DESIGN AND DEVELOPMENT OF E-PASSPORTS USING BIOMETRIC ACCESS CONTROL 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

A biometric passport, also known as an e-passport, ePassport or a digital passport, is a combined paper and electronic passport that contains biometric information that can be used to authenticate the identity of travelers. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page, of the passport. Electronic passports include contactless chip which stores personal data of the passport holder, information about the passport and the issuing institution. In its simplest form an electronic passport contains just a collection of read-only files, more advanced variants can include sophisticated cryptographic mechanisms protecting security of the document and / or privacy of the passport holder. The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented. The specific choice of each country as to biometric security features to include makes a major difference in the level of security and privacy protection.

KEYWORDS

Biometrics, e-Passport, Face, Iris, palmprint and Fingerprint.

I. INTRODUCTION

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

The e-Passport also offers substantial benefits to the rightful holder by providing a more sophisticated means of confirming that the passport belongs to that person and that it is authentic, without jeopardizing privacy. The states are currently issuing e-Passports, which corresponds to more than 50% of all passports being issued worldwide. This represents a great enhancement in national and international security as (1) it improves the integrity of passports by the need to match the information contained in the chip to the one printed in the document and to the physical

DOI: 10.5121/ijassn.2012.2306

characteristics of the holders; and (2) enables machine-assisted verification of biometric and biographic information to confirm the identity of travelers.

The e-Passport standard provides details about establishing a secure communication between an e-Passport and an Inspection System (IS), the authentication of an e-Passport, details on storage mechanisms and biometric identifiers that should be used. The digital photograph of the individual provides a facial biometric that can be used for automated identification processes by employing facial recognition technology. Most implementations of the e-Passports by various countries have a single identifier only, the facial biometric. But the chip has sufficient capacity to include extensions, such as face, fingerprints and iris biometrics.

A. Background of the Study

Ordinary passport (Tourist passport, Regular passport, Passport). Issued to citizens and other nationals, and generally the most-issued type of passport. Sometimes it is possible to have children registered within the ordinary passport of the parent, rendering the passport functionally equal to a family passport.

Official passport (Service passport, also Special passport). Issued to government employees for work-related travel, and to accompanying dependents.

Diplomatic passport: Issued to diplomats and other government officials for work-related international travel, and to accompanying dependents. Although most persons with diplomatic immunity carry diplomatic passports, having a diplomatic passport is not the equivalent of having diplomatic immunity. A grant of diplomatic status, a privilege of which is diplomatic immunity, has to come from the government of the country in relation to which diplomatic status is claimed. Also, having a diplomatic passport does not mean visa-free travel. A holder of a diplomatic passport must obtain a non-diplomatic visa when traveling to a country where he is not currently nor is going to be accredited as a diplomat, if visas are required to nationals of his country. In exceptional circumstances, a diplomatic passport is given to a foreign citizen with no passport of his own, such as an exiled VIP who lives, by invitation, in a foreign country. Such is the case of King Constantine of Greece who has travelled on diplomatic passports.

Collective passport : Issued to defined groups for travel together to particular destinations, such as a group of school children on a school trip to a specified country. Family passport : Issued to family members—father, mother, son, daughter. There is one passport holder. The passport holder may travel alone or with one or more other family members. A family member who is not the passport holder cannot use the passport for travel unless accompanied by the passport holder.

B. E-Passport Features

The currently standardized biometrics used for this type of identification system are facial recognition, fingerprint recognition, and iris recognition. These were adopted after assessment of several different kinds of biometrics including retinal scan. The ICAO defines the biometric file formats and communication protocols to be used in passports. Only the digital image (usually in JPEG or JPEG2000 format) of each biometric feature is actually stored in the chip. The comparison of biometric features is performed outside the passport chip by electronic border control systems (e-borders). To store biometric data on the contactless chip, it includes a minimum of 32 kilobytes of EEPROM storage memory, and runs on an interface in accordance with the international standard, amongst others. These standards intend interoperability between different countries and different manufacturers of passport books. This was a revolutionary advancement that:

- Enabled border officers to automate watch list checks in near-real time during inspection
- Permitted airline staff to generate manifests of passengers without having to resort to more labor-intensive means of data entry such as keystroke
- Created a standardized “token” that could automate inspections by retrieving a traveler’s biometric information from an enrolment database

II. 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 and fingerprints [3].

A. Face Identification

Face detection is a computer technology that determines the locations and sizes of human faces in arbitrary (digital) images. It detects facial features and ignores anything else, such as buildings, trees and bodies. Face detection can be regarded as a specific case of object-class detection. In object-class detection, the task is to find the locations and sizes of all objects in an image that belong to a given class. Examples include upper torsos, pedestrians, and cars. Face detection can be regarded as a more general case of face localization. In face localization, the task is to find the locations and sizes of a known number of faces (usually one). In face detection, one does not have this additional information. Early face-detection algorithms focused on the detection of frontal human faces, whereas newer algorithms attempt to solve the more general and difficult problem of multi-view face detection. That is, the detection of faces that are either rotated along the axis from the face to the observer (in-plane rotation), or rotated along the vertical or left-right axis (out-of-plane rotation), or both. The newer algorithms take into account variations in the image or video by factors such as face appearance, lighting, and pose.

B. Fingerprint Identification

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. [3] In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. A print from the foot can also leave an impression of friction ridges. A friction ridge is a raised portion of the epidermis on the digits (fingers and toes), the palm of the hand or the sole of the foot, consisting of one or more connected ridge units of friction ridge skin. These are sometimes known as "epidermal ridges" which are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis. [4] These epidermal ridges serve to amplify vibrations triggered, for example, when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges also assist in gripping rough surfaces, as well as smooth wet surfaces.

C. Iris Identification

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irides of an individual's eyes, whose complex random patterns are unique and can be seen from some distance. 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 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 [3].

D. 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. The ordinal list shows the ordinal feature based comparisons. The ordinal measurement sub module shows the ordinal values for each region.

III. SECURITY ASSUMPTION

The e-Passport makes several simplifying assumptions which will eliminate many irrelevant details of our empirical analysis and thereby keeps the “big picture” of the analysis observable to the reader. For example, assume that the cryptographic schemes used in e-Passport systems are secure. The analysis uses the following assumption:

Non-traceable chip characteristics. Random chip identifiers reply to each request with a different chip number. This prevents tracing of passport chips. Using random identification numbers is optional.

Basic Access Control (BAC). BAC protects the communication channel between the chip and the reader by encrypting transmitted information. Before data can be read from a chip, the reader needs to provide a key which is derived from the Machine Readable Zone [Mrz]: the date of birth, the date of expiry and the document number. If BAC is used, an attacker cannot (easily) eavesdrop transferred information without knowing the correct key. Using BAC is optional.

Passive Authentication (PA). PA prevents modification of passport chip data. The chip contains a file (SOD) that stores hash values of all files stored in the chip (picture, finger print, etc.) and a digital signature of these hashes. The digital signature is made using a document signing key which itself is signed by a country signing key. If a file in the chip (e.g. the picture) is changed, this can be detected since the hash value is incorrect. Readers need access to all used public country keys to check whether the digital signature is generated by a trusted country. Using PA is mandatory.

Active Authentication (AA). AA prevents cloning of passport chips. The chip contains a private key that cannot be read or copied, but its existence can easily be proven. Using AA is optional.
Extended Access Control (EAC). EAC adds functionality to check the authenticity of both the chip (chip authentication) and the reader (terminal authentication). Furthermore it uses stronger encryption than BAC. EAC is typically used to protect finger prints and iris scans. Using EAC is optional. In the EU, using EAC is mandatory for all documents issued.
Shielding the chip. This prevents unauthorized reading. Some countries – including at least the US – have integrated a very thin metal mesh into the passport's cover to act as a shield when the passport cover is closed.

IV. 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.

TABLE 1: Logical Data Structure

Data Group	Data Element
DG 1	Document Details
DG 2	Encoded Headshot
DG 3	Encoded Face biometrics
DG 4	Encoded Fingerprint
DG 5	Encoded Iris
DG 6	Encoded Palmprint
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

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, each of these hashes should be signed by the issuing state.

V. EXTENDED ACCESS CONTROL

To resolve the security and privacy concerns that have been identified in the first generation e-Passports, the EU issued an e-Passport specification to restrict access to secondary biometric identifiers such as fingerprints and iris scans. Countries with bilateral agreements will be able to perform EAC-based authentication and obtain access to fingerprint and iris images. The EAC e-Passport specification is based on the authentication techniques proposed by D. Kluger from German Federal Office for Information Security (BSI), and now includes two new authentication protocols, Chip Authentication (CA) and Terminal Authentication (TA). The EAC also included modifications to the existing PKI. The Country Signing Certification Authority (CSCA) is now required to certify Document Verifiers (DV) in other countries that in turn certifies Inspection Systems (IS) present at a country's border security checkpoint. Figure 1 provides an overview of the modified PKI hierarchy.

A. E-Passport Operation with the EAC

The e-Passport bearers presents their document to a border security officer who scans the MRZ on the e-Passport through a MRZ reader and then places the e-Passport near an IS to fetch data from the e-Passport chip. Only when all the protocols are completed successfully, does the e-Passport release sensitive information such as secondary biometric identifiers. Extended Access Control ("EAC") is a mechanism specified to allow only authorized Inspection Systems (systems used to read e-passport) to read sensitive biometric data such as fingerprints from ePassports.

B. Chip Authentication

Chip Authentication is a mandatory EAC mechanism that replaces the active authentication proposed in the first-generation e-Passports. It involves a Diffie-Hellman key agreement (DHKA) and is followed by passive authentication. It is performed after a successful basic access control and provides both a means of authenticating the e-Passport and generating a new session key. The e-Passport uses a static Diffie-Hellman public key while the IS uses an ephemeral key. The protocol begins with the e-Passport sending its public key (PK_{eP}) and its domain parameters (D_{eP}) to the IS. The IS then generates an ephemeral Diffie-Hellman key pair (SK'_{IS}, PK'_{IS}) using the same domain parameters and sends the newly-generated public key to the e-Passport. Both the e-Passport and the IS derive a new session key K. Chip authentication is immediately followed by passive authentication, which allows an IS to verify if the PK_{eP} is genuine. The authenticity of the e-Passport is established once the e-Passport proves that it knows the session key; this happens implicitly when the derived session key is used to communicate successfully with the e-Passport.

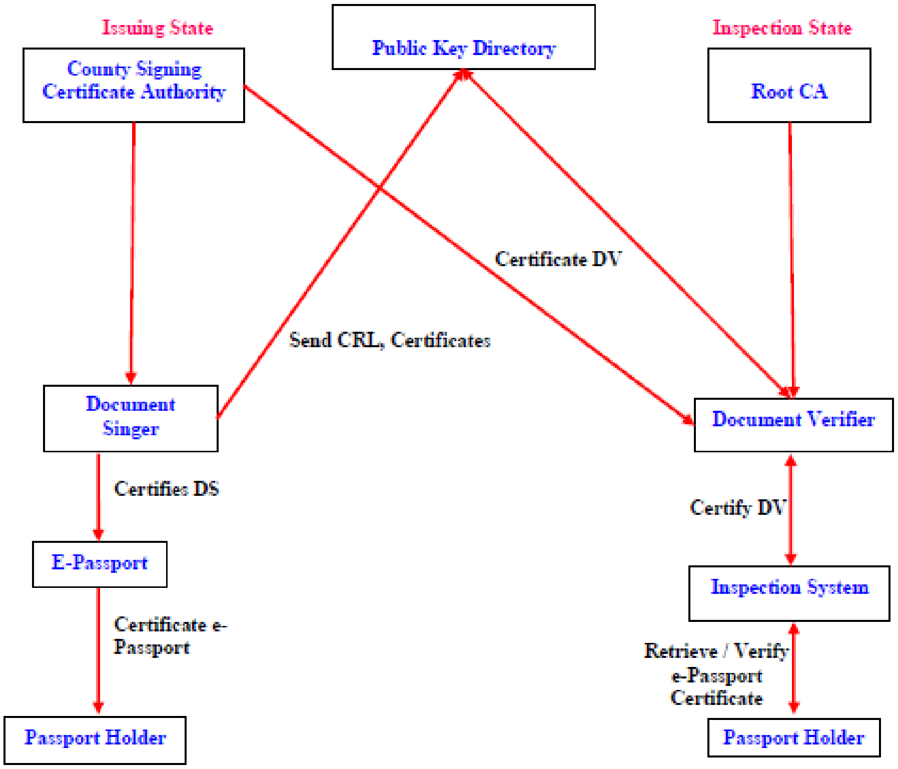


Figure 1: Extended access control in public key infrastructure

C. Active Authentication

Active Authentication is an optional protocol in the ICAO specifications. Using a simple challenge-response mechanism, it aims to detect if a Tag has been substituted or cloned. If Active Authentication is supported, the Tag on the e-Passport stores a public key (KP_{uAA}) in Data and its hash representation. The corresponding private key (KP_{rAA}) is stored in the secure section of Tag memory. In order for the Tag to establish its authenticity, it must prove to the Reader that it possess this private key.

- The Reader sends a randomly generated 64 bit string (R) to the Tag.
- The Reader obtains the public key KP_{uAA} stored in biometric Data.
- The Reader verifies the correctness of the signed string using its knowledge of R and KP_{uAA}.

D. Passive Authentication

Passive Authentication is the only mandatory cryptographic protocol in the ICAO. Its primary goal is to allow a Reader to verify that the biometric face data in the e-Passport is authentic. This scheme is known as passive authentication since the Tag performs no processing and is only passively involved in the protocol. One must note that Passive Authentication does not tie the Tag to a passport. The Inspection System retrieves the certificate of the issuing document verifier; using the public key from the certificate it verifies the digital signature and biometric used to sign the biometric face data. Once the validity of the signature is established, the Reader computes the hash of each of these data elements and compares them with the hashed values stored [7].

E. Basic Access Control

The Basic Access Control (BAC) is an optional protocol that tries to ensure that only Readers with physical access to the passport can read Tag data. When a reader attempts to scan the BAC enabled e-Passport, it engages in a protocol which requires the Reader to prove knowledge of a pair of secret keys (called `access keys') that are derived from biometric data on the Machine Readable Zone (MRZ) of the passport. From these keys, a session key which is used for secure messaging is obtained [8].

VI. PUBLIC KEY INFRASTRUCTURE

In normal situations, certificate-issuing organizations known as Certificates Authorities (CA's) are grouped in a trusted hierarchy. All CA's directly or indirectly trust the top-level Root CA. However, in ICAO, when a private key is compromised, the country cannot automatically invalidate all the passports issued with this key. The passport signed by any private key is expected to last for the issuing period. It is not feasible to ask hundreds or even thousands of passport holders to renew their passports every time a key is revoked. Instead, these passports should be used as normal, and a mechanism should notify the custom officials inspect the passport in greater detail. For each country such as the US, there is a Country Signing CA responsible for creating a public/private key pair, which is used to sign the Document Signer Certificates. This key pair should be generated and stored in a highly protected, offline CA infrastructure by the issuing country [5]. The lifetime of a Country Signing CA Key should be the longer of:

- The length of time the key will be used to issue passports
- The lifetime of the passport issued by the key.

To ensure security, the ICAO recommended the countries to replace the CA key every 3-5 years [5]. Under each country, there are numerous passport-issuing offices. Each of them is a Document Signer with a public/private key pair and has a Document Signer Certificate. Each passport is signed by the Document Signer Certificate to ensure data integrity. In order to avoid large amount of passports with invalid keys when a Document Signer Certificate Key is revoked, the suggested lifetime of the key should be about three months, less if the office issue a lot of passports per period of time. If a key or a certificate needs to be revoked, the Country CA must communicate bilaterally to all other countries and to the ICAO Public Key Directory within 48 hours [7]. In addition, a full revocation list should be exchanged every 90 days. All the private keys of Document Signer is stored in the passport-issuing office, where as the public key is stored in the ICAO Public Key Directory. The directory is a central source used to distribute the public key to the participating countries. Each participant country is responsible for downloading the latest version of the keys and making sure passports are indeed signed by the Document Signer.

VII. 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). 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 [9].

- The OSEP protocol provides proof-of-freshness and the authenticity for messages between the participating entities.
- 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.

A. Passport Initial Setup

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

- p is the modulus, a prime number of the order 1024 bits or more.
- q is a prime number in the range of 159 -160 bits.
- g is a generator of order q, where $Ai < q$, $g^i \neq 1$ mod p.
- Each entity has its own public key and private key pair (PK_i,SK_i) where $PK_i = g^{(SK_i)}$ mod 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.

B. Phase One – Inspection System

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 $eP\ \pounds_R\ 1 \le eP \le q - 1$ and computes $K_{eP} = g^{eP}$ 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 K_{eP} and its domain parameters p, q, g.

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

Step 3 (IS) On receiving the response from the e-Passport, the IS generates a random $IS\ \pounds_R\ 1 \le IS \le q - 1$ and computes its part of the session key as $K_{IS} = g^{IS}$ mod 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}.

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

Step 6 (C) On receiving the message from the IS, the e-Passport computes the session key $K_{ePIS} = (K_{IS})^{eP}$. It decrypts the message received using the session key and verifies the signature SDV and $VERIFY_{PKIS} (SIGN_{SKIS} (K_{IS}, p, q, g))$. 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 $K_{ePIS.}$

C. Phase Two - 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 $S_{eP} = SIGN_{SKeP} (MRZ \| K_{ePIS})$ and sends its domain parameter certificate to the IS.

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

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. EXPERIMENTAL RESULTS

Privacy activists in many countries question and protest the lack of information about exactly what the passports' chip will contain, and whether they impact civil liberties. The main problem they point out is that data on the passports can be transferred with wireless technology, which can become a major vulnerability. Although this could allow ID-check computers to obtain a person's information without a physical connection, it may also allow anyone with the necessary equipment to perform the same task. If the personal information and passport numbers on the chip are not encrypted, the information might wind up in the wrong hands. "Nearly every country issuing this passport has a few security experts who are yelling at the top of their lungs and trying to shout out: 'This is not secure. This is not a good idea to use this technology'", citing a specialist who states "It is much too complicated. It is in places done the wrong way round – reading data first, parsing data, interpreting data, then verifying whether it is right. There are lots of technical flaws in it and there are things that have just been forgotten, so it is basically not doing what it is supposed to do. It is supposed to get a higher security level. It is not." and adding that the Future of Identity in the Information Society network's research team has "also come out against the ePassport scheme... [stating that] European governments have forced a document on its citizens that dramatically decreases security and increases the risk of identity theft." Most security measures are designed against untrusted citizens (the "provers"), but the scientific security community recently also addressed the threats from untrustworthy verifiers, such as corrupt governmental organizations, or nations using poorly implemented, unsecure electronic systems.[22] New cryptographic solutions such as private biometrics are being proposed to mitigate threats of mass theft of identity. These are under scientific study, but not yet implemented in biometric passports.

IX. CONCLUSIONS

The work represents an attempt to acknowledge and account for the presence on biometric access control mechanisms in electronic passports towards their improved identification. The application of biometric 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 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. The main cryptographic features and biometrics used with e-passports and considered the surrounding procedures. E-passports may provide valuable experience in how to build more secure and biometric identification platforms in the years to come.

REFERENCES

[1] PHILLIPS, P.J., MARTIN, A., WILSON, C.L. and PRZYBOCKI, M. (2000): An introduction evaluating biometric systems, IEEE Computer 33(2): 56–63.

[2] JUELS, A., MOLNAR, D. and WAGNER, D. (2005): Security and privacy issues in e-passports, in IEEE SecureComm ’05.

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

[4] ICAO Technical report, “biometric passport machine readable travel documents”, ICAO 2010.

[5] CANETTI, R., A., KRAWZYK, H., RABIN, (2009): Authenticating biometric access controls and preserving privacy for a high-assurance smart card, in 8th European Symposium on Research in Computer Security (ESORICS 2003), Lecture Notes in Computer Science, Springer, Norway, 2808: 191–203.

[6] ICAO, “Machine Readable Travel Documents”, Part 1 Machine Readable Passports. ICAO, Fifth Edition, 2003

[7] SCHNEIDER, S. (1997): Verifying authentication protocols with CSP, in 10th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 2–17.

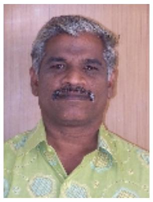
[8] TOM A. KINNGING for ICAO-NTWG, P. T. F.: PKI for machine readable travel documents offering ICC read only access, Technical report. Version I. 2005.

[9] ICAO, “Biometrics Deployment of Machine Readable Travel Documents”, Version 2.0, May 2004.

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 55 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, 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 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.