01 Jan 2007

The Electronic Passport and the Future of Government-Issued RFID-Based Identification

G. Matthew Ezovski

Steve Eugene Watkins
Missouri University of Science and Technology, watkins@mst.edu

2007 IEEE International Conference on RFID
Gaylord Texan Resort, Grapevine, TX, USA
March 26-28, 2007

The Electronic Passport and the Future of Government-Issued RFID-Based Identification

G. Matthew Ezovski, *Student Member, IEEE*, and Steve E. Watkins, *Senior Member, IEEE*

Abstract — **Passports and other identification documents may be enhanced using recent advancements in technology. Various national and international bodies are pursuing machine-readable approaches with biometric information. In particular, the International Civil Aviation Organization (ICAO) has adopted standards whereby passports can store biometric identifiers. Countries that participate in the Visa Waiver Program (VWP) began issuing electronic passports in 2006. However, the selection of technologies remains questionable due to privacy and security concerns. This paper examines policy regarding these electronic approaches and developments toward electronic data storage and transmission. Radio-frequency identification (RFID) devices for electronic passports and other existing identity documents are discussed.**

Keywords — **Electronic Passport, Biometrics, RFID.**

I. Introduction

Travel among countries and security concerns are driving efforts to improve the identification and passport documents. The international community is debating policy and technologies regarding electronic approaches such as radio-frequency identification (RFID) devices. To facilitate travel, the twenty-seven member nations participating in the Visa Waiver Program (VWP) require standardized passport documents [1] based on standards determined by the International Civil Aviation organization (ICAO). The threat of terrorism increases the need for positive identification and anti-counterfeiting. The challenge facing immigration officials today is simple: How do they know that the person carrying the passport is actually the rightful owner of the passport? A 2" X 2" photograph of the owner only provides so many clues as to the answer to this question and photographic means have security limitations. Considering that all of the 9/11 hijackers immigrated or traveled to the U.S. from other countries, it is of the utmost importance to the security of this country that homeland security and immigration officials be confident that they know who is entering and exiting the country. Current passports contain biographical information, photographs, and anti-counterfeiting features like words in invisible ink that are only visible under ultraviolet light.

To help answer this important question, the U.S. Congress began requiring that all countries participating in the Visa Waiver Program, issue a technologically-enhanced passport based on international standards, including contactless smart chips. This new travel document contains electronically stored personal information, along with a digital photograph of the person to whom the passport was issued. The digital picture allows immigration officers to perform biometric comparisons of the individual requesting entry into the United States with the stored picture to determine if the person is the rightful owner of the passport. The U.S. required that all member countries of the VWP began issuing electronic passports by October 2006. The State Department also began issuing small numbers of electronic passports to U.S. diplomats and associated personnel in early 2006, and public issuance has gradually increased beginning in August 2006. International standards are included in the International Civil Aviation Organization Document 9303.

This work examines the role of contactless integrated circuit (IC) technology, commonly referred to as RFID, and other technologies for existing and potential impact on electronic passports. Various efforts are underway to modernize many U.S. identity documents, both political and technical.. Policy discussion includes privacy concerns and the selection of secure technologies. In particular, we discuss how RFID technologies have advantages and disadvantages for electronic passports and other identification documents.

II. Electronic Identity Documents

A. Overview of U.S. Passport and VWP Program

The most commonly used method of establishing identity and citizenship for use in international travel is the passport. Of the numerous passports in the world, a United States passport is often considered the "holy grail" of travel documents, widely respected and accepted by virtually all nations. In 2004 nearly nine million U.S. passports were issued [2]. The U.S. Department of State, in conjunction

Manuscript received January 26, 2007. This work was indirectly supported by the U.S. Department of Homeland Security through the Homeland Security Scholarship and Fellowship Program and by the IEEE-USA through the Washington Internships for Students of Engineering (WISE) Program.

G. Matthew Ezovski is with the Adaptive Communications and Signal Processing Group in the School of Electrical and Computer Engineering at Cornell University, Ithaca, NY 14850 USA (phone: 607-254-8816; e-mail: gme8@cornell.edu).

Steve E. Watkins is with the Department of Electrical and Computer Engineering at the University of Missouri-Rolla, Rolla, MO 65409 USA (phone: 573-341-6321; e-mail: steve.e.watkins@ieee.org).

with the Department of Homeland Security (DHS), began issuing a redesigned passport with incorporated technology to defend against misuse and fraudulent reproduction in limited numbers to U.S. citizens on August 14, 2006.

Nations also often require certain visitors to apply for a visa or official authorization from the government in order to enter. Several western European nations, some south Pacific nations, Japan, and the United States participate in the Visa Waiver Program, which allows travelers from any member country to travel to another member country for up to 90 days without obtaining a visa. Established in 1986, the program aims to improve international travel by "promoting better relations with U.S. allies, eliminating unnecessary barriers to travel, stimulating the tourism industry, and permitting the Department of State to focus consular resources in other areas" [1]. VWP countries generally follow the guidance of the International Civil Aviation Organization (ICAO), an arm of the United Nations, with respect to passport design and often take part in the body's decision-making process [3].

B. Political Timeline for Biometric/Electronic Passports

The 9/11 attacks on the U.S. pushed national security to the forefront of American politics. As the U.S. began its invasion of Afghanistan and assault on the ruling Taliban regime, Congress and the executive branch searched for holes in the nation's intelligence and security infrastructure. Simultaneously with its pursuit of the Patriot Act, the federal government sought both policy and technology-based solutions to the porous border issue. The Enhanced Border Security and Visa Entry Reform Act of 2002 set, among numerous other items, "technology standard and interoperability requirements respecting development and implementation of the integrated entry and exit data system and related tamper-resistant, machine-readable documents containing biometric identifiers" (including October 26, 2004 implementation deadlines) [4]. Sponsored by Rep. James Sensenbrenner (R-Wisc.), House Judiciary Committee chairman, the legislation called for total compliance with ICAO standards for electronic/biometric passports by VWP countries. The law did not specify which revision of the standards needed to be complied with, leading to some recent confusion over what requirements VWP countries needed to meet.

C. Other Federal Government Identity Documents

Numerous recent deployments of technology-based identity documents have taken place under the auspices of government agencies other than the State Department, and more are likely to occur in the near future. In fact, the lack of a government-wide standard for identity documents has been greatly criticized.

Perhaps the most notable recent deployment of identity documents was initiated by the Department of Defense and applies to all military and civilian personnel. Approved in 2001, the Common Access Card (CAC) is now the main form of identification used by Defense employees, serving as the primary indicator of authority to enter U.S. military bases and allowing authorized users to access classified and unclassified computer resources. All CAC's contain a contact IC smart chip, as compared to the contactless RFID, which stores credentials and authentication information [5]. The contact chip requires the user to remove the card and slide it into a reader in order to access the digitally signed and encrypted stored personal information. The CAC also features one-dimensional and two-dimensional barcodes for quicker access to basic, unprotected information.

On the other hand, the Department of Health and Human Services and the Treasury Department are known to use RFID technology for internal access control purposes [6].

TABLE I
IMPLEMENTED STATE LICENSE TECHNOLOGIES

Technology	Number of State Implementations
Magnetic Stripe	21
1-D Barcode	21
2-D Barcode	45
None	1

Summary of technologies used to validate and verify driver's licenses in all 50 states. Some states use more than one technology [7].

D. State-Issued Driver's Licenses and Real ID

The most common form of identification used in the United States is the state-issued driver's license. Each state has its own design, with most currently in circulation having some embedded technology for the purpose of verification or guarding against counterfeit documents. Informal agreements exist for standardization of these identity documents, but no overarching standard currently exists. Table I indicates the current deployment of widely used driver's license technologies by specific technology.

An upcoming potential technology deployment which has garnered substantial attention from politicians and privacy advocates is the implementation of the Real ID Act of 2005. Passed in May 2005 as part of an emergency supplemental appropriations bill for the ongoing war in Iraq, the law calls for interoperability of state driver's license databases, along with a "common machine-readable technology" for all driver's licenses issued nationwide [8]. Nothing in the law dictates what that technology will be, what it will store, or if it can be used to store biometric data. The Department of Homeland Security is charged with determining the standards for these newly revised licenses, and the law specifies 2008 as the year when the DHS-specified standards will go into effect.

Fig. 1. An Australian passport data page with visible machine readable zone (MRZ) on the lower portion [9]

III. Electronic Passport ICAO Standards Development

A. Changes to Passport Design

The first major requirement instituted by the ICAO and subsequently by the United States was the inclusion of a machine-readable zone (MRZ) on the passport. Through the use of optical character recognition hardware and software, a computer can read and capture the data printed in the MRZ, eliminating the need for an immigration or customs officer to manually enter and confirm a portion of the data contained on the passport. The MRZ is the lower two lines of text on the document in Fig. 1.

Beginning on June 26, 2005, all VWP travelers entering the United States were required to possess a passport with an MRZ [10]. The use of standard placement and data formatting, as established by the ICAO, has allowed for relatively uniform dispersion of this technology.

While inclusion of the MRZ sped up passport processing, it did little to improve the document's inherent security. The practice of removing a passport holder's picture and replacing it with another, however, has garnered much attention as a potentially simple means of committing passport fraud. To guard against this security flaw, the U.S. has required that passports from VWP countries all contain what the State Department calls a "digital photograph" on the data page. While there is nothing digital about the printed picture itself, the fact that it is printed directly onto the data page, rather than being subsequently attached, guards against fraud. U.S. passports have contained these digital photographs for several years, and under new Department of Homeland Security guidelines, all VWP countries were required to produce similarly protected passports by October 26, 2005, in order for their passports to continue to be accepted at American points of entry.

B. The Move to Biometric Technologies

Beginning in 1980 the ICAO looked to emerging technologies to enhance the security of passports and identity documents, and in 1999 its Technical Advisory Group on Machine Readable Travel Documents (MRTD) began investigating "the compatibility of currently available biometric technologies with the issuance and inspection processes relevant to MRTDs." [11] According to the Biometric Consortium, "Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic." [12] Many of the earliest uses of primitive biometrics technology focused on identification of criminals. In 1903 the New York state prison system began using fingerprints to identify criminals, and in 1921 Congress established the Identification Division of the Federal Bureau of Investigation [13].

The ICAO's New Technologies Working Group (NTWG) looked to biometric comparisons as a more conclusive means of authenticating documents, both through comparing printed data to electronic data and comparing stored biometric data against samples from the individual attempting to use the passport. The overriding concern was confirming that the holder of the passport was actually the rightful owner of the document. In February 2002, the NTWG endorsed facial feature, fingerprint, and iris recognition technologies as applicable to machine-readable travel documents (MRTDs). Subsequently, in Berlin in June 2002, the NTWG endorsed the "use of face recognition as the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents," leaving iris and fingerprint technologies as optional additions [14].

C. Data Storage Technologies

One of the greatest challenges facing the ICAO was the selection of a technology for storing biometric and other data onboard the passport. The generally accepted technologies included two-dimensional bar codes, contact integrated circuit (IC) chips, contactless IC chips, and optical memory. Each technology has its advantages and drawbacks. Several guidelines were used in determining a standard [15].

- Non-proprietary technology was required.
- "Document integrity" needed to be maintained.
- Stored data needed to be easily accessible.
- Quick transmission times were preferred.
- Memory needed to support in excess of 20 KB of storage on one chip or equivalent.

Two-dimensional bar code technology did not meet the image file storage space requirement, and was eliminated from consideration on most other counts as well. Contactless IC chips showed shorter transmission times than contact chips and also assisted the ICAO's goal of making it easy to access the stored data, since they can be electronically read in any orientation as long as they are

within range of the chip reader. As a result, the ICAO stated in its March 21, 2003 New Orleans Resolution,

> *Member States, in their initial deployment of MRTDs with biometrics identifiers, are encouraged to adopt Contactless IC media of sufficient capacity to facilitate on-board storage of additional MRTD data and biometric identifiers* [15].

According to the main ICAO technical specification for biometric passports, Document 9303, all of the data currently printed on the data page of the passport must be stored on the IC chip. This includes the photograph, which will be used for biometric comparisons. The Logical Data Structure, specified in Document 9303, provides a comprehensive architecture for storing this information, along with additional optional information an individual country might choose to include either for added security or to allow the document to serve purposes other than those normally attributed to the passport [16].

The ICAO has included digital signature protection based on the public key infrastructure (PKI) to help authorities confirm that the data stored on a passport's RFID chip had not been modified. A digital signature is a hash table created using a publicly available key. This table can be compared with the stored data to determine if it has been modified. A skilled computer scientist, given access to the key used to assemble the hash table, could modify the signature to show that the stored data is accurate even if it is not [17].

D. Required Implementation Schedule

The deadlines for U.S. implementation of biometric passports, as well as implementation by other VWP countries, were delayed several times, with the final American deadline being October 26, 2006, for facial images stored on a contactless IC chip. DHS policy at that time indicated that the United States would stop accepting passports under the Visa Waiver Program from individuals who were citizens of countries which had not begun issuing electronic passports by that date [10].

IV. Security Obstacles

A. Skimming

Among the greatest concerns of security and privacy watchdog groups is the idea that an unscrupulous individual could "skim," or secretly steal from a distance, the data stored on an electronic passport or other identity document's RFID chip. While it is unclear what purpose this might serve, Americans have learned through the rise in identity theft that they must keep personal information as close as possible. ICAO and International Organization for Standardization (ISO) standards set a maximum of 10 cm on the distance from which the data can be read, but this limit is likely to have little effect in practice, as explained later in this section [15].

Groups including the American Civil Liberties Union (ACLU) and Privacy International have questioned the use of contactless chips instead of comparable contact-based chips. They feared a combination of identity theft and surveillance, both of which they believe could have been avoided through the use of other data storage technologies. At that time Privacy International indicated that it was "increasingly concerned that the biometric travel document initiative is part and parcel of a larger surveillance infrastructure monitoring the movement of individuals globally that includes Passenger-Name Record transfers, API systems and the creation of an intergovernmental network of interoperable electronic data systems to facilitate access to each country's law enforcement and intelligence information" [18].

Passive RFID chips, instead of requiring batteries for power, are powered by the magnetic field emitted from the reader. The passport does not broadcast its own signal; rather, it reflects a modified version of the signal sent by the reader in order to communicate.

The distance from which the chip can be read is a function of the power of the field generated by the reader, in conjunction with the physical parameters of the RFID chip. It is not a limit that can be completely set through modifications to the chip itself. Studies have shown that the data on some of the early prototype electronic passports can be read using specialized readers from over 30 feet away. The equipment necessary to achieve this, however, cannot at this time be carried or operated discretely [19]. Generally, an increase in the power of the reader can increase the distance from which the chip can be read without the chip knowing the difference. FCC standards prohibit signals from exceeding certain power levels (generally due to health concerns, e.g., cell phones), and often prohibit the production of devices which could deviate from the standard [20]. There is no assurance, however, that an individual or organization trying to gain unauthorized access to another's passport would choose to operate within such boundaries.

B. Basic Access Control

Basic access control (BAC) causes the RFID chip itself to prevent access by unauthorized readers. In order for a reader to access an electronic passport with basic access control, it would have to already know the individual key for that particular chip. ICAO standards for basic access control focus on using a piece of passport-holder data from the printed data page's MRZ as the key for accessing the chip. An incorrect key would result in a denial of access. The standards specify a combination of the individual passport

number and personal information as the key [21].

ICAO standards do not currently require basic access control, but rather recommend it along with other privacy and security enhancements. The U.S. State Department, after substantial public input and outcry over an initial decision to not use BAC, opted to implement it on American passports to protect against unauthorized access.

C. Transmission Encryption

Another potential privacy concern exists during the transmission of data between the chip and the reader. Just like with any wired or wireless communication, there is always the danger of an unauthorized user "snooping," or listening in, on the transmission. A number of different techniques can be employed to encrypt data. Most depend on either a public key, which is a password held by all those authorized to access the data, or a private key, which is created and used for that specific transaction. The ICAO has developed an interface which employs a public/private key encryption scheme, using the information printed on the data page of the passport to produce a key, in particular from the MRZ. Encrypted transmission would commence immediately following basic access control authentication. The widely-recognized industry standard in electronic data transmission is 128-bit Secure Socket Layer technology [22].

D. Faraday Cage

The State Department has recognized that security of the data stored on the chip is an essential piece of the research and development challenge for the electronic passport. This is especially important given the possibility that future revisions of the passport may include additional, less publicly available biometric information like iris or fingerprint scans using the data structure using Document 9303's data structure which could be harmfully used against the rightful owner. In 2005, under continued pressure from privacy groups and Congress, State opted to control access through the use of a Faraday cage, implemented by integrating thin metal fibers into the passport cover [21]. The basic principle of a Faraday cage is that by encasing an object in metal, any electric or magnetic fields, such as the ones used to communicate with and power an RFID chip, can be prevented from passing through to the object. Such protection would theoretically prevent reading of the passport without the cover being physically opened. Increases in the power of the reader field could theoretically "break through" the cage, but it provides an additional layer of security at minimal cost.

V. Efficacy of Passport Revisions

A. Biometric Issues

Questions remain regarding the usefulness of the electronic passport as currently implemented in the United States, though many questions regarding privacy and security have been addressed to the satisfaction of outside interest groups. Transmission and chip speed has proven to be a substantial issue. Also, many have questioned the decision by the State Department to focus solely on facial recognition as a biometric feature of the passport [23].

The ICAO's decision to choose facial recognition as the universal biometric for authenticating passports has also drawn fire from a number of directions. In terms of the scientific community, the National Institute of Standards and Technology (NIST) noted in 2002 the technological superiority of ten-finger fingerprint recognition over most biometrics, including facial recognition [24]. This superiority is shown in Table II,

Congress has also questioned the ICAO's selection of facial recognition, with Congressman Christopher Cox (R-Cal.), past chairman of the House Homeland Security Committee, insisting that a photograph is not a biometric. According to him, fingerprints are a more effective technology. "We should move in the direction of that biometric that is most likely to keep us safe," he indicated during a hearing in early July 2005 [24].

Despite some Congressional disagreement, the State Department continues to insist that Americans would not support a fingerprint-based travel document, given the popular association of fingerprints with criminal activity. Fingerprints are also a cornerstone of the US-VISIT program, though this program does not affect U.S. citizens [25].

Just like any technology, the range of international interest in biometrics includes a complete lack thereof in some countries, as well as daily life implementation in other countries. Despite some resistance to the U.S.-established timeframe for implementation of the Document 9303-compliant passport in all VWP countries, the European Commission endorsed the move to include biometric technologies in its passports. On October 26, 2004, the EU Justice and Home Affairs Council also voted to include fingerprints as a second mandatory identifier in future passports issued by EU members [26].

Debates over the use of biometrics in national identification cards recently center stage in the United Kingdom, with Prime Minister Tony Blair's Labour Party pushing for a biometrically-enhanced national identification card. The British government, looking to capitalize on the research investments made by the ICAO and VWP countries in passport technology, publicly announced its intent to pursue national identification card legislation in late 2004. According to the British Home Office, "The scheme will

TABLE II
ACCURACY OF SELECTED BIOMETRICS

Biometric	Accuracy Percentage	False Positive Rate
Two-finger fingerprint (with all fingerprints taken by experienced officers)	99.6%	1 out of 1000
Face Recognition (with controlled lighting)	90%	1 out of 100
Face Recognition (with uncontrolled lighting)	54%	Unknown

Analysis of the accuracy of biometrics used by some countries in conjunction with the electronic passport, as conducted by NIST in 2002 [24].

provide a simple and secure 'gold standard' for proving identity, protecting people from identity fraud and theft and providing them with a convenient means of verifying their identity in everyday transactions." Public research conducted between July 2002 and January 2003, showed that 79 percent of British respondents favored the introduction of identity cards with technology similar to that of the ICAO-defined electronic passport [27].

B. *Addressing Security Concerns*

Despite the apparent effectiveness of the techniques for maintaining document described in section IV, more subtle concerns have continued to emerge regarding finer details of the integrity of the electronic passport and similar RFID-based identity documents. Techniques like basic access control and the Faraday cage have made it very difficult to track or access identity document data when implemented and have allayed many fears regarding surveillance and identity theft.

One widely-noted outstanding concern relates to the ISO 14443 standard's collision avoidance / medium access control features. Chips designed under the standard's type A specification broadcast a unique identifier which is then received by the tag reader. The reader then uses these identifiers to select tags to broadcast at particular times. Type B devices instead use the slotted aloha MAC protocol, which potentially requires more transmissions and delays transaction completion [14].

The type A scheme could potentially result in a trackable, open-access, unencrypted identifier if not chosen dynamically, even on a chip which uses basic access control. The type B scheme can pose a challenge in certain application environments, however, as it requires more advanced clock function than type A. Document 9303 allows either type A or type B contactless IC's in electronic passports [14].

C. *Rollout Success*

Progress toward deployment of ISO 14443 and ICAO Document 9303-compliant passports varies greatly between member EU member states. Had the U.S. Department of Homeland Security not granted the extension to October 2006, only six European Union members – Austria, Belgium, Finland, Germany, Luxembourg, and Sweden – had a chance of meeting the original 2005 deadline. Once the final deadline was reached, only three countries—Andorra, Brunei, and Liechtenstein—had not begun issuing the electronic passport [28].

VI. RFID'S IMPACT

A. *Electronic Passport*

RFID has opened the door to new opportunities in identity and travel documents, though much of its promise remains out of reach in the interest of privacy and security. With the electronic passport specification as a basis, future licenses and identification cards can be built off of contactless IC technology, taking advantage of its amorphous form factor, ample storage space, and computational power.

The electronic passport itself opens the door to new ways of issuing visas. The Document 9303 logical data structure allows for optional storage of visa information on the RFID chip itself [16]. Additionally, because the contactless design does not require any particular orientation or line of sight, future visas could be RFID tags themselves, attached to blank pages in the passport. Effective MAC protocol design would allow for the reading of both visas and passport data in one swipe.

B. *Common Access Card*

Future versions of the CAC may include RFID for access control purposes, though the existing contact-based version is considered the "gold standard" for internal government identity documents [29]. A 2001 working group also acknowledged the potential use of biometrics on the CAC as a means of achieving "three-factor authentication" and potentially counteracting any added security risk resulting from the use of a contactless chip.

C. *Driver's Licenses*

Initial indications are that RFID may not be the technology of choice for the implementation of the Real ID Act and its resulting standardization of state driver's licenses, as a draft DHS report issued in early 2006 warned against the use of RFID for data storage in identity documents or in any human tracking application. It also noted that though the intended function of an RFID tag could be data storage and easy access, this could morph over time if left unchecked [30]. There is also some speculation that Congress may choose to revisit Real ID as the deadline

for national standards draws near.

VII. Conclusion

The implementation of electronic passport has not been without challenges, and some continue to challenge the use of contactless technology in the passport and other identity documents. Privacy groups voiced substantial concerns about the means by which the data and picture are stored, and questions regarding the effectiveness of the biometric technology still remain. At the same time, other government agencies have chosen different technologies for securing their identity documents, and new opinions on the use of RFID for identity purposes have been formed. Congress has set arbitrary deadlines for implementations without understanding the technological challenges involved.

We analyzed the major current and potential uses of RFID in identity documents. We identified some of the areas of promise for existing and future deployments, and we considered the security concerns which accompany them. Most important among these was the theme that future implementers of RFID-based identity documents should take note of the challenges involved in deploying the electronic passport, and should appreciate the need for document security at all steps in the development process.

Acknowledgment

The author acknowledges the assistance and support of former IEEE State Department Fellow Emily Sopensky, the staff of the Washington, D.C., office of IEEE-USA, and Professor Lang Tong of Cornell University. An early version of this work was prepared as part of the 2005 Washington Internships for Students of Engineering Program (see *JEPP* vol. 9, http://www.wise-intern.org).

References

[1] Bureau of Consular Affairs, U.S. Department of State. *Visa Waiver Program (VWP)*, (2005). Available WWW: http://travel.state.gov/visa/temp/without/without_1990.html

[2] Moss, Frank E. "The State Department's Role in the Western Hemisphere Travel Initiative." Senate Foreign Relations Committee Subcommittee on Western Hemisphere, Peace Corps and Narcotics Affairs. 9 June 2005, available http://travel.state.gov/law/legal/testimony/testimony_2543.html

[3] International Civil Aviation Organization. "Foundation of the International Civil Aviation Organization." 20 June 2005, available http://www.icao.int/cgi/goto_m.pl?icao/en/ro/eurnat/history02.htm

[4] Enhanced Border Security and Visa Reform Act of 2002, Pub. L. no. 107-173, 116 Stat. 543 (2002).

[5] Herrmann, Colleen H. "Common Access Card (CAC), Security, and Privacy." 2006. Available http://www.chips.navy.mil/archives/01_summer/cac.htm

[6] United States Government Acountability Office. "Information Security: Radio Frequency Identification Technology in the Federal Government" May 2005. Available http://www.gao.gov/new.items/d05551.pdf

[7] American Association of Motor Vehicle Administrators. "Standards-U.S. License Technology" 2007. Available http://www.aamva.org/KnowledgeCenter/Standards/technology-use.htm

[8] An Act Making Emergency Supplemental Appropriations for Defense, the Global War on Terror, and Tsunami Relief, for the fiscal year ending September 30, 2005, and for other purposes, Pub. L. no. 109-13, 119 Stat. 231 (2005).

[9] Australian Government Department of Foreign Affairs and Trade. "The United States Visa Waiver Program and Machine Readable Passports." 2005. Available http://www.passports.gov.au/Web/us_visa_entry.aspx

[10] Office of the Press Secretary. U.S. Department of Homeland Security. "DHS To Require Digital Photos in Passports for Visa Waiver Travelers." 15 June 2005, Available http://www.dhs.gov/dhspublic/display?content=4542

[11] International Civil Aviation Organization. "Machine Readable Travel Documents – Biometrics – Introduction." June 2005, Available http://www.icao.int/mrtd/biometrics/intro.cfm.

[12] The Biometric Consortium. "An Introduction to Biometrics." July 2005, Available http://www.biometrics.org/html/introduction.html.

[13] Pike, John. "Fingerprint Identification Systems." 27 April 2005. GlobalSecurity.org, Available http://www.globalsecurity.org/security/systems/fingerprint.htm

[14] ICAO TAG MRTD/NTWG. Biometrics Deployment of Machine Readable Travel Documents: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents. United Nations, May 2004.

[15] ICAO TAG MRTD/NTWG. Annex I: Use of Contactless Integrated Circuits in Machine Readable Travel Documents. United Nations, May 2004.

[16] International Civil Aviation Organization. Machine Readable Travel Documents: Development of a Logical Data Structure—LDS for Optional Capacity Expansion Technologies. United Nations, May 2004.

[17] International Civil Aviation Organization. Machine Readable Travel Documents: PKI for Machine Readable Travel Documents offering ICC Read-Only Access. United Nations, October 2004.

[18] Privacy International, et. Al. "An Open Letter to the ICAO." 30 March 2004. Available http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-43421#_edn3

[19] Yoshida, Junko. "Tests reveal e-passport security flaw," *EETimes*, August 30, 2004. Available http://www.eetimes.com/tech/news/showArticle.jhtml?articleID=45400010

[20] Office of Engineering and Technology. "Radio Frequency Safety." Federal Communications Commission, November 2002. Available http://www.fcc.gov/oet/rfsafety/background.html

[21] Holly, R. Michael. Personal interview. Discussion of progress in implementation of electronic/biometric passports. 29 June 2005.

[22] K. Kant, R. Iyer and P. Mohapatra, "Architectural Impact of Secure Socket Layer on Internet Servers", International Conference on Computer Design (ICCD) 2000.

[23] Krim, Jonathan. "Passport ID Technology Has High Error Rate." *The Washington Post*. 6 Aug. 2004. Available http://www.washingtonpost.com/ac2/wp-dyn/A43944-2004Aug5?language=printer

[24] United States. Cong. House. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the Committee on Homeland Security. *Ensuring the Security of America's Borders through the Use of Biometric Passports and Other Identity Documents*. Hearing, 22 June 2005. 109th Congress, 1st sess.

[25] "Fact Sheet: US-VISIT." *U.S. Department of Homeland Security Official Home Page*. 24 Feb. 2005. U.S. Department of Homeland Security. Available http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0629.xml

[26] eGovernment News. "EU Asks US for More Time to Issue Biometric Passports." iDABC European eGovernment Services, 1 April 2005. Available http://europa.eu.int/idabc/en/document/4068/330

[27] Lettice, John. "UK EU Presidency aims for Europe-wide biometric ID card." *The Register*. 13 July 2005. Available http://www.theregister.co.uk/2005/07/13/uk_eu_id_proposal/

[28] "VWP Countries Meet E-Passport Deadline," *Government Technology*, October 26, 2006. Available http://www.govtech.net/magazine/channel_story.php/101923

[29] Security Equipment Integration Working Group. "Access Control Technologies for the Common Access Card." National Business Center, Department of the Interior. April 2002. Available http://www.doi.gov/nbc/eps/seiwg.pdf

[30] DHS Emerging Applications and Technology Subcommittee. "The Use of RFID for Human Identification." 2006. Available http://www.aeanet.org/governmentaffairs/DHS_RFID_in_Humans_Paper0506.asp

G. Matthew Ezovski is a Ph.D. student in the School of Electrical and Computer Engineering at Cornell University. He received the Bachelor of Science degree electrical engineering / computer and systems engineering from Rensselaer Polytechnic Institute in May 2006. He is a recipient of the U.S. Department of Homeland Security Fellowship and is a corresponding member of the IEEE-USA Committee on Communications and Information Policy. He has previously worked in the Acoustic Signal Processing Branch at the U.S. Army Research Lab and was a 2005 participant in the Washington Internships for Students of Engineering (WISE) program. Matt is primarily interested in the areas of sensor networks and wireless communications, as well as issues in RFID technology, the worldwide deployment of the electronic passport, and general issues in science policy.

Steve E. Watkins received his Ph.D. in electrical engineering from the University of Texas at Austin in 1989. He is Director of the Applied Optics Laboratory and Professor of Electrical and Computer Engineering at the University of Missouri-Rolla. He has been the Faculty-Member-in-Residence for the 2005 WISE program, an IEEE-USA Congressional Fellow in the personal office of California Congressman Dana Rohrabacher, a visiting physicist at Kirtland Air Force Base, and a visiting scholar at NTT in Japan. His research interests include smart structures and sensing systems. He is a member of SPIE, OSA, IEEE, and ASEE. He is the 2000 recipient of the IEEE Region 5 Outstanding Engineering Educator Award, a 1993 finalist in the Eta Kappa Nu Outstanding Young Engineer Award Program, and a past National Science Foundation Graduate Fellow