E-Passports and automated border crossing
A view on interoperability issues

by Antonia Rana

Since the few years that electronic or e-Passports have been in use, considerable experience has been gained regarding their usage. It is obvious that, in order for e-Passports to be read and processed worldwide, implementations in different countries must be able to interoperate, i.e. readers and inspection systems all over the world must be capable of correctly interpreting the data and security measures implemented in e-Passports produced in other countries. However, interoperability is a complex issue and the strict use of technical specifications is only one part of the picture. In this article, Antonia Rana explains which components need further attention. She would like to stress that the views expressed in this article are purely hers and may not in any circumstances be regarded as stating an official position of the European Commission.

Motivations for the e-Passport

The new e-Passport (also known as biometric passport) was first introduced in the EU in 2006 under Council Regulation No 2252/2004, which defined the standards for security features and biometrics in passports and travel documents issued by member States with the purpose of improving document security and preventing falsification of documents. The Regulation further prescribed that as of June 2009 the countries in the Schengen area would be issuing second generation e-Passports, i.e. biometric passports with a secondary biometrics: fingerprints in addition to the facial image required by the ICAO Document 9303 and already stored in first generation biometric passports.

The main motivation for the introduction of the e-Passport was the need to increase global security in the aftermath of 9/11, 2001 by increasing the security of travel documents, but also to prevent forgery and reduce the risk of impersonation by providing a means to strongly link the passport to its owner through the use of biometric features. Use of electronic features which could help automate the validation and verification process, meant that frequent travellers would benefit from a faster, more accurate and convenient border crossing, building on the experience some airports already had with registered travellers schemes.

Integrated circuit contactless card

The new passport described in the ICAO 9303 Document does not replace the classical passport booklet. Rather, as a result of the discussions on the most appropriate technology to respond to the requirements of security and convenience, that booklet is complemented by the introduction of an integrated circuit contactless card and antenna. In its Contactless IC Chip Technical Report of 2003, the ICAO New Technology Working Group (NTWG) established that the contactless card was the most appropriate technology for data storage in the new e-Passport (see box 1 for more information on the technical specifications of the chip).

To authenticate the data stored electronically in the passport chip, public key cryptography is used, making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented. In fact, the EU passport uses two different Public Key Infrastructures (PKIs) in order to provide additional security measures to protect the secondary biometrics: the two fingerprints stored in D63 (see box 1). Whereas access to the facial image and biographical data (which are also printed on the data page) is possible to all inspection systems complying with the ICAO 9303 specifications, access to the secondary biometrics is granted only to authorised border authorities in the EU, due to the additional extended access control which implements terminal authentication and requires additional key management capabilities.

Security and privacy in the e-Passport

Several protection mechanisms have been designed to protect the security and privacy of e-Passports:

- Attacks such as tracking and tracing can be avoided by using randomly generated chip ID, as allowed in ISO/IEC 14443.
- Skimming attacks can be avoided by shielding the chip and antenna.
• Cloning can be avoided by checking that the chip is authentic with Active Authentication (AA) or with Chip Authentication (a component of EAC, Extended Access Control).
• Eavesdropping is avoided by creating a secure encrypted communication channel between the reader and the chip.

**Basic Access Control**
The secure encrypted communication channel between reader and chip is provided through Basic Access Control (BAC), which uses a symmetric encryption key to encrypt the communication derived from the MRZ (see figure 1). What BAC does is:
• It only allows reading the data that is both stored in the chip and printed on the data page. The only element required to access these data is the MRZ. The reader needs to optically read the MRZ printed on the data page in order to calculate the secret key. BAC requires the holder’s consent since it needs the value of the MRZ to calculate the secret encryption key, and by physically handing over the booklet, the holder gives their consent to reading the chip.
• It only allows those who are authorised to read the data on the chip.
• It determines the amount of data that can be read.

**Extended Access Control**
Extended Access Control (EAC) on the other hand, is a more complex protocol. It allows EU border control authorities which have the required chain of certificates in their terminal devices to read those biometrics that are considered ‘sensitive’. In fact, in addition to incorporating chip authentication to prove to the reader that the chip is genuine, EAC also requires the reading device to authenticate the chip and thus prove that it is entitled to access the ‘sensitive’ data (terminal authentication).

**The process explained**
Basically, country A sets up a Country Verifying Certification Authority (CVCA) which will issue certificates for countries to which it wishes to grant access to secondary biometric data. The root certificate of the CVCA of country A is stored in the e-Passport chip issued by country A and serves as the initial point of trust for the validation of the certificate chain sent by the inspection system to the passport chip for terminal authentication. If country B wants to read secondary biometric data in passports from country A, they will have to set up a Document Verifier Certification Authority (DVCA) which must get a certificate from the CVCA of country A. The DVCA then issues terminal certificates to its inspection devices which need to access the biometrics data. During Terminal Authentication, the inspection device is required to send a certificate chain including:
• its certificate signed by its DVCA;
• the DVCA’s certificate signed by its CVCA;
• its CVCA’s certificate signed by the CVCA of the country in which the passport was issued.

The passport chip also contains its CVCA’s certificate which it uses to validate the certificate chain provided by the inspection devices. This simplified description of a complex process (see figure 2) shows that access is granted when the validation of the certificate chain by the e-Passport’s chip is successful. The CVCA certificate is stored in the passport chip in the production or (pre-) personalisation phase. This certificate infrastructure is different from the PKI used to distribute the Country Signing Certification Authority (CSCA) certificates. These CSCA certificate are used to sign the chip content for passive authentication and are X.509 certificates which can be distributed (in addition to the certificate revocation lists) via the ICAO PKD.

On the other hand CVCA/DVCA certificates, distributed through the Single Point of Contact as specified.
in footnote 3 are a simplified version of the X.509 certificates, known as Card Verifiable Certificates (CVC). This choice has been made because of the limited computational power of chips with respect to inspection devices.

**What is interoperability?**

It is obvious that, in order for e-Passports to be read and processed worldwide, readers and inspection systems in different countries must be able to interoperate, i.e. be capable of interpreting the data correctly and security measures implemented in e-Passports produced in other countries. Interoperability was a fundamental goal of ICAO when finalising the technical specifications of the e-Passport. This might seem trivial but in practical terms it is not.

Technical specifications of standards often contain choices and optional parameters which, while giving users the choice to select the most suitable characteristics, can result in systems that may have difficulty in talking to each other efficiently. Interoperability is defined as “… capability of inspection systems (either manual or automated) in different States throughout the world to obtain and exchange data, to process data received from systems in other States, and to utilise that data in inspection operations in their respective States”\(^2\). The standard then continues stating that “Global interoperability is a major objective of the standardised specifications for placement of both eye readable and machine readable data in all MRTDs.”

**Different levels of interoperability**

Figure 3 shows a schematic overview of interoperability layers. At the lowest level, interoperable systems must agree on the same syntax, i.e. on a common language to describe the objects, data and information that two communicating systems (in this case a passport chip and an inspection system) want to share. This level involves the technical aspects related to the specifications, such as the way data is organised in the chip, the communication protocol and the security algorithms.

---

**Box 2**

**The Open Systems Interconnection or OSI model**

The OSI model is considered a primary standard for intercomputing. Today many network communication protocols are based on the standards of this model, which consists of seven layers. The layers further divide the tasks of moving the data across the network into subtasks and hence complete one communication cycle between two computers or two network devices.
At intermediate or semantic level, there has to be a common understanding and interpretation of the data shared between the two communicating systems. On this level the data stored in the passport interpretes, for example the specifications of the biometrics, how to store and interpret the facial image and fingerprints and how these biometrics are to be used in a universally interoperable manner.

Finally, for the two systems to accept the results of the communication and make sure that processes and procedures at the two ends of the communication are comparable, process or organisational interoperability is required. This level includes organisational, procedural and legal aspects, but also the protocols associated with key exchange and key management policies for the correct implementation of the security mechanisms, which often include so-called ‘out of band’ mechanisms which cannot be handled in an electronically processed manner.

**Two steps to ensure interoperability**

Two steps can be distinguished to ensure interoperability. The first one is testing for conformity to the technical specifications at the syntactical layer. Implementation of the standard may differ slightly. Tests specifications aim at covering all possible cases that can be handled by a chip (or a reader), including, in particular, expected behaviour in error conditions. Running a full set of tests covering all possible conditions in data structuring, message passing and error handling is the fundamental component in testing for conformity, because in this way non-compliant behaviour of passports can be identified. These tests can in turn be a cause for non-interoperability.

The second step in testing for interoperability is crossover testing, in which the communication between readers from different vendors, e-Passports and inspection systems is tested. crossover testing helps identifying problematic combinations, which can then be the subject of detailed analysis in order to spot where the problem is: either in the passport chip, the reader or the inspection system.

Communication between the passport chip and reader/inspection system covers all the communication layers of the Open Systems Interconnection or OSI model (see box 2). Similarly, tests suites include tests cases to be run at different layers of the OSI stack. Conformity tests for layers 1, 2, 3 and 4 cover physical parameters and low-level communication, and they are described in the ICAO technical report RF protocol and application test standard for e-Passport - part 2: Tests for air interface, initialisation, anti-collision and transport protocol. This specification comprises about 200 test cases (3 tests on layer 1, 4 tests on layer 2 and...
10 groups of tests on layers 3 and 4. Conformity tests for layers 6 and 7 cover high-level communication and data structures and are described in the ICAO technical report RF protocol and application test standard for e-Passport - part 3: Tests for application protocol and logical data structure. This specification comprises about 160 tests for layer 6 and about 40 test cases for layer 7. An example of an error condition in which the correct behaviour would be assessed by these tests is test case 7816_B_40 on layer 6 which verifies that the passport refuses to send data without encryption once BAC is established. Clearly the test fails if the passport does not refuse.

Interoperability tests and the Brussels Interoperability Group

Starting from 2004, ICAO organised various sessions of interoperability tests. Several areas of basic incompatibilities were uncovered. Early tests revealed that chips were not consistently read and that there were differences in the interpretation of standards. With the last test session held in Berlin in 2006, ICAO concluded that the situation was stable enough to no longer require interoperability events. In the meantime, the Brussels Interoperability Group (BIG) was formed as a forum for EU member States and the European Commission to resolve all technical issues arising from the development, implementation and application of the EAC protocol which was selected and adopted by the EU to protect access to secondary biometrics in the passport.

The aim of BIG was to reach consensus on technical issues related to the introduction by the EU of electronic machine readable travel documents in order to ensure uniformity in its member States. BIG also aimed to develop, coordinate and implement the EU-wide testing strategy which would help to ensure full interoperability for passports and travel documents and to offer support to the establishment of international standards for interoperability testing.

BIG organised several test events; the latest one, the e-Passport EAC Conformity & Interoperability test, being held in Prague in September 2008. The scope of this test was very broad and comprised a conference which was attended by some 500 participants from 35 different countries with around 1400 passports being tested. The objectives of the test were:

- to demonstrate that existing inspection systems were capable of reading EAC passports;
- to test the exchange of card verifiable certificates;
- to log and discuss potential errors;
- to assess the technical specifications and conformity test specifications;
- to reach agreement on any issues surrounding the interpretation of the specification.

Test elements included e-Passports, inspection systems (readers) and test suite/test specifications. As a result of this test, the technical specifications were further refined and implementations were assessed. It was also clear that conformity test specs for inspection
In this respect, ICAO recognises that the security of e-Passports has reached a level where it is no longer worthwhile for fraudsters to create false documents and that fraud is rather moving towards attacking the issuing process. Recently, ICAO issued its *Guide for Assessing Security of Handling and Issuance of Travel Documents*. The guide contains best practice as well as tools for assessing the security of the issuing process.

**Enabling automated border crossing**

During identity verification at a border all the security features within an e-Passport should be checked. The following steps should be performed:

- live capture of biometrics: liveness checking and detection of spoofing;
- document reading of the optical (MRZ, printed data) and electronic (chip content) components;
- document verification of the optical (printed) security features and validity;
- electronic authentication, matching the live detected biometrics with biometrics contained in the chip (and printed on the data page).

This process can be automated with so-called electronic gates or Automated Border Control (ABC) systems. ABC systems make use of the experience of the registered traveller schemes introduced in a number of airports a few years ago. The difference with the registered traveller scheme is that an ABC system does not require previous enrolment and an additional token but uses the e-Passport. Currently introduced in operational or pilot phase in several airports in the EU, ABC systems are complementary to conventional border crossing.

They are supervised by border guards and have been developed independent of any coordinated EU approach. There is room in this respect for further interoperability enhancements through the development of guidelines and best practices which cover the higher layers of the interoperability stack in particular.

**Conclusion**

Since the few years that e-Passports have been in operation, considerable experience has been gained regarding its usage. However, interoperability is complex and the strict use of technical specifications is only one part of the picture. An important component which needs further attention is the organisational aspect, something which is particularly important when public key encryption and the consequent need of certification policies and management are in place. In the use of ABC systems, additional higher protection features for privacy and security need to be put in place also in the form of procedures to control and guarantee proper personal data handling.

---

11 ISO/IEC 14443, Identification cards - Contactless integrated circuit(s) cards - Proximity cards, Radio frequency power and signal interface.
12 ISO/IEC 7816, Identification cards - Integrated circuit(s) cards with contacts.

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