I.J. Information Technology and Computer Science, **2013, 03, 79-89**
Published Online February 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2013.03.10

Internet Passport Authentication System Using Multiple Biometric Identification Technology

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

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

Abstract—Electronic passports (e-Passports) 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 paper consider only those passport scenarios whose passport protocols base on public-key cryptography, certificates, and a public key infrastructure without addressing the protocols itself detailed, but this is no strong constraint. Furthermore assume the potential passport applier to use ordinary PCs with Windows or Linux software and an arbitrary connection to the Internet. Technological securities issues are to be found in several dimension, but below paper focus on hardware, software, and infrastructure as some of the most critical issues.

Index Terms—Biometrics, e-Passport, Internet, Face, Iris, palmprint, Fingerprint

I. Introduction

A Passport is a document issued by a government to one of its citizens that provides a means of authenticating the identity and nationality of that citizen. 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 electronic passports have been successfully deployed in many countries around the world. Besides classical "paper" properties, these travel documents are equipped with an electronic chip employing wireless communication interface, so-called RFID chip (Radio Frequency Identification). In addition to the electronic copy of the data printed in the passport (name of the holder, birth date, photo, etc.), the chip may contain e.g. biometric measures of the holder and may employ sophisticated cryptographic techniques providing enhanced security compared to the classical passports. For instance, it should be much harder to copy an electronic passport compared the classical one.

The e-Passports create opportunities for States to enhance global civil aviation safety while at the same time improving the efficiency of aviation operations. The e-Passport can contribute to this because verification of the public key infrastructure certificates associated with e-Passports can provide border control authorities with an assurance that documents are genuine and unaltered, which in turn allows the biometric information contained in e-Passports to be relied on to automate aspects of the border clearance process.

RFID chip has no conductive power contacts that would supply it with the energy, other means from the world of physics have to be borrowed. The power and the communication channels employ the near magnetic field around the reader. For instance, when the chip needs to send information to the reader, it alters this surrounding field which is detected by the reader. Of course, if this modification is not properly filtered, unwanted information about the behavior of the chip may propagate in the surrounding electromagnetic field, as well. This phenomenon is what cryptologists call a side channel.

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. Its goal is to provide foolproof passport identification using a combination of biometrics and cryptographic security.

II. Literature Survey

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

2.1 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 [5].

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 [3].

2.2 Biometrics in passports

Biometrics in e-passports complying with the ICAO specifications now provide for the optional inclusion of an encoded biometric to confirm the holder's identity, or other data to verify the document's authenticity. This makes possible an unprecedented level of document security, offering border control authorities a high level of confidence in the validity of travel documents. A biometric in a machine readable passport will only be able to contain information of the passport holder, and no other additional person. Therefore, this section only covers the vulnerabilities of facial images, fingerprints, palm print and iris images.

2.3 Face Recognition

Face recognition 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].

2.4 Fingerprint Recognition

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].

2.5 Palmprint Recognition

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 [1].

2.6 Iris Recognition

Iris recognition technology is based on the distinctly colored ring surrounding the pupil of the eye. Made from elastic connective tissue, the iris is a very rich source of biometric data, having approximately 266 distinctive characteristics. These include the trabecular meshwork, a tissue that gives the appearance of dividing the iris radically, with striations, rings, furrows, a corona, and freckles. Iris recognition technology uses about 173 of these distinctive characteristics. Iris recognition can be used in both verification and identification systems. Iris recognition systems use a small, high-quality camera to capture a black and white, high-resolution image of the iris. The systems then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system[9].

2.7 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, 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 systemshould balance all these aspects [7].

III. E-Passport PKI Validation

E-Passport validation achieved via the exchange of Public Key Infrastructure (PKI) certificates is essential for the interoperability benefits of e-Passports to be realised.PKI validation does not require or involve any exchange of the personal data of passport holders, and the validation transactions help combat identity fraud. The business case for validating e-Passports is compelling. Border control authorities can confirm that:

- The document held by the traveler was issued by a bonafide authority.
- The biographical and biometric information endorsed in the document at issuance has not subsequently been altered.
- Provided active authentication and / or chip authentication is supported by the e-Passport, the electronic information in the document is not a copy (i.e. clone).
- If the document has been reported lost or has been cancelled, the validation check can help confirm whether the document remains in the hands of the person to whom it was issued.

As a result passport issuing authorities can better engage border control authorities in participating countries in identifying and removing from circulation bogus documents. E-Passport validation is therefore an essential element to capitalize on the investment made by States in developing e-Passports to contribute to improved border security and safer air travel globally. Because the benefits of e-Passport validation are collective, cumulative and universal, the broadest possible implementation of e-Passport validation is desirable [8].

IV. Data Structure

A logical Data Structure (LDS) for e-passports required for global interoperability. It defines the specifications for the standardized organization of data recorded to a contactless integrated circuit capacity expansion technology of an MRP when selected by an issuing state or organization so that the data is accessible by receiving states. This requires the identification of all mandatory and optional Data Elements and a prescriptive ordering and/or grouping of data elements that must be followed to achieve global

interoperability for reading details (Data Elements) recorded in the capacity expansion technology optionally included on an MRP (e-Passport).

Table 1: E-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
SOD	Security Data Element

For interoperability, the e-Passport specifies details on how the data should be stored in the microchip. The data elements are grouped together as a Data Group (DG) and collectively stored in a Logical Data Structure (LDS). The data elements into 19 data groups and the LDS are categorized into two parts:

Mandatory: Data defined by the issuing state or organization contains the details recorded in the Machine Readable Zone (MRZ) that include passport number, passport bearer's name, nationality, date of birth, date of expiry, encoded facial biometric image and a checksum of the individual data elements that are used to derive the session key.

Optional: Data defined by the issuing state or organization, contains optional biometric data for identification, such as, finger prints, palm prints, iris scans, displayed identification data such as a digitized signature and any additional personal or document details, such as contact details, proof of citizenship and endorsements.

The data groups from one to 16 are defined by the issuing state and are writing protected, whereas the data groups for 17 to 19 will be open for write-access to authorized receiving states or organizations. Write-access is not supported in the first generation, but is available in the second generation of e-Passports. The LDS is stored in the microchip using the file system. The dedicated file (DF) in the chip file system hierarchy stores the encryption, the MAC keys used in basic access control protocol and the private key of the e-Passport bearer that is used in active authentication protocol. The elementary file (EF) in the chip hierarchy will store the security object descriptors (SOD) and data groups. The SOD contains the hashes of the LDS data elements digitally signed by the issuing organization (document signer (DS)) and the corresponding certificate. An important security feature is that the data groups are individually hashed and collectively signed by the issuing state and stored in SOD, thus binding the biometric details with the e-Passport bearer details.

The PKI section of the ICAO's e-Passport document makes an important distinction between an issuing state and an issuing organization. The issuing state represents the country of e-Passport origin whereas the issuing organization represents a passport issuing office within a country [6].

V. Implementation of E-Passport System

In order to implement this internet passport authentication system using multiple biometric identification 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:

Biometric authentication is the process of determining the authenticity of a user based on the user's credentials. Whenever a user logs on to an application, the user is first authenticated and then authorized. The application's web.config file contains all of the configuration settings for an ASP.NET application. It is the job of the authentication provider to verify the credentials of the user and decide whether a particular request should be considered authenticated or not. A biometric authentication provider is used to prove the identity of the users in a system. ASP.NET provides three ways to authenticate a user:

Forms Authentication: This authentication mode is based on cookies where the user name and the password are stored either in a text file or the database. After a user is authenticated, the user's credentials are stored in a cookie for use in that session. When the user has not logged in and requests for a page that is insecure, he or she is redirected to the login page of the application. Forms authentication supports both session and persistent cookies.

Windows Authentication: This is the default authentication mode in ASP.NET. Using this mode, a user is authenticated based on his/her Windows account. Windows Authentication can be used only in an intranet environment where the administrator has full control over the users in the network.

Passport Authentication: Passport authentication is a centralized authentication service that uses Microsoft's Passport Service to authenticate the users of an application. It allows the users to create a single sign-in

name and password to access any site that has implemented the Passport single sign-in (SSI) service.

Authorization is the process of determining the accessibility to a resource for a previously authenticated user. Note that authorization can only work with authenticated users, hence ensuring that no un-authenticated user can access the application. The default authentication mode is anonymous authentication.

5.1 Passport Authentication in Win HTTP

Microsoft Windows HTTP Services (Win HTTP) fully support the client side use of the Passport authentication protocol. It provides an overview of the transactions involved in Passport authentication and how to handle them. Win HTTP provides platform support for e-Passport by implementing the client-side protocol for Passport authentication. It frees applications from the details of interacting with the Passport infrastructure and the Stored User Names, Passwords and biometric identification. The following figure 1 shows overview of Authentication works.

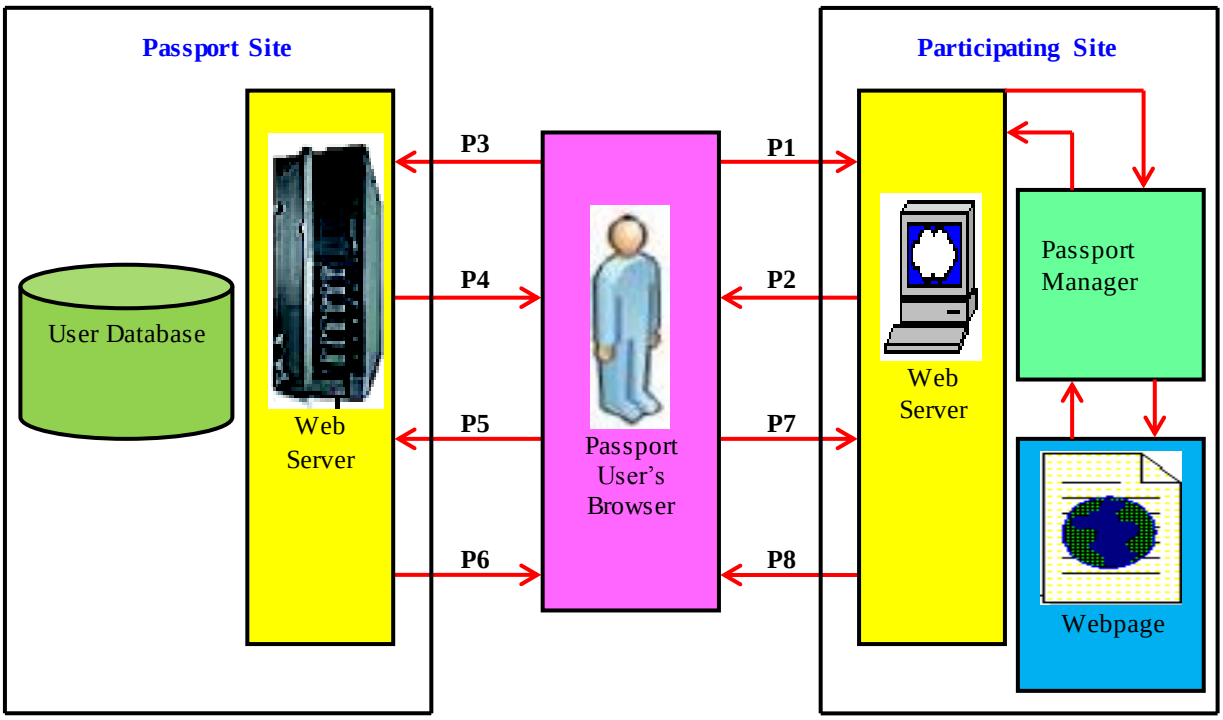

Fig. 1: Overview of Passport Authentication

5.2 Passport Single Sign-In

Passport allows users to create a single sign-in name, password and biometric identification to access passport site that has implemented the Passport single sign-in (SSI) service. By implementing the Passport SSI, it won't have to implement user-authentication mechanism. Users authenticate with the SSI, which passes their identities to passport site securely. Although passport authenticates users, it doesn't grant or deny access to individual sites i.e. Passport does only authentication not authorization. Passport simply tells a participating site who the user is. Each site must implement its own access-control mechanisms based on the user's Passport User ID (PUID).

P1→ Initial Page request,

P2→ Redirect for authentication,

P3→ Authentication request sign-in page,

P4→ Sign-in page,

P5→ User credentials,

P6→ Update website cookies and redirect,

P7→ Encrypted authentication query string,

P8→ Site cookies and requested web page.

First user requests any page from his web server. Since user is not authenticated, passport web server redirects its request for authentication with Sign-In logo. When user presses Sign-In button, request will go to Passport server for Sign-In page. Once the Sign-In page comes to browser, user will enter his authentication details like Passport ID, Password and biometric identification. When user credentials are submitted, Credentials are validated in Passport server. Then Cookies are created in server and response is send to the browser with encrypted query string. Now both cookies and query string is having details about authentication. Once user is authenticating, he will be taken to page which is requested first. The following figure 2 shows Passport Application Chain.

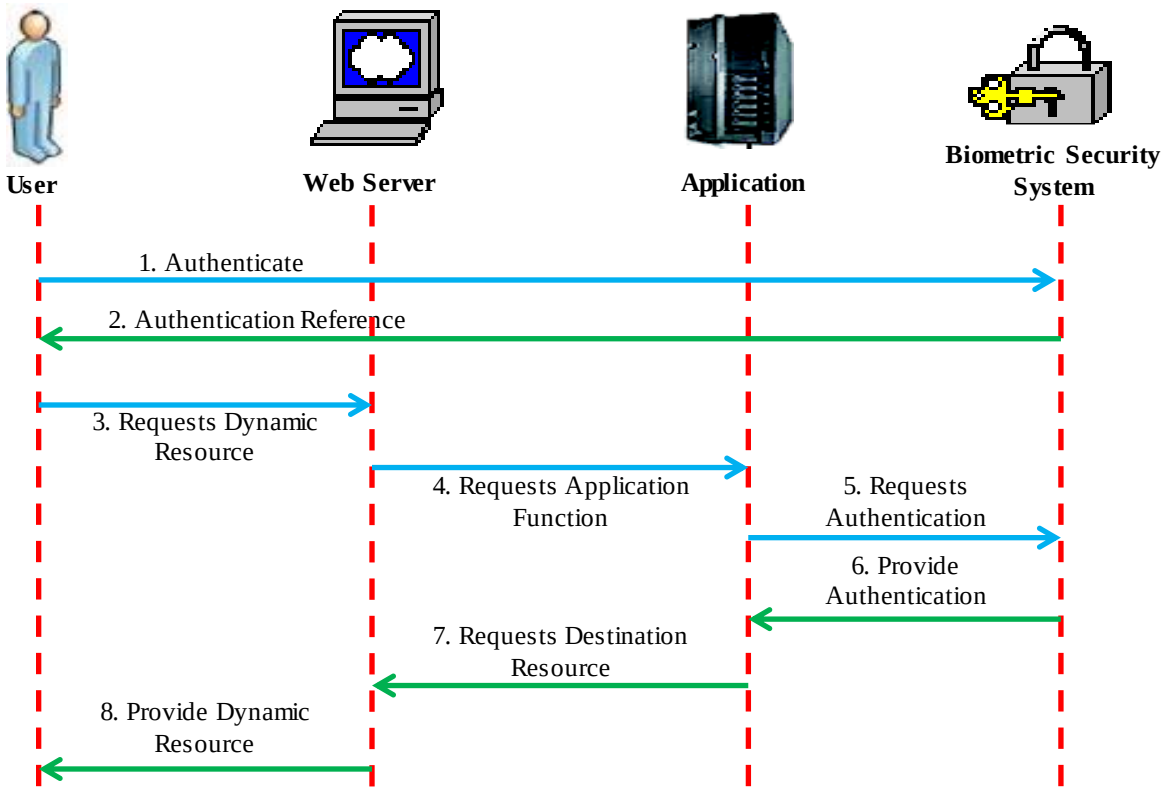

Fig. 2: Passport Application Chain

1. Web user authenticates with enterprise security system(authentication can be through Web server)
2. Enterprise security system provides an authentication reference to Web user
3. Web user requests a dynamic resource from Web server, providing authentication reference
4. Web server requests application function from application on behalf of Web user, providing Web user's authentication reference
5. Application requests authentication document from enterprise security system, corresponding to Web user's authentication reference
6. Enterprise security system provides authentication document, including authorization attributes for the Web user, and authentication event description
7. Application performs application function for Web server
8. Web server generates dynamic resource for Web user

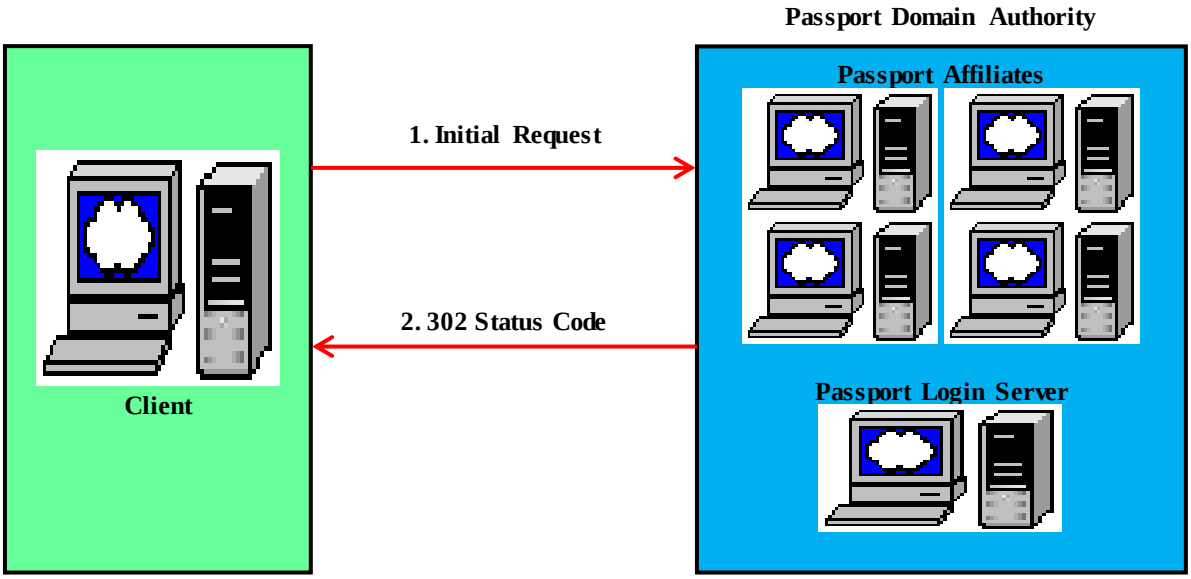

Fig. 3: The initial request to a Passport affiliate

5.3 Initial Request

When a client requests a resource on a server that requires Passport authentication, the server checks the request for the presence of *tickets*. If a valid ticket is sent with the request, the server responds with the requested resource. If the ticket does not exist on the client, the server responds with a 302 status code. The response includes the challenge header, "WWW-Authenticate: Passport". Clients that are not using Passport can follow the redirection to the Passport login server. More advanced clients typically contact the Passport nexus to determine the location of the Passport login server. The following figure 3 shows the initial request to a Passport affiliate.

Central to the Passport network is the Passport *Nexus*, which facilitates synchronization of Passport participant sites to assure that each site has the latest details on network configuration and other issues. Each Passport component (Passport Manager, Login servers, Update servers, and so on) periodically communicates with the Nexus to retrieve the information it needs to locate, and properly communicate with, the other components in the Passport network. This information is retrieved as an XML document called a Component Configuration Document, or CCD.

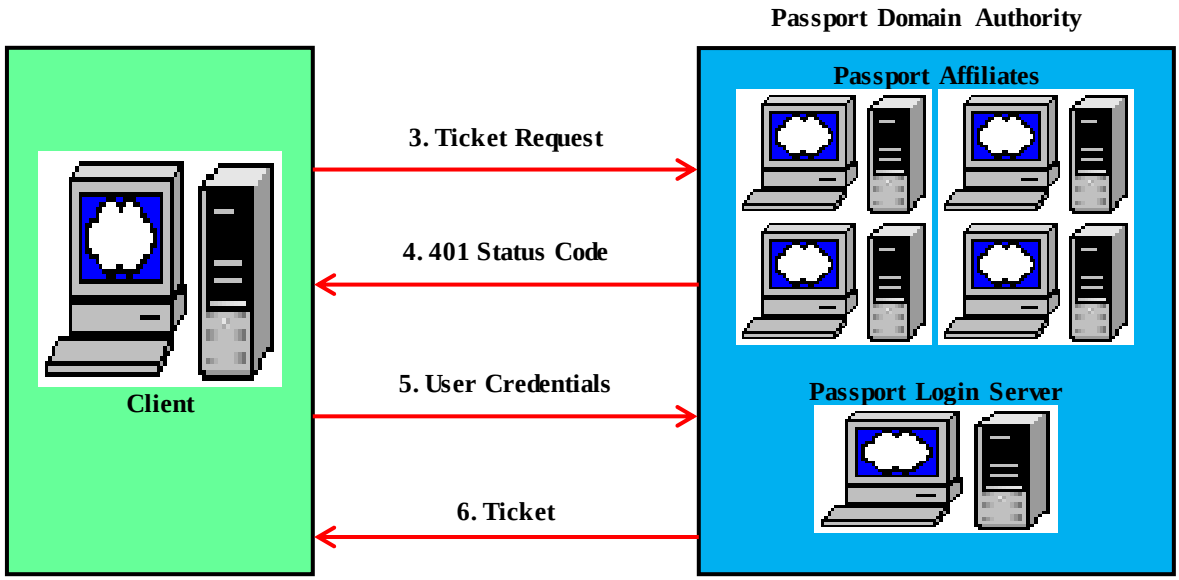

Fig. 4: A client ticket request to a Passport login server

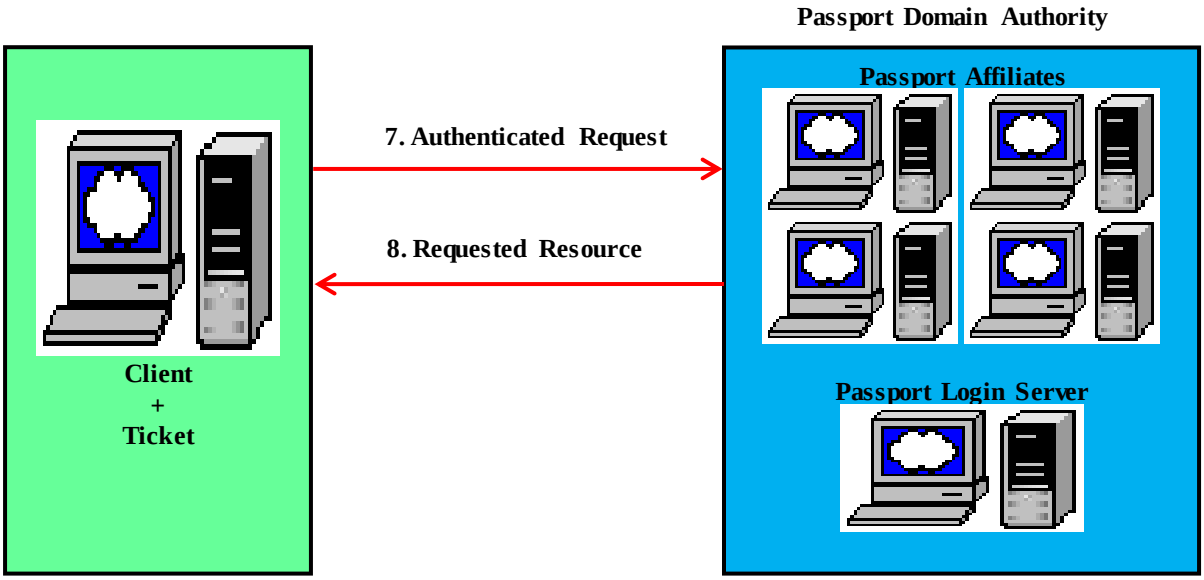

Fig. 5: An authenticated request to the Passport login server

5.4 Passport Login Server

The figure 4 shows the passport login server to a Passport affiliate. A Passport login server handles all requests for tickets for any resource in a Passport domain authority. Before a request can be authenticated using Passport, the client application must contact the login server to obtain the appropriate tickets. When a

client requests tickets from a Passport login server, the login server typically responds with a 401 status code to indicate that user credentials must be provided. When these credentials are provided, the login server responds with the tickets required to access the specified resource on the server that contains the originally requested resource. The login server can also redirect the client to another server that can provide the requested resource.

5.5 Authenticated Request

When the client has the tickets that correspond to a given server, those tickets are included with all requests to that server. If the tickets have not been modified since they were retrieved from the Passport login server, and the tickets are valid for the resource server, the resource server sends a response that includes both the requested resource and cookies that indicate that the user is authenticated for future requests. The following figure 5 shows an authenticated request to the Passport login server.

The additional cookies in the response are intended to speed the authentication process. Additional requests in the same session for resources on servers in the same Passport Domain Authority all include these additional cookies. Credentials do not need to be sent to the login server again until the cookies expire.

5.6 Passport in Win HTTP

Win HTTP handles many of the transaction details internally for Passport authentication. During the initial request, the server responds with a 302 status code when authentication is necessary. The 302 status code actually indicates a redirection and is part of the Passport protocol for backwards compatibility. Win HTTP hides the 302 status code and contacts the Passport nexus, and then the login server. The Win HTTP application is notified of the 401 status code sent by the login server to request user credentials. To the application, however, it appears as if the 401 status originates from the server from which the resource was requested. In this way, the Win HTTP application is unaware of interactions with other servers, and it can handle Passport authentication with the same code that handles other authentication schemes.

Typically, a Win HTTP application responds to a 401 status code by supplying authentication credentials. When credentials are supplied with WinHttpSetCredentials or SetCredentials for passport authentication, the credentials are actually being sent to the login server, not to the server indicated in the request. Once retrieved, tickets are managed internally and are automatically sent to applicable servers in future requests.

Win HTTP can successfully complete the Passport authentication even if an application disables auto redirection. However, after the Passport authentication is complete, an implicit redirect must occur from the Passport login server URL back to the original URL. If an application has disabled automatic redirection, Win HTTP requires that the application give Win HTTP "permission" to redirect automatically in this special case.

VI. Internet 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.

6.1 Internet 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.

6.2 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 $eP \in_R 1 \leq eP \leq q - 1$ 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* $\pounds_R$ $1 \leq IS \leq q - 1$ 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}.

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

6.3 Phase Two – Internet 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. 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.

VII. 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 (i.e. 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.

VIII. Conclusions

The work represents an attempt to acknowledge and account for the presence on internet passport authentication system using multiple biometrics using face, fingerprint, palmprint and iris recognition 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] A. K. Jain, R. Bolle, *"Biometric personal identification in networked society"* 1999, Norwell, MA: Kluwer.

[2] 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.

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

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

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

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

[7] Riscure Security Lab, *"E-passport privacy attack"*, at the Cards Asia Singapore, April 2006.

[8] D. Monar, A. Juels, and D. Wagner, "*Security and privacy issues in e-passports"*, Cryptology ePrint Archive, Report 2005/095, 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 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.

How to cite this paper: V.K. Narendira Kumar, B. Srinivasan,"Internet Passport Authentication System Using Multiple Biometric Identification Technology", International Journal of Information Technology and Computer Science(IJITCS), vol.5, no.3, pp.79-89, 2013.DOI: 10.5815/ijitcs.2013.03.10

