Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley & Sons, Ltd, 2003.
- [11] Riscure Security Lab, "*E-passport privacy attack*", at the Cards Asia Singapore, April 2006.
- [12] M. Lehtonen, F. Michahelles, T. Staake, and E. Fleisch. Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. In *Int. Conf. on Ambient Intelligence Development – Amid'06*, 2006.
- [13] M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum. "A Platform for RFID Security and Privacy Administration" 20th USENIX/SAGE Large Installation System Administration conference (LISA 2006), Washington DC, December 2006.
- [14] Stephen A. Weis. Security and Privacy in Radio-Frequency Identification Devices. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, May 2003.

First Author Profile:



Mr. V.K. NARENDIRA KUMAR M.C.A., M.Phil., Assistant Professor, Department of Information Technology, Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India. He received his M.Phil Degree in Computer Science from Bharathiar University in 2007. He has authored more than 28 International Journal articles. He has authored or co-authored more than 60 technical papers and conference presentations. He is an editorial board member for several international journals. His research interests are focused on Internet Security, Biometrics, Advanced Networking, Visual Human-Computer Interaction, and Multiple Biometrics Technologies.



Dr. B. SRINIVASAN M.C.A., M.Phil., M.B.A., Ph.D., Associate Professor, PG & Research Department of Computer Science, Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India. He received his Ph.D. Degree in Computer Science from Vinayaka Missions University in 11.11.2010. He has authored or co-authored more than 28 International Journal. He has authored or co-authored more than 70 technical papers and conference presentations. He is a reviewer for several scientific e-journals. His research interests include automated biometrics, computer networking, Internet security, and performance evaluation.