

25th
ANNIVERSARY

WISE 
Washington Internships for Students of Engineering

Biometric Passports: Policy for International and Domestic Deployment

G. Matthew Ezovski
2005 WISE Intern
Rensselaer Polytechnic Institute

August 3, 2005

Sponsored by the Institute of Electrical and Electronics Engineers



Rensselaer

Abstract

Advancements in technology have created the possibility of greater assurance of proper travel document ownership, but some concerns regarding security and effectiveness remain unaddressed. Through the International Civil Aviation Organization, the world has adopted standards whereby passports can store biometric identifiers. The United States has required that all member countries of the Visa Waiver Program must begin issuing biometric passports by October 2006 in order to continue to experience the benefits of the program in the U.S. Experts have addressed substantial technical challenges in the areas of data storage and biometric efficacy, but additional political and technical challenges remain. Interest groups must be assured through technical and political means that data stored will be safe, and the State Department must continue to investigate technical means of achieving secure data storage and transfer. Basic access control and the Faraday cage hold the greatest promise in terms of insuring data security, but the negative effects of basic access control on transmission speed and accuracy must be addressed. Other participating countries should work quickly to issue biometric passports, but the U.S. government should also be prepared to extend deadlines to allow for effective implementation.

The biometric passports discussion is a precursor to other debates to come, including standardized technologies for U.S. driver's licenses and the collection of biometric data by government entities. Lessons learned in this debate, both technical and political, should be applied in the development and implementation of forthcoming technology.

Preface

About the Author

Matthew Ezovski is a rising senior at Rensselaer Polytechnic Institute, the nation's oldest technological university, in Troy, New York. He is majoring in electrical engineering and computer and systems engineering and plans to pursue advanced study in communication systems and hardware design upon graduation while continuing involvement in issues of technology policy. His other interests include politics, student rights, tennis, skiing, clarinet, and piano. He has previously worked in the diagnostics and system validation engineering group at Mercury Computer Systems, Inc., a leading supplier of high performance hardware and software for defense, medical, and OEM applications, through its co-op program. A native of North Smithfield, Rhode Island, Matthew was named a Toyota Community Scholar in 2002 and currently serves as chair of the Rensselaer Judicial Board.

About WISE

The Washington Internships for Students of Engineering (WISE) program was founded in 1980. This collaborative effort among several engineering societies has become one of the premier Washington internship programs. Its goal is to groom future leaders in the engineering profession who are aware of and can contribute to the important intersections of technology and public policy. This multi-society program is supported by the American Association of Engineering Societies. Please see <http://www.wise-intern.org> for more information.

Acknowledgements

The author would like to acknowledge the contributions of all of the individuals who helped him to assemble and prepare this report. In particular, he wishes to acknowledge his sponsor, the Institute of Electrical and Electronics Engineers, for providing him with the opportunity to conduct this research and explore the U.S. federal government. He also wishes to acknowledge the staff of IEEE-USA for their contributions in organizing the program and assisting his research.

This report would not have been possible without the assistance and contributions of Dr. Steve Watkins, Emily Sopensky, R. Michael Holly, the office of the European Commission Delegation, Bill Iori, Richard Hartt, Dr. Syed Murtuza, and the other members of the WISE class of 2005.

Paper Citation

Ezovski, G. Matthew. "Biometric Passports: Policy for International and Domestic Deployment." *Journal of Engineering and Public Policy*, vol. 9, (2005) available <http://www.wise-intern.org>.

Table of Contents

1. INTRODUCTION.....	1
2. THE ROAD TO FULL IMPLEMENTATION.....	2
2.1. <i>POLITICAL TIMELINE FOR BIOMETRIC/ELECTRONIC PASSPORTS</i>	3
2.2. <i>ICAO STANDARDS DEVELOPMENT</i>	4
2.3. <i>THE MOVE TO BIOMETRIC TECHNOLOGIES</i>	5
2.4. <i>DATA STORAGE TECHNOLOGIES</i>	6
2.5. <i>FULL IMPLEMENTATION PLANS</i>	7
3. TECHNICAL OBSTACLES	8
3.1. <i>BASIC ACCESS CONTROL & THREAT OF “SKIMMING”</i>	8
3.2. <i>TRANSMISSION ENCRYPTION</i>	10
4. POLITICAL OBSTACLES	11
4.1. <i>AMERICAN USER ACCEPTANCE</i>	11
4.2. <i>INTERNATIONAL USER ACCEPTANCE</i>	13
5. ANALYSIS	15
5.1. <i>TECHNICAL CHALLENGES</i>	15
5.2. <i>DOMESTIC POLITICAL CHALLENGES</i>	16
5.3. <i>INTERNATIONAL CHALLENGES</i>	17
6. RECOMMENDATIONS.....	18
7. CONCLUSIONS	20
REFERENCES.....	22

1. Introduction

In the post-9/11 world, the weapons of war look very different from those of the Cold War era. Rather than only looking outward for enemies, we are forced to look within. The battlefield is everywhere; there are few ways to restrict access or to know friend from foe. To gain access to this battlefield, all one needs is a passport issued by one of the 27 member nations of the Visa Waiver Program (VWP).¹ The passport must have your biographical information, your photo, and anti-counterfeiting features like words in invisible ink that are only visible under ultraviolet light.

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. 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.

To help answer this important question, the United States Congress is requiring all countries participating in the Visa Waiver Program, of which the U.S. is a member, to issue a technologically-enhanced passport based on international standards. This new travel document will contain electronically stored personal information, along with a digital photograph of the person to whom the passport was issued. The digital picture will allow 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. This technology will never be perfect, but it can help the immigration officers analyze the traveler's identity more effectively.

The implementation of this new travel document has not been without challenges, and more challenges lay ahead. Privacy groups have substantial concerns about the means by which the data and picture are stored, and questions regarding the effectiveness of the biometric technology still remain. By considering these concerns, looking ahead to future technologies, and

cooperating with America's international partners, a well thought-out electronic passport system can be developed, and can help America improve its national security.

2. The Road to Full Implementation

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 with the Department of Homeland Security (DHS), is currently revising the passport's design and incorporated technology to defend against misuse and fraudulent reproduction. Additions are being sought to already existing protective features, and a variety of technological and political issues are being addressed in the process.

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 ICAO with respect to passport design and often take part in the body's decision-making process.

The International Civil Aviation Organization (ICAO), an arm of the United Nations, sets nonbinding passport standards which are internationally recognized. Individual countries take these standards into consideration when developing their own passports. It was established in 1947 for the purpose of reducing friction and promoting cooperation in international travel.³

2.1. 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 its oppressive Taliban regime, Congress and the executive branch searched for holes in the nation's intelligence and security infrastructure. The need for a strong response to the attacks boosted presidential approval ratings to some of their highest levels ever, and the Republican majority in Congress began to pursue an agenda of increased internal intelligence and information sharing. Also deemed essential to improving the national security picture was an overhaul of the nation's immigration and travel policies. Enhanced immigration, passport, and visa security gained a new impetus.

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.

By January 5, 2004, the US-VISIT program, which includes fingerprint checks of incoming travelers who are not U.S. citizens and was also authorized in the Enhanced Border Security Act, was operational at 115 airports and 14 seaports for visitors traveling with visas.⁵ This addressed only a portion of what the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, observed when investigating the nation's borders. In its recommendations to the president and Congress, it endorsed

another, however, has garnered much attention from the government as a potentially simple means of committing passport fraud (in addition to pop culture attention from Hollywood).⁹ 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 must produce similarly protected passports by October 26, 2005, in order for their passports to continue to be accepted at American points of entry.⁸

2.3. 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.”¹⁰ According to the Biometric Consortium, “Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic.”¹¹ 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.¹²

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.¹³

2.4. 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.

- Non-proprietary technology was required.
- “Document integrity” needed to be maintained.
- Stored data needed to be easily accessible.
- Quick transmission times were preferred.
- The technology had to support in excess of 20 KB of storage on one chip or equivalent.¹⁴

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.¹⁴

Contactless IC is often referred to as radio frequency identification (RFID) technology, though technically the two have slightly different implementations.

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.¹⁵

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.¹⁶

2.5. Full Implementation Plans

The deadlines for U.S. implementation of biometric passports, as well as implementation by other VWP countries, have been delayed several times, leading to current deadlines of October 26, 2006, for the most advanced of the technological enhancements. Current DHS policy indicates that the United States will stop accepting passports under the Visa Waiver Program from individuals who are citizens of countries which have not begun issuing electronic passports by that date.⁸

The main purpose of implementing the electronic passport can be summarized by one statement. As stated by Fred Fielding, a senior partner at Wiley, Rein, & Fielding, and a member of the now-disbanded 9/11 Commission, we need to "make sure people are who they say they are."¹⁷

3. Technical Obstacles

3.1. Basic Access Control & Threat of “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'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 is likely to have little effect in practice, as explained later in this section.¹⁴

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 fear a combination of identity theft and surveillance, both of which they believe can be avoided through the use of other data storage technologies. According to Privacy International,

We are 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

The most common use of RFID-like technology that the average U.S. consumer might be familiar with is the E-ZPass system. E-ZPass is an electronic toll-collection system used by many of the turnpike authorities across the country. As a vehicle passes through an E-ZPass booth, the booth's antenna emits a signal which activates the E-ZPass RFID transponder in the car. The transponder then broadcasts its unique ID back to the antenna, allowing a computer to associate that ID with the driver's account and subsequently charge the appropriate toll.¹⁹

The technology planned for implementation in the electronic passport differs from the E-ZPass transponder in two significant ways.

1. Instead of requiring batteries for power, the passport's chip will be powered by the magnetic field emitted from the reader.
2. The passport will not broadcast its own signal. It will reflect a modified version of the signal sent by the reader in order to communicate.

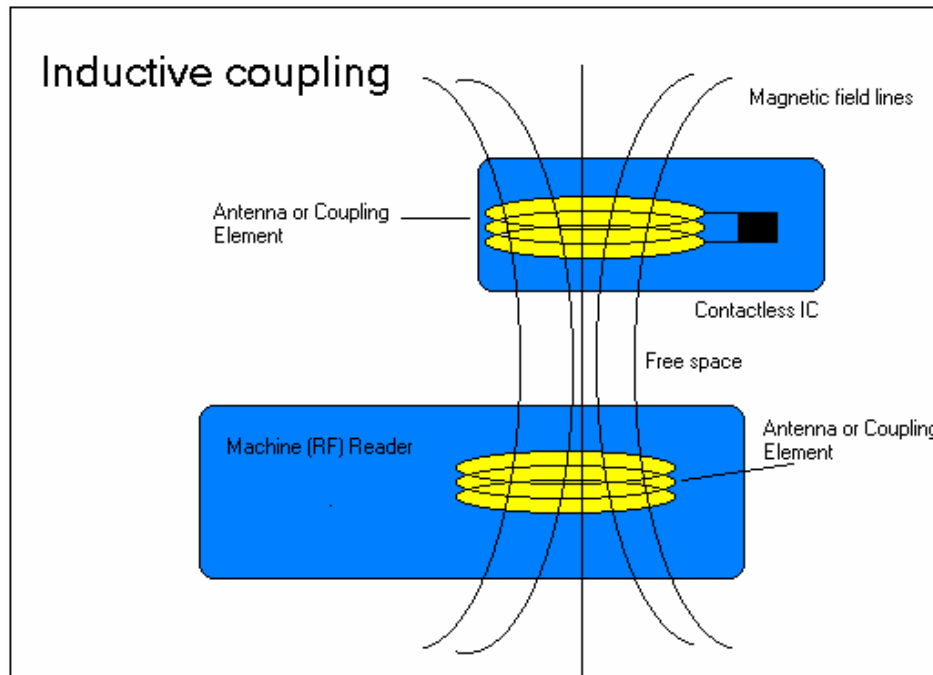


Figure 2- Function diagram for reading a contactless IC chip powered by inductive coupling

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 proposed 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.²⁰ 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.²¹ 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.

Basic access control (BAC) would cause 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.¹⁶ The standards specify a combination of the individual passport number and personal information as the key, but the U.S. has yet to agree to this implementation.²²

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 is currently investigating means of implementing basic access control on American passports, along with its suppliers.

3.2. 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. Very few convenient methods for limiting broadcast range exist, so great care must be taken if the data being transmitted is particularly sensitive.

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. Encrypted transmission would commence immediately following basic access control authentication.¹⁶

The widely-recognized industry standard in electronic data transmission is 128-bit Secure Socket Layer technology. This protocol is often used for submission of credit card data on e-commerce websites, such as Amazon.com. It is generally accepted that without prior knowledge of the 128-

bit key, it would take the world's most powerful known supercomputers many years to decrypt SSL encoded data. The larger the key, the lower the likelihood that the code can be deciphered.²³

4. Political Obstacles

4.1. American User Acceptance

The debate on biometric passports has not become a major conversation topic for the average American citizen. Related privacy topics, such as identity theft and uniform standards for driver licenses, however, have gained the attention of the general public. A wide range of interest groups, including those representing privacy, security, technology, and budgeting interests, have taken a keen interest in the discussion. They have raised a wide variety of concerns, ranging from the effectiveness of the technology and the cost of implementation to the security of on-chip data and the potential for government surveillance.

At the forefront of the biometric passport debate are concerns relating to security of the data stored on the RFID chip. Worries about “skimming” have in many ways stolen the stage from a discussion of whether or not biometrics are a reasonable means of authenticating identity. Both questions have their basis in ICAO and ISO specifications for electronic passports, as well as the overall technical concern surrounding all types of wireless communication.

RFID chips by their very nature open the door to a variety of surveillance opportunities for both friendly and unfriendly organizations. The E-ZPass system essentially creates a limited-capacity surveillance network for tracking its members and issuing applicable charges. Some privacy advocates worry that deploying similar technology could result in development of surveillance networks on a nationwide or international scale, resulting in Americans being tracked without their knowledge.²⁴

The State Department has recognized that security of the data stored on the chip is an essential piece of the R&D challenge for the e-passport. Recently, under continued pressure from privacy

groups and Congress, State began investigating controlling access through the use of a Faraday cage.²² 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 prevent reading of the passport without the cover being physically opened.

Some have expressed concern about the drastic increase in the cost of printing and issuing the new passports. While a current U.S. passport costs approximately \$2.50 to physically print, the State Department estimates that the production cost of an e-passport will increase to between \$7.50 and \$11.50. These costs do not include those incurred in order to actually issue the document to an individual, nor do they include the costs of rolling out the necessary technology for issuing the passports or the increased overhead per passport. Current fees for Americans ages 16 and over total \$97.²⁵

The ICAO’s decision to choose facial recognition as the universal biometric for authenticating e-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.²⁶ This superiority is shown in the following chart, the data for which was provided during Congressional testimony.

Table 1- Accuracy of selected biometrics, provided by NIST ²⁶

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

Congress has also proved inquisitive as to the ICAO's selection of facial recognition, with Congressman Christopher Cox (R-Cal.), 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 2005.²⁶

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. Social norms do appear to be changing, however, based on decisions by major corporate entities to incorporate fingerprint-based biometric technologies in next-generation products. For example, the Thinkpad laptop computer series is among the first to include an integrated fingerprint scanner as an alternative to standard password protection. Beginning with the T43, Lenovo, a Chinese company which recently purchased the Thinkpad line from IBM, will take advantage of support in Microsoft Windows XP for logging on with the swipe of a fingertip. Mr. Bill Iori, marketing manager for Lenovo's Thinkpad division, noted customer desire for a more secure PC, maturity of the technology, and cost efficiency as the primary factors in making the move.²⁷

Fingerprints are also a cornerstone of the US-VISIT program, though this program does not affect U.S. citizens.⁵

4.2. International User Acceptance

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 has 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.²⁸

Currently, debates over the use of biometrics in national identification cards have taken center stage in the United Kingdom, with Prime Minister Tony Blair's Labour Party pushing for a biometrically-enhanced national ID 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 ID card legislation in late 2004. According to the British Home Office, "The scheme will 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 per cent of British respondents favored the introduction of identity cards with technology similar to that of the ICAO-defined electronic passport. Several other EU nations including France already have national ID cards, but the UK is using its current six-month EU presidency to push for continent-wide standards for national ID cards with embedded electronics.²⁹

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 2005 deadline. European Commission agreements now call for a deadline of August 28, 2006, for the implementation of the facial image in EU passports – a date which precedes U.S. requirements.²⁸

Not all Visa Waiver Program countries outside of the U.S. are members of the European Union, though many of them are. Asian nations, such as Japan and Singapore, are also diligently pursuing the electronic passport. Singapore recently awarded a SGD 9.7 million (\$5.8 million U.S.) contract to a consortium led by NEC to produce ICAO standards-compliant passports for issuance beginning in October 2005.³⁰

Hong Kong, though not a VWP country, has established a national ID card system which employs contact-based IC technology. It differs substantially from the design of the ICAO electronic passport in that very little data is actually stored on the document's chip itself.

Instead, the stored information allows a card reader to reference additional data, including some more-detailed biometric data, stored in a remote government database.³¹ Such system designs have met fierce resistance in the United States.

5. Analysis

The international community has taken a bold step by choosing to include electronics and biometric identifiers in its passports. It has attempted to respond to the drastically different security needs of this century, and although it remains to be seen whether this effort will be successful, the fact that it has been undertaken certainly deserves credit. Technical challenges remain, as do political complications, but the ICAO and the U.S. State Department have established reasonable roadmaps for deploying complex technology.

5.1. Technical Challenges

A system of international travel requires some degree of interoperability, and ICAO guidelines have provided some of the framework for that interoperability. Individual states always remain cautious in entering into any international agreement, however, fearing that they will lose some of their individual rights. In its efforts to maintain national sovereignty over passports, the NTWG avoided touching on several implementation issues, particularly in the security arena. These questions are essential to ensuring interoperability between national systems now that advanced electronics are being deployed.

The NTWG's decision to not address questions relating to individual privacy has resulted in individual countries selecting different methods for restricting access to the passport's data. Basic access control has been explored in numerous countries, but important implementation details vary. Transmission encryption possibilities have also been explored, but have met the same difficulties. The U.S. State Department is now looking to implement basic access control, along with a shielded cover, to prevent unauthorized access. Other countries must also be able to implement the U.S. basic access control scheme in order for it to be successful. One can hope that the technical conference of VWP countries announced earlier this summer and taking place

near publication of this paper will come to a common conclusion of how to protect citizens' data while maintaining interoperability.

A March 2005 test session organized by the ICAO indicated that though various private sector entities had generally succeeded in implementing the basics of Document 9303, substantial performance and accuracy degradation occurred when BAC was included. The average reading time without BAC was 3.3 seconds, certainly a realistic value for immigration purposes. The average reading time of 9.24 seconds with BAC showed a great improvement over previous results, but could prove virtually unusable in real-world applications. Several of the test passports did perform well, however, with read times in the 3 second to 5 second range.³² In order for widespread deployment to occur, though, more vendors will need to reach similar performance levels with increased accuracy and detection rates.

5.2. Domestic Political Challenges

Convincing the American public and privacy groups that the electronic passport is secure will prove substantially more difficult than actually securing it. Privacy International and the ACLU have taken staunch positions against RFID technology in passports, supporting contact-based chips instead. 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.

Though privacy concerns related to electronic passports are not currently finding an audience in Congress, the State Department has clearly noticed them through public comments made after the proposed passport changes were published on the Federal Register. Over 2,000 individuals

and interested parties posted comments, and this has led to a decision at the Department to not distribute electronic passports until security concerns can be fully addressed. According to Frank Moss, Deputy Assistant Secretary for Consular Affairs, “The bottom line is that we will not issue biometric passports to the general public until we have successfully addressed these concerns.”³³

Congress, despite some resistance to the executive branch’s diversion from its initially-planned timetable for rollout of electronic passports, has been generally pleased with the progress of electronic passport development. Privacy concerns have not comprised much of the discussion on the Hill; instead, effectiveness of biometric technologies has moved to the forefront. As noted earlier, figures provided by NIST suggested that the accuracy of facial recognition fell far short of well-established biometrics like fingerprints, but the data supporting the NIST expert’s testimony came from the Institute’s last comprehensive study, which was performed in 2002.²⁶ Studies are ongoing, and the volume of research in computer vision with homeland security applications over the past three years suggests that great strides may have occurred in that timeframe.

5.3. International Challenges

U.S. electronic passport rollout plans continue to move forward, but some VWP countries, including Portugal and Austria, continue to lag behind. Certainly, the ongoing debate in the United States over how best to protect data stored on the RFID tags may be preventing some nations from moving forward. Given the complex nature of the project and the need for it to remain static for a substantial number of years, the international community would be well served to take the time necessary to implement it correctly. The Department of Homeland Security recognized that its recent deadline of October 26, 2005, for VWP countries to begin issuing e-passports was too soon, and delayed it by one year. If a similar situation arises in 2006, however, such a delay will require Congressional action. The 2004 Intelligence Reform Act originally set an October 26, 2006 deadline, and though DHS requirements initially set the earlier deadline, they are now in line with that date.³⁵

More biometric selection difficulties may also be brewing on the international front in the time period immediately following the release of the first waves of American and European electronic passports. As indicated earlier, European Commission agreements have instructed member nations to begin their programs by only including one biometric identifier, the facial image. The second wave of passports, released beginning in 2007, will be required to include two fingerprint images as well. This differs from the speculated U.S. approach, which many believe may include a move toward iris scan technology in the years to come. A 2002 WISE publication noted that iris recognition held inherent benefits in the biometric technology space due to ease of image acquisition and the uniqueness of the identifier, but also acknowledged the drastically increased cost over other available options.³⁶ The expiration of a major iris recognition technology U.S. patent held by Iridian Technologies may help to reduce this cost, though the challenge of acquiring an iris scan as part of the passport application process would still exist.³⁷

Though the logical data structure provides an effective means for storing any of a number of biometrics in the RFID chip, the more countries which have the ability to authenticate based on that biometric, the more effective the identifier and the passport.

6. Recommendations

In order to accomplish a successful rollout of electronic passport technology, the following should occur.

- **The U.S. State Department should fully adopt Basic Access Control, pushing suppliers to improve performance and reliability to more reasonable levels.** ICAO standards provide a comprehensive framework for conducting BAC, leaving manufacturers to implement that framework. The performance of transmissions with BAC still lag substantially behind non-BAC transmissions, and State should not settle for such low standards. With additional research, however, there is no reason why these challenges cannot be overcome. State, DHS, and Congress should allow the technology

to mature sufficiently to increase performance. It remains to be seen whether current Congressional deadlines will prevent this from occurring.

- **The U.S. State Department should implement a Faraday Cage in one side of the electronic passport cover.** Doing so will entirely prevent unauthorized access when the passport is closed. Though BAC should generally also achieve this goal, certain pieces of data may be transmitted without authorized access under particular conditions.
- **The State Department, in conjunction with NIST, should conduct a comprehensive analysis of facial recognition technology to determine what improvement in accuracy would be gained by moving to iris scan technology.** Given the administration's unwillingness to consider fingerprint scans due to a number of economic and social acceptance concerns, it should move quickly to determine if it has an interest in further developing and implementing iris scan technology for use in electronic passports.
- **If the U.S. intends to pursue iris scan technology for use in its electronic passports, then it should move quickly to reconcile standards differences with the European Union and adopt a uniform secondary biometric.** The electronic passport system will prove most effective when all participating countries are best able to take advantage of all available data. If different nations are using different biometrics, then the available resources will not be utilized to their fullest abilities.
- **Congress should extend the October 26, 2006 deadline for implementing electronic passports with biometric enhancements if multiple VWP countries are unable to implement their planned systems by that date.** The e-passport represents one of the largest changes the world has ever seen in the area of international travel. It also represents a massive technological challenge, given the scale and complexity of the project. Policymakers should not settle for a mediocre system in order to meet an arbitrary deadline.

That said, **the U.S. Department of Homeland Security, along with the State Department, should continue to pressure VWP countries to meet the October 26, 2006 deadline.** The deadline is not entirely out of reach, if all members of the VWP continue to work to develop uniform standards and prepare suppliers for production. The 9/11 Commission noted the urgent need for border security reform, and the government cannot allow that goal to become bogged down by a lack of commitment from other nations.

7. Conclusions

Despite numerous delays and some unforeseen complications, the electronic passport is making reasonably good progress toward full deployment in all 27 member countries of the Visa Waiver Program. Privacy concerns often took a back seat to the timeline for deployment, but State Department officials and others now acknowledge the need for a more secure version of the electronic passport. The technology exists to make this happen, and though the privacy groups will most likely continue to object to the use of RFID technology, those objections will have virtually no scientific basis. The costs will be substantial, but the potential for benefit is also extremely substantial. As the member nations reach the home stretch, they must work to address remaining concerns like basic access control and differences in secondary biometric technology. Time is of the essence, but time must be taken to ensure that the project is being completed correctly.

Though this endeavor is substantially important on its own merit, its importance as a harbinger of debates and projects to come may prove even more substantial. Biometrics and RFID technology will continue to disseminate to the masses for many years to come. Questions of privacy and security will continue to ride their waves, and must be addressed more effectively than their counterparts in the 1990s: spam and identity theft.

One of the first such debates likely to occur 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.³⁸ Nothing in the law dictates what that technology will be, what it will store, or if it can be used to store biometric data.

These discussions will illustrate one of the great challenges of the 21st century: balancing individual freedom against state security. Technology will help us solve some of these questions, but the real challenge will lie in not creating additional challenges in the process.

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 "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
- ⁶ United States. National Commission on Terrorist Attacks Against the United States. [The 9/11 Commission Report](#). Washington: The Commission, 2004.
- ⁷ 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
- ⁸ 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>
- ⁹ Joffé, Roland (Director). *The Killing Fields*. Hollywood: Warner Bros., 1984.
- ¹⁰ International Civil Aviation Organization. "Machine Readable Travel Documents – Biometrics – Introduction." June 2005, Available <http://www.icao.int/mrtd/biometrics/intro.cfm>.
- ¹¹ The Biometric Consortium. "An Introduction to Biometrics." July 2005, Available <http://www.biometrics.org/html/introduction.html>.
- ¹² Pike, John. "Fingerprint Identification Systems." 27 April 2005. GlobalSecurity.org, Available <http://www.globalsecurity.org/security/systems/fingerprint.htm>

¹³ 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.

¹⁴ ICAO TAG MRTD/NTWG. *Annex I: Use of Contactless Integrated Circuits in Machine Readable Travel Documents*. United Nations, May 2004.

¹⁵ International Civil Aviation Organization. *Machine Readable Travel Documents: Development of a Logical Data Structure—LDS for Optional Capacity Expansion Technologies*. United Nations, May 2004.

¹⁶ International Civil Aviation Organization. *Machine Readable Travel Documents: PKI for Machine Readable Travel Documents offering ICC Read-Only Access*. United Nations, October 2004.

¹⁷ Fielding, Fred F, senior partner, Wiley, Rein, & Fielding. Personal interview. “Meeting with 2005 WISE Interns.” 19 July 2005.

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 Niver, E.; Mouskos, K.; Dwyer, P.; Batz, T. “Evaluation of Transmit’s Communication System.” Electrotechnical Conference, 2000. MELECON 2000. 10th Mediterranean, Vol.2, Iss., 2000 Pages: 664- 667 vol.2

²⁰ Yoshida, Junko. "Tests reveal e-passport security flaw," *EETimes*, August 30, 2004. Available <http://www.eetimes.com/tech/news/showArticle.jhtml?articleID=45400010>

²¹ Office of Engineering and Technology. “Radio Frequency Safety.” Federal Communications Commission, November 2002. Available <http://www.fcc.gov/oet/rfsafety/background.html>.

²² Holly, R. Michael. Personal interview. Discussion of progress in implementation of electronic/biometric passports. 29 June 2005.

²³ Kant, K.; Iyer, R.; Mohapatra, P. “Architectural impact of secure socket layer on Internet servers.” *Computer Design*, 2000. Proceedings. 2000 International Conference on, Vol., Iss., 2000

²⁴ United States. Cong. House. Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce. *RFID Technology: What the Future Holds for Commerce, Security, and the Consumer*. Hearing, 14 July 2004. 108th Congress, 2nd sess. Washington: Government Printing Office, 2004. Available http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearings&docid=f:95455.pdf.

- ²⁵ Bureau of Consular Affairs, U.S. Department of State. *Passport Fees* (2005), Available http://travel.state.gov/passport/get/fees/fees_837.html.
- ²⁶ 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.
- ²⁷ Iori, Bill. "Re: Questions Connecting Biometric Advancements and Passports." 14 July 2005. Personal email.
- ²⁸ 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>.
- ²⁹ 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/
- ³⁰ "NEC Solutions Asia Pacific is awarded Singapore's First Biometric Passport Project." *SecurityInfoWatch.com*. 23 March 2005, Available <http://www.securityinfowatch.com/article/article.jsp?id=3451&siteSection=418>.
- ³¹ Hong Kong Government Information Center. "Smart ID – Smart Idea." 21 July 2005, Available <http://www.smartid.gov.hk/en/index.html>.
- ³² ICAO Testing Test Report – Tsukuba test session. 9 May 2005.
- ³³ Testimony of Frank E. Moss. "How the U.S. Passport Program Enhances Border Security." Available <http://www.state.gov/r/pa/ei/othertstmy/48733.htm>
- ³⁴ 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*.
- ³⁵ Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. no. 108-458, 118 Stat. 3638 (2004).
- ³⁶ Geruso, Michael. "An Analysis of the Use of Iris Recognition Systems in U.S. Travel Document Applications." *Journal of Engineering and Public Policy*, vol. 6, (2002) available <http://www.wise-intern.org>.

³⁷ Kharif, Olga. "Iris Scans' Leader Looks Secure." *BusinessWeek*. 5 July 2005, Available http://www.businessweek.com/technology/content/jul2005/tc2005075_4115_tc119.htm?campaign_id=nws_techn_jul6&link_position=link1

³⁸ 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).