



## **e-Passports: Uses, Limitations, and Impact on Simplifying Passenger Travel Initiatives**

### **Introduction**

Following the events of September 11, 2001 many countries accelerated plans for the adoption of a new passport standard that would increase security of travel documents. The goal was to adopt new technology that would ensure the integrity of the passport issuance process, and improve the ability of border authorities to accurately establish the identity of passport holders who were seeking entry privileges.

With unprecedented speed, a senior group of technical experts working under the structure of the International Civil Aviation Organization (ICAO) formulated a standard for the new document, known familiarly as the e-Passport, in May 2003. The standard called for e-Passports to contain an integrated circuit (IC) chip that could securely house information about the bearer. Specifically, the standard specified that all e-Passports were to contain a “photo” of the traveler in jpeg image format. ICAO also endorsed the addition of additional identifying data such as fingerprints and iris images. In regulations published in December 2004 the European Union required that e-Passports contain a facial image plus “fingerprints in interoperable formats.”

It is exceptionally important to note that while such features are often referred to as “biometrics,” in actuality these enhancements are stored only as true images of the feature. These features will certainly be used in future applications that extract biometric data from the images, but the ICAO standards do not specify how – or if – the images are to be converted or later employed to enable the actual use of biometrics in operational programs.

Schedules for implementation of the new e-Passport vary by nation. While several nations are already issuing such documents, most implementations are scheduled to comply with current US requirements for issuance systems to be in place by October 26, 2006. Due to the typical ten-year expiration cycles of the current generation of passports, however, it will be a decade before countries that provide the major sources of global tourism will be completely converted to the new, more secure format.

As these new capabilities come on line it is important to have a clear picture of how the documents may be used to tighten up issuance systems, establish a traveler’s identity, and assist with the automation of certain travel processes. Some of these uses are obvious;

some are open to interpretation by implementing states; while others may be infeasible because the capabilities of the technology do not match the security requirements for sensitive programs and applications. This document explores those issues within the specific framework of the goals of the IATA Simplifying Passenger Travel Interest Group (SPTIG) initiatives: to use biometrics and other technologies to speed up and automate services for the purpose of improving the travel experience.

## **E-Passport Features**

The e-Passport expands upon ICAO standards that have been in place since 1978, when states adopted the machine readable zone (MRZ) format that is now a nearly universal characteristic of passports. That format required the use of either a two-line (for passports) or three-line (for identity cards) zone that displayed critical biographical information on the document bearer in a manner that could be automatically scanned and converted to usable data by a new generation of passport readers. This was a revolutionary advancement that:

- Enabled border officers to automate watch list checks in near-real time during inspection
- Permitted airline staff to generate manifests of passengers without having to resort to more labor-intensive means of data entry such as keystroke
- Created a standardized “token” that could automate inspections by retrieving a traveler’s biometric information from an enrolment database

The e-Passport standard preserves the machine readable zone (MRZ) and adds all of those visible data elements to the IC chip: full name, date and place of birth, date and place of issuance, and passport number. As noted above, the 72-kilobyte chip (64K of which is available for data storage) also contains one or more images of biological features of the bearer, with the face image being mandatory. These images are secured on the chip and stored with other data in a “read only” format; in theory, the information may not be changed after it is written to the chip. This quality enables the introduction of a public key infrastructure (PKI) scheme to provide an even higher level of reassurance to border officials that the document being proffered at the port of entry is genuine.

## **Uses for e-Passports**

The attributes inherent in the e-Passport provide a heretofore unavailable means of improving the security of the international travel system. These are described below under three general categories: preventing the use of multiple identities; linking the bearer to the document in a traditional border operations environment; and serving as a strong token to drive a biometric identification process. After these uses have been explored in some detail, the paper will examine why the e-Passport may not be universally accepted by states as the sole device used to fully automate the border clearance process for registered participants as envisioned by the SPTIG ideal process flow.

## **1. Preventing Identity Fraud**

Requiring applicants for passports to submit photographs is nothing new; photos have been mandatory features of passports for nearly 100 years. Only recently, however, have these images been stored in a computerized format that could facilitate searches that might determine if the same person is using multiple identities to circumvent visa requirements, hide from authorities, or otherwise evade controls.

As it became more common to house such information in passport databases, a number of states launched research programs to determine if new biometric applications could be used to compare one image against all other stored images for the purpose of revealing those who may be attempting to commit identity fraud. Biometric face recognition programs have demonstrated some success at this task, suggesting possible matches and ranking them for human operators to discern who may be an imposter.

Two components are required for such a system to successfully cull out identity thieves: first, a biometric program that is accurate enough to run “one to many” (1:n) checks of databases that can easily exceed 50 million records; and second, a comprehensive data set of applicant images that are stored in a common format. The ICAO e-Passport standard provides the path to acquiring that second component by ensuring that future images are received and stored in a form that makes them amenable to biometric-based checks. Once a full passport issuance cycle of 5-10 years has been completed, authorities will have both the tools and the data required to tighten up identity management processes for all travel document holders.

This type of application is most likely to be used by passport and visa issuance authorities. Improvements in the accuracy and speed of face recognition technologies may eventually make it feasible to conduct such 1:n searches in other high-risk security environments, including at the border. In either instance – during issuance or in a real-time border operations mode – the e-Passport with its imbedded jpeg image of the bearer provides the key to better control over who is attempting to defraud the international travel network.

From the viewpoint of SPT processes, this suggests that a person traveling with an e-Passport was probably subject to more strict issuance practices. It also becomes more likely that those intent on fraud will be inclined to seek passports that are not chip-enabled, and will tend to travel to countries that do not use 1:n comparisons for visa issuance purposes.

## **2. Supporting the Staffed Border Inspection Process**

The second benefit to be derived from the universal adaptation of the e-Passport standard is to establish the certainty of the relationship between the travel document and the bearer. When a traveler presents the new e-Passport at the border, the inspector will use updated reader technology to scan the chip and view the image that is stored in the document. This will enable officers or check-in staff (if airline or ground handling agents are authorized to do so) to make a quick check to determine:

- That the image printed on the document biographical information page matches exactly the image that is stored on the IC chip
- That the same image matches the person standing at the inspection checkpoint or airline counter

Note that this is a manual process; the traveler must appear before the person who is making the decision on whether they should be allowed to board or be admitted as a visitor or returning resident. An examination that takes advantage of the data on the IC chip is not guaranteed to be quicker, but is likely to be more accurate than processes that do not make use of the information.

Further automation may play a role in helping that decision maker to ascertain if there is a true match between the stored image, the printed image, and a captured image of the bearer: Face recognition technology may be adapted to compare the three sources of information and provide input on the accuracy of the data match. In its ultimate form the combination of manual examination of the data, automated input from a biometric subsystem, and validation of the document through PKI should significantly improve the accuracy of an inspection.

From the standpoint of supporting SPT ideal flows, the ability to tie a particular person to his or her document at a staffed checkpoint has several related benefits. On one hand, it creates a strong base from which to draw an expanded group of participants for an expedited traveler program. Less directly, it helps border officials to manage risks between those who possess the new generation passports and those who may be trying to fool the system by relying on less secure forms of identification.

### **3. Serving as Secure, Common Tokens for Automated Programs**

To date, trials that have been designed to test how biometrics may be used to automate passenger services have usually relied on different types of “tokens” to trigger the process of confirming the traveler’s identity against a stored record. Typically this token – sometimes a simple pointer like a magnetic stripe card or personal identification number, other times a complex PKI-protected smart card – implies a relationship between a “live” biometric check and data that is housed in a database or on the token itself. Using a token simplifies a task that might otherwise require a search every record in a database to confirm identity. The existing ICAO MRP passport has been used as this type of token since the means of printing and reading the data in the MRZ is fully standardized.

Certain programs have avoided this operational model by using 1:n technologies such as iris recognition. Nevertheless, most biometric-based automation projects rely on tokens for a variety of reasons: tie-ins with marketing programs, flexibility in the choice of biometric technologies, usability features that make operation similar to other familiar applications such as automated teller machines, and compatibility with commercial standards for card and data storage formats. While implementation of such systems was relatively simple, there were a few disadvantages:

- Tokens were different from program to program, which in turn limited the scale of any passenger automation scheme
- Consensus was difficult to obtain on selecting any one token that could be used bring programs to critical mass, i.e., achieve enough acceptance world wide to favorably affect operations and truly simplify traveler services
- Concerns about data privacy led to objections over the use of MRZ-based passports as tokens for accessing biometric information held in databases

The advent of the e-Passport provides a way to get around most of these barriers. By setting a standard for the secure storage of chip-based data and thereby providing a key component of a PKI-based architecture, the e-Passport surmounts practical technical questions that may have otherwise prevented agreement on specifications for tokens. By virtue of its global acceptance, the e-Passport may also resolve conflicts over how to achieve the all-important critical mass that is essential to the success of any plan to divert low-risk travelers to reliable, secure automated services.

In operation the e-Passport fulfills the requirement for a standard pointer/token that can be used to initiate checks against biometric information that is stored by a valid enrollment authority. By placing the e-Passport on a chip reader, a traveler making use of an automated service notifies the authority that (a) a unique string in the form of a passport number is telling the system which record is to be checked to confirm his or her identity, and (b) that unique string is valid according to the PKI management scheme. This provides both a robust and universal method of establishing and expanding large scale programs that would otherwise be stalled by a balkanized token issuance process.

For SPT this is a welcome if somewhat deferred step. As noted elsewhere in this document, conversion to the e-Passport standard will not take place overnight. Authorities who are seeking quicker progress in automating low-risk traffic at border control checkpoints may be inclined to substitute other tokens such as passports that comply with the older MRZ standard. While clumsier to use by passengers, the introduction of a process that relies on the existing passport to activate biometric checks will carry over into future iterations that use e-Passports to do the same thing. Taking such an initiative now ensures that border authorities can free up and redirect resources to critical security priorities much sooner than if they were to await full adoption of the new standard.

### **Where e-Passports May Fall Short**

In the introduction above it was noted that e-Passports do not contain biometrics per se, but rather encrypted images that are stored in jpeg format. In many cases the only image on the chip will be that of the face of the bearer. While it is clearly possible to import that image into a biometric face recognition application and compare it to the live image of the user, many border authorities have expressed reluctance about relying on such a comparison to determine admissibility on a fully automated basis. As a result, the e-Passport containing a stored face image alone is not likely to be widely used as a “closed loop” solution to border automation, wherein a check of the individual’s video image

against the data on the IC chip is the sole basis for granting access without officer intervention.

There are several reasons for the concerns that will inhibit border authorities from relying on a biometric that is derived from the face image stored on the chip:

- Face recognition technology is susceptible to spoofing by imposters who may use an active disguise to look like someone else, or may simply have features that are very similar to those of the passport holder
- Even if authorities are willing to tolerate some level of risk caused by false acceptances (“false match” in biometric industry terminology), the false rejection (“false non-match”) rates for face recognition technologies may have a negative effect on border officers who must be called on to resolve any system errors before a traveler may be allowed to proceed through controls
- Opportunities for chip tampering (altering the information on the IC chip) and data skimming (illicitly reading the information on the chip from a distance) raise major security risks in an automated clearance environment

Adding additional biometric images to the chip may reduce some of the security and operational concerns, as both fingerprint and iris recognition biometrics will provide more accurate performance in border control applications at the present level of technical development. Again, however, simply adding more data to the chip is not likely to provide full protection against penetration attempts that are built around the vulnerability of a setup that makes decision solely on the basis of information on passport.

This weakness may be overcome if the additional images (fingerprints in the case of the EU, and perhaps iris elsewhere) that are contained on the e-Passport are first validated by an enrollment authority and then stored separately in a database. An architecture in which these verified images are used to confirm an identity that is linked to a particular passport by checking against a secure database is a powerful concept of operations that could be used to eventually cover a large percentage of travelers.

This is a very optimistic scenario, however – so much so that SPT efforts will be weakened or subverted if they are designed around such an assumption. Countries are not likely to adopt a more stringent data collection requirement in connection with passport applications, and will instead adhere to the basic standard by requiring applicants to submit photographs that may be digitized for use on the IC chip. In some cases this will be due to privacy concerns about the amount of information that should be provided to governments; in other cases it will be attributable to the logistic impediments involved in acquiring fingerprints, iris images or other biometrics as part of an issuance regime. With this being the case, automated traveler programs will have to rely upon a separate data collection and biometric enrollment scheme that build on rather than rely strictly upon information contained in the E-Passport.

## Summary

The impact of these circumstances on SPT programs is complex and profound. Since the ICAO standard was adopted, there has been a tendency within the Interest Group to look to the e-Passport as the sole tool to be used in all automated initiatives. While the documents will be certain to play a key role in any future SPT architecture, the e-Passport cannot fulfill all the requirements to automate and expedite passenger flows due to the limitations described above. Briefly:

- The ease of use associated with chip-based e-Passports will make them useful as a token in many future automation schemes
- Border authorities will benefit by being able to establish a clear link between a valid document and the traveler at a staffed primary checkpoint
- The ten-year deployment cycle for e-Passports will not be quick enough to satisfy the demand for large scale IPF-based programs in the near term (3-5 years), necessitating the adoption of an architecture that relies on a separate token such as the existing MRZ passport, or that uses 1:n biometric search techniques
- For both technical and policy reasons, the e-Passport that contains only a face image will rarely be used as a stand-alone solution to security-sensitive traveler automation programs. For e-Passports to be employed in this fashion, other data such as fingerprint templates, iris templates, or WSQ finger images will have to be included on the chip.
- Near-term projects that are aimed at automating passenger services are likely to continue to collect and store additional biometric information that will be placed on secure cards or in databases. Some sharing of information or trust levels between cooperating states may ease enrollment challenges assuming traveler participation is voluntary and such use is specifically authorized by that user

Given these circumstances it is imperative that the SPTIG adopt a pragmatic approach to implementation that will provide measurable results soon. The group cannot wait both for the full emergence of the e-Passport, and for improvements to be made to the technologies related to those documents. To make this mistake will cause needless and ill-advised delays in achieving the goals of the SPT initiative within a reasonable time frame.

## Recommendations

Over the course of five years SPTIG has led a global initiative to solve some of the critical problems that continue to stifle growth in tourism and hinder enforcement efforts. As put forth here, now is not the time to freeze SPT initiatives while waiting for external developments to take root. The E-Passport holds promise for fulfilling some important functions in travel control and facilitation systems, but it will be many years before it can stand alone as the only “key” required to expedite travelers through automated processes.

SPTIG can continue to provide leadership in the introduction of well-designed, innovative concepts that can be implemented throughout the global travel network. To do so, however, it must advocate a clear vision of how its goals can be reached soon

enough so that its continuation as an organization is justified. The recommendations below are meant to serve as guidelines that can be followed to ensure that the momentum of the group is not stalled, and advancements can be made in time to make a difference.

1. As the pace of issuance picks up over the coming decade, e-Passports will become an important new tool that will prevent multiple identity fraud, facilitate prompt verification of a traveler's identity at a staffed checkpoint, and function as a secure pointer/token that helps automate key stages in the SPT Ideal Passenger Flow.
2. SPTIG fully supports the aggressive use of e-Passports for these and other applications that are designed to make travel safer and improve enforcement. SPTIG also strongly endorses issuance standards that enable border authorities to access the data in a uniform, consistent manner, and that facilitate interactive data verification programs at points of embarkation.
3. Standing alone, e-Passports that are limited to storing just the face image may be used to automate some checks depending on national policies and the level of threat associated with the service being performed. In many instances, however, such documents may not contain sufficiently secure information about the traveler to always enable full automation of sensitive processes such as check-in, security checks, boarding, and border crossing.
4. SPTIG encourages states to supplement baseline 2003 ICAO requirements for e-Passports with additional biometric information such as fingerprint or iris images.
5. To press forward in the near term with Ideal Process Flow-based programs that meet the requirements of border and security authorities, additional biometric information may need to be collected and stored in a secure database consistent with data protection laws and with the full permission of the traveler.
6. If the biometric information is to be stored in a database, then the e-Passport, a card, the existing MRZ passport or in some cases the biometric itself may be used as the token that facilitates the automated transaction.
7. SPTIG strongly advocates the immediate implementation of the Ideal Process Flows that can later be improved and upgraded as the e-Passport enters the deployment phase.

Richard Norton  
Executive Vice President  
National Biometric Security Project  
601 13<sup>th</sup> Street, N.W.  
Washington, DC 20005 USA  
Tel. +1 970 259 3015