Security and Privacy Issues in E-passports

Ari Juels[*], David Molnar[†], and David Wagner[‡]

Abstract

Within the next year, travelers from dozens of nations may be carrying a new form of passport in response to a mandate by the United States government. The e-passport*, as it is sometimes called, represents a bold initiative in the deployment of two new technologies: Radio-Frequency Identification (RFID) and biometrics. Important in their own right, e-passports are also the harbinger of a wave of next-generation ID cards: several national governments plan to deploy identity cards integrating RFID and biometrics for domestic use. We explore the privacy and security implications of this impending worldwide experiment in next-generation authentication technology. We describe privacy and security issues that apply to e-passports, then analyze these issues in the context of the International Civil Aviation Organization (ICAO) standard for e-passports.*

1 Introduction

Major initiatives by the United States and other governments aim to fuse Radio Frequency Identification (RFID) and biometric technologies in a new generation of identity cards. Together, RFID and biometric technologies promise to reduce fraud, ease identity checks, and enhance security. At the same time, these technologies raise new risks. We explore the privacy and security implications of this worldwide experiment with a new type of authentication platform, with particular attention to its deployment in passports.

As part of its US-VISIT program, the United States government has mandated adoption by October 2006 of biometrically-enabled passports by the twenty-seven nations in its Visa-Waiver Program (VWP), among them Japan, most of the nations of Western Europe, and a handful of others[1]. By the end of 2005, all passports produced in the U.S. will carry biometric information. These passports are based on guidelines issued by the International Civil Aviation Organization (ICAO), a body run by the United Nations with a mandate for setting international passport standards [15]. The ICAO guidelines, detailed in ICAO Document 9303, call for incorporation of RFID chips, microchips capable of storing data and transmitting it in a wireless manner, into passports. (In this paper we refer to the ICAO guidelines as a 'standard.' They are certainly a de facto standard but not a ratified standard.) Such chips will be present in initial deployments of biometrically enabled United States passports, and in the biometrically enabled passports of other nations as well. Next-generation passports, sometimes called *e-passports*, will be a prominent and widespread form of identification within a couple of years.

The ICAO standard specifies face recognition as the globally interoperable biometric for identity verification in travel documents. Thus e-passports will contain digitized photographic images of the faces of their bearers. The standard additionally specifies fingerprints and iris data as optional biometrics. The US-VISIT program in fact requires visitors to provide two fingerprint images in addition to a headshot. The ICAO standard also envisions that e-passports will someday include a write capability for storage of information like digital visas.

Interestingly, one nation has already deployed e-passports in a project pre-dating the ICAO standard. Since 1998, Malaysian passports have included a chip containing an image of a thumbprint of the passport holder; a second generation of e-passports rolled out in 2003 that contains extracted fingerprint information only. When flying through Kuala Lumpur International Airport, a Malaysian citizen passes through an automated gate that reads the thumbprint from the chip and compares it to the thumb pressed on a scanner. Today, over 5,000,000 first generation and 125,000 second generation e-passports are in circulation.

While e-passports are important in their own right, they also merit scrutiny as the harbinger of a wave of a fusion of RFID and biometrics in identity documents. Another next-generation ID card slated for deployment in the near future in the United States, for example, is the Personal Identity Verification (PIV) card. PIV cards will serve as ID badges and access cards for employees and contractors of

[*]RSA Laboratories, ajuels@rsasecurity.com
[†]UC-Berkeley, dmolnar@eecs.berkeley.edu
[‡]UC-Berkeley, daw@eecs.berkeley.edu

[1]The deadline was originally October 2005, but it was extended after European nations protested [26].

the federal government in the United States. A standard for government ID cards (FIPS 201) is seeing rapid development by the National Institute of Standards and Technology (NIST). We expect PIV cards will include the same blend of technical mechanisms as e-passports: a combination of RFID and biometrics. The biometric of choice for PIV cards, however, will probably be fingerprint recognition. At the time of writing, the U.S. House of Representatives recently passed a bill called the Real ID Act; this seems a likely impetus for states to issue identity cards containing biometrics, and probably RFID tags as well [23].

The goal of the ICAO and PIV projects is the same: strong authentication through documents that unequivocally identify their bearers. Data integrity and physical integrity are vital to the security of ID cards as authenticators. For authorities to establish the identity of John Doe with certainty, for example, Doe's passport must carry a photograph of irrefutable pedigree, with a guarantee that no substitution or tampering has taken place. Without this guarantee, passports can be forged, enabling unauthorized persons to enter a country.

Strong authentication requires more than resistance to tampering. *Data confidentiality*, i.e., secrecy of data stored on ID cards, is also critical. Protecting biometric and biographical data is essential to the value and integrity of an authentication system. In particular, data secrecy affords an important form of protection against forgery and spoofing attacks. Therefore protecting e-passport data against unauthorized access is a crucial part of the security of the entire system.

Confidentiality protection for stored data is important for other reasons as well. Both RFID and biometrics are highly privacy-sensitive technologies. Sensitive data, such as birthdate or nationality, are carried on passports. The privacy, physical safety, and psychological comfort of the users of next-generation passports and ID cards will depend on the quality of data-protection mechanisms and supporting architecture.

We identify security and privacy threats to e-passports generally, then evaluate emerging and impending e-passport types with respect to these threats. We primarily analyze the ICAO standard and the specific deployment choices of early adopter nations. Where appropriate, we also discuss the Malaysian e-passport. Here is a summary of the major points we touch on:

1. **Clandestine scanning**: It is well known that RFID tags are subject to clandestine scanning. Baseline ICAO guidelines do not require authenticated or encrypted communications between passports and readers. Consequently, an unprotected e-passport chip is subject to short-range clandestine scanning (up to a few feet), with attendant leakage of sensitive personal information including date of birth and place of birth.

2. **Clandestine tracking:** The standard for e-passport RFID chips (ISO 14443) stipulates the emission (without authentication) of a chip ID on protocol initiation. If this ID is different for every passport, it could enable tracking the movements of the passport holder by unauthorized parties. Tracking is possible even if the data on the chip cannot be read. We also show that the ICAO Active Authentication feature enables tracking when used with RSA or Rabin-Williams signatures.

3. **Skimming and cloning:** Baseline ICAO regulations require digital signatures on e-passport data. In principle, such signatures allow the reader to verify that the data came from the correct passport-issuing authority.[2] Digital signatures do not, however, bind the data to a particular passport or chip, so they offer no defense against passport cloning.

4. **Eavesdropping**: "Faraday cages" are an oft-discussed countermeasure to clandestine RFID scanning. In an e-passport, a Faraday cage would take the form of metallic material in the cover or holder that prevents the penetration of RFID signals. Passports equipped with Faraday cages would be subject to scanning only when expressly presented by their holders, and would seem on first blush to allay most privacy concerns.

   Faraday cages, however, do not prevent eavesdropping on legitimate passport-to-reader communications, like those taking place in airports. Eavesdropping is particularly problematic for three reasons.

   - *Function creep:* As envisioned in the ICAO guidelines, e-passports will likely see use not just in airports, but in new areas like e-commerce; thus eavesdropping will be possible in a variety of circumstances.
   - *Feasibility:* Unlike clandestine scanning, eavesdropping may be feasible at a longer distance—given that eavesdropping is a passive operation [31].
   - *Detection difficulty:* As it is purely passive and does not involve powered signal emission, eavesdropping is difficult to detect (unlike clandestine scanning).

5. **Biometric data-leakage**: Among other data, e-passports will include biometric images. In accordance

[2] Digital signatures and indeed, e-passports and secure ID cards in general do not solve the problem of validating *enrollment*. Depending on how new users are validated, it may be possible to obtain an authentic ID by presenting inauthentic credentials or through circumventing issuing guidelines. Indeed, the 9/11 hijackers had perfectly authentic drivers' licenses. Digital signatures would merely have confirmed their validity. We do not treat the issue of enrollment here, but note that it is pivotal in any ID system.

with the ICAO standard, these will initially be digitized headshots, while thumbprints are used for the Malaysian e-passport. These images would not need to be secret to support authentication if the physical environment were strictly controlled. However, existing and proposed deployments of e-passports will facilitate automation, and therefore a weakening of human oversight. This makes secrecy of biometric data important.

6. **Cryptographic weaknesses:** ICAO guidelines include an optional mechanism for authenticating and encrypting passport-to-reader communications. The idea is that a reader initially makes optical contact with a passport, and scans the name, date of birth, and passport number to derive a cryptographic key K with two functions:

   - It allows the passport to establish that it is talking to a legitimate reader before releasing RFID tag information
   - It is used to encrypt all data transmitted between the passport and the reader.[3]

   Once a reader knows the key K, however, there is no mechanism for revoking access. A passport holder traveling to a foreign country gives that country's Customs agents the ability to scan his or her passport in perpetuity. Further, we find that the cryptography relied upon by the ICAO standard itself has some minor flaws.

Related Work

Existing media stories, e.g., [27], have recognized the first three of the points enumerated above. The other issues, more technical in nature, have seen less exposition; the major previous effort we are aware of is Pattinson's whitepaper that outlines the privacy problems with e-passports that may be readable by anyone and argues, as we do, for Basic Access Control [25]. Pattinson also points out the need for a direct link between optically scanned card data and secret keys embedded in an e-passport. He does not, however, consider the issue of biometric data leakage or the cryptographic issues we address. Jacobs discusses issues in e-passport deployment in the Netherlands and reports on work with a prototype Netherlands biometric passport; he highlights the importance of Basic Access control and also investigates the issues surrounding a national database of biometric identifiers [18]. Finally, the smart card research group at IBM Zurich has demonstrated a Javacard application running on a Philips chip that performs Basic Access Control and Active Authentication in under 2 seconds, showing that these technologies are feasible in practice [13].

[3] The need for optical scanning of passports seems to negate the benefits of wireless communication conferred by RFID. Our supposition is that ICAO guidelines favor RFID chips over contact chips because wireless data transmission causes less wear and tear than physical contact.

Organization

In section 2, we provide some basic technical background on RFID and biometrics. We turn in section 3 to a detailed discussion of the data contained in e-passports deployments and the risks posed by data exposure. We focus on the ICAO standard and the choices of specific countries in implementing the standard, and also briefly describe the Malaysian program as an illustration of likely deployment features. We consider the cryptographic security measures of the ICAO standard in section 4, illuminating some potential weaknesses and discussing the selection of features the United States has made for its US-VISIT program. In section 5, we sketch a few countermeasures to the security weaknesses we highlight. We discuss security issues likely to arise in future e-passport and ID-card systems in section 6. We conclude in section 7 with summary recommendations for improved e-passport deployment and with pointers to ID projects with similar underpinnings.

2 Technical Background

2.1 RFID in brief

The term Radio Frequency Identification (RFID) has come to stand for a family of technologies that communicate data wirelessly from a small chip, often called a "tag," to a reading device. The ICAO specification for e-passports relies on the International Organization for Standardization (ISO) 14443 standard, which specifies a radio frequency of 13.56MHz. Tags in the ISO 14443 standard are *passive*, meaning that they carry no on-board source of power, and instead derive power indirectly from the interrogating signal of a reader. The intended read range of tags in this standard is about 10 centimeters.

Because WalMart, the U.S. Department of Defense, and others have received much attention for their RFID deployments, we stress that the RFID used for e-passports is not the same as the RFID used by WalMart and others for supply chain management. Supply chain tags are designed to be as simple and cheap as possible, with no support for cryptography and minimal additional features beyond holding a single identifier. For example, the only privacy feature in the tags specified by the industry body EPCglobal is a special "kill" command that renders the tag permanently inoperative. These supply chain tags operate at a frequency of 915MHz and have an intended read range of five meters. In contrast, e-passport RFID devices have a shorter intended read range, and they include other features such as tamper resistance and cryptography.

We write *intended* read range to mean the ranges achievable with vendor-standard readers. An adversary willing to build its own readers may achieve longer read ranges, especially if it is willing to violate applicable laws regulating radio devices. It may also be possible to eavesdrop on a conversation between a legitimate reader and an RFID tag over a greater distance than is possible with direct scanning. E-passport trials held in October 2004 reportedly showed the possibility of eavesdropping from a range of 30 feet [31]. Others have shown how relay devices can be used to read ISO 14443 chips, the kind used in e-passports, from even greater distances [21].

2.2 Biometrics in brief

Biometric authentication is the verification of human identity through measurement of biological characteristics. It is the main mechanism by which human beings authenticate one another. When you recognize a friend by her voice or face, you are performing biometric authentication. Computers are able to perform very much the same process with increasing efficacy, and biometric authentication is gaining currency as a means for people to authenticate themselves to computing systems. We use the term *biometrics* in this paper to refer to human-to-computer authentication.

The range of practical biometrics for computing systems is different than for human-to-human authentication. Popular computer-oriented biometrics, for instance, include fingerprints, face recognition, and irises; these are the three biometrics favored for e-passport deployments.

Face recognition involves photographic imaging of the face; it is essentially the automated analog of the ordinary human process of face recognition. Fingerprint recognition likewise relies on imaging and an automated process very loosely analogous to the fingerprint matching used in criminal investigations (but often based on a different class of fingerprint features). Fingerprint scanners can take on optical or silicon-sensor forms. Iris recognition also involves imaging. The iris is the colored annular portion of the eye around the pupil. Someone with "blue eyes," for instance, has blue irises. (The iris is not to be confused with the retina, an internal physiological structure.) Iris scanning in biometric systems takes place via non-invasive scanning with a high-precision camera. The device that captures user data in a biometric system is often called a *sensor*.

The process of biometric authentication is roughly similar in most systems. An authenticated user enrolls by presenting an initial, high-quality biometric image to the sensor. The system stores information extracted during enrollment in a data structure known as a *template*. The template serves as the reference for later authentication of the user. It may consist of an explicit image of the biometric, e.g, a fingerprint image, or of some derived information, such as the relative locations of special points in the fingerprint. To prove her identity during an authentication session, the user again presents the biometric to a sensor. The verifying entity compares the freshly presented biometric information with that contained in the template for the user in a process generally called *matching*. The template and authentication image are deemed to match successfully only if they are sufficiently similar according to a predetermined—and often complicated and vendor-specific—metric.

While conceptually simple, the process of biometric authentication abounds with privacy and security complications. Most germane to our discussion here is the issue of biometric authenticity: How does the verifying entity know that the image presented for authentication is fresh and comes from a human being rather than a prosthetic or a digital image? The manufacturers of biometric sensors try to design them to resist spoofing via prosthetics; the designers of biometric systems employ data security techniques to authenticate that the origin of biometric information is a trusted sensor. As we shall explain, however, the *privacy* of templates is ultimately quite important and yet insufficiently assured in the baseline ICAO standard.

3 E-passport Threats

3.1 Data leakage threats

Without protective measures, e-passports are vulnerable to "skimming," meaning surreptitious reading of their contents. Even a short read range is enough for some threats. For example, a 3-foot read range makes it possible to install RFID readers in doorways; tags can then be read from anyone passing through the doorway. Such readers could be set up as part of security checkpoints at airports, sporting events, or concerts. Alternatively, clandestine readers could be placed in shops or entrances to buildings. Such readers might look much like the anti-theft gates already used in thousands of retail stores. A network of such readers would enable fine-grained surveillance of e-passports.

Skimming is problematic because e-passports contain sensitive data. The ICAO standard for e-passports mandates that the RFID chip contain the passport holder's name, date of birth, passport number. Actual deployments will include further biometric information, including at a minimum a photograph. Optional data items include such data as nationality, profession, and place of birth. First generation Malaysian e-passports contain an image of the passport holder's thumbprint as the biometric instead of a photograph. Second generation ICAO e-passports may also store a thumbprint template, as well as a small amount of writable memory for storing recent travel locations.

The RFID protocols executed by an e-passport may also leak information. For example, consider the ISO 14443 collision avoidance protocol, used by ICAO and Malaysian second generation passports. This protocol uses a special UID value to avoid link-layer collisions. If the UID value is fixed and different for each e-passport, then it acts as a static identifier for tracking the movement of e-passports. A static identifier also enables *hotlisting*. In hotlisting, the adversary builds a database matching identifiers to persons of interest. Later, when the identifier is seen again, the adversary knows the person without needing to directly access the e-passport contents. For example, a video camera plus an RFID reader might allow an adversary to link a face with a UID. Then subsequent sightings of that UID can be linked with the face, even if no video camera is present.

Leakage of e-passport data thus presents two problems with consequences that extend beyond the e-passport system itself:

Identity Theft: A photograph, name, and birthday give a head start to a criminal seeking to commit identity theft. With the addition of a social security number, the criminal has most of the ingredients necessary to build a new identity or create a fake document.

Tracking and Hotlisting: Any static identifier allows for tracking the movements of an RFID device. By itself, the movements of an individual may not be that interesting. When combined with other information, however, it can yield insight into a particular person's movements. Further, this information only becomes more useful over time, as additional information is aggregated.

Hotlisting is potentially more dangerous than simple tracking, because it explicitly allows targeting specific individuals. One unpleasant prospect is an "RFID-enabled bomb," an explosive device that is keyed to explode at particular individual's RFID reading [14]. In the case of e-passports, this might be keyed on the collision avoidance UID. Of course, one can detonate bombs remotely without the help of RFID, but RFID paves the way for unattended triggering and more comprehensive targeting. For example, e-passports might enable the construction of "American-sniffing" bombs, since U.S. e-passports will not use encryption to protect confidentiality of data.

3.2 The biometric threat

Leakage of the biometric data on an e-passport poses its own special risks: compromise of security both for the e-passport deployment itself, and potentially for external biometric systems as well.

While designated as optional in this figure, biometric information will play a central role in e-passport systems. A facial image—a digitized headshot—is designated the "global interchange feature," meaning that it will serve as the international standard for biometric authentication. Indeed, ICAO guidelines describe it as the mandatory minimum for global interoperability [16]. Optional fields exist for iris and fingerprint data, which may be used at the issuing nation's discretion. We note that the US-VISIT program requires fingerprint biometrics from visitors; these fingerprints could be stored in the appropriate fields on an ICAO e-passport.

Advocates of biometric authentication systems sometimes suggest that secrecy is not important to the integrity of such systems. The fact that an image of John Doe's fingerprints is made public, for instance, does not preclude verification of Doe's identity: Comparison of the public image with the prints on her hands should still in principle establish her identity. This is all the more true when such comparison takes place in a secure environment like an airport, where physical spoofing might seem difficult to achieve.

At first glance, secrecy would seem particularly superfluous in the US-VISIT initiative and first deployments of ICAO passports. The globally interoperable biometric, as mentioned above, is face recognition. Thus the biometric image stored in passports will be headshots, which is in some sense public information to begin with.

Data secrecy in biometric systems, however, is a subtle issue. Two trends erode security in the face of public disclosure of biometric data:

1. *Automation:* Because biometric authentication is an automated process, it leads naturally to the relaxation of human oversight, and even to self-service application. This is already the case with e-passports. At Kuala Lumpur International Airport, Malaysian citizens present their e-passports to an "AutoGate" and authenticate themselves via a fingerprint scanner, without any direct human contact. If the fingerprint matches the e-passport data, the gate opens and the e-passport holder continues to his or her flight [20]. Australia plans to introduce similar "SmartGate" technology with face recognition in conjunction with its e-passport deployment. These deployments are instructive, because they tell us what airport procedures might look like in a world where e-passports are ubiquitous.

   The pressures of passenger convenience and airport staff costs are likely to reinforce this trend towads unattended use of biometrics. The result will be diminished human oversight of passenger authentication and greater opportunities for spoofing of biometric authentication systems.

2. *Spillover:* As biometrics serve to authenticate users in multiple contexts, compromise of data in one system will threaten the integrity of other, unrelated ones. For

example, biometric authentication is gaining in popularity as a tool for local authentication to computing devices and remote authentication to networks. For example, Microsoft is initiating support for optical fingerprint scanning devices in 2005 [24]. Even if the secrecy of John Doe's fingerprint image is relatively unimportant at a supervised immigration station in an airport, it may be of critical importance to the security of his home PC or corporate network if they also rely on biometrics for authentication, as an attacker able to simulate Doe's finger in these settings may do so in the absence of human oversight. (An unclassified State Department whitepaper recognizes the need to protect the privacy of iris and fingerprint data, but does not explain why [28].)

These risks apply even to passport photos. While John Doe's face is a feature of public record, his passport photo is not. Passport photos have two special properties:

1. *Image quality:* Doe's passport photo is likely to be of a higher quality than the image of Doe's face that an attacker can obtain in casual circumstances. Passport photos are taken under rigorously stipulated conditions. One example is particularly illuminating with respect to these conditions: To comply with the technical requirements of facial recognition, applicants for U.K. passports may not smile for their photos [8].

2. *Disclosure may enable forgery:* Passport photos are the target authenticator: they are the reference point for an attacker aiming to spoof a facial recognition system. Forgery of a face in a biometric authentication systems may seem implausible, but Adler shows that holding up a photo is sufficient to spoof some face-recognition systems [4].

Going further, iris scans and fingerprints are secondary biometrics specified in the ICAO document, and fingerprints are the primary biometric for Malaysian e-passports. In unattended settings, spoofing these biometrics is also possible given enough preparation time. For example, Matsumoto showed how several fingerprint recognition systems could be fooled when presented with gelatin "fingers" inscribed with ridges created from pictures of fingerprints [22].

4 Cryptography in E-passports

4.1 The ICAO specification

As we have explained, the ICAO guidelines specify a large range of mandatory and optional data elements. To ensure the authenticity and privacy of this data, the guidelines include an array of cryptographic measures, discussed next.

The ICAO standard specifies one *mandatory* cryptographic feature for e-passports [15, 16]:

Passive authentication: The data stored on a e-passport will be signed by the issuing nation [16]. Permitted signature algorithms include RSA, DSA and ECDSA. As noted in the ICAO guidelines, passive authentication demonstrates only that the data is authentic. It does *not* prove that the container for the data, namely the e-passport, is authentic.

The ICAO guidelines additionally specify two *optional* cryptographic features for improved security in e-passports:

Basic Access Control and Secure Messaging: To ensure that tag data can be read only by authorized RFID readers, Basic Access Control stores a pair of secret cryptographic keys $(K_{\text{ENC}}, K_{\text{MAC}})$ in the passport chip. When a reader attempts to scan the passport, it engages in a challenge-response protocol that proves knowledge of the pair of keys and derives a session key. If authentication is successful, the passport releases its data contents; otherwise, the reader is deemed unauthorized and the passport refuses read access. The keys K_{ENC} and K_{MAC} derive from optically scannable data printed on the passport, namely:

- The passport number, typically a nine-character value;
- The date of birth of the bearer;
- The date of expiration of the passport; and,
- Three check digits, one for each of the three preceding values.

E-passports use the ISO 11770-2 Key Establishment Mechanism 6:

Type	Feature Name	Purpose
Mandatory	Passive Authentication	Prevent data modification
	Biometric: Photo	Identify passport holder
Optional	Active Authentication	Anti-cloning
	Basic Access Control	Data confidentiality
	Biometric: Fingerprint	Identify passport holder

Figure 1. Summary of ICAO security features.

Reader $\qquad\qquad\qquad\qquad$ Tag

$$\xrightarrow{\text{Get challenge}}$$

$$r_T \in_R \{0,1\}^{64}$$

$$\xleftarrow{r_T}$$

$$r_R, k_R \in_R \{0,1\}^{64}$$

$$S_R := r_R || r_T || k_R$$

$$C_R := E_{K_{\text{ENC}}}(S_R)$$

$$M_R := M_{K_{\text{MAC}}}(E_R)$$

$$\xrightarrow{C_R || M_R}$$

$$k_T \in_R \{0,1\}^{64}$$

$$S_T := r_T || r_R || k_T$$

$$C_T := E_{K_{\text{ENC}}}(S_T)$$

$$M_T := \text{MAC}_{K_{\text{MAC}}}(E_T)$$

$$\xleftarrow{C_T || M_T}$$

Here E is two-key triple-DES in CBC mode with an all-0 IV, and M is the ANSI "retail MAC" [17]. In this protocol, the Tag first checks the MAC M_R and then decrypts the value C_R. The Tag then checks that the r_T in the decrypted value matches the r_T which it previously sent. If either check fails, the Tag aborts.

Similarly, when the Reader receives C_T and M_T, it first checks the MAC M_T and then decrypts C_T. The Reader then checks that the correct r_R appears in the decryption of C_T. If either check fails, the Reader aborts. Otherwise, the Reader and Tag proceed to derive a shared session key from the "key seed" $k_R \oplus k_T$, by using the key derivation mechanism in Section E.1 of the ICAO PKI report [16].

The intent of Basic Access Control is clearly spelled out in the ICAO report: the Basic Access Control keys, and hence the ability to read the passport contents, should be available *only* when a passport holder intends to show his or her passport. Unfortunately, the scheme falls short of this goal in two ways.

First, the entropy of the keys is too small. The ICAO PKI Technical Report warns that the entropy of the key is at most 56 bits. The ICAO report acknowledges that some of these bits may be guessable in some circumstances. We believe that the key length is in fact slightly shorter for a general population. We estimate that the birth date yields about 14 bits of entropy and the expiration date, which has a 10-year maximum period, yields roughly 11 bits of entropy. The remaining entropy depends on the passport number scheme of the issuing nation. For concreteness, we discuss the passport number scheme of the United States [5].

United States passports issued since 1981 have 9-digit passport numbers. The first two digits encode one of fifteen passport issuing offices, such as "10" for Boston or "03" for Los Angeles. The remaining seven digits are assigned arbitrarily. Probably some two-digit leading codes are more likely than others, as some offices presumably issue more passports than others, but we will conservatively ignore this effect. Given fifteen passport issuing agencies currently in the United States, U.S. passport numbers have at most $\lg(15 \times 10^7) \approx 27$ bits of entropy. This means Basic Access Control keys have a total of about 52 bits of entropy.

Furthermore, the passport number is not typically considered a secret. Entities such as cruise ships, travel agents, airlines, and many others will see the number and may include it on paper documents.

Second, a single fixed key is used for the lifetime of the e-passport. As a consequence, it is impossible to revoke a reader's access to the e-passport once it has been read. If a passport holder visits a foreign nation, he or she must give that nation's border control the key for Basic Access Control. Because the key never changes, this enables that nation to read the e-passport in perpetuity. This capability may be misused in the future, or databases of keys may be inadvertently compromised.

Despite its shortcomings, Basic Access Control is much better than no encryption at all. As we will see, however, the United States originally elected not to include Basic Access Control in its e-passport deployment. In contrast, the Netherlands and Germany both plan to include Basic Access Control in their ICAO passport deployments.

"Active Authentication": The ICAO spec urges use of

Country	RFID Type	Deployment	Security	Biometric
Malaysia Gen1	non-standard	1998	Passive Authentication + Unknown	Fingerprint
Malaysia Gen2	14443	2003	Passive Authentication + Unknown	Fingerprint
Belgium	14443	2004	Unknown	Photo
U.S.	14443	2005	Passive, Active Authentication	Photo
Australia	14443	2005	Unknown	Photo
Netherlands	14443	2005	Passsive, Active Authentication, BAC	Photo
Germany	14443	2005	Passsive, Active Authentication, BAC	Photo

Figure 2. Current and near-future e-passport deployments. The Belgium, U.S., Australia, and Netherlands deployments follow the ICAO standard, while Malaysia's deployment predates the standard. The chart shows the type of RFID technology, estimated time of first deployment, security features employed, and type of biometric used. Here "BAC" stands for Basic Access Control. "Unknown" indicates a lack of reliable public information.

another, optional security feature called "Active Authentication." While Basic Access Control is a confidentiality feature, Active Authentication is an anti-cloning feature. It does not prevent unauthorized parties from reading e-passport contents.

Active Authentication relies on public-key cryptography. It works by having the e-passport prove possession of a private key. The corresponding public key is stored as part of the signed data on the passport. The ICAO guidelines are somewhat ambiguous, but appear to specify an integer factorization based signature such as RSA or Rabin-Williams. To authenticate, the passport receives an 8-byte challenge from the reader. It digitally signs this value using its private key, and returns the result. The reader can verify the correctness of the response against the public key for the passport. The ICAO guidelines specify use of the ISO/IEC 7816 Internal Authenticate mechanism, with ISO 9796-2 Signature Scheme 1 padding for the underlying signature:

Reader   Tag

$$r_R \in_R \{0,1\}^{64}$$

$$\xrightarrow{r_R}$$

$$M_1 \in_R \{0,1\}^{64}$$

$$X := M_1 || r_R$$

$$\xleftarrow{\mathrm{Sig}_{SK}(X)}$$

Here $\mathrm{Sig}_{SK}(X)$ is an RSA or Rabin-Williams signature with 9796-2 padding signed with the secret key SK of the e-passport. Notice that X contains both a random nonce generated by the Tag and a challenge from the reader; we speculate that this may be intended to counteract padding attacks such as those of Coron, Naccache, and Stern [10]. The 9796-2 padding itself makes use of a hash function, which may be SHA-1 or another hash function; the ICAO standard does not restrict the choice of hash. The signature can then be verified with the public key supposedly associated with the passport. If the signature verifies, the Reader gains some confidence that the passport presented is the contained which is supposed to hold the presented biometric data. The U.S. RFP for e-passports further specifies in Section C.2.7.2.2 a security policy that e-passport chips must support, namely that data cannot be overwritten on the chip after personalization [11]. Signing the chip's public key is a statement that the chip with the corresponding secret key is trusted to implement the security policy.

The public key used for Active Authentication must be tied to the specific e-passport and biometric data presented. Otherwise a man-in-the-middle attack is possible in which one passport is presented, but a different passport is used as an oracle to answer Active Authentication queries. The ICAO specification recognizes this threat, and as a result mandates that Active Authentication occur in conjunction with an optical scan by the reader of the machine-readable zone of the e-passport. As a result, every reader capable of Active Authentication and compliant with the ICAO specification also has the hardware capability necessary for Basic Access Control. Deployments which neglect this part of the specification open themselves to a risk of cloned e-passports.

Furthermore, to be effective, the private key used in Active Authentication must never leave a particular e-passport. Here the guidelines in the ICAO PKI report are vague, simply saying that the keys shall be generated "in a secure way" and then stating that "no Key Management is applicable for these keys." In particular, the report does not forbid these keys from being read by a remote reader; while allowing such reading is almost surely not the intention of the standard, the exact requirements are not clear. The U.S. Concept of Operations document is also vague. While it specifies requirements on what data cannot be overwritten after passport personalization, it does not appear to specify that Active Authentication keys cannot be read after personalization. The chips used in e-passports must also resist the same range of side channel and fault injection attacks traditionally applied to smart cards.

Active Authentication also raises subtle issues concerning its interaction with Basic Access Control and privacy. The certificate required for verifying Active Authentication also contains enough information to derive a key for Basic Access Control; as a result the certificate must be kept secret. In addition, when Active Authentication is used with RSA or Rabin-Williams signatures, responses with different moduli, and hence from different e-passports, can be distinguished. As a result, Active Authentication enables tracking and hotlisting attacks even if Basic Access Control is in use. We recommend that Active Authentication be carried out only over a secure session after Basic Access Control has been employed and session keys derived. Because Active Authentication requires an optical scan of the e-passport, just as Basic Access Control does, we do not believe this presents more of a burden than the existing specification.

4.2 Cryptographic measures in planned deployments

At this point, more information is publicly available for the United States deployment of ICAO e-passports than any other of which we are aware. An unclassified State Department memo obtained by the ACLU describes elements of the U.S. PKI architecture as envisioned in 2003 [28]. A Federal Register notice dated 18 February 2005 provides a number of details on U.S. e-passport plans [2]. Appendix D of the State Department Concept of Operations document specifies that readers should support Active Authentication, leaving open the possibility of its future deployment in U.S. and foreign e-passports [11]. The Federal Register notice, however, confirms that U.S. passports will not implement Basic Access Control. The Federal notice offers three reasons for the decision not to implement Basic Access Control: (1) The data stored in the chip are identical to those printed in the passport; (2) Encrypted data would slow entry processing time[4]; and (3) Encryption would impose more difficult technical coordination requirements among nations implementing the e-passport system. Further, this notice intimates that e-passports will carry Faraday cages and that e-passport readers will be shielded to prevent eavesdropping.

Our analysis suggests this reasoning is flawed. Active Authentication requires an optical scan of a passport to provide the claimed anti-cloning benefit. This is why the ICAO spec mandates readers supporting Active Authentication be able to optically scan e-passports; this optical scan capability is also sufficient for Basic Access Control. Reason (3) is also flawed: because all the data required to derive keys for Basic Access Control is present on the data page of the e-passport, no coordination among nations is required. Coordination among vendors is required for interoperability of e-passports and readers, but such coordination is already required for e-passports without Basic Access Control. Finally, as we have argued, Faraday cages are not sufficient to protect against unauthorized eavesdropping, and so they do not rule out the attacks on security and privacy we have outlined.

In fact, our analysis shows that the original deployment choices of the United States put e-passport holders at risk for tracking, hotlisting, and biometric leakage. The lack of Basic Access Control means that any ISO 14443 compliant reader can easily read data from an e-passport, leading directly to these attacks. We are also concerned that a push towards automatic remote reading of e-passports may lead the U.S. to neglect optical scanning of e-passports, thereby weakening the anti-cloning protections of Active Authentication. Following the original publication of this paper and the receipt of over 2400 public comments responding to e-passport policy, the U.S. State Department indicated that it would reconsider Basic Access Control, but at this writing no final decision has been announced.

As it pre-dates the ICAO standard, the Malaysian identity card/passport is not compliant with that standard. Published information suggests that it employs digital signatures ("passive authentication") [3]. There appears to be no reliable public information on other security mechanisms, although the US patent filed on the technology suggests a "proprietary and secret" encryption algorithm is used for mutual authentication between e-passport and reader [30]. Belgium began issuing e-passports to citizens in November 2004, while the United States, Australia, and the Netherlands expect large-scale issuing by the end of 2005. For the ICAO e-passport deployments, the specific choices of each country as to which security features to include or not include makes a major difference in the level of security and privacy protections available. We summarize the known deployments, both current and impending shortly, in Figure 2.

Other nations may or may not meet the United States mandate for deployment in 2005. Indeed, the reason that the United States has favored a minimal set of security features appears to stem from problems with basic operation and compatibility in the emerging international infrastructure [1]. Following complaints by several contries, in June 2005 the United States extended its original October 2005 deadline for electronic passports to October 2006, but retained a requirement for digital photographs associated with passports.

[4]Presumably this refers to the requirement for optical scanning in association with Basic Access Control.

5 Strengthening Today's E-passports

5.1 Faraday cages

One of the simplest measures for preventing unauthorized reading of e-passports is to add RF blocking material to the cover of an e-passport. Materials such as aluminum fiber are opaque to RF signals and could be used to create a Faraday cage, which prevents reading the RFID device inside the e-passport. Before such a passport could be read, therefore, it would have to be physically opened.

The ICAO considered Faraday cages for e-passports, as shown in a discussion of "physical measures" in Section 2.4 of [16]. Because Faraday cages do not prevent eavesdropping on legitimate conversations between readers and tags, however, Faraday cages were deprecated in favor of Basic Access Control.

While a Faraday cage does not prevent an eavesdropper from snooping on a legitimate reading, it is a simple and effective method for reducing the opportunity for unauthorized reading of the passport at times when the holder does not expect it. Recently, the U.S. State Department indicated that U.S. e-passports may include metallized covers, following discussion of privacy risks by the ACLU and other groups.

The research community has proposed a number of tools for protecting RFID privacy, including "Blocker Tags" [19] and "Antenna Energy Analysis" [12]. While either of these mechanisms would be helpful, in the special context of e-passports they would be no more practical or protective than a Faraday cage, given that passive eavesdropping during legitimate read sessions is likely to constitute perhaps the major vulnerability to data leakage.

5.2 Larger secrets for basic access control

As we have discussed, the long-term keys for Basic Access Control have roughly 52 bits of entropy, which is too low to resist a brute-force attack. A simple countermeasure here would be to add a 128-bit secret, unique to each passport, to the key derivation algorithm. The secret would be printed, together with other passport information, on the passport. Such a secret could take the form of a larger passport ID number or a separate field on an e-passport. To aid mechanical reading, the secret might be represented as a two-dimensional bar code or written in an OCR font to the Machine Readable Zone (MRZ) of each passport.

5.3 Private collision avoidance

Even if a larger passport secret is used as part of key derivation, the collision avoidance protocol in ISO 14443 uses a UID as part of its collision avoidance protocol. Care must be taken that the UID is different on each reading and that UIDs are unlinkable across sessions. One simple countermeasure is to pick a new random identifier on every tag read. In general, e-passports and other IDs should use *private collision avoidance* protocols. Avoine analyzes several existing protocols and proposes methods for converting them into private protocols [7].

5.4 Beyond optically readable keys

The ICAO Basic Access Control mechanism takes advantage of the fact that passports carry optically readable information as well as biometric data. In the passport context, the ICAO approach neatly ties together physical presence and the ability to read biometric data. In general, however, we cannot count on this kind of tight coupling for next-generation ID cards. Furthermore, the use of a static, optically readable key leads to readers that must be trusted in perpetuity when all that is desired is to allow a single passport read. Therefore an important problem is to create a keying mechanism that limits a reader's power to reuse secret keys and a matching authorization infrastructure for e-passport readers.

Before we can move beyond optically readable keys, a key management problem reveals itself. Which key should an authorized party use to authenticate with a e-passport? The e-passport dare not reveal its identity to an untrusted reader, but at the same time the reader does not know which key to use.

An earlier version of our protocol suggested using the JFKr authenticated Diffie-Hellman key agreement protocol of Aiello et al. for this problem [6]. We also highlighted reader revocation as an open issue in e-passports. We have since learned that the German government has proposed a Diffie-Hellman based protocol for "Extended Access Control" in the ICAO specification [9].

Reader revocation in the German proposal is accomplished by time-expiring certificates issued to readers combined with a time-stamping service run by each nation. On each interaction with a legitimate reader, the reader provides the passport with the most recent known timestamp from that passport's nation. While this raises a denial-of-service risk if a nation ever signs a timestamp far in the future, it fits with the constraints imposed by a mostly-offline reader architecture. In particular, border control readers in southeastern Europe may be offline for weeks or months at a time [29].

6 Future Issues in E-passports

6.1 Visas and writeable e-passports

Once basic e-passports become accepted, there will be a push for e-passports that support visas and other endorsements. (We note that the presently proposed approach to changes in basic passport data is issuance of a new passport [2]; this may eventually become unworkable.) Because different RFID tags on the same passport can interfere with each other, it may not be feasible to include a new RFID tag with each visa stamp. Instead, we would like to keep the visa information on the same chip as the standard passport data. These features require writing new data to an e-passport after issuance.

A simple first attempt at visas for e-passports might specify an area of append-only memory that is reserved for visas. Each visa would name an e-passport explicitly, then be signed by an issuing government authority just as e-passport credentials are signed. An e-passport might even implement "sanity checks" to ensure that a visa is properly signed and names the correct e-passport before committing it to the visa memory area.

In some cases, however, a passport holder may not want border control to know that she has traveled to a particular location. For example, most Arab countries will refuse entry to holders of passports which bear Israeli visas. As another example, someone entering the United States via Canada may wish to conceal a recent visit to a nation believed to be harboring terrorists. The first example is widely considered a legitimate reason to suppress visas on a passport; in fact, visitors to Israel request special removable visa passport pages for exactly this reason. The second motivation may be considered less legitimate, and preventing it may become a goal of future visa-enabled e-passports.

6.2 Function creep

The proliferation of identification standards and devices is certain to engender unforeseen and unintended applications that will affect the value and integrity of the authentication process. For example, passports might come to serve as authenticators for consumer payments or as mass transit passes. Indeed, the ICAO standard briefly discusses the idea that e-passports might one day support digital commerce.

Function creep has the potential to undermine data protection features, as it will spread bearer data more widely across divergent systems. Moreover, function creep may lead to consumer demands for greater convenience, leading to the erosion of protective measures like optical-scanning-based access control and Faraday-cage use. Passport holders may wish to pass through turnstiles, for instance, without having to pause to have their documents optically scanned. Unless some new privacy-enhancing features are added, it is conceivable that e-passports will reveal an aggregate record of private information whenever the passport is used, for instance to prove the bearer's age when entering a bar. The leaked information could include the bearer's birthdate, passport number, place of birth, and possibly elements of her travel history, as well as optional information like her profession and emergency contact information. While some of this information is already present in printed form on driver's licenses, its availability in electronic form will make it much easier to aggregate and share.

Web cookies are an instructive example of function creep. Originally introduced to overcome the stateless nature of the HTTP protocol, it was quickly discovered that they could be used to track a user's browsing habits. Today, web sites such as doubleclick.com use cookies extensively to gather information about customers.

7 Conclusion

We have identified principles for secure biometric identity cards and analyzed these principles in the context of the ICAO e-passport standard, current ICAO deployments, and Malaysian e-passports. We can draw several conclusions:

- The secrecy requirements for biometric data imply that unauthorized reading of e-passport data is a security risk as well as a privacy risk. The risk will only grow with the push towards unsupervised use of biometric authentication.
- At a minimum, a Faraday Cage and Basic Access Control should be used in ICAO deployments to prevent unauthorized remote reading of e-passports. In particular, the United States deployment of ICAO e-passports does not provide sufficient protection for its biometric data.
- Because the United States deployment uses Active Authentication, readers supplied to the United States are required by the ICAO spec to include the capability to optically scan e-passports. This capability is sufficient for Basic Access Control. No change to the readers or coordination with other nations is required to implement Basic Access Control in the U.S. deployment of ICAO e-passports. Therefore, the reasons cited for foregoing Basic Access Control in the US deployment are not convincing.

Today's e-passport deployments are just the first wave of next-generation identification devices. E-passports may provide valuable experience in how to build more secure and more private identification platforms in the years to come.

8 Acknowledgements

We thank Neville Pattinson for helpful discussions and for giving us access to his white paper. We thank Seth Schoen and Lee Tien for helpful discussions on e-passports and Lea Kissner for her comments. We also thank Bart Jacobs, Tamas Visegrady, and researchers at IBM Zurich for discussions regarding European electronic passports. This research was supported by NSF grants CCR-0093337 and CCR-0325311 and by a generous donation from British Telecom.

References

[1] New-look passports. *Economist*, 17 February 2005. http://economist.com/science/displayStory.cfm?story_id=3666171.

[2] Department of State, 22 CFR Part 51, Public Notice 4993, RIN 1400-AB93, Electronic Passport. *Federal Register*, 70(33), 18 February 2005. Action: Proposed Rule. Available at http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.htm.

[3] Digicert PKI toolkit — dcTools specification sheet, 2005. http://www.digicert.com.my/toolkits.htm.

[4] A. Adler. Sample images can be independently restored from face recognition templates, June 2003. http://www.site.uottawa.ca/~adler/publications/2003/adler-2003-fr-templates.pdf.

[5] U. S. S. Administration. Passports as evidence, 2005. http://policy.ssa.gov/poms.nsf/lnx/0302640050?OpenDocument&Click=.

[6] W. Aiello, S. M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. D. Keromytis, and O. Reingold. Just fast keying: Key agreement in a hostile internet. *ACM Trans. Inf. Syst. Secur.*, 7(2):242–273, 2004.

[7] G. Avoine. RFID privacy: A multilayer problem. In *Financial Cryptography*, 2005.

[8] BBC. Grins banned from passport pics, 2004. http://news.bbc.co.uk/2/hi/uk_news/politics/3541444.stm.

[9] G. BSI. Alternative extended authentication, 2005.

[10] J. Coron, D. Naccache, and J. Stern. On the security of RSA padding. In *CRYPTO 99*, 1999.

[11] U. S. Department. Abstract of the concept of operations for integration of contactless chip in the US passport, 2004. http://www.statewatch.org/news/2004/jul/us-biometric-passport-original.pdf.

[12] K. Fishkin and S. Roy. Enhancing RFID privacy through antenna energy analysis. In *MIT RFID Privacy Workshop*, 2003. http://www.rfidprivacy.org/papers/fishkin.pdf.

[13] I. Z. S. C. Group. Personal demonstration, 2005.

[14] T. Halfhill. Is RFID paranoia rational?, 2005. http://www.maximumpc.com/reprints/reprint_2005-01-14a.html.

[15] ICAO. Document 9303, machine readable travel documents, October 2004.

[16] ICAO. PKI for machine readable travel documents offering ICC read-only access, version 1.1, October 2004.

[17] ISO. ISO/IEC 9797-1 algorithm 3, 1999.

[18] B. Jacobs. Biometry in passports, 2005. http://www.sos.cs.ru.nl/research/society/passport/index.html.

[19] A. Juels, R. L. Rivest, and M. Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *Proceedings of the 10th ACM conference on Computer and communication security*, pages 103–111. ACM Press, 2003.

[20] D. M. J. Kamdi. The Malaysian electronic passport, 2004. Presentation to ICAO, http://www.icao.int/icao/en/atb/fal/fal12/Presentations/Malaysia.ppt.

[21] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. Cryptology ePrint Archive, Report 2005/052, 2005.

[22] T. Matsumoto. Gummy and conductive silicone rubber fingers. In *ASIACRYPT 2002*, 2002.

[23] D. McCullugh. House backs major shift to electronic IDs. *CNET News*, 10 February 2005. http://news.zdnet.com/2100-9595_22-5571898.html.

[24] W. Ness. Microsoft optical desktop comes with fingerprint reader, January 2005.

[25] N. Pattinson. Securing and enhancing the privacy of the e-passport with contactless electronic chips, 2004. Contact: pattinson@axalto.com.

[26] Reuters. US pushes back europe's e-passport deadline, 2005. http://ecoustics-cnet.com.com/U.S.+pushes+back+Europes+e-passport+deadline/2100-7348_3-5748629.html.

[27] R. Singel. No encryption for e-passports. *Wired News*, 24 February 2005. http://www.wired.com/news/privacy/0,1848,66686,00.html?tw=wn_tophead_1.

[28] A. Team". IC embedded passport PKI requirements, 20 October 2003. http://www.aclu.org/passports/PKIRequirements.pdf.

[29] T. Visegrady. Personal communication, 2005. tvi@zurich.ibm.com.

[30] C. H. E. Yap and F. M. Chua. U.S. patent 6,111,506 method of making an improved security identification document including contactless communication insert unit, 2000. http://tinyurl.com/7ymch.

[31] J. Yoshida. Tests reveal e-passport security flaw, August 2004. *EE Times*.