

Towards Registered Traveler program implementation

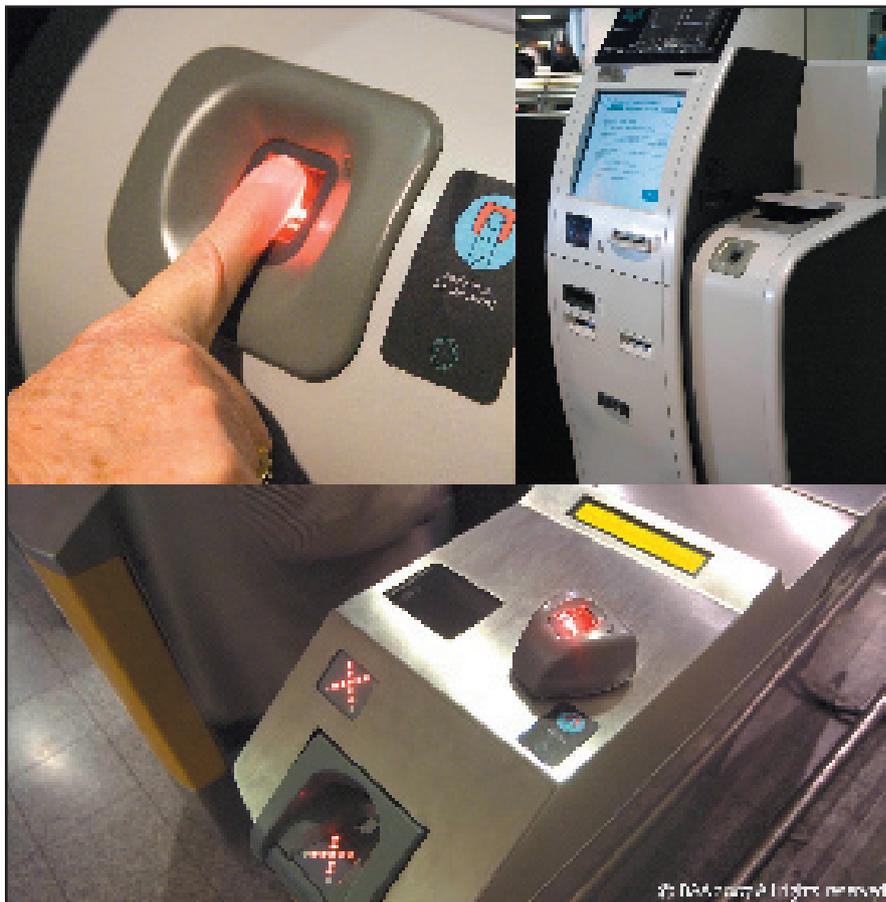
Numerous Frequent Traveler pilots have shown their “queue-busting” benefits as well as their popularity with passengers. To develop further, however, a number of restricting elements, such as interoperability, still need addressing

With Daedalus’ son Icarus finally crashing into the sea below, the wax gluing his wings having melted in the heat of the sun, Greek mythology presented us with the world’s first pair of frequent flyers. Chronologically, the first element needed to build a modern Registered (or Trusted) Traveler program - a Frequent Traveler card - was probably field-trialed in approximately 450 BC, and is the first official travel document ever encountered. It was delivered by the Persian King Artaxerxes as a request to the governors of the provinces beyond the river to grant safe passage to his official Nehemiah while on a trip to Judea. Nehemiah’s security background check was judged safe enough by the King’s officials, and he thus became the first ever FT enrollee.

The next elements of the puzzle, namely the first Bilaterals, were the first safe conducts ever granted to foreigners. They were provided to certain travelers during the reign of King Henry V, starting 1413, and already included reciprocity as a unique deterrent, since the offended country had no recourse other than to declare a war of retaliation in the case of a safe conduct breach.

The earliest “MRTD” still in existence is British. Granted in 1641 and signed by King Charles I, it enabled the bearer to “pass through ports” (doors, rather than sea ports), culminating in the term that we all know and use today. The first occurrence of the term “visa” in travel terminology, meanwhile, defined as “an official signature or endorsement on a passport”, was reported in 1831.

The first real frequent traveler to cross a border was Charles Blondin (the stage name of Jean-François Gravelet), a former Barnum funambulist, who crossed the Canadian-US border in 1859 on a tightrope anchored 190-feet high over the Niagara gorge. He



Heathrow’s BAA miSense RT pilot: IER Passport reader side-car, check-in kiosk and access control portal with fingerprint capture, to speed up and enhance security

made this “journey” several times over the following months, even breaching the most elementary of security rules by carrying his boss on his back on one occasion. Official records of Canadian-US border crossings for nationals from both countries followed this acrobatic border crossing only from 1895.

The RT paradox

All Registered Traveler programs aim at speeding passengers through airports, via

prior enrolment, using specific fast tracks and procedures open only to authenticated members. As these programs almost invariably involve border crossing, a growing interest has been shown in coupling automated controlled entry into a given fast track with the subsequent (automated) border crossing.

There are still two main factors restricting the development of Frequent Traveler programs, however. Firstly, there is an inherent conflict of interest amongst the indus-



Charles Blondin - the first true frequent cross-border traveler?

try stakeholders favoring such programs, between facilitation (mainly backed-up by airports, airlines and ground handlers) and security (restrictions mainly imposed by Border Control and Immigration but also state laws in the destination country). Secondly there are the technological obstacles to providing scalability (present diversity of ID authentication tokens, methods and infrastructures) and the subsequent basic lack of interoperability between potential FT program partners.

Paradoxically, industry stakeholders wishing to further “democratize” Frequent Traveler schemes, for example by offering biometrics-enabled access to special Fast Tracks to pre-registered Frequent Flyers at airport premises, will have to negotiate enrolment procedures and conditions of maintaining the passenger status with the relevant Control Authorities in the departing and possibly even at the destination country.

One of today’s quandaries concerning the frequent travelers to whom airports want to propose accelerated services is whether they should be considered as “known”, “registered”, or even “trusted” when they show up at the airport. In general, “trusted” is a qualifier loathed by many immigration departments, who generally prefer (and practice!) the term “known”.

Some successful FT Program pilots

Numerous Frequent Traveler programs have been quite successfully introduced both in Europe and the Far East, as part

of either government or private initiatives to speed up passenger transit, including automated border control.

One of the most successful Registered Traveler programs is the IRIS biometrics program for border crossing activated at major BAA airports in the UK. It accepts UK as well as non-UK citizens who successfully pass the background checks performed while they wait to enroll at the airport. It uses neither a smart card nor a token. All biometrics data collected at enrollment is stored into a government secure database. The program, aimed at expediting border crossing for known travelers, was launched about 2 years ago. It is offered for free and continues to develop (over 61,000 enrolled with over 210,000 border crossings by February 2007) as a precursor to the e-Borders UK project, and thus with a strong Control Authority connotation.

Similarly, the French “Pegase” program, originally a 6-month trial, has been extended for more than a year and now has around 10,000 enrollees. It is also free. It was originally geared to Air France frequent flyers traveling outside of the Schengen area, but was opened to citizens from various countries for immediate enrolment following background checks by an official immigration police officer. Here, the token is a smart card holding fingerprints of the passenger’s 2 index fingers. The trial will terminate shortly and is expected to evolve into a full-scale automated border control deployment in France under the name “Parafes”. Secure border crossing (both at departure and arrival) is achieved using an airlock which guarantees the presence of a single individual during the biometric authentication process.

Other border crossing programs are run by private organizations, such as the Schiphol “Privium” program, active for almost 5 years now, which for a yearly fee offers EU and Swiss citizens a “queue buster” to automated immigration control with associated privileges such as priority and discount parking. Membership had grown steadily to over 30,000 members by October 2006.

Automated Border Control using official MRTDs (actually contact smart cards

checked inside of an airlock) has been going on in Malaysia for many years and is currently also deployed in Hong Kong. Here, all nationals can benefit from the automated process, since they are required to present a valid National ID smart card at the immigration checkpoint.

Finally, in North America, existing Registered Traveler programs across the US-Canada border include Canpass and Nexus-Air, soon to be merged with other sea/land US-Canada border crossing programs. Nexus includes biometrics enrolment (iris) but has not grown as quickly in terms of enrollee numbers as its European counterparts. An alternative fee-paying program has been launched by Orlando airport with TSA approval and private funding, specifically targeting “queue busting access” to the security checkpoint. A few other US airport sites are being targeted by this program.

MiSense and MiSense Plus

Another recent pilot was successfully undertaken at Heathrow by BAA and the UK Home Office. The trial was put together by a consortium of corporations, all members of IATA’s Simplified Passenger Travel Interest Group, as a working prototype for the first world-scalable and multiple stake-

Secure IER Airlock at Charles De Gaulle airport for Pegase Automated Border Control



holder common Registered Traveler program, including both departure and arrival immigration Fast Tracks. It has received a lot of attention from the media, which has understood its potential for scalability and global implementation.

The pilot involved around 2,000 volunteers who agreed to immediate biometric enrolment, with the capture of the (standard) passport data page and a complete online background check, followed by fast track, biometrics-controlled access to the security checkpoint. Symmetrical features were granted to registered travelers upon arrival, including those who had earlier enrolled in the parent Dubai and Hong Kong automated border control schemes. MiSense is the first working model for multi-site registrations in different countries to allow for common passenger travel facilitation in a totally secure process.

Interoperability issues

One major drawback to the majority of Registered Traveler programs is their lack of interoperability, since not every document checking scheme is compatible, as yet, with ICAO recommended practices for MRTD's (ePassports or National IDs using contactless ISO 14443 at 13.56 MHz).

Currently very few of the 40 countries al-

ready producing ePassports have deployed the necessary ePassport reader infrastructure at their customs clearance locations to check even their own ePassport-holding citizens. This really should be a top priority.

Visa seekers from non-visa waiver countries

Another twist to the Frequent Traveler program concept is the fate of all visa seekers (from non-visa waiver countries). Paradoxically, these visa seekers form a particularly "safe" category resembling Frequent Travelers. They are obliged to first pay, queue at a consulate in their country of origin, willingly submit to full biometrics capture (10 fingers, face, etc), then wait for days or weeks before either receiving or being denied a visa.

So, what better level of security could the receiving country dream of than taking all the time it needs to cross-check each visa seeker's background, for example for non-duplicate earlier submission/rejection to/by the same country (or to/by any other neighboring country in the case of a Schengen visa request)?

Paradoxically again, these same visa seekers, once in possession of their visa, tend to spend extra time at border control upon arrival even though they should logically represent much

less of a risk to the receiving country if their biometric match was found to be OK.

The 35 million visa seekers across the world each year certainly surpass "classical" frequent traveler deployment volumes by more than an order of magnitude, yet they represent a massive traveler control overhead, which could be helped by secure and automated visa processing.

This is one of the areas where full data sharing, say at the SIS II level (Schengen Information System), should bring tangible and uniform results. Obviously too, even those visa requests that have been rejected (around 25% of Schengen applications) are of particular interest to the various security forces too, since all visa seekers are now fully identified by their biometrics.

Towards supranational Frequent Traveler schemes?

Extending Frequent Traveler schemes beyond the national level, say under Schengen sharing conditions, is one challenge currently being addressed by the EU. However many other aspects remain complex and ill-defined. For example, how can you envision such programs when no emigration border control is in place (such as in the US)? If Frequent Traveler programs are eventually developed on a bi-national level, how does the second country control membership cancellation if the traveler's status changes following a security update by the first country? What would be the common basis for the MRTD infrastructure examination at arrival? Will there be a chasm between more stringent EU requirements for the new generation of ePassports in 2009 (with embedded fingerprints and their associated Extended Access Control) and the ePassports of non-Schengen based visitors? And if so, what will be the best practice for MRTD usage?

These questions (and others) are still being debated as ICAO slowly evolves to further bolster MRTD security in an interoperable way, possibly zeroing in on a standard ISO 14443 13.56 MHz common reader infrastructure platform for both ePassports and other eTravel documents such as electronic National IDs.

by Jean Salomon,
IER

If the inherent conflict of interest between industry stakeholders, and between facilitation and security can be resolved, passengers may begin to enjoy the real benefits of RT programs

