



ePassport Update

**US Traveler Security Task Force
Association of Corporate Travel Executives (ACTE)**

October 17, 2005

The Association of Corporate Travel Executives (ACTE) is a not for profit association established by business travel managers in 1988 to provide meaningful education and networking opportunities.

ACTE recognizes the interdependence between corporate travel purchasers and corporate travel suppliers and accords both sectors equal membership. ACTE's membership span all sectors of business travel, from corporate buyers to agencies to suppliers. ACTE currently serves more than 2,500 executives in over 40 countries.

TABLE OF CONTENTS

<u>TOPIC</u>	<u>PAGE</u>
I. Introduction & Background	2
II. A Brief Review of the ePassport System	3
III. Important Dates Regarding ePassport	3
IV. Issues, ACTE Recommendation, & Current Status:	6
V. Next Steps	8
VI. Appendix A: Additional Information Resources	9
VII. Appendix B: Terminology	10

I. INTRODUCTION:

Background:

In 2003, ACTE initiated the ACTE Traveler Security Task Force to provide information to the corporate travel industry regarding security issues. The task force is comprised of ACTE members who have volunteered their time and expertise.

All materials developed by the task force are made available through the ACTE Initiatives website at http://www.acte.org/initiatives/TravellerSecurity_clearinghouse.shtml. Task Force members as well as ACTE members are encouraged to submit any additional information regarding specific initiatives for posting on the ACTE Resource Center, which is accessible to all ACTE members. Information for posting to the clearinghouse should be submitted to Clearinghouse@acte.org. The purpose of this Travelers Security Task Force as well as all of ACTE's initiative task forces is to provide information to our members on a variety of topics and concurrently allow members to share their ideas with their ACTE colleagues.

As part of the Task Force, in April 2005, ACTE conducted a member survey regarding the U.S. State Departments' proposal to employ contactless smart card technology, which included embedding Radio Frequency Identification tags (RFID) in passports. Ninety-three percent of the survey respondents were opposed to the use of contactless smart card technology at that time. In addition over half of the respondents indicated that more information was needed to fully understand contactless smart card technology and its potential impact on the business travel community.

In response to the members' request for additional information, ACTE's Traveler Security Task Force released a RFID Industry Analysis (April 2005) to educate members on contactless smart card technology, terminology, and the major issues and concerns being publicly discussed in the media regarding the use of contactless smart cards and related RFID technology. The RFID Industry Analysis can be found at <http://www.acte.org/rfid.shtml>.

As a result of the task force's analysis, ACTE concluded that ePassports in the form originally proposed posed a potential threat to both traveler security and personal privacy. On May 1, 2005, ACTE called for a moratorium on the use of RFID chips in passports until the technology is fully tested by the State Department. ACTE demanded that the testing must ensure that:

- The RFID chips cannot identify U.S. citizens at an distance form an unauthorized passport reader
- The encryption technology used to code traveler information must be virtually foolproof.

Objective:

The objective of this document is to update ACTE members on the status of the ePassport initiative in light of ACTE's concerns and recommendations. The document overviews the functionality of the ePassport, identifies key dates and milestones for implementation and issuance by governments globally, and reports on the current status of ACTE's concerns and recommendations and actions underway to address these concerns.

II. A BRIEF REVIEW OF THE ePASSPORT SYSTEM

The ePassport system consists of three key components:

1. A scanning antenna at the station
2. The embedded chip in the passport
3. Border security-related information technology infrastructure

The scanning antenna uses magnetic or electromagnetic fields to power the contactless smart card embedded in the ePassport (since there is no battery) as well to exchange data between the card and the reader. The antenna puts out radio frequency (RF) signals in relatively short range - 4 to 6 inches for the passport program – to activate and communicate with the chip. Since these chips do not need batteries they can be made very small (and flat) and the information stored on the chip can be held for as long as 10 years to possibly decades.

When the contactless chip passes through the signal from the scanning antenna the chip is energized. If Basic Access Control (BAC) technology is employed, the chip authenticates the reader as an authorized reader by demanding an access code. If the code is provided, the chip creates an encrypted communication to the authorized reader that transmits the data stored on it. The scanning antenna picks up the return signal from the chip and captures the information.

The captured information is then used by border control authorities to verify identity and check information against various security-related databases, via various government-controlled security systems, networks, and other infrastructure. Once captured, the information is subject to the privacy policies and other legal limitations imposed by the respective national governments.

III. IMPORTANT DATES & MILESTONES REGARDING ePASSPORT:¹

DATE	EVENT or ACTION
Currently in Progress	US Department of State (DOS) finalizing the design of the new electronic passport. The US ePassport will comply with the ICAO standard for machine-readable passports (MRP). The Department of Homeland security is currently evaluating ePassport readers for compliance with ICAO specifications for the purposes of machine-readable passport requirements.
Currently in Progress	US Department of State (DOS) testing of the proposed components of the new electronic passport.²

¹ According to the Department of Homeland Security (DHS) (www.dhs.gov/us-visit), International Civil Aviation Organization (ICAO) (<http://www.icao.int/index.html> and <http://www.icao.int/mrtd/overview/overview.cfm>)

² According to the US Department of State (http://travel.state.gov/passport/cppt/eppt_2502.html)

III. IMPORTANT DATES & MILESTONES REGARDING ePASSPORT:³ (continued)

DATE	EVENT or ACTION
June 15, 2005	<p>Live test of ePassports launched at Los Angeles and Sydney, Australia airports.</p> <p>Volunteers participating in the test include airline crew and officials of United Airlines, Air New Zealand and Qantas Airlines. These volunteers will present their new e-Passports when arriving in the United States through LAX, or upon arrival in Australia through Sydney Airport.</p>
July 11, 2005	<p>The machine-readable passport (MRP) format specified by the International Civil Aviation Organization (ICAO) becomes the worldwide standard.</p> <p>The current ICAO blueprint for the harmonized, worldwide integration of biometric identification in machine readable travel documents includes:</p> <ul style="list-style-type: none">• Face as the primary, mandatory biometric; iris or fingerprint as secondary and optional• Contactless integrated circuit chip as the storage medium• Logical data structure for programming the chip• Modified public key infrastructure (PKI) scheme to secure the data against unauthorized alteration
September 28-29, 2005	<p>ICAO international symposium in Montreal</p> <p>Symposium will focus on ICAO-standard Machine Readable Travel Documents (MRTD) and biometric enhancement mechanisms to support the full implementation of Machine Readable Passports (MRP) around the world.</p>
October 26, 2005	<p>The United States Department of Homeland Security (DHS) will require a digital photograph of the passport holder's face printed on the data page of the passport for Visa Waiver Program (VWP) countries.</p> <p>One year later (October 26, 2006) DHS will require the integrated circuit chip, or ePassport, capable of storing the biographic information from the data page, a digitized photograph, and other biometric information in travel documents. Valid passports issued before October 26, 2005, will still be accepted for travel under the auspices of the VWP provided that the passports are machine-readable.</p>

³ According to the US Department of State (http://travel.state.gov/passport/cppt/eppt_2502.html)

³ According to the Department of Homeland Security (DHS) (www.dhs.gov/us-visit), International Civil Aviation Organization (ICAO) (<http://www.icao.int/index.html> and <http://www.icao.int/mrtd/overview/overview.cfm>)

III. IMPORTANT DATES & MILESTONES REGARDING ePASSPORT:⁴ (continued)

DATE	EVENT or ACTION
December 2005	The Department of State plans to issue the first full validity U.S. electronic passports.²
October 2006	All 16 passport issuance locations in the domestic United States will issue electronic passports.²
April 10, 2010	All of the 188 Contracting States of the ICAO must begin issuing ICAO standard MRPs no later than April 1, 2010. Some 110 States currently do so. Of the States already issuing ICAO-standard MRPs, more than forty plan to upgrade to the biometrically-enabled version, or ePassport, by the end of 2006.

⁴ According to the US Department of State (http://travel.state.gov/passport/cppt/eppt_2502.html)

⁴ According to the Department of Homeland Security (DHS) (www.dhs.gov/us-visit), International Civil Aviation Organization (ICAO) (<http://www.icao.int/index.html> and <http://www.icao.int/mrtd/overview/overview.cfm>)

IV. ISSUES, ACTE RECOMMENDATIONS, & CURRENT STATUS:

Issue: An unauthorized party with an appropriately equipped scanner could activate the RFID chip and read its contents or at a minimum identify the issuing country of the passport.

ACTE

- Recommendation:**
- Regardless of the technology employed, assure that all components of the ePassport are fully tested and that security and privacy concerns are addressed prior to deployment of the ePassport.
 - Consider using contact technology to eliminate the need to implement expensive and complex technology to protect the data transmission.
 - If contactless technology will be used, then we would further recommend the following:
 - Encrypting all passport data when it is transmitted using a robust and virtually foolproof encryption system.
 - Utilize technology, such as Basic Access Control (BAC) to authenticate the reader sending the transmission.

- Current Status:**
- The United States Department of State (DOS) has installed anti-skimming materials into the ePassports being pilot tested this summer.⁵ This feature physically prevents skimming information off the chip while the passport is closed.
 - The DOS is also considering the implementation a higher level of ICAO security, Basic Access Control (BAC). BAC would prevent any transmission of data without appropriate codes to first “unlock” the chip, and then use the code to encrypt the resulting transmission of data.⁴
 - The DOS has stated that they will not issue its first passports with embedded biometrics until they are confident that the security issues associated with contactless chips have been successfully addressed.⁴

⁵ According to Frank Moss, Deputy Assistant Secretary for Passport Services, US Department of State in an interview appearing in the ACTE Global Business Journal, Summer 2005

IV. ISSUES, ACTE RECOMMENDATIONS, & CURRENT STATUS: (continued)

Issue: The difficulty in developing standards for the biometric data stored on the chips could make global interchange and standard use hard to achieve for some time.

ACTE

Recommendation:

- Encourage the ICAO to develop interoperable biometric standards prior to October 2006 when the U.S. Visa Waiver Program will require ePassports with biometric data.

Current Status:

- The ICAO is responsible for creating the biometric encoding standards. The ICAO held a global symposium on Machine Readable Travel Documents (MRTD) and Biometric-enhanced ePassports on September 29-30, 2005. Progress reports from the meeting are not yet available.

Issue: The recording of facial biometrics as the primary identifier.

Facial biometrics, though less intrusive, are considered less accurate considering environmental factors, the potential use of disguises, etc.

ACTE

Recommendation:

- Consider using iris scan or fingerprints in addition to or in lieu of facial recognition in international travel and border security identity verification (including in ePassports).

Iris scans and fingerprints are more accurate than facial recognition and address privacy concerns since a photo can be used to track an individual without his or her knowledge and iris scans or fingerprints require the physical presence of the individual.

- Recommend to governments globally that the use of biometrics collected at border control points be restricted to travel-related identity verification (see Mission Creep below).

Current Status: The current ICAO blueprint for the harmonized, worldwide integration of biometric identification in machine readable travel documents adopted on July 11, 2005 includes face as the primary, mandatory biometric; iris or fingerprint as secondary and optional.

IV. ISSUES, ACTE RECOMMENDATIONS, & CURRENT STATUS: (continued)

Issue: Mission Creep - using the information gathered for purposes other than border control.

ACTE

Recommendation:

- Obtain clear and concise definition from DOS regarding items such as the creation of a database with information gathered from ePassports, retention of data, communication with other databases, and securing the process from outside interference.

Current Status:

- The DOS is currently reviewing the many comments received from the public in response to their Proposed Rule on the new passport technology. DOS will publish a Final rule in the near future that will serve as their response to those comments.

V. NEXT STEPS

The State Department has two stated goals for the ePassport system:

1. To enhance the security of the passport, in particular by preventing counterfeiting, and
2. To expedite the processing of travelers through all border checkpoints.

ACTE supports these goals as long as their achievement does not negatively impact traveler safety and security, protects personal privacy, maintains the integrity of personal data, and limits the use of information to the defined application.

ACTE will continue to work together with Department of State and other government agencies to provide member input and represent the perspective of the business travel community.

To follow the development of the ePassport initiative, please look for updates from ACTE. Both the US and EMEA Traveller Security Task Forces will be following this issue and will provide ACTE Membership with updates. To contact the members of the ACTE Traveller Security Task Forces, please send an email to: security@acte.org.

VI. APPENDIX A: ADDITIONAL INFORMATION RESOURCES:

- Association of Corporate Travel Executives - www.acte.org
- American Civil Liberties Union - Privacy & Technology - www.alcu.org
- Business Travel Coalition - <http://btcweb.biz/rfid.htm>
- Electronic Privacy Information Center - www.epic.org
- The International Civil Aviation Organization - <http://www.icao.org/>
- Privacy.org – www.privacy.org
- Progressive Policy Institute - <http://www.ppionline.org/>
- Smart Card Alliance - <http://www.smartcardalliance.org/>
- The United States Department of Homeland Security - <http://www.dhs.gov/dhspublic/>
- The United States Department of State -
http://travel.state.gov/passport/eppt/eppt_2498.html
- The US-VISIT Program - <http://www.dhs.gov/us-visit>

VII. Appendix B: Terminology:⁶

Basic Access Control (BAC) Technology⁷:

A Machine Readable Travel Document (MRTD) with a Basic Access Control (BAC) mechanism is offered to the inspection system optically or visually. Read information is used to gain access to the chip and sets up a Secure Channel for communications between the MRTD's chip and the inspection system. A MRTD chip that supports BAC must respond to unauthenticated read attempts with 'Security status not satisfied.'

Contactless Smart Card Technology:

A contactless smart card includes an embedded smart card secure microcontroller or equivalent intelligence, internal memory and a small antenna and communicates with a reader through a contactless radio frequency (RF) interface. Contactless smart card technology is used in applications that need to protect personal information and/or deliver fast, secure transactions, such as transit fare payment cards, government and corporate identification cards, documents such as electronic passports and visas, and financial payment cards. Contactless smart cards have the ability to manage, store and provide access to data on the card, perform on-card functions (e.g., encryption) and interact intelligently with a contactless smart card reader. The contactless interface provides users with the convenience of allowing the contactless card to be read at short distances with fast transfer of data.

Contact Smart Card Technology:

Contact Smart Cards offer similar capabilities to contactless smart cards but require physical contact with the reading mechanism rather than using a radio frequency (contactless) interface.

Electronic Passports (ePassports):

The proposed U.S. Electronic Passport is the same as a regular passport with the addition of a small contactless integrated circuit (smart card computer chip) embedded in the back cover. The chip will store the same data visually displayed on the photo page of the passport, and will additionally include a digital photograph. The inclusion of the digital photograph is to enable biometric comparison through the use of facial recognition technology. Passports without chips will still be valid for the full extent of their validity period.⁸ The International Civil Aviation Organization (ICAO) determined that new machine-readable passports were the best option to provide a more secure border control system. These passports embed a type of contactless smart card technology (integrated circuit), which works when a low power radio frequency signal is applied within a few inches of the passport. The passport chip, having no batteries or power source of its own, relies on getting its power from the reader's RF signal to operate.

⁶ Definitions of the terms listed from "RFID Tags and Contactless Smart Card Technology: Comparing and Contrasting Applications and Capabilities" and "RFID Tags, Contactless Smart Card Technology and Electronic Passports: Frequently Asked Questions" found on the Smart Card Alliance website (www.smartcardalliance.org) unless otherwise noted.

⁷ Definition according to ICAO as appears on www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf

⁸ Definition according to the US Department of State as appears on http://travel.state.gov/passport/eppt/eppt_2498.html

International Civil Aviation Organization (ICAO)⁹:

One of ICAO's chief activities is standardization, the establishment of International Standards, Recommended Practices and Procedures covering the technical fields of aviation: licensing of personnel, rules of the air, aeronautical meteorology, aeronautical charts, units of measurement, operation of aircraft, nationality and registration marks, airworthiness, aeronautical telecommunications, air traffic services, search and rescue, aircraft accident investigation, aerodromes, aeronautical information services, aircraft noise and engine missions, security, and the safe transport of dangerous goods. After a standard is adopted it is put into effect by each ICAO contracting state in its own territories. As aviation technology continues to develop rapidly, the Standards are kept under constant review and amended as necessary.

Machine Readable Travel Document (MRTD)¹⁰:

An international travel document (e.g. a passport or visa) containing eye- and machine-readable data. Each type of MRTD contains, in a standard format, the holder's identification details, including a photograph or digital image with mandatory identity elements reflected in a two-line machine readable zone (MRZ) printed in Optical Character Recognition-B (OCR-B) style. Standardization of elements in the travel document allows all participating countries using properly configured readers to read the MRZs of the MRTDs of all other countries issuing the same type of document. MRTDs are developed by ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD). The TAG drafts and adopts "specifications" (i.e. detailed technical requirements) for the design of these travel documents. These specifications are published in ICAO Doc 9303. The TAG also drafts guidance material to assist states in implementing the specifications, and Technical Reports and Information Papers to guide states and private industry on present and future aspects of its work.

RFID tags (Radio Frequency Identification tags):

RFID tags are electronic chips with a variety of applications, including: identifying animals, tracking goods logistically and replacing printed bar codes at retailers. The chip stores an identifying number and an antenna that enables the chip to transmit the stored number to an RF reader. When the tag comes within range of the appropriate RF reader, the chip is powered and transmits its number to the reader. There is little to no security on the RFID tag or during communication with the reader. Any reader using the appropriate signal can power the RFID tag to communicate its contents. Typical RFID tags can be easily read from distances of several centimeters to several meters.

Visa Waiver Program (VWP)¹¹:

Travelers from Visa Waiver Countries are allowed to apply for entry to the U.S. on a passport for up to 90 days for business or pleasure without obtaining a visa. The following 27 countries are currently in the VWP: Andorra, Austria, Australia, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom (for citizens with the unrestricted right of permanent abode in England, Scotland, Wales, Northern Ireland, the Channel Islands and the Isle of Man).

⁹ Definition according to ICAO as appears on http://www.icao.org/cgi/goto_m.pl?icao/en/aimstext.htm#Standardization

¹⁰ Definition according to ICAO as appears on <http://www.icao.int/mrtd/overview/overview.cfm>

¹¹ Definition according to the Department of Homeland Security's US-VISIT program (www.dhs.gov/us-visit)