INQUIRY OVER BIOMETRIC PASSPORTS

MA Student : Ionela Camelia Cioacătă

AGENDA

- ◊ What is the biometric passport
- ◊ Biometric Technology Overview
- ◊ Biometry in passports
- ◊ Types of biometric passports
- ◊ Reading ePassports
- ◊ The process of implementing ePassports in Romania

What is the biometric passport

The **biometric passport** is the new type of passports, which from October 2006 are required for entry to the US by the VWP (see also later on the section ***Types of biometric passports***). The passports must contain an RFID-chip, which holds digitized information about the passport's owner. The individual government decides much of the specific digital information, but certain demands are made by the US and the ICAO standard.

As an example, a digitized photo of the passport's owner is required both by the standard and by the US. Some of the information on the passport must also be optically readable. *Other terms used include "electronic" or "digitized" passports, or simply E-passports or ePassports.*

EPassport is a term used for all passports that includes an electronic device, or Contactless Integrated Circuit (IC) such as a RFID chip. The RFID chip contains biometric data, so an ePassport is also a biometric passport. This definition is in compliance with the ICAO terminology.

In other words, a **biometric passport** is a combined paper and electronic identity document that uses *biometrics* to authenticate the citizenship of travelers. The passport's critical information is stored on a tiny *RFID* (**Radio Frequency Identification**) computer chip, much like information stored on *smartcards*. Like some smartcards, the *passport* book design calls for an embedded contactless chip that is able to hold *digital signature* data to ensure the integrity of the passport and the biometric data.

The current staged *biometrics* for this type of identification system is facial recognition, *fingerprint* recognition, and *iris scans*. The ***International Civil Aviation Organisation*** defines the biometric standards to be used in passports. **ICAO** does not currently have plans to use ***retinal*** scanning. *Only the digital image (usually in jpeg format) of each biometric feature is actually stored in the chip.* The biometric algorithm is computed outside of the passport chip by electronic border control systems (e-borders). To store biometric data on the contactless chip, it includes a minimum of 32 kilobytes of *EEPROM* storage memory, and runs on an interface in accordance with the *ISO* 14443 international standard, amongst others. These standards ensure interoperability between the different countries and the different manufacturers of the passport books.

Figure 1. Symbol for biometric passports, usually printed on the cover of the passports

Biometric Technology Overview

Fingerprinting

The use of fingerprinting is well-known because of its use in forensic science and law enforcement. Large-scale fingerprint technology works by using coordinates of points on the fingerprint where ridges end or split. It is also possible to match the whole fingerprint pattern but such systems are rarely used on a large scale.

There are two main ways of recording fingerprints: **rolling and slapping**. Rolled fingerprints are used in law enforcement where the maximum print is recorded. Slapped fingerprints only record the pad of the finger but the process is less intrusive. *There are different types of fingerprint reader*: slap readers (10 prints), single-finger optical readers, single-finger capacitive readers, ultrasound readers and rolled fingerprint readers. It is likely that the ID Cards Programme would use a 10-finger slap reader.

The basic characteristics of fingerprints do not change, although fingerprints can be damaged by injury, burns or wear due to work. When recording fingerprints, it is important the finger is clean because any grease or dirt can distort the image. The image can also be distorted by pressure on the finger that alters the fingerprint pattern.

There are hundreds of fingerprint companies but only four or five provide **AFIS** *(automated finger identification systems)*. There are several large-scale fingerprint databases including the **FBI AFIS database**, which has a database of 47 million fingerprints and **Ident1** in the **UK**, which holds six million sets of prints.

Facial Recognition

Facial recognition works by identifying people according to sections of the face least susceptible to alteration eg. upper outline of eye, sides of mouth, cheekbones.

The two main methods are: local feature analysis and the Eigenface method. Local feature analysis measures the relative distances between landmarks on the face. The Eigenface method looks at the face as a whole and uses combinations of 2D templates that represent distinctive characteristics of a facial image.

Face recognition readers vary greatly in technology and the lighting of the face can have a great effect upon the performance of the technology. There are approximately 10 companies offering 3D technology and less than 100 companies offering 2D solutions.

Iris Scanning

Iris recognition measures the iris pattern in the colored part of the eye. Iris patterns are formed randomly at birth and iris patterns are different for every eye. The iris can have more than 250 distinct features compared with 40 or 50 comparison points for fingerprints.

Iris scanning involves a camera capturing an image of one or both eyes. The camera focuses on the eye, locates the iris and accounts for areas obstructed by eyelashes or eyelids. This image is broken into circular grids and each area is analyzed for unique patterns. This information is converted into an algorithm in the camera that can be used as a template.

Iris patterns are unique, even between identical twins, and these patterns are stable throughout life. There can be some difficulties with iris scanning if individuals are wearing glasses or contact lenses, if they have aniridia (lack an iris) or glaucoma.

The iris recognition market is currently dominated by Iridian, although it may become increasingly competitive as patents expire. Iris performance statistics from independent tests are limited to 100’s. However, the technology is widely used in the United Arab Emirates, which has a database of over 350,000 iris scans.

Biometry in passports

Biometry is used to identify people by measuring some aspect of one's individual anatomy or physiology, such as fingerprint, facial features, iris, DNA or simply a photograph. In digital form, this measurement is usually called a **template**. It should be unique for each person. The attractive features of

biometric measurements are that people always carry them around, that they are usually non-trivial to fake, and that the identification process can be *automated* (to a large extend).

Basically, there are 2 ways to use a biometric system.

- **Verification:** given both a person and a template, is there a match?
- **Identification:** given a measurement of a (as yet unknown) person, for instance a fingerprint at a crime scene or a picture from a surveillance camera, is there a matching template in the database, so that the identity of the owner of the biometric datum can be established?

In practice there is not always a perfect match between templates and individuals. One speaks of a *false positive* if the biometric recognition system says 'yes', but the answer should be 'no'. A *false negative* works the other way round: the system says 'no', where it should be a 'yes'. **One of the main challenges with biometric systems is to minimise the rates of both false positives and of false negatives**. In theory one is inclined to keep the false positives low, but in practical situations it often works the other way round: people that operate these systems hate false negatives, because they slow down the process and result in extra work and people complaining.

When a PIN code is used to authenticate people (via "what you know"), it is not a disaster if the code is lost or compromised (known to others): you simply ask your bank for a new PIN code. However, this is not possible with biometric templates (using "what you are"): you can not simply get a new iris, fingerprint or DNA print. Hence, biometric templates carry sensitive and very private information, that should be handled with great care. Loss or compromise of biometric templates may lead to serious cases of identity theft. *Restoration is basically impossible.*

Storing biometric templates

When biometric information is used in a system such as a passport, the first question should always be: where is the biometric template stored, and how does the comparison with the measurements take place? More concretely, when a passport carries a chip with a biometric template, in a proper set-up, the template should never leave the chip, and the comparison should take place on the chip itself. Also, the device that does the measurement (e.g. an irisscanner) should be secure, in the sense that it does not leak information to the outside. In such a set-up it is important to check the authenticity of the passport/chip, because a fake one could always answer 'yes'.

When the biometric templates are stored only in (the chip in) a passport, it can be used only for verification purposes, as explained above: to establish the relation between an individual and a passport. This will combat the so-called look-alike fraud.

As argued, there are serious privacy concerns when biometric templates are stored outside passports, for instance in large databases. Such databases can be used in order to identify people, for instance when a fingerprint is found at a crime scene. Such application may be justifiable, but a large database raises serious privacy concerns: it can be misused to track the whereabouts of all individuals. Typically, a database is kept only of convicted criminals (of a sufficiently serious criminal act). But there is growing pressure towards centralized databases.

Security mechanisms in the biometric passport

The International Civil Aviation Organization ***(ICAO)*** has selected facial recognition (to be stored in chips) as main biometric for "machine readable" travel documents. Additional biometrics, such as fingerprints or iris scans are allowed, see their ***dedicated webpage*** with lots of material, including many

standards documents. The biometric passport in the Netherlands (and likely also in Europe) will contain pictures of the face, and also of two fingers (left and right, in principle). The ***ICAO*** standards allow several levels of security. **The Netherlands will implement the highest level.**

1. **Basic access control** is optional (but implemented in NL), and means that the chip embedded in the passport will only respond after receiving a specific (cryptographic) key. This key can be derived (automatically) from the so-called ***Machine Readable Zone (MRZ***). It is the two-line text at the bottom of a special page in the passport. It contains the passport number, name of the holder, date of birth, date of issuance, together with some check-bits. This basic access control is not really a security mechanism. It makes sure that the holder of the passport must physically hand over the document before it can be read. This is meant to establish consent.
2. **Passive authentication** is not optional. It is the checking of the signature of the so-called security document inside the passport. This security document contains hashes of all the crucial data. It is signed with the private key of the issuing state. The corresponding public key must be made available via some international PKI---also because these public-private key pairs should be renewed every three months. This passive authentication mechanism must prevent the fabrication of fake passports.
3. **Active authentication** is optional, but also implemented in NL. It is a challenge-response mechanism with the card, where the card signs a challenge with its own private key. The corresponding public key can be read from the passport. Its hash is part of the security document (**as in 2**). This active authentication mechanism must prevent cloning of existing passports.
4. **Extended authentication** can be used to restrict access to some of the biometrical data. The facial image can simply be read out, once the basic access control protocol (from 1) has been carried out. The fingerprints however are encrypted (*in a test version in the Netherlands*). It is not clear yet which mechanism will be used for extended authentication.

Types of biometric passports

There are several types of biometric passports:

- ***European***

The European version of the passport is planned to have digital imaging and **fingerprint** scan biometrics placed on the contactless chip. This combination of the **biometrics** aims to create an unrivaled level of security and protection against **counterfeit** **and** **fraudulent** identification papers. Currently, the British biometric passport only uses a digital image and not fingerprinting, however this is being considered by the United Kingdom Passport Service.

Figure 2. The contactless chip of the British National (Overseas) Passport.

It can be seen below different types of European biometric passports. Also it can easily be observed that all the passports have printed on its covers the symbol from ***Figure 1***.

- ***U.S.***

The U.S. version of the biometric passport (which is also referred to as an ***"Electronic Passport"***) will only have digital imaging placed onto the contactless chip, *as opposed to the European version*. However, the chip used in the U.S. passport will be large enough (64 kilobytes) to allow it to contain additional biometric identifiers should the need arise in the future. The *U.S. Department of State* began issuing biometric passports to government officials and diplomats in early 2006. It began issuing regular biometric passports at its Colorado Passport Agency on August 14, 2006; though they still expect that nearly all new or renewed passports issued by the department to American citizens will be biometric by the end of 2006, other sources say it won't happen until mid-2007.

A high level of security became a top priority **in late 2001** for the United States. This tightened security required border control to take steps in cracking down on counterfeit paper passports. In October 2004, the production stages of this high-tech passport commenced as the **U.S. Government Printing Office (GPO)** issued awards to the top bidders of the program. The awards totaled to roughly $1,000,000 for startup, development, and testing. The driving force of the initiative is the U.S. Enhanced Border Security and Visa Entry Reform Act of 2002 (also known as the "Border Security Act"), which states that such **smartcard IDs** will be able to replace **visas**. As for foreigners traveling to the U.S., if they wish to enter U.S. visa-free under the ***Visa Waiver Program (VWP)***, they are now are required to possess *machine-readable passports* that comply with international standards. Additionally, for travelers holding a valid passport issued on or after October 26, 2006, such a passport must be a biometric passport if used to enter the U.S. visa-free under the VWP.

- ***Australian***

The Australian biometric passport was introduced in October 2005. *Like the U.S. version*, the chip will only have a digital image of the bearer's face as on their passport photo. Airport security has been upgraded to allow Australian ePassport bearers to clear immigration controls more rapidly, and face recognition technology has been installed at immigration gates.

- ***Canadian***

Canada has recently introduced biometrics in the use of passports with the help of digitized photos. The future passports may contain a chip that holds a picture of the person and personal information such as name and date of birth.

This technology is being used at border crossings that have electronic readers that are able to read the chip in the cards and verify the information present in the card and on the passport. This method allows for increased efficiency and accuracy of identifying people at the border crossing. CANPASS, developed by Canada Border Services Agency, is currently being used by some major airports that have kiosks set up to take digital pictures of a person's eye as a means of identification.

- ***Dutch***

The situation in the Netherlands was quite reasonable at first, but changed to radical and this is due to the fact that encryption scheme used to protect the flow of information between the Dutch biometric passport and a passport reader was cracked on *July 28 2005*.

This is due to the Dutch passport numbering scheme which does not provide sufficient randomness to generate a strong enough key to secure the exchange of information between the passport and reader. *Other passports such as the U.S. passport do not contain this flaw* as they use a stronger key to encrypt the data exchange. Also, some readers provide shielding for the passport while it is being read, thus preventing signal leakage that might be intercepted by another device.

However, it was an experiment conducted in laboratory conditions, not in the field where immigration officers would have the opportunity to notice the likely damage and/or alterations to the chip and the passport booklet.

"*Security mechanisms in the biometric passport*" section, mentioned earlier, explains how the dutch biometric passport works.

Reading ePassports

Figure 3 shows that if no RFID exists in the passport there a standard manual control will be initiated. If the document is valid the passport will be checked against a database (like the American one) to see if there is any irregularities. If the document is not valid a closer inspection will be done.

If an RFID tag exists in the passport, one of two things will happen. Either the passport is presented to an RFID reader, or there is a manual check of security features. When a manual check is performed the passport will be deemed valid if nothing else suspicious appears while it is scanned as an MRP. Specifically, the data page, passport covers and the passport in general are inspected. When the passport is presented to an RFID reader, ***digital signatures*** will be checked. If these are not valid a closer inspection is preformed, if they are valid the MRZ will be compared with the information in the chip to see if there is anything suspicious there. If everything is OK the check against the database (watch list) will be performed, if something is strange the passport will again be inspected closer.

Abbreviations

- **RFID (chip)**: Radio Frequency IDentifier (chip) is a family of small chips that are capable of permanently and/or temporarily store information and duplex communication with a reader using radio waves.

- **MRTD**: Machine-Readable Travel Documents, an abbreviation used by the ICAO, meaning machine-readable passports, visas and official travel documents. The machine readable

information is at present either contained in a machine-readable code or a Contactless Integrated Circuit (IC), i.e. an RFID chip.

- **MRP**: Machine-Readable Passport. See also the definition of MRTDs above, as a MRP is an example of an MRTD. MRP is the foundation for the new ePassport.

- **MRZ**: The Machine-Readable Zone is the two lines on the bottom of the MRP data page. These lines can be read by machine and contains some of the same information as is written on the rest of the data page.

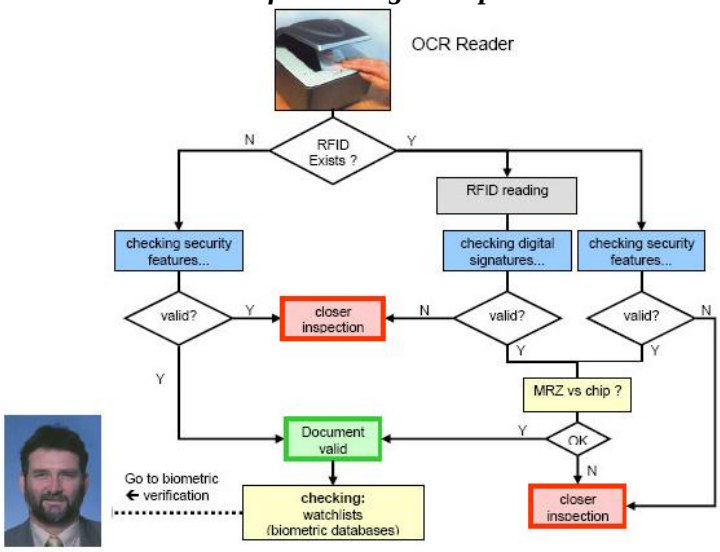
- **Digital Signature**:

The encryption/decryption concept embodied in the ICAO PKI specification is "asymmetric". In this concept keys are issued in pairs consisting of a private key and a public key. The passport issuing authority uses the private key (so called because it is held only by the issuer and kept secret) to encrypt the computed "hash" of the data in the chip, and the result is the ***"digital signature".***

With a digital signature the data is doubly protected. First, the digital signature can be decrypted back to the hash value, but only with the use of a "key" that was made available by the authority that entered the data in the chip. If the issuing authority's key successfully decrypts the signature, then it is certain that the data in the chip was entered there by that authority. Conversely, if the key does not decrypt the signature, it is evident that the data was entered by someone else.

Second, the mechanical reader recalculates the hash of the data in the chip and compares the result to the decrypted digital signature. If the two values are the same, then it is certain that the data has not been altered in any way. Conversely, if the values are not the same, it is evident that the data was altered by an unauthorized person.

Figure 3. Typical Business Process for reading ePassports



The process of implementing ePassports in Romania

The biometric passport it is expected to be released in Romania by the end of this year and it will cost approximately 60 Euros. Also it was announced that the electronic ID cards will be used starting the year 2008.

It was stated that the reason of this delay (because it was forecasted the new passports will be ready to use by January 1st, 2007) with implementing the new passport was due to the fact that the actual passports are secure and that there is no need to rush the process of introducing the new type of passport.

Also the auction that will designate the company that will be in charge with the producing of these passports will take place in the summer of 2007.

Bibliography

1. http://www.passport.gov.uk/general_biometrics.asp
2. http://www.iridiantech.com/
3. http://www.icao.int/mrtd/download/technical.cfm
4. http://wwwes.cs.utwente.nl/safe-nl/meetings/24-6-2005.html
5. http://www.epass.de
6. http://www.realitatea.net
7. http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/
8. http://www.passport.gov.uk/general_biometrics.asp
9. http://www.state.gov/documents/organization/77115.pdf
10. www.bundesdruckerei.de