SAFETY MEASURES AND PRIVACY IN E-PASSPORT SCHEME USING CRYPTOGRAPHIC PROTOCOLS AND BIOMETRICS TECHNOLOGY

V.K. Narendira Kumar [1] and B. Srinivasan [2]

[1]Assistant Professor, Department of Information Technology,
[2]Associate Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453,
Erode District, Tamil Nadu, India.
Email ID: kumarmcagobi@yahoo.com,srinivasan_gasc@yahoo.com

ABSTRACT

Electronic passports have known a wide and fast employment all around the world since the International Civil Aviation Organization (ICAO) the human race has adopted standards whereby electronic passports can store biometrics identifiers. The purpose of electronic passports is to prevent the illegal entry of traveler into a particular country and frontier the use of counterfeit documents by more accurate recognition of an individual. The electronic passport, as it is sometimes called, represents a bold initiative in the employment of two new technologies: Cryptography protocols and biometrics. An electronic passport contains the significant 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 dealing out at border crossings, but also to increase safety measures and privacy. Important in their own right, electronic passports are also the harbinger of a wave of next-generation electronic passports: numerous national governments plan to set up electronic passport integrating cryptography safety measures algorithm and biometrics. We walk around the privacy and safety measures implications of this impending worldwide experiment in biometrics certification technology. We describe privacy issues that apply to electronic passports, and then analyze these issues in the context of the ICAO standard for electronic passports. An overall safety measures process that involves people, technology and procedures can overcome limitations of the cryptography protocols and biometrics technologies.

KEYWORDS

Biometrics, Electronic Passport, Face, Fingerprint, Palmprint, Iris, Recognition, Verification and Database.

1. INTRODUCTION

An electronic Passport is a document issued by a government to one of its citizens that provides a means of authenticate the individuality and nationality of that citizen. An electronic Passport is required for almost all worldwide travel. An electronic passport is constructed by attaching an electronic chip to a passports document. In the electronic passport, this chip is a Radio Frequency Identification device that includes the information within the customary electronic passport and can be read by a machine at border crossings [10].

DOI:10.5121/ijcis.2012.2302

The electronic passport is an enhancement upon the old system because it provides additional protection against fake as well as a potential decrease in the time required at customs checkpoints. The electronic passport system, however, does not improve the strength of the confirmation of a person's identity. Considering that identity confirmation is the primary function of a passport, that additional measures to facilitate identity authentication should be included in the electronic passport [11].

The deployment of biometrics technology in passports and other travel documents, for purposes of machine-assisted identity confirmation, is one aspects of the ICAO strategy to improve border clearance process with machine readable travel document and associated technology. Moreover, ICAO urges Contracting States to make stronger their efforts to protect the security and truthfulness of their electronic passports, to protect their passports against electronic passport hoax, and to assist one another in this subject.

Electronic passport honesty is a significant factor in the security of the worldwide travel system, and confidence in the integrity of a State's pass through documents on the part of border control authorities promotes facilitation of border control formalities. Biometrics detection is considered an important tool for States to use to strengthen the safety measures of their documents and enlarge the level of that confidence [9].

The electronic passport specifies the choice of facial recognition as the internationally interoperable biometrics technology for machine-assisted individuality confirmation. The technical and realistic consideration in deploy biometrics technologies in MRTDs lists the reasons for this choice. At the same time, acknowledges that States may elect to add fingerprint, palmprint and/or iris recognition to supplement facial recognition to support machine-assisted verification and/or identification. The technical specifies that the chosen biometric(s) be stored on the document as images rather than templates, in the interests of global interoperability.

The prepared measurement of the compatibility of biometrics technologies sought to assess each currently available biometric data from a comprehensive scheme requirements perspective. The study considered that biometrics equipment must support both verification and identification, defined as follows [1]:

- **Verification** confirming individuality by comparing individuality details of the person claiming to be a specific living individual against details previously recorded on that person.
- **Identification** determining possible individuality by comparing individuality details of the presenting person beside details previously recorded on a number of living persons.

1.1. Purpose of the Study

The primary goal of the study is to produce new knowledge with respect to safety measures of biometric techniques in an electronic passport setting. The results of the work should be useful for those making electronic passport design decisions with respect to cryptographic protocols and multiple biometric technologies in electronic passport settings.

1.2. Statement of the Problem

The purpose of electronic passports is to prevent the against the law entry of travelers into a specific country and to edge the use of fake documents by more correct identification of persons. It is interesting to find out to what extent the integration of cryptographic protocols and biometric recognition information into electronic passports will improve their healthiness against identity theft.

2. LITERATURE SURVEY

Juels *et al* 2005 discussed security and privacy issues that apply to electronic passports. They articulated concerns that, the contact-less chip entrenched in an electronic passport permit the electronic passport contents to be read without straight contact with an Inspection System and, more importantly, with the electronic passport booklet closed. They argued that information stored in the chip could be covertly composed by means of "skimming" or "eavesdropping". Because of small entropy, secret keys stored would be weak to brute force attacks as confirmed by Laurie 2007. Karger 2005 recommended that an electronic passport may be vulnerable to "splicing attack", "fake finger show aggression" and other related attacks that can be approved out when an electronic passport holder current the electronic passport to hotel clerks. There has been significant press coverage Johnson, 2006, Knight, 2006 and Reid, 2006 on security weakness in electronic passports. These reports point out that it might be possible to "clone" an electronic passport.

2.1. Technology Evaluation

The technology test evaluates the knowledge itself: it measures the concert of the corresponding algorithms under controlled conditions in a laboratory. The reason of an expertise evaluation is to determine the state of the art and to determine the most capable approaches. In a technology evaluation, the algorithms to be experienced are given a database of biometric identifiers. One part of the database is given to the passport applicant so that they can be familiar with the biometrics identifiers in the database and the additional part is used for testing. The outcomes from an expertise test are repeatable since the technology tests are done under controlled conditions. The products of the technology evaluation are the verification, identification and pocket watch list performance metrics.

2.2. Technical Challenges

The electronic passport is secure will prove considerably more difficult than actually secure it biometrics technology in passports. It is fairly clear, however, that contactless chips offer important advantages, including larger capacities and lesser costs. The expertise also has yet to experience extensive deployment in either the private or public sector, though such exploitation can be expected in the private sector in the next few years. Contact-based chips purely lack the strength of contactless technology. A lack of accessible barcodes, in addition to the fact that RFID is a superior tracking technology compared to virtually any available, has led main retailers like Walmart to consider inclusion of RFID in its supply chain. As this deployment occurs, RFID may also turn out to be an integral part of many other everyday tasks, such as toward the inside a place of work or creation a credit card transaction.

2.3. Biometric

Biometrics technologies are automated method of recognize an person based on their physiological or behavioral characteristics such as face, fingerprints, palm print, hand and iris. Biometric systems are application of biometrics technologies and can be used to confirm a person's claimed individuality and to establish a person's individuality.

In an ideal biometrics system, every person has the characteristic, no two persons have the similar characteristic, the characteristic remain everlasting over time and does not vary under the conditions in which it is composed and the biometrics system resists counter measures. Assessment of biometric systems quantifies how well biometrics systems contain the properties

of a perfect biometric system. All of existing biometrics systems suffers from the same problems: false acceptance & false rejection caused by the unpredictability of conditions at the human-machine boundary. A common characteristic of any system that uses biometrics is a tradeoff between high safety measures and a more usable system.

2.4. Multiple Biometric Systems

Limits of single biometric systems can be defeat by using multiple biometrics system. A multiple biometrics systems use multiple applications to capture different kind of biometrics. This allows the combination of two or more types of biometric identification and verification systems in order to meet severe performance requirements. Such systems are predictable to be more reliable due to the being there of multiple, independent pieces of confirmation. These systems are also able to get together the strict performance requirements compulsory by a variety of applications [5].

A multiple scheme could be, for instance, a arrangement of fingerprint authentication, face identification, voice authentication and smart-card or any other combination of biometric. This enhanced structure takes advantage of the proficiency of each person biometric and can be used to overcome some of the limits of a single biometric. For instance, it is estimated that 5% of the people does not have legible fingerprints, a voice could be altered by a cold and face identification systems are susceptible to change in ambient glow and the pose of the subject's head. A multiple system, which combines the finale made by a number of not related biometrics indicator, can overcome many of these limitations [3].

2.5. Biometrics in Electronic passports

Biometrics in electronic passports meet the terms with the ICAO standard consists of a compulsory facial image and fingerprints. While the former are used by a important number of countries and thus in order on them is widely accessible, the latter is at present used seldom. Therefore, this section only covers the vulnerabilities of facial images, fingerprints, palm print and iris images.

2.5.1. Face Image

Facial images are the most frequent biometric trait used by humans to make an individual recognition, hence the idea to use this biometrics in technology. This is a nonintrusive method and is appropriate for covert identification applications. Face authentication involves extracting a characteristic set from a two-dimensional image of the user face and matching it with the template store in a database. The most popular approaches to face identification are based on either: The location and shape of facial attribute such as eyes, eyebrows, nose, lips and chin, and their spatial relationships, or the overall analysis of the face image that represent a face as a weighted combination of a amount of canonical faces. It is questionable if a face itself is an adequate basis for recognize a person from a great number of identity with an tremendously high level of confidence. Facial detection system should be able to by design sense a face in an image, extract its features and then identify it from a general point of view (i.e., from any pose) which is a rather hard task. An additional problem is the fact that the face is a variable social organ display a variety of expressions [4].

2.5.2. Fingerprint

A fingerprint is a model of ridges and furrows positioned on the tip of each finger. Fingerprints were used for individual recognition for many centuries and the matching correctness was very

high. Patterns have been extracting by creating an inked idea of the fingertip on paper. Today, solid sensors provide digital descriptions of these patterns. Fingerprint identification for recognition acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validates attributes such as high temperature and pulse. In real-time authentication systems, images acquired by sensors are used by the feature extraction component to compute the feature values. The feature values characteristically correspond to the position and orientation of certain critical points known as minutiae points. One problem with the current fingerprint identification systems is that they need a large amount of computational possessions [2].

2.5.3. Palmprint

The palmprint identification module is designed to carry out the person recognition process for the unknown person. The palmprint image is the only enter data for the identification process. The person recognition details are the expected output value. The input image feature is compare with the database image features. The relevancy is predictable with reference to the entry value. The most appropriate image is selected for the person's detection. If the relationship result does not match with the input image then the identification process is declared as unknown person. The identification module is divided into four sub modules. They are palmprint collection, result particulars, ordinal list and ordinal measurement. The palmprint image selection sub unit is designed to select the palmprint input image. The file open dialog is used to choose the input image file. The result particulars produce the list of applicable palmprint with their similarity ratio details. The ordinal list shows the ordinal feature based comparison. The ordinal measurement sub section shows the ordinal values for each region.

2.5.4. Iris Recognition

Iris identification technology is based on the distinctly colored ring contiguous the pupil of the eye. Made from expandable connective tissue, the iris is a very well-off source of biometric information, having approximately 266 distinctive characteristics. These include the trabecular meshwork, a tissue that gives the look of dividing the iris very, with striations, rings, furrows, a corona, and freckles. Iris identification technology uses about 173 of these distinctive characteristics. Iris identification can be used in both verification and recognition systems. Iris identification systems use a small, high-class camera to capture a black and white, high-resolution image of the iris. The system then defines the limitations of the iris, establish a organize system over the iris, and define the zones for examination within the coordinate system [12].

2.6. Biometric System Modules

Enrollment Unit: The enrollment section registers individuals into the biometrics system database. During this phase, a biometrics reader scans the individual's biometrics characteristic to produce its digital illustration.

Feature Extraction Unit: This section processes the input model to generate a compact image called the template, which is then stored in a central database or a smartcard issued to the person.

Matching Unit: This module compare the current input with the pattern. If the system performs identity authentication, it compares the new characteristics to the users' master template and produce a score or match value (one to one matching). A system performing arts identification matches the new characteristics against the master templates of several users resulting in many match values (one too many matching).

Decision Maker: This section accepts or rejects the client based on a safety measures threshold and matching score [5].

2.7. Cryptographic

The information stored in the electronic passport is highly top secret; the Contactless IC chip must have mechanism for safeguard and truthfulness of the data. A cryptographic protocols checksum is used to keep data integrity. The system can identify if information has been altered by compare the checksum in the electronic passport against the real-time working out of the stored data. Symmetric or asymmetric secret keys can be use to make sure data privacy. Electronic Passport issuing country has the option not to encrypt the information. A digital watermark is used to save from harm the integrity of face, fingerprint, palmprint and iris image. A number of digital bits may be buried into an image for further authentication purposes without degrading the excellence of the image. Unique IC chip serial numbers are used to check cloning of chips. A Public Key Infrastructure for production and management is required.

3. ELECTRONIC PASSPORT SPECIFICATION

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

- Basic Access Control: It provides encrypted communication involving the chip and the Inspection System.
- Passive Authentication: A border safety measures officer reads and verifies the legitimacy of electronic passport content store in the chip.
- Active Authentication: It provides honesty verification of electronic passport information. The two novel protocols that intend to replace active authentication and thus now consists of the subsequent four protocols:
- Basic Access Control: It smooths the progress of the electronic passport and the inspection system to establish an encrypted communication channel.
- Chip Authentication: A method to identify cloned electronic passports
- Passive Authentication Protocol: As in earliest generation electronic passport customary.
- Terminal Authentication: Only if all protocols are finished successfully, the electronic passport releases sensitive in order like secondary biometrics identifiers. The electronic passports perform the gathering of protocols as specified in the first generation electronic passports, therefore providing backward compatibility [6].

4. ELECTRONIC PASSPORT LOGICAL DATA STRUCTURE

The ICAO issued a consistent data structure called Logical Data Structure for the storage of data essentials. This was to ensure that worldwide interoperability for electronic passport Tags and Readers could be maintain. The provision state that all the 16 data groups are write confined and can be written only at the point in time of issue of the electronic passport by the issuing state shown in table 1. A mix up of data groups 1-15 are store in the safety measures data element, each of these mix up should be indication by the issuing state [6].

Table 1: Passport Logical Data Structure

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

Requirements of the Logical Data Structure: The predefined, consistent LDS must meet a number of compulsory requirements: Guarantee well-organized and optimum facilitation of the legal holder. Ensure safety measures of details recorded in the possible capacity growth technology. Allow worldwide interchange of capacity expanded information based on the use of a solitary LDS familiar to all. Address the various optional capacity development needs of issuing state. It provides development capacity as client needs and available knowledge evolve. It supports a mixture of data protection options. It supports the adding together of details by a receiving state while maintain the legitimacy and truthfulness of data shaped by the issuing state. LDS make use of existing global standards to the utmost extent possible in exacting the emerging worldwide standards for internationally interoperable biometrics.

5. IMPLEMENTATION OF ELECTRONIC PASSPORT SYSTEM

In order to employ this electronic passport scheme using cryptographic safety measures and biometrics technology efficiently, ASP.NET language is used. ASP.NET language could speed up the enlargement of this scheme because it has facilities to represent forms and to insert library easily. There are three ways of doing authentication and authorization in ASP.NET:

Windows Authentication: In this method ASP.NET web pages will use local windows users and groups to verify and give permission resources.

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

Passport Authentication: Passport authentication is based on the electronic passport website provided by the ASP.NET. So when user login with credentials it will be accomplish to the electronic passport website where verification will happen. If verification is successful it will return a token to your website.

Anonymous access: If you do not want any kind of verification then you will go for anonymous right of entry.

5.1. Public Key Infrastructure

In normal situations, certificate issuing association known as Certificates Authorities are grouped in a trust pecking order. All CA's in a straight line or indirectly trust the top-level Root CA. When a private key is compromise, the country cannot robotically cancel all the electronic passports issued with this key. The electronic passport signed by any private key is predictable to last for the issuing time. It is not feasible to ask hundreds or still thousands of electronic passport holders to renew their electronic passports every point in time a key is revoked. Instead, these electronic passports should be used as usual, and a system should alert the custom officials inspect the electronic passport in superior detail. For each country, there is a Country Signing CA responsible for create a public and private key pair, which is used to sign the Document Signer Certificates. This key pair should be generate and stored in an extremely protected, offline CA communications by the issuing country. The lifetime of a Country Signing CA Key is supposed to be the longer of:

- The length of moment in time the key will be used to issue electronic passports
- The duration of the electronic passport issued by the key.

To ensure safety measures, the recommended the countries to put back the CA key every 3-5 years. Under each country, there are several electronic passports issuing office. Each of them is a Document Signer with a public and private key pair and has a Document Signer Certificate. Each electronic passport is signed by the Document Signer Certificate to ensure data honesty.
In order to keep away from large amount of electronic passports with invalid keys when a Document Signer Certificate Key is revoked, the recommended duration of the key should be about three months, less if the office issue a lot of electronic passports per period of time. If a key or a permit needs to be revoked, the Country CA must be in touch bilaterally to all other countries and to the Public Key Directory within 48 hours [7]. In addition, a full revocation list should be exchange every 90 days.

All the private key of Document Signer is store in the electronic passport issuing office; where as the public key is store in the Public Key Directory. The directory is a innermost source used to deal out the public key to the participate countries. Each member country is accountable for downloading the newest version of the keys and making sure electronic passports are indeed signed by the Document Signer [9].

5.2. Passive Authentication

Passive Authentication is the only compulsory cryptographic protocol. Its main goal is to permit a Reader to confirm that the biometric data in the electronic passport is genuine. This method is known as passive authentication since the Tag carry out no dispensation and is only inertly involved in the protocol. One must note that Passive Authentication does not tie the Tag to a electronic passport.

The Inspection System gets back the official document of the issuing essay verifier; using the public key from the official document it verifies the digital signature and biometrics used to sign the biometric data. Once the legitimacy of the signature is recognized, the Reader calculates the mix up of each of these passport data elements and compares them with the mix up values store. If there is a match, it can be recognized that the data on the Tag was not manipulate [7].

5.3. Active Authentication

Active Authentication is a non-compulsory protocol. Using a simple challenge response method, it aims to notice if a Tag has been substituted or cloned. If Active Authentication is support, the Tag on the electronic passport provisions a public key KP_{uAA} in Data and its mix up representation. The corresponding private key KP_{rAA} is stored in the safe and sound section of Tag memory. In order for the Tag to set up its authenticity, it must prove to the Reader that it have this private key.

- The Reader sends an arbitrarily generated 64 bit string (R) to the Tag.
- The Tag signs this string using the key and sends this signature to the Reader.
- The Reader gets hold of the public key store in biometrics Data.
- The Reader confirms the correctness of the signed string using its information of R and KP_{uAA}.

5.4. Basic Access Control

Basic Access Control (BAC) is a non-compulsory protocol that tries to ensure that only Readers with substantial access to the electronic passport can read Tag data. When a reader attempts to scan the Basic Access Control enabled electronic passport, it engages in a protocol which requires the Reader to prove information of a pair of secret keys called “access keys” that are derived from biometrics data on the Machine Readable Zone of the electronic passport. From these keys, a session key which is used for safe and sound messaging is obtained [8].

5.5. Chip Authentication

The Chip Authentication protocol is aims to replace Active Authentication as a mechanism to detect cloned electronic passports. If Chip Authentication is performing effectively it establishes a new pair of encryption and MAC keys to replace Basic Access Control C derived session keys and enable protected messaging. Note that the electronic passport Tag by now has a Chip Authentication public key and private key (in secure memory) [13].

6. ELECTRONIC PASSPORT AUTHENTICATE

Figure 1 shows the different entities involved in confirm with electronic passport state of affairs and the traffic that is exchange between them. A TCP connection from the electronic passport to the user is created as soon as the user loads the login page. In the current performance this is accomplished by placing an ASP.NET owned by the identity supplier 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 electronic passport web server so that the Runtime Environment at the users’ client trusts this piece to allow it to set up a connection back to the electronic passport server. The website was given permission to connect to the contactless reader in a electronic passport policy file which was installed during employment. The TCP connection is used for subsequent communication between the identity provider and the user’s electronic passport.

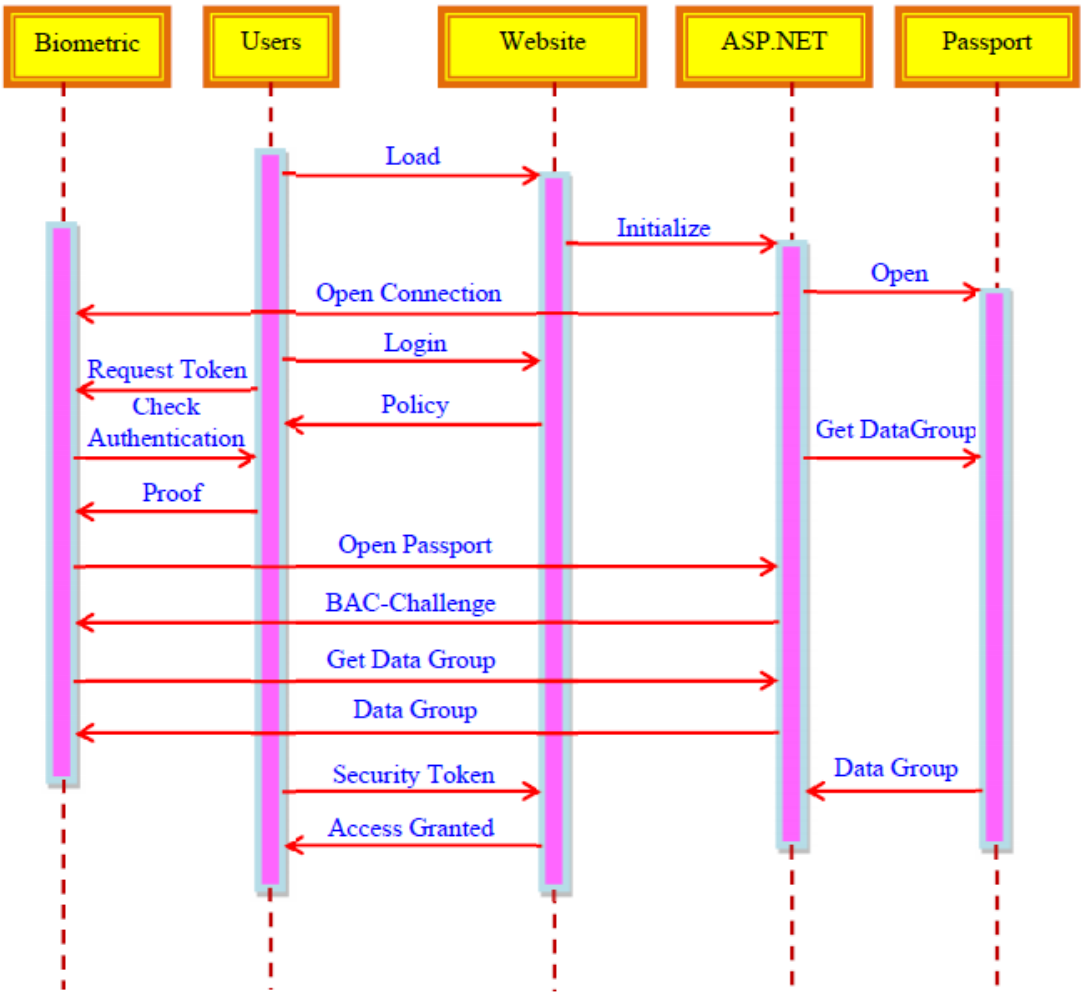

Figure 1. Message sequence chart of validate with electronic passport development

Using the managed electronic 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 electronic passport and it reads the user's details from the e-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 e-passport authenticating the identity provider at the electronic passport. The identity provider will request the electronic 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 electronic 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 electronic passport to confirm to the token request. The token is sent back to the client and from here on the normal Information scenario continues.

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 electronic passport.

7. ELECTRONIC PASSPORT PROTOCOLS

The electronic passport is a complex protocol suite that consists of three sub protocols namely, Basic Access Control, Passive Authentication and Active Authentication. Such a protocol suite is not only difficult to formalize, but also confirmation of such systems more often leads to an exponential state-space explosions. Examiner model the flow of electronic passport protocols according to the following stages:

- When an electronic passport is presented at a border safety measures checkpoint, the chip and the electronic passport reader carry out the Basic Access Control protocol, in order to establish a secure encrypted communication channel between them.
- On successful completion of Basic Access Control, the electronic passport reader performs Passive Authentication.
- On successful completion of Passive Authentication the chip and the electronic passport reader perform the Active Authentication protocol.

The electronic passport verification heavily relies on PKI. Examiner representation only one level of certification hierarchy, up to the document signer and we assume that document signer public key is certified by its country signing influence and, is valid and secluded. This does not weaken the confirmation process of the electronic passport protocol suite, but only indicates that the model assumes the "ideal" PKI implementation. Researcher also presumes that cryptographic primitives and biometrics used in the system like face, fingerprints, palmprint, iris and generation of keys are safe [8]. In the electronic passport protocol, this verification protocol was used only when access to biometrics data was required.

7.2. Electronic 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 electronic passport are also certified by its root certification authority [14].

7.3. Phase One – Passport Inspection System Verification

Step 1: When an electronic passport is presented to an Inspection System, the Inspection System reads the MRZ information on the electronic passport using an MRZ reader and issues the command GET CHALLENGE to the electronic passport chip.

Step 2: The electronic passport chip then generates a random eP £ $_R$ $1 \leq eP \leq q - 1$ and computes $K_{eP} = g^{eP} \bmod p$, playing its part in the key agreement process to establish a session key. The electronic passport replies to the GET CHALLENGE command by sending K_{eP} and its domain parameters *p, q, g*.

$$eP \rightarrow \text{Inspection System} : K_{eP}, p, q, g$$

Step 3: On receiving the response from the electronic passport, the Inspection System generates a random *Inspection System* £$_R$ $1 \leq IS \leq q - 1$ and computes its part of the session key as $K_{IS} = g^{IS} \bmod p$. The Inspection System digitally signs the message containing MRZ value of the electronic passport and K_{eP}.

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

It then contacts the nearest DV of the electronic passports issuing country and obtains its public key. The Inspection System encrypts and sends its signature S_{IS} along with the electronic passport's MRZ information and K_{eP} using the DV's public key PK_{DV}.

$$\text{Inspection System} \rightarrow \text{DV}: ENC_{PK\,DV} (S_{IS}, MRZ, K_{eP}), CERT_{CVCA}(PK_{IS}, IS)$$

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

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

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

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

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

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

$$\text{Inspection System} \rightarrow eP : K_{IS}, SIGN_{SKIS} (K_{IS}, p, q, g), ENCK_{ePIS} (S_{DV}, MRZ, K_{eP})$$

Step 6: On receiving the message from the Inspection System, the electronic 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 $VERIFY_{PKIS} (SIGN_{SKIS} (K_{IS}, p, q, g))$. On successful

verification, the electronic passport is convinced that the Inspection System system is genuine and can proceed further in releasing its details. All further communications between an electronic passport and Inspection System are encrypted using the session key $K_{ePIS.}$

7.4. Phase Two - Electronic Passport Authentication

Step 1: The Inspection System issues an INTERNAL AUTHENTICATE command to the electronic passport. The electronic passport on receiving the command, the electronic passport creates a signature $S_{eP} = SIGN_{SKeP}$ (MRZ || K_{ePIS}) and sends its domain parameter certificate to the Inspection System. The entire message is encrypted using the session key K_{ePIS}.

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

Step 2: The Inspection System decrypts the message and verifies $CERT_{DV}$ (p, q, g), $CERT_{DV}$ (PK_{eP}) and S_{eP}. If all three verifications hold then the Inspection System is convinced that the electronic passport is genuine and authentic.

During the Inspection System authentication phase, and Inspection System sends the electronic passport's MRZ information to the nearest electronic passport's DV, which could be an electronic passport country's embassy. Embassies are DV's because they are allowed to issue electronic passports to their citizens and because most embassies are located within an Inspection System'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.

8. EXPERIMENTAL RESULTS

A successful design, deployment and process of biometric passport scheme depend extremely on the results for presented biometrics technology and mechanism. These presented technologies as well as new solutions need to be evaluating on their electronic passport system performance. However it is often forgotten that the biometrics such as iris, finger, face, and palm prints is only one part of a fully organize application.

As biometric systems are often not intended with safety measures and or privacy in mind, system integrators will need to deal with the requirements of the deployed purpose in this light. The fears and concern of an important segment of the user inhabitants need to be addressed as early as achievable in the design progression, to ensure that suitable mechanisms are in place to restore confidence such users. These concerns may relate to privacy or to safety concern, which may be addressed in part through authorized and authoritarian measures. This article discusses the requirements, design and application scenarios of biometrics systems in general and the introduction of a new biometrical passport in particular.

The chip in the electronic passport will be a nearness contactless chip that must be held within ten centimeters of a reader in order to be read. Moreover, the data on the chip cannot be access unless the machine-readable zone on read, which means that the electronic passport book must be open. Border authorities equipped with electronic passport readers will insert the traveler's electronic passport into a biometric scanner, which will read the machine-readable zone, thereby opening

the chip so that it can be read as well. The machine also checks other safety measures features, such as the country's signature. Border authorities who are not operational with electronic passport readers will continue to scrutinize travelers' biometric passports as they do now.

9. CONCLUSIONS

The work represents an attempt to acknowledge and account for the presence on electronic passport using biometrics recognition towards their improved identification. The application of facial, fingerprint, palm print and iris identification in electronic passports requires high accurateness rates; safe and sound data storage, protected transfer of data and reliable generation of biometrics data. The electronic 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 worldwide implementation and recognition of biometric passport. A possible solution to unencrypted wireless right of entry to electronic passport data is to store a unique cryptographic key in printed form that is also obtained upon justification. The key is then used to decrypt electronic passport data and forces thieves to physically obtain electronic passports to steal personal information. More research into the technology, additional access and auditing policies, and further safety measures enhancements are required before biometric identification is considered as a viable solution to biometric safety measures in electronic passports. The adversaries might exploit the electronic passports with the lowest level of safety measures. The inclusion of biometrics recognition information into machine readable electronic passports will improve their robustness against identity theft if additional security measures are employing in order to compensate for the limitations of the biometric technologies. It enables countries to digitize their safety measures at border control and provides faster and safer dealing out of an electronic passport bearer. The main cryptographic features and biometrics used with electronic passports and considered the surrounding procedures. Electronic passports may provide valuable experience in how to build more safe and sound and biometric recognition platforms in the years to come.

REFERENCES

[1] A.K.Jain, R.Bolle, "Biometrics identification in networked society" Norwell, MA: Kluwer, 2010.
[2] Barral and A. Tria. "Fake fingers in fingerprint identification: Glycerin supersedes gelatin", In Formal to Practical Security. Springer, 2009.
[3] Bergman, "Multiple biometric match-on-card alliance formed," Biometric Technology Today, vol. 13, no. 5, p. 6, 2005.
[4] C.Hesher, A.Srivastava, G.Erlebacher, "A novel technique for face identification using range images" in the Proceedings of Seventh International Symposium on Signal Processing and Its Application, 2003.
[5] Chang, "New multiple biometric approaches for improved personal identification," PhD Dissertation, Department of Computer Science and Engineering, University of Notre Dame, 2004.
[6] D. Monar, A. Juels, and D. Wagner, "Security and privacy issues in e-passports", Cryptology ePrint Archive, 2005.
[7] Gaurav S. Kc and Paul A. Karger. "Security and privacy issues in machine readable passport travel documents", IBM Technical Report, IBM T. J.Watson Research Labs, April 2005.
[8] HOME AFFAIRS JUSTICE, "Specifications for security features and biometrics in passport", Technical report, European Union, 2006.
[9] ICAO, "Machine readable passport documents", Technical report, ICAO 2006.
[10] ICAO, "Machine Readable Travel Documents", Part 1 Machine Readable Passports. ICAO, Fifth Edition, 2003.
[11] ICAO, "Biometrics passport Deployment of Machine Readable Travel Documents", Version 2.0, May 2004.

[12] John Daugman, "How iris identification works." IEEE Transactions on Circuits and Systems for Video Technology, 21–30, 2009.
[13] KLUGLER, D., "Advance security mechanisms for passport machine readable travel documents, Technical report", Federal Office for Information Security (BSI), Germany, 2005.
[14] Riscure Security Lab, "Electronic passport security and privacy attack", at the Cards Asia Singapore, April 2006.

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 22 articles in international journal. He has authored or co-authored more than 58 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, Electronic Identification Systems, 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 authored more than 22 articles in international journal. He has authored or co-authored more than 70 technical papers and conference presentations. He is a editorial board for several scientific e-journals. His research interests include automated biometrics, computer networking, Internet security, and performance evaluation.