I.J. Information Engineering and Electronic Business, 2013, 2, 34-43
Published Online August 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2013.02.06

Next Generation Electronic Passport Scheme using Cryptographic Authentication Protocols and Multiple Biometrics Technology

V.K. Narendira Kumar
Assistant Professor, Department of Information Technology, Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
Email ID: kumarmcagobi@yahoo.com

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

***Abstract*—**Electronic passports (e-passports) are to prevent the illegal entry of traveller into a specific country and limit the use of counterfeit documents by more accurate identification of an individual. The e-passport, as it is sometimes called, represents a bold initiative in the deployment of two new technologies: cryptography security and biometrics (face, fingerprints, palm prints and iris). A passport contains the important personal information of holder such as photo, name, date of birth and place, nationality, date of issue, date of expiry, authority and so on. The goal of the adoption of the electronic passport is not only to expedite processing at border crossings, but also to increase security. The paper explores the privacy and security implications of this impending worldwide experiment in biometrics authentication technology.

***Index Terms*—** Biometrics, Cryptographic, Electronic Passport, Face, Fingerprint, Palmprint, Iris.

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.

The International Civil Aviation Organization has adopted a global, harmonized blueprint for the integration of biometric identification information into machine readable passports. The purpose of the new 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 authentication of individuals. 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 International Civil Aviation Organization (ICAO), which plays a major role in setting global travel standards, has adopted a global, harmonized blueprint for the integration of biometric identification information into passports and other machine readable travel documents. The blueprint requires that a high-capacity contact-less integrated circuit containing a raw image file of the holder's face in addition to other identity information such as name and date of birth be included in the machine readable passports and other travel documents.

The purpose of biometric passports is to prevent the illegal entry of travelers into a specific country and limit the use of fraudulent documents, including counterfeit and modified documents and the impostor's use of legitimate documents.

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, iris, palm print 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 [1]:

- Something you have - card, token, key.
- Something you know- PIN, password.
- Something you are - biometric.

The remaining sections are organized as follows: Brief outline of Biometric in the e-passports is presented in section 2. E-Passport methodology is mentioned in Section 3 and logical data structures are in the section 4. The other phases of the implementations of the e-passport protocol are briefly explained in section 5. Experimental results are given in Section 6. Finally, Section 7 describes the concluding remarks.

II. LITERATURE SURVEY

Juels 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 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.

2.1. Purpose of the Study

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

2.2. 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 cryptographic security and biometric identification information into passports will improve their robustness against identity theft.

2.3. Biometric

Biometric technologies are automated methods of recognizing an individual based on their physiological or behavioral characteristics such as face, fingerprints, palm print and iris. Biometric systems are applications of biometric technologies and can be used to verify a person's claimed identity and to establish a person's identity [1].

In an ideal biometric system, every person possess the characteristic, no two persons have the same characteristic, the characteristic remain permanent over time and does not vary under the conditions in which it is collected and the biometric system resists countermeasures. Evaluation of biometric systems quantifies how well biometric systems accommodate the properties of an ideal biometric system. All of existing biometric systems suffer from the same problems: false acceptance and false rejection caused by the variability of conditions at the human-machine interface. A common feature of any system that uses biometric is a trade-off between high security and a more usable system.

2.4. Multiple Biometric Systems

Limitations of unimodal biometric systems can be overcome by using multiple biometric systems. A multiple biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. Such systems are expected to be more reliable due to the presence of multiple, independent pieces of evidence. These systems are also able to meet the strict performance requirements imposed by various applications [3].

A multiple system could be, for instance, a combination of fingerprint verification, face recognition, voice verification and smart-card or any other combination of biometrics. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric. For instance, it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject's head. A multiple system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions [5].

2.5. Technical Challenges

The electronic passport is secure will prove substantially more difficult than actually securing it biometric technology in passports. It is quite clear, however, that contactless chips offer significant advantages, including larger capacities and lower costs. The technology also has yet to experience widespread deployment in either the private or public sector, though such deployment can be expected in the private sector in the next few years. Contact-based chips simply lack the robustness of contactless technology. A lack of available barcodes, in addition to the fact that RFID is a superior tracking technology compared to virtually any available, has led major retailers like Walmart to investigate inclusion of RFID in its supply chain. As this deployment occurs, RFID may also become an integral part of numerous other everyday tasks, such as entering a place of work or making a credit card transaction.

III. 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 [7]:

- Basic Access Control (BAC) protocol (optional): It provides encrypted communication between the 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 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: 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.

3.1. 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, palm print and iris images [8].

3.2. 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].

3.3. 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 [2].

3.4. Palm Print

The palm print recognition module is designed to carry out the person identification process for the unknown person. The palm print 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 palm print selection, result details, ordinal list and ordinal measurement. The palm print image selection sub module is designed to select the palm print input image. The file open dialog is used to select the input image file. The result details produce the list of relevant palm print with their similarity ratio details [1]. The ordinal list shows the ordinal feature based comparisons. The ordinal measurement sub module shows the ordinal values for each region.

3.5. 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 [9].

3.6. 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.

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. E-PASSPORT 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 1. A hash of data groups 1-15 are stored in the security data element (SOD), each of these hashes should be signed by the issuing state.

TABLE 1: 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 Palm print 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

Requirements of the Logical Data Structure: ICAO has determined that the predefined, standardized LDS must meet a number of mandatory requirements:

Ensure efficient and optimum facilitation of the rightful holder. Ensure protection of details recorded in the optional capacity expansion technology. Allow global interchange of capacity expanded data based on the use of a single LDS common to all. Address the diverse optional capacity expansion needs of issuing state. It provides expansion capacity as user needs and available technology evolve.

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.

4.1. Data Confidentiality

Data confidentiality ensures the privacy of e-passport details and encryption is the common technique that provides confidentiality [11]. 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 (data elements within the LDS or keys stored in the DF).

4.2. 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.

4.3. Data Authentication

Data origin authentication ensure that the source of the transmission in a protocol is authentic, i.e., the data on the 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.

4.4. Mutual Authentication

Mutual authentication is the process where both participants prove their identities to each other. As in the goal 3, where the e-passport reader authenticates an e-passport, this goal protects the e-passport bearer, as it is crucial for an e-passport to authenticate the e-passport reader before divulging any personal information. This prevents an unauthorized e-passport reader from obtaining biometric and personal details from an e-passport.

4.5. 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. However, it is 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.

V. IMPLEMENTATION OF E-PASSPORT 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 logins 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.

5.1. E-Passport Authenticate

Figure 1 shows the different entities involved in authenticate with *e-Passport* scenario and the traffic that is exchanged between them. A TCP connection from the e-Passport to the user is created as soon as the user loads the login page. In the current implementation this is accomplished by placing an ASP.NET owned by the identity provider on the web page (to be more precise, what is placed on the web page is an HTML tag linking to code on the web server). The website is signed by the identity provider and also loaded from the passport web server so that the Runtime Environment at the user's client trusts this piece to allow it to set up a connection back to the passport server. The website was given permission to connect to the contactless reader in a passport policy file which was installed during enrollment. The TCP connection is used for subsequent communication between the identity provider and the user's e-Passport.

Using the managed passport acquired during enrollment the user can attempt to login. One extra step is taken by the identity provider after receiving a token request from the client. In this extra step the identity provider checks if the user has a valid passport and it reads the user's details from the passport. As soon as the client actually requests a token at the identity provider, the identity provider will look at the provided token and send the appropriate BAC data to the passport authenticating the identity provider at the passport. The identity provider will request the e-Passport's AA public key and SOD. With the SOD it can check if the public key has been signed by the issuing country. It can then send a random challenge to the e-Passport which encrypts it using the AA private key. This proves that the passport is authentic and not a simple clone. The identity provider will request the minimal needed information from the e-Passport to confirm to the token request. The token is sent back to the client and from here on the normal Information scenario continues [6].

To summarize, the identity provider uses BAC, AA, and PA and then reads Data Group. Based on the results of the security protocols the identity provider knows that the information in Data Group correctly identifies a citizen of the issuing country (for as far as the identity provider trusts the country's CSC, of course). Remember that Data Group contains basic textual card holder information (name, date of birth, date of expiry of document, document number, gender, nationality, and in the case even the citizen ID). The information in this data group is used in the token created by the identity provider and only the required fields (as requested by the relying party's policy) are sent to the relying party (via the user's client). No other information is sent to the relying party and the relying party needs to trust the identity provider that it has done its job in checking the validity of the user's e-Passport.

5.2. E-Passport Initial Setup

All entities involved in the protocol share the public quantities p, q, 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 $Ai < q, g^i \neq 1 \bmod p$.
- Each entity has its own public key and private key pair (PK_i, SK_i) where $PK_i = g^{(SK_i)} \bmod p$
- 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.

5.3. Phase One – IS 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 chip.
- Step 2 (P) The e-Passport chip then generates a randomeP £ R 1≤ eP ≤ q - 1 and computes KeP = geP mod 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 KeP and its domain parameters p, q, g.

  $$eP \rightarrow IS : KeP, p, q, g$$
- Step 3 (IS) On receiving the response from the e-Passport, the IS generates a random IS £R 1 ≤ IS ≤ q - 1 and computes its part of the session

key as KIS = gIS mod p. The IS digitally signs the message containing MRZ value of the e-Passport and KeP.

SIS = SIGNSKIS (MRZ || KeP)

It then contacts the nearest DV of the e-Passports issuing country and obtains its public key. The IS encrypts and sends its signature SIS along with the e-Passport's MRZ information and KeP using the DV's public key PKDV.

IS → DV: ENCPK DV (SIS, MRZ, KeP), CERTCVCA (PKIS, IS)

- Step 4 (DV) The DV decrypts the message received from the IS and verifies the CERTCVCA (PKIS, IS) and the signature SIS. If the verification holds, the DV knows that the IS is genuine, and creates a digitally-signed message SDV to prove the IS's authenticity to the e-Passport.

SDV = SIGNSKDV (MRZ || KeP || PKIS), CERTCVCA (PKDV, DV)

The DV encrypts and sends the signature SDV using the public key PKIS of IS.

DV→ IS: ENCPKIS (SDV, [PKeP])

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 KePIS = (KIS) eP and encrypts the signature received from the DV, the e-Passport MRZ information and KeP using KePIS. It also digitally signs its part of the session key KIS.

IS → eP: KIS, SIGNSKIS (KIS, p, q, g), ENCKePIS (SDV, MRZ, KeP)

- Step 6 C On receiving the message from the IS, the e-Passport computes the session key KePIS = (KIS)eP. It decrypts the message received using the session key and verifies the signature SDV and VERIFYPKIS (SIGNSKIS (KIS, p, q, 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 KePIS.

5.4. 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 SeP = SIGNSKeP (MRZ ‖ KePIS) and sends its domain parameter certificate to the IS. The entire message is encrypted using the session key KePIS.

eP → IS : ENCKePIS (SeP , CERTDV (PKeP), CERTDV (p, q, g))

- Step 2 (IS) The IS decrypts the message and verifies CERTDV (p, q, g), CERTDV (PKeP) and SeP. If all three verifications hold then the 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. Sending the MRZ information is also advantageous, 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.

VI. 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. However it is often forgotten that the biometric (iris, finger, face, 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 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.

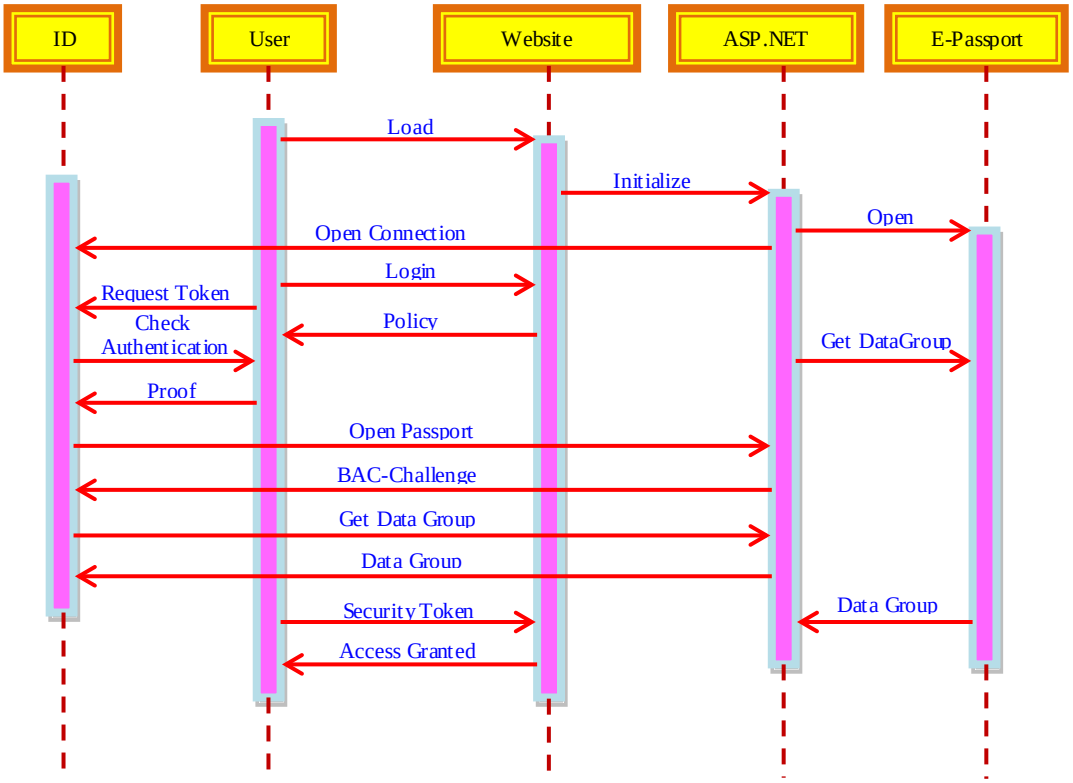

Figure 1: Message sequence chart of authenticate with *e*-Passport scenario

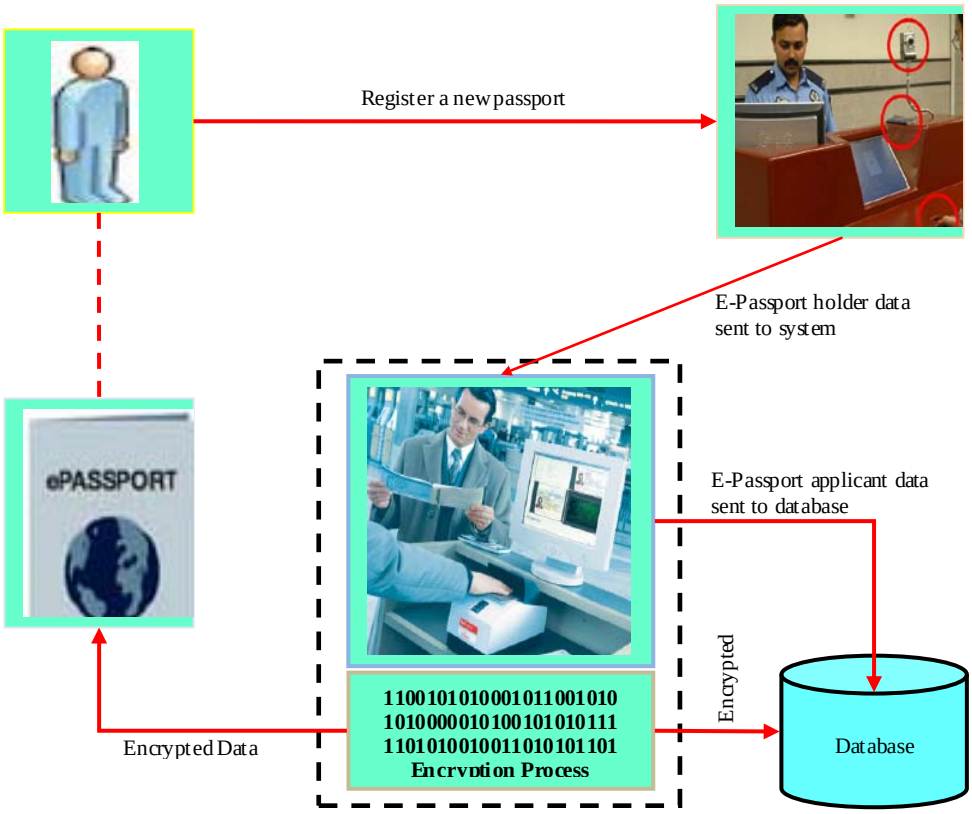

Figure 2: Enrollment Module of E-passport Authentication Architecture

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.

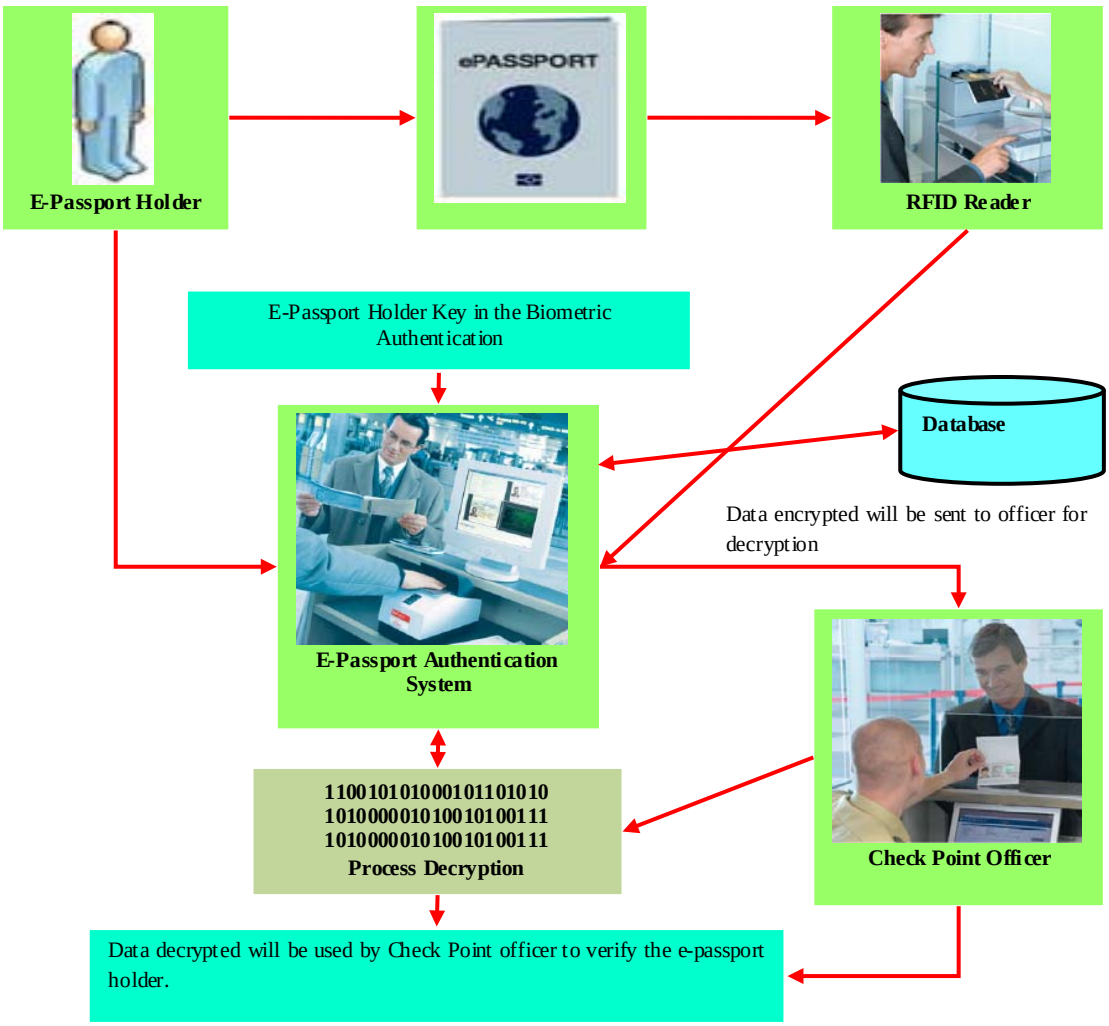

Figure 3: Authentication Module of E-passport Authentication Architecture

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.

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 2: Comparison of Biometric Technologies

Technology	Face	Finger	Iris	Palm
How it works	Captures and compares facial patterns	Captures and compares fingertip patterns	Captures and compares iris patterns	Captures and compares dimensions of palm
Enrollment time	About 3 minutes	3 minutes, 30 Seconds	2 minutes, 15 seconds	About 1 minute
Transaction time	10 seconds	9 to 19 seconds	12 seconds	6 to 10 seconds
False non-match rate	3.3% – 70%	0.2% – 36%	1.9% – 6%	0% – 5%
False match rate	0.3% – 5%	0% – 8%	Less than 1%	0% – 2.1%
User acceptance issues	Potential for privacy misuse	Associated with law enforcement, hygiene concerns	User resistance, use difficulty	Hygiene concerns
Factors affecting Performance	Lighting, orientation of face, and sunglasses	Dirty, dry, or worn fingertips	Poor eyesight, glare, or reflections	Hand injuries, arthritis, swelling
Variability with age	Affected by aging	Stable	Stable	Stable

Every type of biometric measurement can be classified with a number of characteristics that should be considered in a selection process see table 2. Being familiar with these characteristics will help you to better understand how to think objectively about each type. Sure, some of the available biometric technologies are cool, but it's no longer we have to make *rational* decisions about purchasing and using technology.

Universality: This refers to whether each person has the characteristic being measured. For instance, nearly everyone in your organization will have at least one finger for fingerprint biometrics, but gait-based biometrics may be more difficult if you have any wheelchair-bound staff members.

Uniqueness: How well the particular biometric distinguishes people. Palm is the best, and fingerprints and iris scans are pretty good too.

Permanence: A good biometric system should measure something that changes slowly (if at all) over time. DNA and fingerprints are very good over the long term; handwriting and voice change somewhat from decade to decade.

Collectability: This refers to how easily the biometric can be measured. face scores very low (it isn't easy to collect); fingerprint and palm-scan biometrics rate quite high. Gait requires a person to walk over a distance, which would be hard to do while sitting at a workstation. Retina scan requires the subject get really close to a digital camera.

Performance: This refers to the overall technology burden: how much equipment, time, and calculation go into performing a comparison. The fingerprint method fares very well; fingerprint readers are small, compact, and accurate. Biometrics tends to be costly, slow, and labor-intensive.

Accuracy: How well does a biometric system distinguish between subjects, and what are the false acceptance and false rejection rates?

Acceptability: Will users be willing to use the biometric technology? face will score low because of privacy reasons. Retina scans will score low because some people will be uncomfortable putting their eye really close to something that seems intrusive. Similarly, people won't mind swiping a finger across a surface-type fingerprint scanner or getting an iris photographed from a few feet away, but some are squeamish about sticking their fingers into a device (too many "B" movies).

Circumvention: This refers to how easily a forgery can be made that will fool the biometric system (early fingerprint devices, for example, could be fooled with "gummy fingers"). Proof of life testing — a feature that determines whether a sample comes from a *living* body part — is incorporated into many biometric systems so digital images of body parts are less likely to fool the system. But circumvention also refers to whether someone can attack a biometric system in other ways, such as replaying known good credentials through a network connection.

VII. 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. The passport data is not required to be encrypted, identity thief and terrorists can easily obtain the biometric information. 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. More research into the technology, additional access and auditing policies, and further security enhancements are required before biometric recognition is considered as a viable solution to biometric security in passports. The adversaries might

exploit the passports with the lowest level of security. The inclusion of multiple 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] A.K.Jain, R.Bolle, "Biometrics-Personal Identification in Networked Society" Norwell, 1999, Page No. 23-36.

[2] Barral and A. Tria. "Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin", In Formal to Practical Security. Springer, 2000. Page No. 83-92. DOI:10.1007/978-3-642-02002-5_4.

[3] Bergman, "Multi-Biometric Match-on-Card Alliance Formed," Biometric Technology Today, vol. 13, no. 5, 2003. Page No. 1-9.

[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, 2005. Page No. 58-69. DOI:10.1109/ISSPA.2003.1224850.

[5] Chang, "New Multi-Biometric Approaches for Improved Person Identification," PhD Dissertation, Department of Computer Science and Engineering, University of Notre Dame, 2006. Page No. 153-159.

[6] D. Monar, A. Juels, and D. Wagner, "Security and Privacy Issues in E-Passports", Cryptology ePrint Archive, Report 2005/095, 2007. Page No. 72-78. DOI:10.1109/SECURECOMM.2005.59.

[7] Gaurav S. Kc and Paul A. Karger. "E-Passport Authentication Protocols", IBM Technical Report (RC 23575), IBM T. J.Watson Research Labs, April 2008. Page No. 315-322.

[8] HOME AFFAIRS JUSTICE, "EU Standard Specifications for Security Features and Biometrics in Passports and Travel Documents", Technical report, European Union, 2010. Page No. 62-65.

[9] John Daugman, "How Iris Recognition Works." IEEE Transactions on Circuits and Systems for Video Technology, 14(1):21–30, 2010. Page No. 103-109. DOI:10.1109/TCSVT.2003.818350.

[10] KLUGLER, D., "Advance Security Mechanisms for E-Passport Protocols Implementation, Technical Report", Federal Office for Information Security (BSI), Germany, 2011. Page No. 41-46.

[11] Riscure Security Lab, "E-Passport Privacy Attack", at the Cards Asia Singapore, April 2011. Page No. 1-56.

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 author more than 40 international journal article publications. He has authored or co-authored more than 60 technical papers and conference presentations. He is an editorial board member for several scientific international journals. His research interests are focused on Internet Security, Biometrics, Advanced Networking, Visual Human-Computer Interaction, and Multiple Biometrics Technologies.

Second Author Profile:

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 author or co-authored more than 30 international journal article publications. 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.

