Online Secure Electronic Passport Scheme using Cryptographic Authentication Protocols and Biometrics Technology

V.K. Narendira Kumar and B. Srinivasan, Department of Information Technology, Gobi Arts & Science College (Autonomous),Gobichettipalayam 638 453, Erode District, Tamil Nadu, India
B. Srinivasan, PG & Research Department of Computer Science, Gobi Arts & Science College (Autonomous), Gobichettipalayam 638 453, Erode District, Tamil Nadu, India

Electronic passports (e-Passports) have known a wide and fast deployment all around the world since the International Civil Aviation Organization (ICAO) the world has adopted standards whereby passports can store biometric identifiers. The purpose of biometric passports is to prevent the illegal entry of traveler into a specific country and limit the use of counterfeit documents by more accurate identification of an individual. The e-passport, as it is sometimes called, represents a bold initiative in the deployment of two new technologies: Cryptography security and multiple biometrics (face, fingerprints, palm prints and iris). A passport contains the important personal information of holder such as photo, name, date of birth and place, nationality, date of issue, date of expiry, authority and so on. The goal of the adoption of the electronic passport is not only to expedite processing at border crossings, but also to increase security. Important in their own right, e-passports are also the harbinger of a wave of next-generation e-passport: several national governments plan to deploy e-passport integrating cryptography algorithm and multiple biometrics. Researchers explore the privacy and security implications of this impending worldwide experiment in multiple biometrics authentication technology. Researcher describes privacy and security issues that apply to e-passports, and then analyze these issues in the context of the International Civil Aviation Organization standard for e-passports. An overall security process that involves people, technology and procedures can overcome limitations of the Cryptography security and multiple biometric technologies.

Categories and Subject Descriptors: COMPUTING [**C.2**] COMPUTER-COMMUNICATION NETWORKS

General Terms: Networking

Additional Key Words and Phrases: Biometrics, E-Passport, Face, Fingerprint, Palmprint, Iris, Recognition, Verification and Database

ACM Reference Format:

V.K. Narendira Kumar and B. Srinivasan, **Receipt-Free Electronic Voting Scheme with Smart Card Using Blind Signature**, *International Journal of Computer Communications and Networks (IJCCN)*, 3(2), pp 1–16, 2013

1. 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 [ICAO 2006].

The International Civil Aviation Organization has adopted a global, harmonized blueprint for the integration of biometric identification information into machine readable passports. The purpose of the

Corresponding Author: V.K. Narendira Kumar, 1Assistant Professor, Department of Information Technology, Gobi Arts Science College (Autonomous), Gobichettipalayam 638 453, Erode District, Tamil Nadu, India *or* kumarmcagobi@yahoo.com

e-ISSN (online) : 2289-3369, ISSN (printed) : 2289-3350

new biometric passports is to prevent the illegal entry of travelers into a specific country and to limit the use of fraudulent documents by more accurate authentication of individuals. This study aims to find out to what extent the integration of biometric identification information into passports will improve their robustness against identity theft.

The International Civil Aviation Organization (ICAO), which plays a major role in setting global travel standards, has adopted a global, harmonized blueprint for the integration of biometric identification information into passports and other machine readable travel documents. The passport requires that a high-capacity contact-less integrated circuit containing a raw image file of the holder's face in addition to other identity information such as name and date of birth be included in the machine readable passports and other travel documents [ICAO 2004].

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 [ICAO 2003].

The integration of multiple biometrics can provide better verification performance than the individual biometrics. Multiple 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 [Jain and Bolle 1999].

1.1 Purpose of the Study

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

1.2 Statement of the Problem

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

2. LITERATURE SURVEY

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

2.1 Technology Evaluation

The technology test evaluates the technology itself: it measures the performance of the matching algorithms under controlled conditions in a laboratory. The purpose of a technology evaluation is to measure the state of the art and to determine the most promising approaches. In a technology evaluation, the algorithms to be tested are given a database of biometric identifiers (e.g. facial and fingerprint images). One part of the database is given to the participants so that they can be familiar with the biometric identifiers in the database and the other part is used for testing. The results from a technology test are repeatable since the technology tests are done under controlled conditions. The products of the technology evaluation are the verification, identification and watch list performance metrics.

2.2 Technical Challenges

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

2.3 Biometric

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

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

2.4 Multiple Biometric Systems

Limitations of unimodal biometric systems can be overcome by using multiple biometric systems. A multiple biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. Such systems are expected to be more reliable due to the presence of multiple, independent pieces of evidence. These systems are also able to meet the strict performance requirements imposed by various applications [Chang 2004].

A multiple system could be, for instance, a combination of fingerprint verification, face recognition, voice verification and smart-card or any other combination of biometrics. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric. For instance, it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject's head. A multiple system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions [Bergman 2005].

2.5 Biometrics in E-Passports

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

2.5.1 *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 [Hesher et al. 2003].

2.5.2 *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 [Barral and Tria 2009].

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

2.5.4 *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 [Daugman 2004].

2.6 Biometric System Modules

Enrollment Unit: The enrollment module registers individuals into the biometric system database. During this phase, a biometric reader scans the individual's biometric characteristic to produce its digital representation. Feature Extraction Unit: This module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual. Matching Unit: This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user's master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one too many matching). Decision Maker: This module accepts or rejects the user based on a security threshold and matching score [Chang 2004].

2.7 Cryptographic

The data stored in the passport is highly confidential; the Contactless IC chip must have mechanisms for protection and integrity of the data. A cryptographic checksum is used to protect data integrity. The system can detect if data has been altered by comparing the checksum in the passport against the real-time computation of the stored data. Symmetric or asymmetric secret keys can be used to ensure data privacy. Passport-issuing countries have the option not to encrypt the data. A digital watermark is used to protect the integrity of facial, fingerprint, palm print and iris image. Some digital bits may be buried into an image for further verification purposes without degrading the quality of the image. Unique IC chip serial numbers are used to prevent cloning of chips. A Public Key Infrastructure (PKI) for generation and management is required.

3. E-PASSPORT SPECIFICATION

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

—Basic Access Control (BAC) protocol (optional): It provides encrypted communication between the chip and the Inspection System (IS).

—Passive Authentication (PA) protocol (mandatory): A border security officer reads and verifies the authenticity of e-passport content stored in the chip.

—Active Authentication (AA) protocol (optional): It provides integrity verification of e-passport's data.

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

—Basic Access Control (BAC) protocol (mandatory): It facilitates the e-passport and the IS to establish an encrypted communication channel.

—Chip Authentication (CA) protocol (mandatory): A mechanism to detect cloned e-Passports.

—Passive Authentication (PA) protocol (mandatory): As in first generation passport standard.

—Terminal authentication (TA): Only if all protocols are completed successfully, the e-passport releases sensitive information like

secondary biometric identifiers. The e-passport performs the collection of protocols as specified in the first generation e-passports, therefore providing backward compatibility [Monar et al. 2005].

4. SECURITY GOALS

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

4.1 Data Confidentiality

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

4.2 Data Integrity

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

4.3 Data Authentication

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

4.4 Non-Repudiation

Non repudiation provides the ability to prove an action or an event that has taken place, such that protocol participants cannot later deny having processed that data. Passport bearer will be physically present at the border security checkpoint. Nevertheless, it would be important to obtain an undeniable biometric data from the e-passport for future processing.

4.5 Mutual Authentication

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

Table I. Passport Logical Data Structure

Data Group	Data Element
DG 1	Document Details
DG 2	Encoded Headshot
DG 3	Encoded Face
DG 4	Encoded Fingerprint
DG 5	Encoded Palmprint
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
SOD	Security Data Element

4.6 Certificate Manipulation

Certificates acts as an off-line assurance from a trusted authority that the certified public key really does belong to the principal who is in possession of corresponding secret key. However, it is the responsibility of the protocol to validate that the corresponding secret key is actually held by the principal claiming ownership of the public key. The e-passport reader should have a guarantee that certificates presented by the e-passport are valid and match the data on the e-passport. ICAO has implemented a PKI which would store signature certificates from issuing state and organizations [Monar et al. 2005].

5. LOGICAL DATA STRUCTURE

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

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.

6. IMPLEMENTATION OF E-PASSPORT SYSTEM

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

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

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

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

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

6.1 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. 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. 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 [Kc and Karger 2005]. 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 [ICAO 2006].

6.2 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. If there is a match, it can be established that the data on the Tag was not manipulated [Kc and Karger 2005].

6.3 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 Tag signs this string using the key KP$_{rAA}$ and sends this signature to the Reader.

—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$_{uAA}$.

6.4 Basic Access Control

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 [Justice 2006].

6.5 Chip Authentication

The Chip Authentication protocol is aims to replace Active Authentication as a mechanism to detect cloned e-Passports. If Chip Authentication is performed successfully it establishes a new pair of encryption and MAC keys to replace BAC derived session keys and enable secure messaging. It does this using the static Diffie-Hellman key agreement protocol. Note that the e-Passport Tag already has a Chip Authentication public key and private key (in secure memory).

6.6 E-Passport Security Properties

By placing a secure sketch of a biometrics on the e-passport, the proposed system has implemented a strong mapping between a passport and its owner. The act of using someone else's passport as your own has now become quite a bit more difficult. Also, the system increases the reliability of a passport without putting any personal data at risk. The passport owner's biometric data is not stored anywhere on the passport. Through the use of cryptography, a secure sketch of a biometric data is all that is needed to regenerate the key that is associated with a person's face, fingerprint, palm print and iris [Klugler 2005].

Very little overhead is placed upon the passport holder. Anyone who is having their passport examined must already present the passport to the person who is performing the check. After implementing the proposed system, the only additional burden will be that the passport holder will need to place his biometric data on biometric scanners for identity verification.

An advantage that using a multiple biometric has over another scheme is that the user is only presenting himself. This is something that the user always has with him and cannot forget at home. There is no need to remember an extra passphrase or physical key. In any case, using biometrics is preferred over either of those two methods because a key or passphrase only prove that you know something that the owner of the passport should know. It does not prove that the passport actually belongs to you.

Since the key is merely the passport holder's biometric there is no need to create a large infrastructure for the scheme that is proposed by this biometric passport system. An example of a large infrastructure would be setting up a secure, replicated database that holds the public and private key pairs of all of the citizens. Another example would involve creating an entirely new form of identification such as "passport" Implementing an entirely new system results in the need for new departments within the government, distribution and adjustment to the new card, and installation costs.

The e-passport system already involves installing passport readers at every passport check station. Implementing the notion of a secure sketch and associated public key requires only that biometric scanners be installed along with the new tag reading units. In addition to the cost of purchasing biometric scanners, there is also the cost of implementing software that will perform the scanning of face and finger prints and the transformations that are necessary for comparing two biometric data scans reliably [Klugler 2005].

7. E-PASSPORT AUTHENTICATE

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

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

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

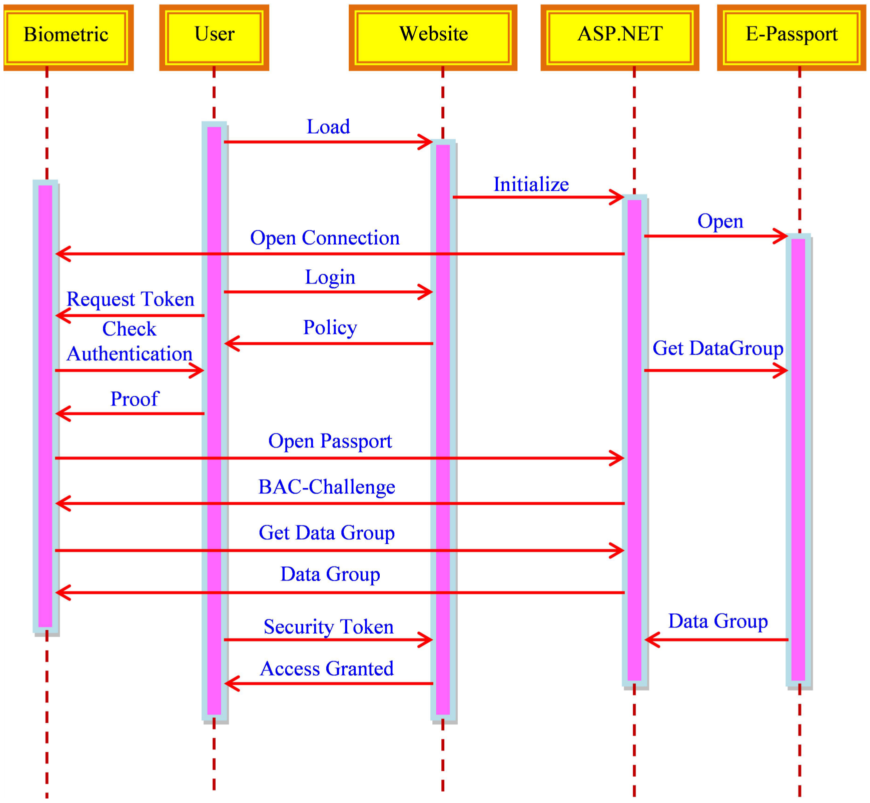

Fig. 1. Message sequence chart of authenticate with e-Passport scenario

the citizen ID). The information in this data group is used in the token created by the identity provider and only the required fields (as requested by the relying party's policy) are sent to the relying party (via the user's client). No other information is sent to the relying party and the relying party needs to trust the identity provider that it has done its job in checking the validity of the user's e-Passport.

8. E-PASSPORT PROTOCOLS

The ICAO e-passport is a complex 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:

—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 [Justice 2006]. In the e-Passport protocol, this authentication protocol was used only when access to biometric data was required.

8.1 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. 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 [Lab 2006].

- 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.

8.2 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 $A_i < q$, $g^i \neq 1$ mod p.
- Each entity has its own public key and private key pair (PK_i,SK_i) where PK_i = $g^{(SK_i)}$ p
- Entity i’s public key (PKi) is certified by its root certification authority (j), and is represented as $\mathrm{CERT}_j(PK_i$, i).
- The public parameters p, q, g used by an e-Passport are also certified by its root certification authority.

8.3 Phase One Inspection System Authentication

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

Step 2 (P) The e-Passport chip then generates a random eP $\pounds_R$ $1 \leq \text{eP} \leq \text{q - 1}$ 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.

$$\text{eP} \rightarrow \text{IS} : \text{K}_{eP}\ , \text{p, q, g}$$

Step 3 (IS) On receiving the response from the e-Passport, the IS generates a random IS $\pounds_R$ $1 \leq \text{IS} \leq$ 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}.

$$\text{S}_{IS} = \text{SIGN}_{SKIS}\ (\text{MRZ} \parallel \text{K}_{eP})$$

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}.

$$\text{IS} \rightarrow \text{DV: ENC}_{PKDV}\ (\text{S}_{IS}, \text{MRZ, K}_{eP}), \text{CERT}_{CVCA}(\text{PK}_{IS}, \text{IS})$$

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.

$$\text{SDV} = \text{SIGN}_{SKDV}\ (\text{MRZ} \parallel \text{K}_{eP} \parallel \text{PK}_{IS}), \text{CERT}_{CVCA}\ (\text{PK}_{DV}, \text{DV})$$

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

$$\text{DV} \rightarrow \text{IS: ENC}_{PKIS}\ (\text{S}_{DV}, [\text{PK}_{eP}])$$

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 $\text{K}_{ePIS} = (\text{K}_{IS})^{eP}$ 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}.

$$\text{IS} \rightarrow \text{eP} : \text{K}_{IS}, \text{SIGN}_{SKIS}\ (\text{K}_{IS}, \text{p, q, g}), \text{ENCK}_{ePIS}\ (\text{S}_{DV},\text{MRZ},\text{K}_{eP}\ )$$

Step 6 C On receiving the message from the IS, the e-Passport computes the session key $\text{K}_{ePIS} = (\text{K}_{IS})^{eP}$. 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}.

8.4 Phase Two - E-Passport Authentication

Step 1 C The IS issues an INTERNAL AUTHENTICATE command to the e-Passport. The e-Passport on receiving the command, the e-Passport creates a signature $\text{S}_{eP} = \text{SIGN}_{SKeP}\ (\text{MRZ} \parallel \text{K}_{ePIS})$ and sends its domain parameter certificate to the IS. The entire message is encrypted using the session key K_{ePIS}.

$$\text{eP} \rightarrow \text{IS} : \text{ENCK}_{ePIS}\ (\text{S}_{eP}\ , \text{CERT}_{DV}\ (\text{PK}_{eP}), \text{CERT}_{DV}\ (\text{p, q, g}))$$

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.

9. EXPERIMENTAL RESULTS

The key application of a biometrics solution is the identity verification problem of physically tying an MRTD holder to the MRTD they are carrying. There are several typical applications for biometrics during the enrolment process of applying for a passport:

The applicant's biometric template(s) generated by the enrolment process can be searched against one or more biometric databases (identification) to determine whether the applicant is known to any of the corresponding systems (for example, holding a passport under a different identity, criminal record, holding a passport from another state).

When the applicant collects the passport (or presents them for any step in the issuance process after the initial application is made and the biometric data is captured) their biometric data can be taken again and verified against the initially captured template The identities of the staff undertaking the enrolment can be verified to confirm they have the authority to perform their assigned tasks. This may include biometric authentication to initiate digital signature of audit logs of various steps in the issuance process, allowing biometrics to link the staff members to those actions for which they are responsible.

Each time traveler (ie. MRTD holders) enters or exit a State, their identities can be verified against the images or templates created at the time their travel documents were issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any Advance Passenger Information (API) system. Ideally, the biometric template or templates should be stored on the travel document along with the image, so that travelers' identities can be verified in locations where access to the central database is unavailable or for jurisdictions where permanent centralized storage of biometric data is unacceptable.

Two-way check - The traveler's current captured biometric image data, and the biometric template from their travel document (or from a central database), can be matched to confirm that the travel document has not been altered.

Three-way check - The traveler's current biometric image data, the image from their travel document, and the image stored in a central database can be matched (via constructing biometric templates of each) to confirm that the travel document has not been altered. This technique matches the person, with their passport; with the database recording the data that was put in that passport at the time it was issued.

Four-way check - A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the 3-way check with the digitized photograph on the Data Page of the traveler's passport.

Besides the enrolment and border security applications of biometrics as manifested in one-to-one and one-to-many matching, States should also have regard to, and set their own criteria, in regard to:

Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint, palm print or iris biometrics on the MRTD as per LDS standards (or on a database accessible to the Receiving State). Given an ICAO-standardized biometric image and/or template, Receiving States must select their own biometric verification software, and determine their own biometric scoring thresholds for identity verification acceptance rates and referral of imposters.

10. 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 multiple 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 multiple 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

Barral and A. Tria. 2009. Fake fingers in fingerprint recognition: Glycerin supersedes gelatin. *In Formal to Practical Security, Springer* (2009).

Bergman. 2005. Multi-biometric match-on-card alliance formed. *Biometric Technology Today* 13 (2005), 6.

Chang. 2004. New multi-biometric approaches for improved person identification. (2004).

John Daugman. 2004. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology* 14 (2004), 21–30.

C. Hesher, A. Srivastava, and G. Erlebacher. 2003. A novel technique for face recognition using range images. In *Proceedings of Seventh International Symposium on Signal Processing and Its Application*.

ICAO. 2003. *Machine Readable Travel Documents*. Part 1 Machine Readable Passports. ICAO, Fifth Edition.

ICAO. 2004. *Biometrics Deployment of Machine Readable Travel Documents*. Technical Report. ICAO.

ICAO. 2006. *Machine readable travel documents*. Technical Report. ICAO.

A. K. Jain and R. Bolle. 1999. Biometrics-personal identification in networked society. (1999).

Home Affairs Justice. 2006. *EU standard specifications for security features and biometrics in passports and travel documents*. Technical Report. European Union.

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

D. Klugler. 2005. *Advance security mechanisms for machine readable travel documents, Technical report*. Technical Report. Federal Office for Information Security (BSI), Germany.

Riscure Security Lab. 2006. *E-passport privacy attack*. Technical Report. at the Cards Asia Singapore.

D. Monar, A. Juels, and D. Wagner. 2005. *Security and privacy issues in e-passports*. Technical Report. Cryptology ePrint Archive.

First Author Profile:

Mr. V.K. NARENDIRA KUMAR M.C.A., M.Phil., Assistant Professor, Department of Information Tech-

nology, Gobi Arts and 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 24 international journal articles. He has authored or co-authored more than 58 technical papers and conference presentations. He is an editorial board member for several scientific 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 and Research Department of Computer Science, Gobi Arts and 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.