I. J. Computer Network and Information Security, 2012, 2, 50-58
Published Online March 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.02.08

Evolution of Electronic Passport Scheme using Cryptographic Protocol along with Biometrics Authentication System

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

[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: [1]kumarmcagobi@yahoo.com, [2] srinivasan_gasc@yahoo.com

***Abstract*—Millions of citizens around the world have already acquired their new electronic passport. The e-passport is equipped with contactless chip which stores personal data of the passport holder, information about the passport and the issuing institution, as well as with a multiple biometrics enabling cryptographic functionality. Countries are required to build a Public Key Infrastructure, biometric and Radio Frequency Identification to support various cryptographic, as this is considered the basic tools to prove the authenticity and integrity of the Machine Readable Travel Documents. The large-scale worldwide PKI is construction, by means of bilateral trust relationships between Countries. Investigate the good practices, which are essential for the establishment of a global identification scheme based on e-passports. The paper explores the privacy and security implications of this impending worldwide experiment in biometrics authentication technology.**

***Index Terms*—Biometrics, E-Passport, Face, Fingerprint, Palm print, Iris.**

I. INTRODUCTION

A passport is an internationally recognized travel document that verifies the identity and nationality of the bearer. An electronic passport is a passport containing an electronic chip encoded with the information that is printed on the data page of the passport, as well as a digital picture of the passport holder to be used for biometric facial recognition, a unique chip number, and a digital signature of the data. The addition of the electronic chip is intended to provide additional resistance to forgery and, therefore, a stronger guarantee on the identity of the bearer. This improved security is also hoped to be accompanied with a faster processing time at border crossings.

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 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 [10].

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].

A. Electronic Personalization

The new e-Passport adds another dimension to the passport personalization process. As the visual information recorded on the passport is stored in the contactless chip, it is also absolutely essential that all details held on the data page exactly match the information stored in the chip. Furthermore, the inclusion of biometric technology creates new logistical questions in terms of where and how citizens enroll their individual biometrics.

One approach to personalization is to develop a generic solution to personalize chip data in central sites. This could include fast generation of personalization scripts as well as digital signing and securing of both biometric and other sensitive data using algorithms such as RSA. The electronic personalization process for e-Passports basically consists of the following steps:

- Prepare the data to be stored in the contactless chip in the so called "Logical Data Structure" (LDS).

- The face as the primary, mandatory biometric; the fingerprint, Palmprint or iris as secondary and optional.
- Electronically signing the data using a public key infrastructure to protect the integrity of the contents and to prove authenticity during the verification process.
- Write the prepared data in the memory of the chip.

The public key infrastructure needed for ICAO compliant e-Passports has a Country Signing Certification Authority (CSCA) as the root certification authority of the infrastructure. The CSCA is typically run by a ministry and installed at their premises. The Document Signer (DS) forms the unit which signs the Logical Data Structure. The key material used by the DS is signed by the CSCA. Thereby the whole certificate chain can be checked for authenticity during the verification process.

B. 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.

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.

C. Necessary Infrastructure

The proposed biometric systems (face, fingerprint, palmprint and iris) do not require much additional infrastructure beyond what is required by the e-Passport system already being deployed.

One obvious requirement is the addition of face, fingerprint, palmprint and iris scanners, at all passport offices and the border checkpoints of any country wishing to recognize biometric data.

In addition, each country that chooses to use cryptography with their passport system must publish the biometric feature detection algorithms, related data formats, and appropriate codings/decodings. If no international standard is decided, there could be hundreds of such variations. However, this could be considered strength because it allows each country to define its own biometric security standards without affecting the standards of other countries.

Lastly, a simple public key infrastructure is required to securely transport passport data to the entities that actually program the e-Passports with data. We speculate, however, that this infrastructure already exists as part of the standard e-Passport deployment and is not an extra burden imposed by the proposed system [3].

D. Validity Period for an E-Passport

The validity period of an e-Passport is at the discretion of the issuing State; however, in consideration of the limited durability of documents and the changing appearance of the passport holder over time, a validity period of not more than ten years is recommended. States may wish to consider a shorter period to enable the progressive upgrading of the e-Passport as the technology evolves.

E. Visual Uniformity

The visual appearance of a passport holder's information conforms to a uniform standard that is adopted worldwide. As passports have become more technically advanced, visual requirements have changed a lot. This information, along with other visible data – classed as level one identity verification – is incorporated into the passport during personalization for future visual inspection. The following level one identity data is included in all passports:

- Unique passport number;
- Unique national identity number;
- Full name of passport holder;
- Country code;
- Color photograph;
- Passport holder's signature;
- Passport holder's nationality;
- Date of issue of passport;
- Expiry date of passport;
- Passport holder's date of birth;
- Passport holder's place of birth;
- Passport holder's sex;
- Passport issuing authority;
- Machine Readable Zone

II. BACKGROUND OF THE STUDY

The concept of e-passport was introduced by Davida and Desmedt in 1988. One of the first study on privacy issues from RFID protocols, including singulation ones, is due to Avoine and Oechslin. In 2005, Juels, Molnar and Wagner presented a survey on MRTD and RFID. Among other issues, they discussed about the "biometric threat" and shortcomings in the Basic Access Control (BAC) protocol. In 2006, Hoepman et al. discussed more about unauthorized access and skimming over the BAC protocol. They studied the entropy of the access key. They also discussed about the Extended Access Control (EAC). They detailed a revocation issue related to terminal authentication. They further discussed on biometrics. An experimental attack based on the BAC weaknesses was reported in 2006 by Hancke and Carluccio et al. In 2006, Lehtonen et al. studied ways to make optical memory and contactless IC chip interact for

the benefit of security. Hlav´a¡c and Rosa have demonstrated a man-in-the-middle attack on Active Authentication in 2007. Finally, Monnerat et al. have discussed on transferability of digital evidence and studied ways to fix it.

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.

A. 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 [5].

B. 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].

C. 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].

D. 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. 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 [6].

E. 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 [12].

F. Design of Biometric System

Five objectives, cost, user acceptance and environment constraints, accuracy, computation speed and security should be considered when designing a biometric system. They are inter-related, as is shown in Figure 1.2. Reducing accuracy can increase speed. Typical examples are hierarchical approaches. Reducing user acceptance can improve accuracy. For instance, users are required to provide more samples for training the system. Increasing cost can enhance security. More sensors can be embedded to collect different signals for aliveness detection. In some applications, some environmental constraints such as memory usage, power consumption, size of templates, and size of devices have to be factored into a design. A biometric system installed in a PDA (Personal Digital Assistant) requires low power and memory usage, but these requirements are not essential for access control. A practical biometric system should balance all these aspects [7].

G. Requirement Analysis

The two most important requirements for providing border security are the identification of the passport bearer and the authentication of the passport data. The digital nature of the data stored in an e-Passport makes them easy to be either copied or altered. Therefore, an e-Passport protocol will need to ensure security requirements that will affect the electronic data storage and transmission. Though provides a brief overview security goals for e-Passports, their description are limited and do not consider the goals that are essential for analyzing the cryptographic protocols. The security goals for an e-Passport system are:

Goal 1 *Identification:* After the successful completion of an e-Passport protocol, both the e-Passport and the IS must obtain guarantees (unforgeable proof) of other entity's identity.

Goal 2 *Authenticity:* After a successful completion of an e-Passport protocol, both the e-Passport and the IS must have guarantees on the authenticity of the messages received during the conversation with each other, and should also have an undeniable proof-of-origin of the messages.

Goal 3 *Data confidentiality:* Data confidentiality during an e-Passport protocol run is guaranteed by the security of the session key agreed between the e-Passport and the IS. Therefore, if an e-Passport completes a single protocol run with the understanding that it has negotiated a session key K with an IS, the same e-Passport is guaranteed that no other third-party has learnt key the K and if the IS completes the protocol run, then it associates the key K with the e-Passport. Data confidentiality of the information stored in an e-Passport chip is not considered, because it is protocol-independent, but is necessary for the e-Passport protocol to detect if information was tampered with; this is provided by our integrity goal.

Goal 4 *Integrity:* The integrity of the data in an e-Passport chip is guaranteed by signatures. Therefore, during a run of an e-Passport protocol, if an IS successfully verifies and validates the signatures on the messages from an e-Passport, then the IS obtains a guarantee that the information held in an e-Passport chip has not been modified by any third party or the e-Passport bearer after its initialization by the document issuer.

Goal 5 *Privacy:* In every run of an e-Passport protocol, the e-Passport bearers are assured that their e-Passport's digital identities are revealed only to the authenticated IS involved in the current protocol run.

Goal 6 *Session key security:* Both entities, an e-Passport and an IS, have proof that each run of an e-Passport protocol is unique and comprises long term keys, and does not compromise the session keys derived in previous protocol runs.

III. E-PASSPORT LIFE CYCLE

The e-Passport life cycle is made of four phases: Development, Manufacturing, Personalization, and Operational Use that involve the participation of various users in different roles. Figure 1 shows the workflow of phases.

A. Phase 1: Development

The IC Manufacturer develops the IC on its own. The Software Developer develops the IC Embedded Software (RTE and VGP), the LDS application and the guidance documentation associated with these components. The Software Developer uses tools and manuals provided by the IC Manufacturer and specifications of standards provided by SUN Microsystems, Global Platform and ICAO.

B. Phase 2: Manufacturing

The IC Manufacturer has already developed the integrated circuit, the IC Dedicated Software and the associated guidance documentation. The IC Manufacturer produces an integrated circuit containing the Dedicated Software, the Initialization Data that corresponds to this step and the Embedded Software. The IC is delivered from the IC Manufacturer to the Passport Manufacturer. The Passport Manufacturer (i) packs the IC with hardware for the contactless interface in the passport book and (ii) writes Pre-personalization Data. The pre-personalized MRTD is delivered from the Passport Manufacturer to the Personalization Agent.

C. Phase 3 Personalization of the E-Passport

The personalization is requires authentication as Personalization Agent. Once the personalization is finished, the personalized MRTD is handed over to the MRTD holder for operational use. This phase is not re-entered once the MRTD reached the Operational Use phase.

D. Phase 4 Operational Uses

The e-passport is used embedded into a MRTD by the Traveler and the Inspection System.

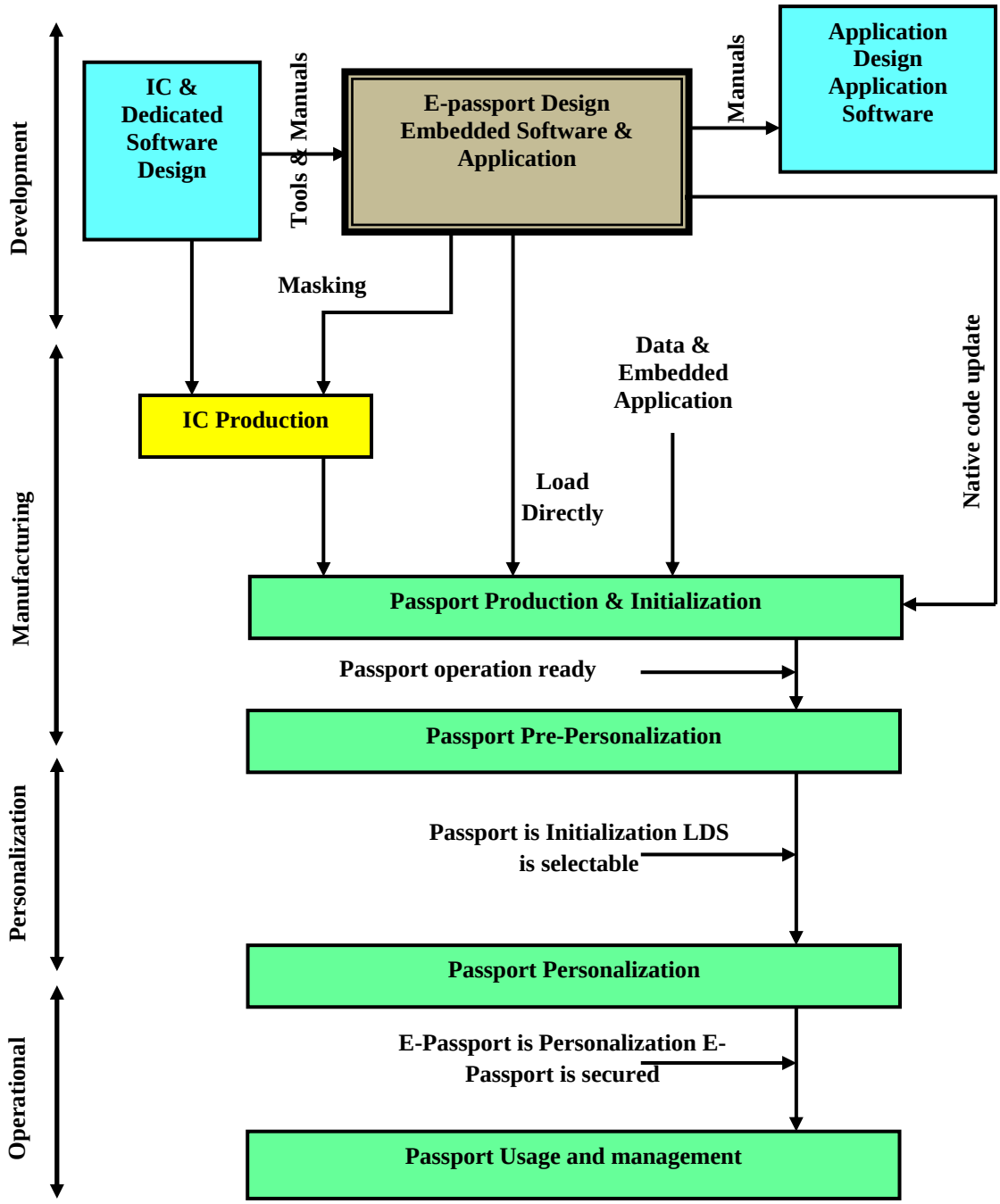

Figure 1: E-Passport Life Cycle

IV. E-PASSPORT SECURITY MECHANISMS

The ICAO standard defines the following security mechanisms to ensure privacy and prevent passport fraud:

A. Passive Authentication

The goal of passive authentication is to verify the authenticity and integrity of the e-passports LDS. Besides the LDS (section 2.1), the chip also contains a Document Security Object (DSO). The DSO contains a hash of the LDS data signed by the issuing state.The hash is signed with the Document Signer private key. An inspection system will contain or download the Document signer certificate to verify the signature [9].

B. Active Authentication

The goal is to prevent chip substitution. The e-passport chip may contain an active authentication key pair. The public key is stored in the DSO; the private key is stored in secure memory. An inspection system would compare the visual MRZ with the MRZ data stored in the LDS to ensure the visual MRZ is authentic. Next, a challenge-response protocol using the active authentication public key will assert that the DSO is not a copy.

C. Basic Access Control

The goal is to prevent skimming and eavesdropping.

D. Extended Access Control

The goal is to provide extra protection for sensitive biometrics. The ICAO standard leaves the design and implementation to the issuing states.

E. Data encryption

The goal is to further restrict access to the LDS data.

V. 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 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

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.
- It supports a variety of data protection options.
- It supports the addition of details by a receiving state while maintaining the authenticity and integrity of data created by the issuing state.
- LDS utilize existing international standards to the maximum extent possible in particular the emerging international standards for globally interoperable biometrics.

VI. PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure (PKI) helps to bind public keys to entities and enables other entities to verify those bindings. The infrastructure consists of the following components:

A. Certification Authority (CA)

It is the central component in a PKI, and performs the following functions - issuing certificates, maintaining certificate revocation lists and publishing certificates and revocation lists. The CA issues certificates to PKI users by digitally signing a certificate with its private key and, during verification; a user confirms the authenticity of the certificate by verifying the CA's signature using the CA's public key.

B. Registration Authority (RA)

It is an entity trusted by the CA, to register or validate the identity of users to a CA, that is, its primary responsibility is to verify whether the certificate contents reflect the information presented by the entity requesting the certificate.

C. Repository

A repository is a database of active (valid) digital certificates. The repository provides information, to allow users who receive digitally signed messages to confirm the status of the digital certificates.

D. Public Key Certificates

The CA issues a public key certificate for each identity. A digital certificate typically includes the public key, information about the identity of the entity holding the corresponding private key, the validity of the certificate, and the CA's own digital signature.

E. Certificate Revocation List (CRL)

CAs also issues and processes certificate revocation lists (CRLs), which list revoked certificates. Every PKI user validating a certificate is also required to process the CRL to check if the certificate has been revoked.

F. PKI Users

PKI users are those who use and rely on PKI components to obtain and verify certificates of other entities with whom they transact.

Using PKI is the dominant method for verifying an entity's pubic key, and thus plays an important role in both semi-passive devices and active hardware-based security devices, for example, e-Passports rely extensively on PKI for the validation of certificates.

VII. E-PASSPORT CRYPTOGRAPHIC PROTOCOLS

The e-passport is a cryptographic protocol suite that consists of three sub protocols namely, BAC, PA and AA. Such a protocol suite is not only difficult to formalize, but also verification of such systems more often leads to an exponential state-space explosions. Researcher model the

flow of e-passport protocol according to the following stages [11]:

- When an e-passport is presented at a border security checkpoint, the 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 BAC, the e-passport reader performs PA.
- On successful completion of PA the chip and the e-passport reader execute the AA protocol.

The e-passport authentication heavily relies on PKI. Researcher model only one level of certification hierarchy, up to the document signer and researcher assume that document signer public key is certified by its country signing authority and, is valid and secure. This does not weaken the verification process of the e-passport protocol suite, but only indicates that the model assumes the "ideal" PKI implementation. Researcher also supposes that cryptographic primitives and multiple biometric used in the system like face, fingerprints and generation of keys are secure [8]. In the e-Passport protocol, this authentication protocol was used only when access to biometric data was required.

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). The OSEP protocol changes this to an active monitoring system. The border security check-point or the DV can now crosscheck against the database of known offenders themselves, thus simplifying the process of the identification of criminals [13].

The on-line secure e-Passport protocol provides the following security features: An e-Passport discloses its information stored on the e-Passport 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 provides proof-of-freshness and the authenticity for messages between the participating entities.
- 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. 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.

C. 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 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 e-Passport replies to the GET CHALLENGE command by sending K_{eP} and its domain parameters p, q, g.

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

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

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

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}.

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

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.

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

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

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

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}.

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

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 $VERIFY_{PKIS} (SIGN_{SKIS} (K_{IS}, p, q, g))$. 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 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 $S_{eP} = SIGN_{SKeP} (MRZ \parallel K_{ePIS})$ and sends its domain parameter certificate to the IS. The entire message is encrypted using the session key K_{ePIS}.

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

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. 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.

VIII. FINDINGS AND RESULTS

States are encouraged to use biometrics to establish or validate identity at border control. The use of biometric data does not ensure that a person has provided their correct name, citizenship and other information, but when biometric identity has been confirmed, it does help to prevent the person from using another name in their dealings. Biometric identity should be identified at ports of entry and ideally points of exit.

If the biometric verification is negative, or there are other actions to be taken determined at the primary port of entry, the traveller may be sent to secondary inspection for detailed inspection.

Primary or Secondary inspection can include a three-way visual comparison of the MRTD holder, the printed portrait image on the Data Page of MRTD and the stored digital record read from the biometric storage medium in their MRTD (passport) or central database (visa)

Ideal would be a gate/booth that captures those biometrics noted as in that holders passport ie. booth capable of capturing all four (face, fingerprint, palmprint and iris), but only actually captures based on read of the LDS eg. if passport holder has face and fingerprint biometric only stored, face (image) and fingerprint is captured; if passport holder has face, palmprint and iris biometrics in their LDS, face, palmprint and iris is captured.

Procedures need to be determined for how inspection officers would handle exceptions such as when the biometrics on the MRTD do not match the person at the border because the document is not working, the storage medium is damaged or not functioning properly, the verification software does not match the person successfully, the document has been physically tampered with, or the traveller is an imposter. Similarly inspection officers need to be aware of, and have procedures in place, with respect to liveness checking and detection of spoofing.

States need to change the focus of border systems from merely processing entries and exits, to systems that confirm identities through automated systems; and thereby seek to also identify fraudulent identities and fraudulent travel documents.

One-to-one verification systems (and one-to-few watch list checking systems) are the appropriate ones to implement at primary inspection. These could be supplemented by use of one-to-many systems at borders as appropriate.

States need to be aware that land borders present unique challenges – many people cross the same land border regularly for commuting purposes and several people may cross in the same vehicle.

Border Control systems can be complemented by the use of pre-entry systems including API (Advanced Passenger Information) which may also use verification systems as part of their processing.

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. 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"* 1999, Norwell, MA: Kluwer.

[2] Barral and A. Tria. "Fake fingers in fingerprint recognition: Glycerin supersedes gelatin", In Formal to Practical Security. Springer, 2009.

[3] Bergman, "Multi-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 recognition using range images"* in the Proceedings of Seventh International Symposium on Signal Processing and Its Application, 2003.

[5] Chang, "New multi-biometric approaches for improved person 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, Report 2005/095, 2005.

[7] Gaurav S. Kc and Paul A. Karger. Security and privacy issues in machine readable travel documents (MRTDs). IBM Technical Report (RC 23575), IBM T. J.Watson Research Labs, April 2005.

[8] HOME AFFAIRS JUSTICE, *"EU standard specifications for security features and biometrics in passports and travel documents"*, Technical report, European Union, 2006.

[9] ICAO, "Machine readable travel documents", Technical report, ICAO 2006.

[10] ICAO, "*Machine Readable Travel Documents",* Part 1 Machine Readable Passports. ICAO, Fifth Edition, 2003.

[11] ICAO, *"Biometrics Deployment of Machine Readable Travel Documents"*, Version 2.0, May 2004.

[12] John Daugman, "How iris recognition works." IEEE Transactions on Circuits and Systems for Video Technology, 14(1):21–30, 2004.

[13] KLUGLER, D., *"Advance security mechanisms for machine readable travel documents, Technical report"*, Federal Office for Information Security (BSI), Germany, 2005.

[14] Riscure Security Lab, *"E-passport 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 or co-authored more than 42 technical papers and conference presentations. He is a reviewer for several scientific 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 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.

