39 myths about e-passports

The facts behind e-passports and RFID technology

by Mike Ellis

The International Civil Aviation Organisation (ICAO) - and the NTWG[1] in particular - first started work on what is commonly referred to as the biometric or e-passport in 1998. Its objective was to improve passport security by creating a stronger link between the passport and its holder. At the time, the use of forged passports - by for example, drug couriers and illegal immigrants - was increasing. One of the most common forging techniques was photo substitution, often in combination with data alteration (the date of birth, for example). At the same time, cases of look-alike fraud - requiring no photo substitution at all - had also risen.

As the NTWG started work on a biometric passport to establish a stronger link between the document and its holder, several issues needed to be resolved at an early stage. Which biometric should be used? Where should the biometric be stored? How should biometric data be read and authenticated?

There are currently more than 100 million e-passports in circulation, issued by over 50 countries. This number continues to grow every day, with 70 million new e-passports being issued every year. Almost all e-passports comply with ICAO standards. As a consequence, they are globally interoperable. A Public Key Infrastructure (PKI) system provides the certificates needed to check their authenticity. While the project was initially motivated by security considerations, several interesting facilitation schemes have emerged. These are based on facial, fingerprint or iris data and facilitate the efficient, high-speed processing of travellers at border control points.

Despite this success, some commentators have been critical of the e-passport. Most of this criticism is based on fiction, a misinterpretation of the facts, or a confusion of technologies. Some articles are written by hackers seeking recognition, others by security researchers working in pristine laboratories, a little divorced from reality. Journalists jump on the bandwagon, combine several false stories and report that the end of the world is fast approaching. There are also articles by activists writing for political gain. While we have no quarrel with other points of view, the twisting of technical data and communication of selective information is objectionable. Unfortunately though, a vast majority of the stories in newspapers and on the web are highly critical.

It is worth contrasting years of painstaking work by the TAG MRTD and the International Organisation for Standards (ISO), work that has resulted in the development of e-passport standards, with the short-term publicity and hype circulated by some observers. This article looks to rebut some of the myths that surround the e-passport and that risk derailing the introduction of the more secure ID document unless debunked.

Myth #1

The e-passport replaces border officials

E-passports were not introduced to supersede the judgement of border officials. We have always trusted humans to intervene and determine whether an individual should be permitted to enter a given country, and the e-passport merely serves to assist them. The e-passport is a traditional passport with an electronic chip. It still has traditional security features - watermarks, special inks, etc. - features that need to be checked by a border official. The same official is trained to observe the person who presents the document (for signs of unease, for example). Moreover, any automated border control system will be supervised by a border official. In the absence of a perfect biometric match, or in the event of doubts about the document's authenticity, the holder will automatically be referred to a border official.

Myth #2

The e-passport was introduced for reasons of facilitation and results in lax border control

The reasoning behind this myth may be summarised as follows: e-passports allow governments to introduce automated border control systems, facilitating the passage of travellers at their borders. This gives rise to cost savings but also a lowering of standards (criminals would somehow trick the biometric system with plastic surgery, contact lenses or rubber finger tips).

***Mike Ellis** - an electronics engineer - has been involved in machine readable passport printing and reading since 1982. He is CEO of Dynjab Technologies, which designs and manufactures passport readers. Since 1990, he has been a member of the ISO Working Group WG3 and an ISO delegate to the ICAO TAG/MRTD. On behalf of the NTWG, he drafted the first Technical Report on contactless ICs, which led to the development of the e-passport. Mike is currently involved in the Arabic transliteration initiative.*

As noted in the introduction, the e-passport was primarily introduced to combat forgery. A direct consequence of the more secure passport, with its definitive link to its owner, is that automated border control is made possible. All systems currently being introduced focus on security which is of paramount importance. The systems are supervised - e-passports do not supersede the judgement of border officials.

Myth #3

The e-passport was introduced in response to 9/11; or the US Government designed it for the visa waiver program

ICAO started work on the e-passport in 1998, well before 9/11 and the changes this event gave rise to, including the requirement of the e-passport for the US visa waiver program. The e-passport is able to accommodate the growing need for security that resulted from 9/11.

Myth #4

The e-passport was introduced as the smartcard/RFID industry were desperate for sales

The NTWG spent several years analysing the best way to incorporate biometrics in e-passports. The first step was to decide on the biometric. The facial image was an obvious candidate as photos were already included in passports and because this practice was widely accepted. For e-passports to be introduced, they must be accepted by all countries, covering a wide range of cultures.

As well there was the redundancy aspect - if automatic facial recognition failed then the normal inspection process could take place, which would not be the case with fingerprints or iris. Some countries consider the use of fingerprints an excessive breach of privacy and would never incorporate them in their passports. Mandatory face, with optional fingerprints and iris, were selected after an exhaustive study.

The NTWG subsequently reviewed how to incorporate the biometric in the passport (complicated by the need for considerable storage space - up to 10K bytes or more). These requirements placed some technologies, such as magnetic stripe, offside. Although the two-dimensional bar code was an early favourite, it offered insufficient data storage capacity. The contact chip used in credit and telephone cards was also considered, but rejected because it proved too difficult to attach the contacts to the paper document. In the end, the short-range proximity radio-frequency chip was selected. It stores enough information (typically 75K) and can easily be integrated into the passport (either in the booklet, the covers or the inside pages). The NTWG wisely specified the ISO/IEC 14443 standard for the contactless chip. The smartcard industry became involved once that decision had been taken.

Myth #5

The e-passport was introduced as a plot by the UN (or ICAO, or the US Government, etc) to regiment the world by gathering biometrics

Conspiracy theories are often difficult to debunk as they seldom involve evidence. However, passports are issued by a country to its citizens to enable international travel. Most e-passports only contain a facial image, just like the traditional passport. E-passports that contain fingerprints or iris patterns are provided with greater privacy protection, severely restricting who can access the data. Countries have always collected photographs of the face, which have been stored in a database to catch out people who apply for passports in a different name. A country does not have to introduce an e-passport to collect biometrics from either its citizens or visitors - such biometrics can simply be obtained at the border.

These days, most countries have privacy laws that restrict the dissemination of biometrics to other organizations. The international exchange of biometric data is neither regular nor organised.

Myth #6

All countries must issue e-passports by 2015

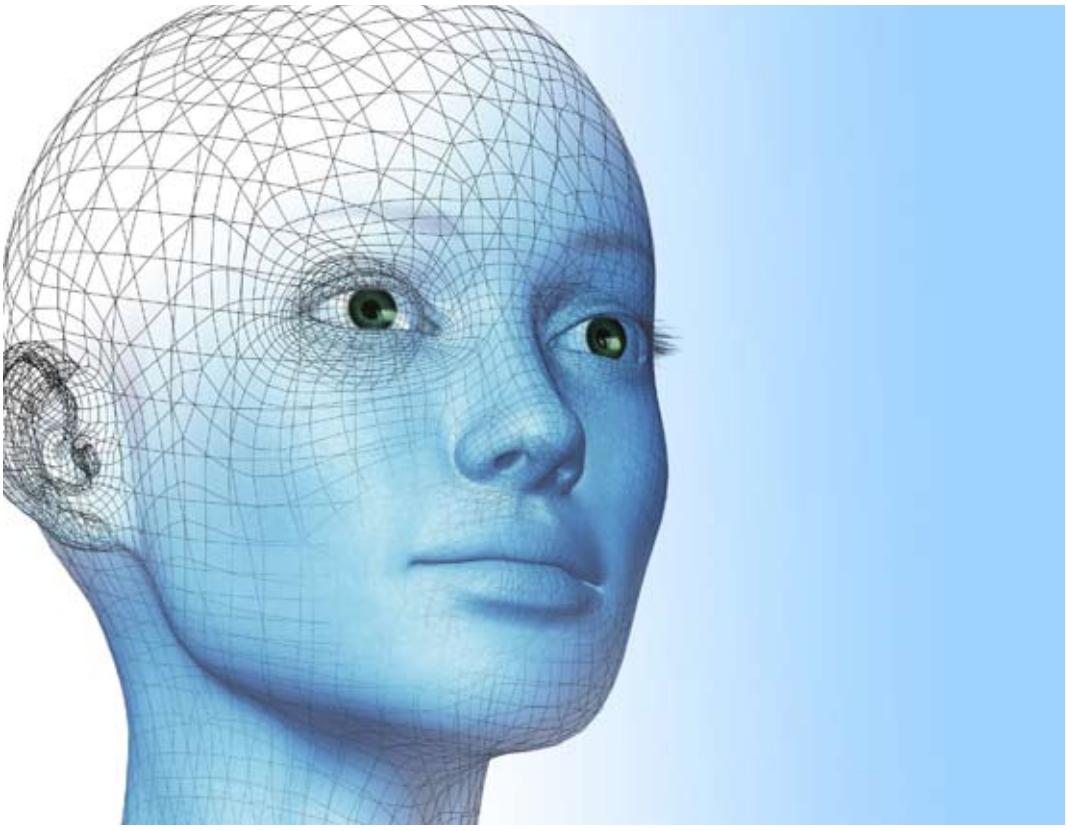
ICAO forms part of the UN and has been charged with the development of international standards for passports (under the Chicago Convention of 1944). Most countries issue machine readable passports that comply with minimum recommended security standards. ICAO requires all countries that have signed up to the Chicago Convention (nearly all the countries of the world) to issue machine readable passports (MRPs) by 1 April 2010, and that all traditional non-MRP passports must be withdrawn from circulation by 2015. There is no requirement for countries to issue e-passports. However, most countries recognise the benefits of e-passports and it is expected that over 100 countries will issue them by 2010.

Myth #7

The e-passport was introduced by 'a bunch of bureaucrats making decisions about technologies they don't understand'

Nearly all NTWG members are either involved in passport production or border control. Between them they have many years of practical experience. Some are PKI experts. The NTWG is supported by technical experts from ISO. Under the ISO/IEC rules, members of the ISO technical committees share their professional expertise; they do not represent the commercial interests of their companies.

The ISO representatives that attend NTWG meetings include chemists, engineers, physicists, IT experts, and lawyers. They work for a diversity of companies - security printers, reader manufacturers, software



development companies. The NTWG includes a number of observers from Interpol, International Air Transport Association (IATA) and the Airports Council International (ACI). It would be hard to describe the NTWG as 'a bunch of bureaucrats'. The technologies are well understood, especially as they apply to travel documents.

Myth #8

E-passport chip data should be secret

Some of the more sensational newspaper articles to emerge in recent years have reported how security researchers have retrieved data from the chip. They typically obtain a copy of the ICAO standard, implement the reading process, and seem surprised when it works. This is exactly how e-passports are meant to work. If they didn't, border officials in other countries would not be able to read them.

To prevent unauthorized reading, ICAO has specified the Basic Access Control (BAC), which most countries have implemented even though it is optional. Unauthorized reading involves either a hidden reader, which captures data at up to 10cm (this distance can be increased to about 75cm if the power and antenna size are increased) or a device that intercepts data in transit between the chip and a legitimate reader (a process known as eavesdropping). BAC uses a combination of printed data to generate a key that allows access to the chip data. In other words, any person who has access to the printed data is entitled to access the chip data. Journalists also seem surprised that the BAC procedure is in the public domain - but how else could international border control officials access the chip data?

Some countries also equip their e-passports with metal foil pages. The metal foil decouples the chip's antenna whenever the booklet is closed, effectively disabling it. As soon as the e-passport is opened, the chip can be powered up again if it is close to the reading machine.

Although the chip data may be accessed by authorised parties, this does not mean that the data is insecure. Using passive authentication reveals whether data has been tampered with (photo substitution, for example). The issuing authority calculates the digital signatures using its private key and writes these to the chip; the border official authenticates the same digital signatures using the public key. This public key is contained in a certificate, which is often stored on the chip. The certificate can in turn be authenticated by reference to ICAO's Public Key Infrastructure (PKI) directory, or by means of bilateral exchange.

It is recognised that some biometric data - including fingerprints and iris data - is more sensitive and therefore warrants greater security. To accommodate

this requirement, use is made of Extended Access Control (EAC), which requires an inspection system to authenticate itself before the data is released.

Myth #9

Contact cards are more secure

This argument is often voiced by those who object to radio frequency technology, and the ability to intercept radio signals in particular (eavesdropping). Of course, contact cards have also been intercepted - criminals intent on capturing credit card details at ATMs have been very inventive. The NTWG has investigated eavesdropping and found that data can also be intercepted elsewhere in the computer system (the radio waves from a USB link, the modulation of the power supply, etc.). Eavesdropping is a pan-system problem and must be tackled as such. It does not affect radio frequency technology alone. The incorporation of shields in e-passports and the introduction of BAC and EAC have effectively resolved the problem of eavesdropping and unauthorized access. It has also been argued that bar codes are more secure. Again, system security would be no different. However, the problem with bar codes is that they do not offer enough capacity to store biometric data.

Myth #10

The e-passport chip transmits personal information continuously

The e-passport chip is powered by the electromagnetic field of the reader; it has no battery or other power source of its own. Until the chip is close to a reader and powered up, it cannot transmit data. When powered, the chip only responds to commands sent from the reader. Moreover, the data is at all times protected by BAC encryption.

E-passport chips are power hungry and draw power from the electromagnetic field. They work at a distance of up to 10 cm from the reader. While it is perfectly possible to build non-standard readers that supply more power and use large antennas, the law of diminishing returns applies. In our analysis, the practical range is limited to about 75 cm (30").

Myth #11

The RF chip was chosen so that people could be tracked

The most radical version of this myth is that the RF chip can be queried from a great distance, even using satellites. This is not possible. While some RFID devices - including RF tags used in shops - can be tracked at a distance of up to tens of metres, such devices comply with other ISO standards. They are generally much smaller and have minute power requirements.

Even if an e-passport is within the range of an unauthorized reader, say within 75cm (30"), it takes about 3 or 4 seconds to retrieve the data. The e-passport must be within range for this whole time. Should the transmission be disrupted for any reason, the entire process will be aborted. This means that tracking is very difficult to achieve under the best conditions. This scenario is academic, however, as all e-passports now have BAC (which prevents unauthorized access), and this makes tracking impossible.

Some commentators have pointed out that the intention is to track the Unique Identifier (UID). When the e-passport is initially accessed by the reader, it identifies itself by sending a UID. In theory, the passport can be tracked once it has been associated with a UID (though no data can be read from the document itself). It should be noted, however, that most if not all countries use random UIDs. Each time the e-passport is accessed, it generates a different UID for that session. This prevents tracking.

Interestingly enough, the efficient tracking systems that are already widely used do not seem to raise the same concerns. Think of car registration numbers, mobile telephony, and public CCTV systems, each of which can be used to track our movements. While this does not justify tracking e-passports, the likelihood of the e-passport being used to track people is remote.

Myth #12

The contactless chip in the e-passport is prone to failure

The NTWG was concerned about chip failure. In response, most countries advise their citizens to care for their e-passports (by not bending, twisting or puncturing them). The warranty period of the chip was also an issue, not least because chips had not been used in combination with passports before. The preliminary evidence indicates that the chips are reliable. Some countries have reported no chip failure after 3 or 4 years. As the chip has been designed to operate in the field under adverse conditions, there is every reason to believe that the chip will survive for 5 to 10 years.

Myth #13

The Machine Readable Zone (MRZ) is a 'bar code'

The MRZ consists of two lines of printing (88 characters) at the foot of the data page. The MRZ is printed using Optical Character Recognition Type B (OCR-B) and is not a 'bar code'. ICAO specified OCR-B in the first edition of Doc 9303 released in 1980 as OCR-B was at that stage a mature technology.

Myth #14

E-passports vary from one country to the next

This comment is usually made within the context of comparing passports of different countries with the aim of grading or remotely identifying them. Practically all

e-passports meet ICAO standard Doc 9303. They also comply with a set of minimum security standards. While there are small differences between the e-passports issued by different countries, they have much in common.

To achieve global interoperability, all e-passports must conform to Doc 9303 in all mandatory aspects. As a result, the level of variation is minor.

Myth #15

The e-passport is read in two stages, which slows down passenger processing

Some commentators emphasise that it takes too much time to read an e-passport. The reading process consists of two stages. First, the MRZ is read using an optical reader. Next, an RF reader is used to capture data from the chip. Although some readers will use this two-stage process, there are many readers on the market that combine optical and RF data retrieval in a seamless manner.

While not recommending one form of reader over another, use of the single combined reader is the preferred way to implement e-passport reading.

Myth #16

The e-passport is authentic if the data in the booklet and the data on the chip are the same

While the printed information included in the passport must be the same as the chip data, this does not guarantee that the e-passport is authentic. Authenticity is established on the basis of identity integrity and paper security features in combination with PKI verification of the digital signatures in the chip. It cannot be stressed enough: the chip is only one aspect of the passport. Any attempt to forge physical security features will also be detected.

Myth #17

The chip data merely confirms the printed data

Although the chip data included in mandatory data groups 1 and 2 (MRZ and facial image) is used to confirm the printed data, the chip can also be used to store optional data, including additional fingerprint and iris templates. The chip data is secured by the PKI, which provides an additional strong level of security. Chip data can also help border officials in other ways. For example, the facial image stored in the chip has a higher resolution than the printed photo, making a comparison with the person easier.

Myth #18

A fake passport with a cloned chip will not be detected

If the chip is cloned, it will contain data relating to the original holder. If it is cloned and subsequently altered - by replacing the photograph, for example - this will be detected as a result of PKI verification. While forging paper-based security features sounds straightforward enough, it is, in fact, exceptionally difficult. Of course, border officials know exactly what to look for.

Many e-passports are now equipped with Active Authentication (AA), which detects cloning. This is a public/private key protocol where the private key is embedded in the original chip. It cannot therefore be copied. The cloned chip does not contain this private key, allowing it to be detected.

While e-passports are highly secure, the assumption that this will result in cursory inspections is unfounded. As indicated above, the e-passport does not supersede border officials. It is an extra tool in the detection of forgeries. This also applies to look-alike fraud (a problem that pre-dates the introduction of the e-passport). Border officials are able to base their judgement on a higher resolution photograph in the chip while sophisticated facial recognition systems can be used to highlight any differences.

Myth #19

The US PASS card is an e-passport

The PASS card is a vicinity card containing a number and can be read at a distance of typically 50 metres. It offers no protection against unauthorized reading (although the holder can place it in a protective metal-lined pouch to prevent access). The card was developed to enable US border officials to retrieve data as the holder approaches the border control point. The number is used to access a database. The card identifies US citizens at the US land and sea borders by means of this number, but does not contain any personal information itself.

Many journalists and bloggers mistake the PASS card for an e-passport, and claim that the latter can also be read at a distance of 50 metres. This is a fallacy. The US PASS card is not an e-passport.

Myth #20

Golden Reader software is the ICAO standard

ICAO used the Golden Reader software to conduct e-passport and reader interoperability tests. It was never intended, nor was it ever advertised, as the de facto border control software. The myth persists because security researchers, having altered the digital signature hash, were able to read their new hash using Golden Reader. It should be noted that Golden Reader does not check PKI certificates. Border control software does check these certificates and will detect these forgeries.

Myth #21

A wanted person can use someone else's chip to pass border control

This is not particularly credible. The belief that a criminal whose name appears on a watch list could carry an e-passport containing his real name and photograph but a chip that was cloned from someone else's e-passport, and pass border control, is far-fetched. As we indicated above, the e-passport does not supersede border officials. No border control system is going to allow a person to pass solely on the basis of unseen chip data. If passports are inspected manually, the border official will first check the chip data against the printed data. This will highlight the forgery. If passports are inspected automatically, the chip data will also be checked against the printed data. In addition, the biometric data in the chip will be checked against the holder.

Myth #22

The e-passport can be programmed to crash a border control system or install viruses

This myth is based on the exploits of another security researcher, who altered the JPEG image stored in an e-passport chip. He subsequently found two readers at a trade fair that crashed while trying to read the altered JPEG image. From this he surmised that he would be able to control the inspection system or introduce viruses.

The equipment on display at fairs does not operate like the equipment installed at border crossing points. The former are set up to read sample as well as genuine documents and to display their content without conducting any serious check. Vendors are primarily interested in showing off the functionality of their equipment; they are not unduly bothered about checking the PKI (which is not a reader function as such). If the reader software has not been properly written, a corrupted JPEG will cause it to crash, requiring a system reboot.

A border inspection system will initially read the chip data and check its authenticity by means of passive authentication. Other code will only be executed if this check is successful (reading the JPEG file, for example). A virus would not be able to install itself, as it would be detected by the passive authentication check.

Myth #23

The biometric data can be used for other purposes, thus violating privacy

The facial image is the mandatory biometric. As a

photograph can be captured by other devices (a camera, for example), the retrieval of a facial image from the chip should hardly be cause for concern (this can only be done if the BAC protection is compromised). Other biometrics, including fingerprints and the iris, are considered more sensitive and protected by EAC.

Myth #24

Criminals can steal your identity by remotely reading your e-passport

The e-passport is protected against unauthorized reading and eavesdropping by BAC. In some cases, metallic shields are used (see myth #8 for a description). To overcome the BAC and gain access to personal data, criminals must either have physical possession of the document or the passport must be within range of their reader for a very long time (allowing a brute force attack). Remote reading of the ePassport, even at the maximum 75cm (30") range, is therefore impractical.

Myth #25

A faulty chip will invalidate the e-passport causing access to be denied

ICAO has repeatedly stated that an e-passport with a faulty chip should be treated as a legitimate travel document. The holder should not be denied entry on the basis of a faulty chip only. However most border officials will recommend users to replace their faulty e-passport as soon as possible.

Needless to say, criminals that are unable to subvert the chip will be tempted to destroy it rather than risk being detected. As a consequence, border officials will carefully inspect e-passports with faulty chips, looking for signs of tampering.

Any blogger proposing the destruction of the chip on whatever grounds should at least be aware of the practical consequences of his or her suggestion. All nations have laws against intentionally damaging the passport, which in fact remains the property of the issuing government.

Myth #26

Look-alikes can use e-passports too

Look-alikes have always been a problem. In theory a criminal can steal a passport and alter his appearance using hair dye and what have you to make himself look like the original holder. Traditional passports present an even greater problem in that the photo on the data page is small, making it difficult to detect look-alikes.

In contrast, the e-passport contains a high resolution facial image that can be displayed in a larger size, making it much easier to detect look-alikes. If a facial recognition system is used, the likelihood of the criminal being detected is even greater.

The Smartgate system installed at Sydney airport, and similar systems in other countries such as Germany, Portugal, the UAE and the UK, include facial recognition

software that matches the facial image in the e-passport to the holder's face. If a perfect match is not obtained, the holder is referred to a customs officer for manual processing. Smartgate also checks the digital signature to make sure that the image and personal data have not been altered.

Myth #27

The EU has stated that e-passport security is 'poorly conceived'

In September 2006, FIDIS (Future of Identity in the Information Society) published its Budapest Declaration attacking the e-passport. Unfortunately the declaration was based on early reports from hackers and security researchers. The FIDIS report concludes that 'the current implementation of the European passport utilises technologies and standards that are poorly conceived for its purpose'.

While FIDIS was funded by the EU, its declaration does not necessarily represent the EU's views. If it did, it would be inconceivable that all EU countries would have introduced e-passports. The "weaknesses" highlighted by the FIDIS, and which the FIDIS relied on for its declaration, included myth #8, myth #11, myth #23 and myth #31. Again, the chip is only one aspect of today's secure passport.

Myth #28

Outsourcing the manufacture of e-passports to foreign companies is a national security threat

This myth took hold after the United States outsourced the manufacture of its inlays (i.e. the chip-antenna sub assembly) to a company that was manufacturing them in Thailand. This was done to save costs and did not compromise national security. Rarely is a nation able to make an e-passport solely from national sources. Each nation should vet their suppliers with regard to security and competence, but restricting sources to one nation can result in use of less than the best or most secure product.

While the theft or diversion of traditional passports represents a security threat (blank passports can be easily populated), this is not the case for e-passports, which are only personalised after they have been delivered. PKI will detect any stolen e-passport that has been authenticated using third party equipment (see myth #20).

Myth #29

The e-passport should be protected by a PIN

Some belief that the use of a PIN could provide an alternative to the BAC key derived from the MRZ. There are several problems with this idea. First, passports tend to be used infrequently and a high percentage of travellers might forget their PIN. This could lead to them being refused entry. Second, people can reliably remember 4 to 5 digits (a few might even remember 8). This potentially opens the door to hackers who would try to guess the PIN by brute force attack (unless the passport shuts down after a predefined number of attempts). The BAC contains 24 digits.

Efficiency is another consideration - reading the optical MRZ to generate a key is much faster (and takes less time than manually entering a PIN on a keypad).

Myth #30

Metal shields or jackets do not offer a defence against unauthorized access

The e-passport chip cannot be read if the booklet is placed in a metal jacket. The latter effectively creates a Faraday Cage, preventing radio waves from reaching the chip's antenna. A metal shield - such as a metal insert - is just as effective as it decouples the antenna and prevents it from resonating at the same frequency as the radio waves. As the chip derives its power from these radio waves, it cannot communicate. The myth is based on the use of non-metal shields or jackets. While aluminium-coated plastic is a common alternative, it is too thin to block strong radio waves.

Myth #31

The e-passport can be used to set off explosives

In 2006, a company called Flexilis set off a small explosive device with a partly opened e-passport. It was open about 12mm (1/2") and the claimed reading distance was 10cm (4"). The e-passport contained a single metal shield inlay. The company was attempting to demonstrate that a dual shield inlay provides more effective protection. The e-passport in their test was not protected by BAC.

This demonstration is often cited to show the dangerous aspect of carrying an e-passport. But the chances of a person walking past a reader that is attached to an explosive charge, with an e-passport not protected by BAC and partially open, is minute. The e-passport must also be in range of the reader for several seconds for the reader to get useful information, e.g. nationality. It is also clear that this demonstration merely relied on the presence of the e-passport, rather than a comprehensive reading of the chip data.

Most e-passports are now protected by BAC. Those that are not have metal shields. A system targeting one nationality or specific people based on reading their e-passport as they pass by is just a myth.

Myth #32

Sending illegal commands and registering the e-passport response allows the nationality of the holder to be established

A group of security researchers experimented with

illegal commands, observing the responses from different e-passports. As illegal commands are not specified in the ICAO standard, different manufacturers have implemented different ways to process such commands. The researchers claimed they were able to identify the nationalities of the document holders, and concluded that terrorists would be able to do the same.

Rather than identity the nationality of the holders, the researchers had in fact established the nationality of the chip manufacturer. It just so happened that the e-passports they used were all made by different manufacturers. As the number of manufacturers is limited, many countries buy from the same manufacturer. Likewise countries are able to change supplier for whatever reason. Thus the nationality of the holder cannot be reliably determined by this method.

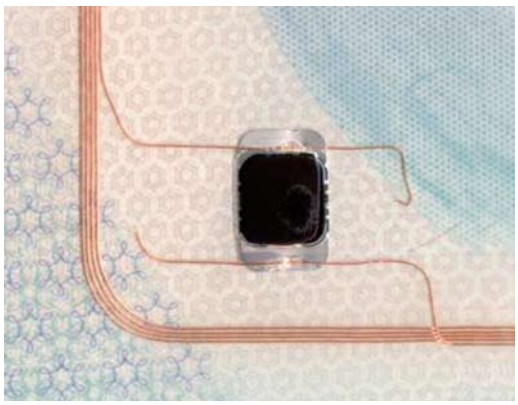
Myth #33

The BAC is easily compromised

Hackers have in the past attacked the e-passport by brute force, trying to guess the BAC key by trying different combinations. While broadly publicised, these attacks were always based on a limited number of combinations (derived from the document number, the date of birth and the expiry date), making the code comparatively easy to break.

For example, we can guess the person's age to within 5 years either way, the passport number to within 3,000,000 (one year's production) and we can restrict the expiry date to within one year to correspond to this particular year's production. Each guess takes 30ms to process as the e-passport chip takes this long to respond, but even with this simplification cracking the code would take a long time, typically 2,000 years. For completeness' sake, we should add that most countries now use random passport numbers (so the expiry date cannot be related to the passport number) making the above odds even higher.

In this example calculating the time to crack the code is as follows: taking the date of birth 5 years either way means a total of 10 years, or 3650 possible dates. If there are 3,000,000 passports issued in one year: this is 3,000,000 possible passport numbers. If we restrict the expiry date to one year: this is 365 dates. So now the total possible combinations are 3650 x 3,000,000 x 365, which equals 3,996,750,000,000. We know each combination takes the chip 30ms to process: so 3,996,750,000,000 x 30ms equals 119,902,500,000 seconds, or if you express this in years, a bit over 3,802 years. If we assume that it is reasonable that there is a 50/50 chance of the right key being guessed by half-way through the guesses: this is still over 1,901 years. Of course, the hackers assume they know the person's date of birth from other sources, but even so the calculation results in a 50/50 chance of a guess being right in 6 months. The hackers have to try to reduce the number of combinations to achieve any success at all. In reality, none of this data would be known and cracking the code would take a long time.



Myth #34

The BAC is based on the holders place of birth, name, etc.

The BAC is derived from the passport number, the date of birth and the expiry date. As only the date of birth is potentially available from other sources, the above combination provides considerable protection. As issuing authorities use random passport numbers, there is no correlation between the number and the expiry date (which could be the case if passports were issued in chronological and numerical order).

Myth #35

E-passport data can be intercepted by listening to radio wave transmissions

BAC is also used to encrypt radio wave transmissions between the e-passport and the reader, which can be intercepted at a distance. The furthest distance we have seen so far is about 10m, although some hackers have claimed a distance of 50m or more. However, even if data is intercepted over a larger distance it would need to be decrypted by brute force. This gives rise to the same limitations described in myth #33. As a consequence, e-passport data cannot simply be intercepted.

Modern readers tend to feature anti-eavesdropping functionality, either by reducing stray transmissions or by masking transmissions with noise. Where multiple systems are used - at airports, for example - radio transmissions are likely to interfere, making eavesdropping impractical.

It is worth noting the all electronic devices radiate to some extent. This includes the computers that process e-passport data. Power and communication lines (USB) also radiate. As a consequence, authorities usually adopt a system-wide approach to resolve this problem.

Myth #36

The e-passport can easily be cloned

This is a common claim. In practice, all the claimants have done is read data from one e-passport chip, which they have subsequently written to another chip. Reading the data from the chip is exactly how the system is supposed to work. Programming another chip with the same data is about as useful as photocopying a traditional passport - the cloned chip still needs to be embedded in the passport booklet, which is protected by a range of security features. Again, if the data is altered after the chip has been cloned, this will be detected by the digital signatures and the PKI authentication process. ICAO Doc 9303 also specifies Active Authentication (AA) as an optional protection technique. AA works on the basis of a private/public key pair. The private key cannot be copied, so in the cloned chip the keys will no longer match and an AA authentication check will fail. Many countries have adopted AA.

Myth #37

AA can be defeated by turning off the indicator in the Data Group Presence map

We have to delve into the technicalities here. The Data Group Presence Map (the EF.COM file) indicates which data groups are present in the e-passport's chip. It has been added for the benefit of reading systems, which would otherwise waste time trying to read non-existent data. As the EF.COM file is not protected by a digital signature, hackers are able to remove the AA indicator. In practice, this means the AA check is skipped so that the cloned chip is not inspected for AA and detected. In fact, hackers could remove the indicator for any data group - including fingerprints - in an attempt to circumvent border controls. As a matter of good design, ICAO has recommended that the EF.COM should not be relied upon. Instead, the Document Security Object (the EF.SOD) should be used to find which data groups are present. The EF.SOD is protected by a digital signature so any tampering will be detected.

Myth #38

Extended Access Control can be circumvented as the chip has no clock and cannot establish whether a stolen reader certificate has expired

Another technical myth. EAC uses certificates to authorise two-way communication between the e-passport chip and the inspection system. Both the e-passport chip and the inspection system prove to each other, by means of certificates, that they are authorised to access each other. If an inspection system is stolen, its certificate will expire preventing it from accessing sensitive EAC protected data (fingerprints and iris data) on the chip. Some claim that the absence of an on-board clock means the chip is unaware of the date and cannot therefore establish whether the certificate used by a stolen inspection system has expired. However, the date on the e-passport chip is refreshed each time it connects to an inspection system. For the chip to be fooled, the first inspection system used by the traveller would have to be stolen, which is very unlikely. We would add that certificates are typically valid for one day. It should also be noted that the certificate does not generally reside within the reading module of the inspection system. If a machine reader is stolen, it is unlikely to contain the necessary certificate.

Myth #39

Because only a small percentage of countries have joined ICAO's Public Key Directory, country signing certificates are not being checked and forged e-passports are being used successfully

The ICAO Public Key Directory (PKD) is the best way for countries to obtain current Document Signer (DS) certificates and Country Signing Certification Authority (CSCA) certificates. The PKD also contains Certificate Revocation Lists (CRLs) of compromised certificates. The PKD is not the only channel through which border authorities are able to obtain certificates. They can also be obtained by bi-lateral means (eg, diplomatic channels) or via master lists. Therefore hackers should not assume that because a country does not belong to the PKD that it is not using DS and CSCA certificates to validate e-passports at its borders.

Conclusion

This article has attempted to address some of the prevalent misconceptions about e-passports. The e-passport system and its reader infrastructure has been constructed in a relatively short time, yet has received unprecedented global acceptance and attained interoperability, working in areas where errors can have profound consequences. The e-passport system is under constant evaluation and on-going monitoring for ways to make it better. We hope that the level of discussion can also move forward, based on new issues, not rehashing of old canards.

An excellent, in-depth article describing the history, interoperability and implementation of Machine Readable Travel Documents - entitled The History of Interoperability - is available via the 'downloads/ technical reports' section of the ICAO website: http://www2.icao.int/en/MRTD/Pages/default.aspx. I gratefully acknowledge the valuable assistance given by TF3 and TAG members in the preparation of this article.

1 NTWG - the New Technologies Working Group of the Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTDs).

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