

# Is e-passport security effective yet?

## Improvements needed for next generation

by Marc Witteman

The first generation of electronic passports has arrived. Although the technology still has imperfections when it comes to safeguarding privacy, it offers good anti-forgery protection. The next generation of e-passports will include reliable biometrics and Extended Access Control (EAC). However, these features have not yet been standardised and could still be improved. Future e-passports, incorporating reliable biometrics, may offer strong protection against look-alike fraud, but this will only benefit immigration authorities if all e-passports contain biometrics (thus preventing fraudsters from exploring the weaknesses of legacy passports). It is therefore important that ICAO finalises its EAC standardisation, and that issuing countries continue to adopt e-passports with reliable biometrics.

The global introduction of e-passports involves a broad-based and coordinated effort aimed at increasing passport security. Issuing countries can use e-passport technology to combat passport forgery and look-alike fraud. While addressing these security problems is clearly important, other security considerations, including privacy, should not be overlooked. This paper discusses the theoretical and practical security issues that affect citizens as well as issuing authorities. Several countries have introduced e-passport programmes since 2005. Although the first generation of e-passports includes some planned security features, biometric verification is, on the whole, not yet supported. From 2007 onward, immigration services will be ready to start processing e-passports. Authorities can promote the introduction and use of e-passports by implementing visa-waiver programs for travellers carrying e-passports.

### Electronic Passport security mechanisms

The MRTD specs defined by ICAO, which were drawn up to reduce passport crime, primarily address methods

to prove the authenticity of the passport, the passport data and the passport holder. The authentication technologies used include PKI (Public Key Infrastructure), dynamic data signing and biometrics, which is still under discussion and not yet fully defined in the specifications. It should be noted that all e-passport features complement existing physical document features.

#### Passive Authentication

PKI technology is used to authenticate passport data, and chosen for this reason. It is also successfully applied in combination with e-commerce applications. Certificate-based authentication only requires the certificate to be read by the inspection system, which can then use a cryptographic computation to validate data authenticity (using the public key of the issuing country). This method is referred to as passive authentication and can be used in combination with RFID chips without public key cryptographic facilities. After all, only static data is read. Although the authenticity of data can be verified, passive authentication does not guarantee the authenticity of the passport itself, which can still be counterfeit (referred to as a clone or electronically identical copy).

#### Active Authentication

Although passport cloning can be resolved using an optional signing mechanism (active authentication), this method requires the presence, in the chip, of an asymmetric key pair as well as public key cryptographic capabilities. The public key, which is signed by the issuing country and verified by means of passive authentication, can be disclosed to the inspection system, which allows a dynamic challenge signed with a private key to be verified. The private key is well protected by the chip, effectively preventing cloning. The inspection system can establish the authenticity of the passport chip using the active authentication mechanism.

#### RFID

To allow modern electronic technology to be incorporated in existing paper documents, ICAO decided to use (contactless) RFID chips. These chips can be embedded in a document page, and do not require any modifications to the physical appearance of the passport. In contrast, the form factor of a contact smart card would complicate chip embedding in a passport booklet. In addition, contacts may be



*Marc Witteman has a long track record in the smart card security industry. He has authored several articles on smart cards security issues and gained extensive experience as a trainer. Marc has an MSc in Electrical Engineering from Delft University of Technology in the Netherlands. Between 1989 and 2001, he worked for several telecom operators, the ETSI standardization body and a smart card evaluation facility. Marc founded Riscure, a security laboratory based in the Netherlands, in 2001. Riscure offers a broad range of consulting and testing services.*

## Box 1

## Abbreviations

<b>BAC</b>	<i>Basic Access Control</i>
<b>DES</b>	<i>Data Encryption Standard</i>
<b>DSA</b>	<i>Digital Signature Algorithm</i>
<b>EAC</b>	<i>Extended Access Control</i>
<b>ECDSA</b>	<i>Elliptic Curve Digital Signature Algorithm</i>
<b>ICAO</b>	<i>International Civil Aviation Organization</i>
<b>MRTD</b>	<i>Machine Readable Travel Documents</i>
<b>MRZ</b>	<i>Machine Readable Zone</i>
<b>OCR</b>	<i>Optical Character Recognition</i>
<b>PKCS</b>	<i>Public Key Crypto System</i>
<b>PKI</b>	<i>Public Key Infrastructure</i>
<b>PSS</b>	<i>Probabilistic Signature Scheme</i>
<b>RFID</b>	<i>Radio Frequency Identification</i>
<b>RSA</b>	<i>Rivest Shamir Adleman (public key encryption algorithm)</i>
<b>SHA</b>	<i>Secure Hashing Algorithm</i>
<b>UID</b>	<i>Unique IDentification number</i>

sensitive to movements as a result of travel. The choice in favour of RFID also gives rise to privacy issues. RFIDs can be accessed from up to 30cm. Moreover, the radio traffic between a terminal and an RFID-enabled passport can be intercepted at a distance of several metres (eavesdropping). In other words, it is possible for someone using dedicated radio equipment to retrieve personal data without the passport owner's consent. This enables terrorists to select victims on the basis of their nationality, and allows criminals to commit identity theft (for any number of reasons). The attendant risk is significant. Although it is possible to protect a passport using metal foil (faraday cage), such shielding is not effective when the booklet is opened for reading. Neither can it prevent eavesdropping. To safeguard privacy, the optional Basic Access Control (BAC) mechanism was designed (figure 1). This mechanism requires an inspection system to use symmetric encryption when transmitting/receiving data. The encryption key is static and derived from three primary passport parameters:

1. the date of birth of the holder;
2. the expiry date of the passport and;
3. the passport number.

The above data is stored on the Machine Readable Zone (MRZ), a strip located at the bottom of the biographical data page (figure 2). During normal access procedures, the MRZ data is read first, using an OCR scanner. The inspection system derives the access key from the MRZ data. It subsequently establishes an encrypted radio communication channel, via which confidential data is retrieved from the chip.

Although this procedure can be automated, it makes considerable demands of inspection systems and impacts the inspection performance.

While the BAC mechanism does provide some additional privacy protection, there are two limiting factors:

- The BAC key is individual but static - it is computed and used each time communication takes place. Any wrongdoer would only have to obtain the key once to access a passport's data in perpetuity. As a passport could also contain dynamic data, the passport holder may perceive this to be a disadvantage.
- The BAC key is derived from data that may lack sufficient entropy: the date of expiry is always less than ten years, the date of birth can often be estimated and the document number may be related to the expiry date.

The author encountered several BAC security issues in July 2005, and demonstrated that the key entropy, which could be as high as 66 bits, may drop below 35 bits due to internal data dependencies. For example, passport numbers that are issued sequentially have a strong correlation to the expiry date, effectively reducing the key entropy. It would take an eavesdropper a few hours to compute the BAC key, allowing him to decode all confidential data exchanged between the document and the inspection system.

The Dutch authorities, and possibly several other authorities, have adjusted their issuance procedures since this report (with the aim of strengthening the BAC key). The UID (Unique Identification) number emitted by an RFID immediately after start-up also presents a privacy problem. This number, if static, makes it easy to track a passport holder. As far as e-passports are concerned, it is important that this number is dynamically randomized, and that it cannot be used to identify or track the e-passport holder.



**Figure 1**  
Radio communication  
between inspection  
system and passport  
(Basic Access Control)

For completeness' sake, it should be noted that these privacy issues originate from the decision to use RFID instead of contact card technology. Had this decision been otherwise, the privacy debate would have been different since it would have been up to the passport holder to decide who can read his passport (consent is given when the passport is inserted in the terminal).

### Inspection system security issues

The use of electronic passports requires inspection systems to verify the passport as well as the passport holder. These inspection systems are primarily intended for immigration authorities at border controls. Obviously the inspection systems need to support the security mechanisms implemented in an e-passport. Given the diversity of options that may be supported by individual passports, this presents a major challenge.

In terms of security protocols and information retrieval, the following basic options are permitted:

- use of Basic Access Control (including OCR scanning of MRZ data);
- use of Active Authentication;
- amount of personal data included;
- number of certificates (additional PKI certificates in the validation chain);
- inclusion of dynamic data (for example visa).

The following options depend on future technological developments:

- use of biometrics;
- choice of biometrics (eg, finger prints, facial scan, iris patterns, etc);
- biometric verification methods;
- extended Access Control (enhanced privacy protection mechanism);

In terms of cryptography, a variety of algorithms and various key lengths are (or will be) involved:

- Triple DES;
- RSA (PSS or PKCS1);
- DSA;
- ECDSA;
- SHA-1, 224, 256, 384, 512.

Having all these options also gives rise to a problem: whereas a passport can use a set of preferred options, an inspection system must support them all! A derived problem is that the testing of inspection systems can be very cumbersome. To be sure that false passports are rejected, the full range of options must be verified for invalid (combinations of) values.

The secure implementation of various cryptographic schemes is not trivial. Only recently, a vulnerability was discovered that appeared to impact several major PKCS-1 implementations. PKCS-1 is one of the signing schemes that has been allowed for passive e-passport authentication. This means that inspection systems

must be able to accept passports using this scheme. Clearly any inspection system that has this vulnerability is susceptible to passport crime. Immigration authorities can defend themselves against this type of attack (as well as other hidden weaknesses) by properly evaluating the inspection terminals so that any weaknesses cannot be exploited.

### Biometrics and Extended Access Control

#### **Biometrics**

E-passport security hinges on the biometric verification of the passport holder. The chip contains signed biometric data that may be verified by the inspection system. It is only this feature that prohibits look-alike fraud. Although all other measures address passport forgery, look-alike fraud requires improved verification, whereby it is established that the person carrying the passport is also the person authenticated by the passport. Note that the first generation of e-passports generally includes a stored facial image. While this information can be useful for verification purposes, it cannot be used for the purpose of automated biometric verification.

Many countries have started issuing e-passports. The use of biometrics (eg, fingerprints) is nevertheless delayed. There are two main reasons for this:

1. Biometric verification only works if the software outperforms the immigration officer. The effectiveness of biometric verification, and the suitability of various biometric features, is still being debated. There are also some secondary problems, such as failure to enrol, that need to be resolved.
2. Biometric data are considered sensitive. Whereas the threat of identity theft clearly exists, the revocation of biometric data is obviously not an option. Countries do not necessarily want to share the biometric data of their citizens with all other countries.

As the quality of biometric systems gets better over time, the impact of point 1 becomes less significant. Having said that, prevailing shortcomings may slow down the introduction of biometrics in e-passports. At this moment, limited experience has been gained with representative pilot projects. The second point is more fundamental - issuing countries will always consider who to share sensitive data with. To alleviate these concerns, the ICAO standardization body has introduced the concept of Extended Access Control.

#### **Extended Access Control (EAC)**

The Basic Access Control (BAC) mechanism described above restricts access to inspection systems that are able to read MRZ data. By allowing an e-passport to authenticate an inspection system, EAC goes one step further. Only authenticated inspection systems get access to sensitive (eg, biometric) data. The authentication of inspection systems is based on certificate validation. As the requisite certificates are

issued by counties, the issuing authorities of these countries effectively decide which Inspection System issuers are granted access to the sensitive data.

EAC requires a rather heavy PKI for two reasons:

1. Each Inspection System must be equipped with certificates for each country whose biometric details may be verified.
2. Certificates should have a short period of validity; if not, a stolen Inspection System can be used to illegally read sensitive data.

The current EAC specification foresees a certificate validity of several days. The above will cause an enormous (electronic) flow of certificates (updates). However, as acknowledged by the EAC specifications, e-passports do not have a concept of time. Since the RFID chips are not powered between sessions, they do not have a reliable means of obtaining the time. To solve this problem, an e-passport could remember the effective (starting) date of validated certificates, and consider this as the current date. This could, however, lead to denial-of-service problems: if an e-passport accepts an inspection system's certificate before its period of validity has commenced, it may reject a subsequent inspection system certificate that is still valid. To avoid this problem, the specification proposes to use only certificates of trusted domestic terminals for the purposes of date synchronization.

Although date synchronization based on the validity dates of domestic certificates would give the e-passport a rough indication of the current date, this mechanism does not cover all potential user situations. Infrequent users of e-passports and users who reside abroad for a prolonged period of time will find that their e-passport date lags significantly. For example, if an e-passport validated a domestic, EAC-capable terminal 6 months ago, it will reveal sensitive data to any rogue terminal stolen during this period.

The above problem could be alleviated by using a different date synchronization method. Instead of using the effective dates of inspection system certificates, we would use a separate source of time. To this end, ICAO or another global Certification Authority should issue date certificates on a daily basis, allowing the certificates held by inspection systems to be frequently updated. A passport could then use the date certificates signed by a trusted party to get a reliable and more accurate source of time. This approach also facilitates synchronization on the basis of foreign systems, allowing us to use the current date instead of the inspection system certificate effective date.

As far as EAC and biometrics is concerned, several practical and standardization issues have yet to be resolved. Although EAC, in its current specification, offers strong benefits over BAC, it is certainly not a



**Figure 2**  
Passport with Machine Readable Zone (MRZ).

panacea. There is clearly room for improvement. Having said that, to combat crime effectively we need to equip our e-passports with biometrics.

## Conclusion

The first generation of e-passports, which has been introduced around the world, supports digital signatures for document authentication. The system builds on the latest technology, and considerable expertise is needed to implement and configure e-passports and inspection systems securely. The decision to use contactless RFID technology has complicated matters and additional security measures have been introduced as a result of privacy concerns. These measures appear to offer limited privacy protection at the cost of procedural and technological complexity.

The next generation of e-passports will include more biometrics (eg, fingerprints) and Extended Access Control (EAC). The standardization of these features has not yet been completed, and could be improved. Future e-passports, using all security features, will offer strong fraud protection. In the end, it is more difficult to forge an e-passport that supports active authentication. Likewise, look-alike fraud is more difficult with an e-passport that supports biometrics.

High levels of security can only be attained if these features are implemented in all passports; if not, fraudsters can target less advanced or even legacy passports.