E-passports in border processing
Survey offers unique insight into e-passport inspection and validation practices

by Stéphanie Brodeur & Nicoletta Bouwman

In 2008, members of the Roma/Lyon Migration Experts Sub-Group (MESG) conducted a survey among the G8 member states and the participating states of the NTWG. Their objective was to establish the extent to which states read and validate e-passport chips at border crossings points. Stéphanie Brodeur and Nicoletta Bouwman of Passport Canada report.

The International Civil Aviation Organization (ICAO) New Technologies Working Group (NTWG) was tasked with the introduction of globally interoperable biometrics in travel documents in 1997. Their objective: to create a biometrically verifiable link between the document and the person to whom it is issued. The first e-passports appeared a mere eight years later, in 2005. Four years on, some 66 countries issue e-passports, while a further 17 are expected to do so by the end of the year. Significant investments have been made in the development and roll-out of e-passports, resulting in a document that combines the latest technology with tried-and-tested security features.

The full benefits of e-passports in terms of security and facilitation are not realised until the information stored on the e-passport chip is read and validated. An integrity check involves verifying the original data to make sure that it hasn’t been tampered with since the document was issued. The check also establishes that the document was issued by a bona fide issuing authority. E-passports are validated on the basis of Public Key Infrastructure (PKI) certificates. The PKI infrastructure allows border control officials to authenticate the travel documents with which they are presented.

Information about the number of countries with the infrastructure needed to read and validate e-passport chips was limited in 2008. As the G8 Roma/Lyon Counter-terrorism and Transnational Organized Crime Group continued to prioritise measure aimed at tackling the fraudulent use of travel documents, the Roma/Lyon Migration Experts Sub-Group (MESG for short) initiated a project to fill the knowledge gap.

Project methodology
In July 2008, MESG sent all G8 member states and NTWG participating states a questionnaire covering the use of e-passports at border crossing points. The aim of the survey was to establish the extent to which states read and validate e-passport chips at border crossings points. It also sought to identify the different types of implementation strategies and operational processes currently in use. A total of fourteen countries responded (Australia, Canada, France, Germany, Italy, Japan, Latvia, The Netherlands, Norway, Portugal, Russia, the United Kingdom, the United States and Switzerland).

Findings
Of the fourteen respondents, eleven indicated that they retrieved data from e-passports presented at border crossing points. Two additional countries signalled that they intend to do so within two years. The degree to which chip-reading functionality has been implemented varies - whereas some countries have initiated trial projects, others have opted for full-scale implementation. Another interesting finding is that the majority of respondents read (or intend to read) e-passport data at entry as well as exit points.

Implementation process
Most countries have opted in favour of the phased implementation of e-passport chip readers. In practice, pilot projects or trials based on specific document types (eg, diplomatic and official passport), specific ports of entry (eg, air, land, or sea) or specific regions are generally followed by the gradual roll-out of e-passport readers at key crossing points. The next step in the process is to initiate a nation-wide implementation.

Reading the e-passport chip
The survey showed that most respondents (intend to) read e-passport data at primary and secondary inspection points. States that have implemented automated border control (ABC) systems read all passports presented by travellers eligible to use these
systems. As is the case today with machine readable passports, some countries will continue to risk-manage their border management by focusing on those that are deemed to be of higher risk.

In all instances where e-passports are read, the data retrieved from the chip is compared to the biographical data page as well as a database of lost and stolen passports. A total of ten countries compare data to a watch list. A handful of countries additionally compare the chip data to a database maintained by the domestic issuing agency.

All countries that retrieve e-passport data compare the digital image stored on the chip to both the photograph on the biographical data page and the actual passport holder. Four countries have integrated facial recognition in their border clearance processes while one retains a copy of the digital photograph (which is compared to the photo on the chip during subsequent inspections to ensure that the chip has not been tampered with).

**Verification of the e-passport chip**

Six states verify the Country Signing Certificate Authority (CSCA) when the e-passport chip is read. This check is conducted at all automated border control points and, in some states, only when a traveller is referred for a secondary inspection. Several countries have indicated that they intend to conduct this check in future.

The ICAO Public Key Directory (PKD) was created to establish a central entity for authentication of e-passports by verifying document signing (DS) certificates and checking certificate revocation lists (CRLs) rather than relying on bilateral exchanges of such information between individual states (see for an extensive description of PKD’s role and functions the article of Markus Hartmann and Stephan Körtling on page 3 of this issue). It ensures that uploads are timely and that technical standards aimed at interoperability are implemented and adhered to². Eight respondent countries - six G8 member states, Australia and Switzerland - have already joined the ICAO PKD while four other countries have expressed an interest in doing so.

**Lessons learned**

**Interoperability challenges**

While all states were able to read their own e-passports, several reported difficulties reading foreign documents. Issues raised primarily relate to differences in processing times due to the use of different chip types. Chips in earlier e-passports proved problematic, suggesting that interoperability has improved as technology has advanced. According to some states, several travel documents failed to meet ICAO’s standards. The use of different image types, incomplete or inconsistent data, and uncertainty about the authenticity of digital signatures due to missing country signing certificates were quoted as the main underlying reasons. Interoperability hinges on compliance with ICAO standards, not least because existing systems are designed to read documents that meet these standards. To ensure interoperability, it was suggested that states exchange specimen e-passport documents to test their readability. Such tests could also be used to verify reading systems. If necessary, such tests would also allow modifications to be made to an e-passport prior to its large-scale production.

**Security**

Several countries have detected tampered documents on the strength of the digital image stored in the
passport chip. The verification of digital signatures was considered the best security measure. One state indicated that facial recognition had helped to raise security considerably. No countries encountered instances of eavesdropping (the unauthorized interception of communications between chip and reader).

**Facilitation**

In some countries reading e-passports raised processing times by up to 10 seconds per document. Other countries reported relatively stable processing times. The time needed to process e-passports at ABC systems varied between 10 and 45 seconds.

**Experience**

The participating states identified several factors to be taken into account when developing and implementing an e-passport reading system at border crossing points. The two most common recommendations were to ensure readers were capable of data processing at acceptable time levels and that border systems are flexible enough to accommodate future upgrades and improvements to readers as well as e-passports. Some states considered the human aspect to be of critical importance. According to these countries, it is necessary to have highly skilled and properly trained immigration inspectors working with e-passport reading systems and not relying solely on document technology for the border control function.

Countries using ABC systems mentioned ease of use and fault tolerance levels as being of key importance. It was felt that end-users should be involved at the project inception stage while public education and awareness were also deemed crucial.

Many states emphasized the importance of early planning (recommended as a best practice). Clear communication between the document issuing authority and the border control authority also featured high on the list. Several respondents emphasized the need for relevant expertise and adequate staff training. For these countries, technology is a tool rather than a necessity.

**Communication of results to ICAO**

A report setting out the survey findings has been sent to the NTWG and the ICAO Implementation and Capacity Building Working Group (ICBWG). The outcome may be used to define areas where existing technologies can be improved. It can also be used to assist ICAO in determining where capacity building assistance may be required in the future.

The final report recommends that the G8 member states and ICAO jointly encourage countries to integrate the reading and validation of e-passports in their border control processes. It also proposes to recognize the ICAO PKD as the mechanism of choice for achieving this objective. This not only promotes the use of more secure travel documents and border control processes around the world, it also encourages closer collaboration between passport issuing authorities on the one hand, and border control authorities on the other. On 30 May 2009, following their meeting in Rome, the G8 Justice and Home Affairs Ministers issued a final declaration that not only recognises the need to verify data stored on e-passport chips, but also the role played by the ICAO PKD: “As e-passports add new security capabilities, interoperability will be crucial. We request all states to verify the authenticity of the information in e-passport chips and to use the International Civil Aviation Organization Public Key Directory to do so when their national legislation permits. The G8 fully supports the ICAO recommended practice that Contracting States issuing or intending to issue e-passport and/implementing at border controls automated checks on e-passport should participate in the ICAO PKD.”

---

1 The primary inspection point is the first point of contact a traveller has with border officials when entering a country. If the primary inspection is successful, the traveller is admitted to the country. If not, he or she is referred to a secondary inspection point where additional checks are performed. The secondary inspection officer subsequently determines whether to admit or deny entry to the traveller.

2 ICAO PKD website: http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx.

If you would like to respond to the contents of this article, please send an email to kjd@keesing.nl