

How to achieve and enhance interoperability of e-passports

Jan Löschner and Zdeněk Říha (DG JRC, European Commission)

1 Abstract

Electronic passports combine the classical passport booklet with a contactless chip. The chip stores information about the passport holder and the issuing institution in up to 16 data groups. The e-passport in general can store biometric information in the form of a facial photograph, fingerprint image and/or template and iris image. Within the EU it was decided to use the facial image and fingerprint images only.

Due to function of a passport it is clear that interoperability is very important in this area. Passport must be usable at any border in the world. This holds true also for the electronic part. Not only must the inspection system be able to read the data from the passport. It must be also able to verify and interpret the data. Interoperability of electronic passports is a process which starts with specification standards continues with interoperability testing which can be divided into conformity tests and crossover tests.

Fingerprints in the European passports are protected with an additional mechanism (EAC), not standardized at the ICAO level yet. To achieve interoperability in this area, EAC interoperability testing events are coordinated by the BIG (Brussels Interoperability Group).

2 Electronic passport

ICAO (International Civil Aviation Organization – a UN agency responsible for civil aviation and international travel) is actively working on standardization in the area of passports. Already in the 1980s the storage of some passport data in two machine processible lines has been standardized. These lines, called the Machine Readable Zone (MRZ), contain basic data about the passport and its holder (name, surname, date of birth, date of expiry etc.) and it is printed in a standardized font so that it is machine readable and processible. Because the amount of data storable in the MRZ is only very small (88 characters) and the only security factor is the check digit, new ways of storing data for automated processing were investigated. The 6th version of the ICAO Doc 9303, describing travel documents, introduces the technology of contactless chips, symmetric and asymmetric cryptography and biometrics. The new passports equipped with a contactless chip are called electronic passports.

Contactless chips do not require contact with the reading device, they use fast communication protocols and when equipped with modern chips, have a large memory (at least tens of KB) as well as cryptographic coprocessors.

The data in electronic passports is stored in several files in a common directory. One file (EF.COM) is reserved for metadata (data format version and the list of stored data groups), one file (EF.SOD) contains security attributes (digital signatures of hashes of all the files) and other files include the data, which are grouped in 16 data groups (DG).

Data Group	Stored Data
DG1	Machine readable zone (MRZ)

DG2	Biometric data: face
DG3	Biometric data: fingerprints
DG4	Biometric data: iris
DG5	Picture of the holder as printed in the passport
DG6	Reserved for future use
DG7	Signature of the holder as printed in the passport
DG8	Encoded security features – data features
DG9	Encoded security features – structure features
DG10	Encoded security features – substance features
DG11	Additional personal details (address, phone)
DG12	Additional document details (issue date, issued by)
DG13	Optional data (anything)
DG14	Protection of secondary biometrics (e.g. EAC)
DG15	Active Authentication public key info
DG16	Next of kin

Table 1: The data structure of electronic passports.

2.1 Passive Authentication

Data stored in the electronic passports must be digitally signed by the issuing institution. The PKI (Public Key Infrastructure) hierarchy is made of a single level. Every country creates its own national CA (Country Signing Certification Authority) which signs the document signing authority keys (Document Signers – DS); these Document Signers then sign data in electronic passports.

Passive authentication is a mandatory feature of all electronic passports. To be able to perform the verification of the validity of the data stored in the electronic passport the CSCA certificate of the issuing country and a recent CRL (Certificate Revocation List) is necessary. To obtain the CSCA certificates of other countries a bilateral exchange of the certificates is envisaged. Because the integrity of the certificate plays an important role in the security of the verification procedure, secure diplomatic mail should be used to perform the exchange of certificates or at least hashes of the certificates. Unfortunately it turns out that the diplomatic way is a bit problematic in practice (in particular it is difficult to reach the right people to obtain certificates of other countries).

3 Interoperability

Because of the purpose of electronic passports and passports in general, it is clear that interoperability plays an important role in this area. Passports must be usable at any border crossing points worldwide. Currently not all the border control points are equipped for reading

of electronic passports but when doing so, the verification should not be disturbed by interoperability issues. One of the definitions of interoperability is:

Interoperability is the ability of products, systems, or business processes to work together to accomplish a common task. The term can be defined in a technical way or in a broad way, taking into account social, political and organizational factors.

4 Interoperability testing

The technical interoperability of electronic passports is a result of several steps. First of all the behavior of electronic passports is defined in a standard (ICAO Doc 9303 and its Supplements, indeed referring many ISO and other standards). Then the conformity of the behavior of the passport is tested against a conformity standard. Last but not least the interoperability is tested in practice in a crossover test (see paragraph 4.2) with a number of passports and readers/inspection systems.

4.1 Conformity testing

Conformity testing verifies the conformity of the electronic passport to the ICAO Doc 9303 and other referenced standards. Conformity testing is based on the ICAO technical reports and for EAC passports additionally on European specifications. Conformity tests comprise of hundreds of test cases on seven OSI/OSI layers of communication (seven layers of abstraction from the physical properties through the communication up to the interpretation of the data). Conformity test cases verify the behavior of the chip in certain situations and help to identify potential security or interoperability issues.

The conformity tests of electronic passports are based on two ICAO technical reports:

- For the layers 1, 2, 3 and 4 (i.e. physical parameters and low level communication) the following document is used: “*ICAO technical report: RF protocol and application test standard for e-passport – part 2: Tests for air interface, initialisation, anticollision and transport protocol*”. The document defines 3 tests on layer 1, 4 tests on layer 2, 10 groups of tests on layers 3 and 4 (that defines about 200 test cases).
- For the layer 6 (high level communication) and 7 (data structure) the following document is used: “*ICAO technical report: RF protocol and application test standard for e-passport – part 3: Tests for application protocol and logical data structure*”. The technical report defines 165 test cases on layer 6 and 38 test cases on layer 7.

Note: The layer 5 is not used in the field of electronic passports. Conformity tests of the passports of the second generation (with EAC) are supplemented with additional tests on layers 6 and 7 (see below).

For conformity testing of e-passport readers one technical report is available. The ISO/OSI layers 2, 3 and 4 (i.e. the low level communication) is covered by the document: “*ICAO technical report: RF protocol and application test standard for e-passport – part 4: E-passport reader tests for air interface, initialisation, anticollision and transport protocol*”. There are no conformity tests for inspection systems for higher ISO/OSI layers.

The conformity testing of electronic passports can be illustrated on an example of a conformity test for BAC (Basic Access Control) protected passports. The test case 7816_B_40 on layer 6 (high level communication) verifies the enforcement of Secure Messaging

(encryption of the communication) while basic access is granted (the reader has successfully authenticated itself with the data from MRZ).

The test verifies whether the passport denies sending data in an unencrypted way, even if the reader has already authenticated itself and started the secure encrypted communication. The unsecured command can originate from the same reader or can also come from a completely different one (we have to bear in mind that the communication is contactless).

To run the test case, the BAC is established and then the file DG2 is selected and read using SM: the following command is sent '0C B0 82 00 0D 97 01 06 8E 08 <checksum> 00'. As a reply the passport must return 90 00 using SM, meaning the command was performed successfully.

Then an unprotected command (trying to read the data without encryption) is sent: '00 B0 00 00 00'. The passport MUST return an ISO checking error (i.e. one of the status codes from the range 67 XX – 6F XX). If the passport replies in a different way (e.g. the command is accepted and data sent) the test case fails.

4.2 Crossover testing

The conformity tests are complemented with crossover tests. In crossover tests, as the name already suggests, various passports are read by various readers/inspection systems. The result of the crossover test only indicates problematic combinations and a detailed analysis must follow to investigate the issue and find out whether the problem is on the side of the passport or the inspection system. Crossover testing often reveals ambiguities in specifications, when different implementers interpret the same specification in different ways. The value of the crossover tests lies in identification of these unclarities. Results of crossover tests often serve as a base for modifications of the specification standards and also as an impulse to design a conformity test case for that particular issue.

As passports must be interoperable on worldwide level, interoperability tests have been organized under the wings of ICAO. There have been numerous interoperability events in the past:

- 2 / 2004 Canberra
- 7 / 2004 Morgantown
- 9 / 2004 Sydney
- 12 / 2004 Baltimore
- 3 / 2005 Tsukuba
- 11 / 2005 Singapore
- 5 / 2006 Berlin

After these interoperability events ICAO has concluded that the situation in interoperability is stable and that no further interoperability events need to be organized by ICAO. Still there are already plans to have another interoperability event (however not directly organized by ICAO)

- 9 / 2008 Prague
-

4.3 Interoperability is not only readability

Although the focus of interoperability is often on readability of the document, interoperability is not only readability. To be able to verify validity of the data stored in electronic passports, the **CSCA certificates and CRLs** are necessary. ICAO PKD (public key directory) was designed to facilitate the passive authentication. The PKD would include DS certificates and CRL. As DS certificates are typically stored in the passports, and CSCA certificates were not stored in PKD, the added value of PKD was relatively small. Recently a modification of PKD was proposed to include also cross certificates of CSCA certificates. This could facilitate the problematic bilateral exchange of CSCA certificates.

Active authentication, a protocol for verification of chip authenticity (to prevent cloning), is not addressed by conformity tests, it is only being tested in the crossover tests.

Data structure of the basic files stored on the chip is touched by the conformity tests on layer 7. These tests, however, do not go deeply into the biometric data. Quality of the **biometric data** is very important. ICAO Doc 9303 specifies requirements on the quality of facial images (referring to ISO 19794-5), conformance to these requirements are, however, not tested in an automated way during conformity tests. Also crossover tests only verify whether the biometric data can be displayed and do not address the quality of the data.

Last but not least the **Optical Character Recognition** of the Machine Readable Zone plays an important role because the content of the chip cannot be accessed without authentication of the reader based on the information in the MRZ. Without MRZ the BAC-protected passports cannot be read and manual data entry is extremely slow and unusable in larger scale. Not much attention is paid to the OCR of the MRZ at this moment.

5 Extended Access Control

Biometric data in the form of fingerprints or irises are considered to be more sensitive data than facial images as their recognition capabilities are stronger. These biometric characteristics are protected with additional protection mechanism (called Extended Access Control) in the passports of EU countries. The introduction of fingerprints into European electronic passports is specified by Council regulation of 13 December 2004 (Regulation (EC) 2252/2004). The Commission Decision C(2006) 2909 from 28 June 2006 specifies more details of EAC protected passports. The decision has also indirectly set the deadline for introduction of the EAC passports which is 28 June 2009. After the deadline (at the latest) the passports will have to include two fingerprints (index fingers) in file DG3. Passports storing the fingerprints protected with EAC are also called passports of the second generation.

For the purposes of Extended Access Control each country sets up a CV (Country Verifying) CA, which by issuing certificates will determine who (which countries) will have access to secondary biometric data in passports issued by that country. The root certificate of the CA is stored in the passport and serves as the initial point of the access control. Countries, which want to read secondary biometric data (in domestic or foreigner passports), will have to set up DV (Document Verifier) CA. This CA needs to get certificates from CV's CAs of the countries, which will allow access to fingerprint and/or irises in their passports. This DV CA then issues certificates to end entities accessing the biometric data (so called inspection systems). The PKI hierarchy is illustrated on figure 1.

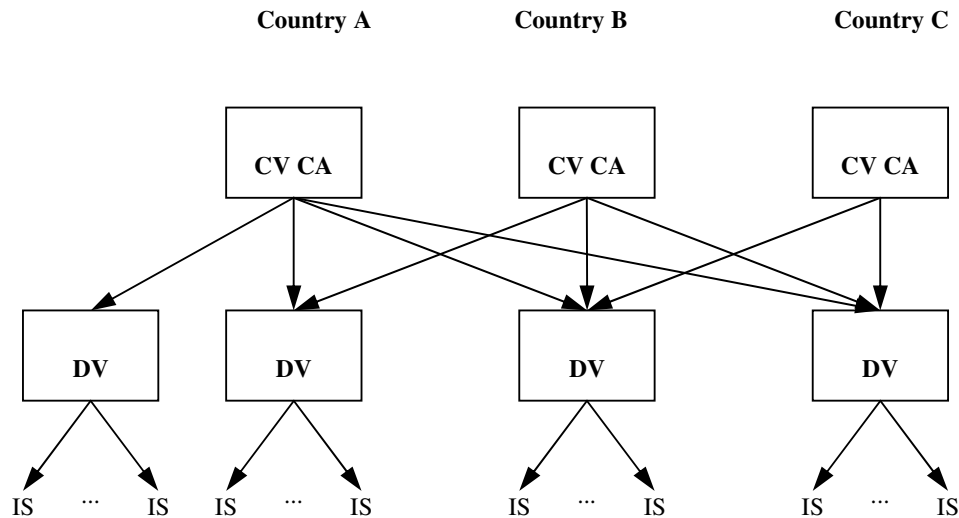


Figure 1: PKI hierarchy of the Extended Access Control.

In addition to Terminal Authentication (which protects the confidentiality of the secondary biometric data) the Extended Access Control also introduces the Chip Authentication, which eliminates the low entropy problem of Basic Access Control key because the result of the Chip Authentication is a new secure channel. The Chip Authentication also replaces the active authentication in verification of the chip authenticity.

Because the computational power of chips is only limited, simplified (so called Card Verifiable) certificates are used instead of classical X.509 certificates. Although CV certificates are standardized by ISO standards some important interoperability issues appeared. First it was not clear whether to include the 7F21 tag in the certificate and second ASN1 coding of some fields was not straightforward as the ASN1 does not specify a separate coding for unsigned integers.

The verification of the certificate time validity is interesting. The chip does not have its own clock and the only information about the date is the certificate date of issue. If the chip successfully verifies the signature of a certificate issued on a particular day, it can presume that day has passed (or it is today) and then can update its internal time estimate to that day (if the day is newer than the current value).

5.1 EAC technical interoperability

As the EAC is a European protocol, also the interoperability events are organized on the European level. The tests are coordinated by the BIG (Brussels Interoperability Group). The BIG has already organized several EAC interoperability events:

Conformity tests:

- Lisbon, May 2007 (small subset of test cases only)
- Paris, Oct 2007 (all test cases, 6 independent testers)

Crossover tests:

- Ispra, Dec 2006
- Prague, March 2007
- Paris, Oct 2007

5.2 EAC Crossover tests in Paris

For the EAC crossover test in Paris 33 passports and 16 inspection systems were registered. A passport was successfully processed by an inspection system if the following steps were successful:

- Data readable
- Passive authentication successful
- Active authentication successful (if implemented by passport)
- Chip authentication successful
- Terminal authentication successful
- Data displayed (photo and fingerprints)

The results of the EAC crossover test in October 2007 in Paris are summarized in the following figure:
