April 4, 2005

Chief, Legal Division
Office of Passport Policy, Planning and Advisory Services
2100 Pennsylvania Ave., NW.
Washington, DC 20037

Re: RIN 1400-AB93
Electronic Passport

The Electronic Frontier Foundation, Electronic Privacy Information Center, PrivacyActivism, Privacy Rights Clearinghouse, the World Privacy Forum, and privacy activist Bill Scannell appreciate the opportunity to comment on the Department of State's request for comments on the Department's proposal to issue enhanced passports that use radio-frequency identification (RFID) technology to American citizens. 70 Fed.Reg. 8305 (Feb. 18, 2005). We urge the Department to abandon this misguided proposal.

According to its notice of proposed rule-making (NPRM), the Department's proposed rule would amend current passport regulations to reflect changes required for the intended implementation of the RFID passport. The rule would: define "electronic passport," include a damaged electronic chip as an additional basis for possible invalidation of a passport, abolish the U.S. passport amendment process except for the convenience of the U.S. government, and enlarge the reasons for issuing a replacement passport at no fee. The rule would also add unpaid fees as a ground for invalidating a passport.

We believe that the proposed RFID passport unjustifiably endangers passport holders' privacy and creates substantial security and other problems. Our comments will specifically address:

- The State Department's lack of authority to issue RFID passports;
- Lack of evidence presented to support the necessity or purported security benefits of RFID passports;
- Substantial lack of analysis of costs and benefits of the RFID passport, including lack of a technology assessment of RFID;
- Lack of a privacy impact assessment (PIA) as mandated by the eGovernment Act of 2002;
- Lack of evidence justifying the use of RFID technology, particularly in contactless and unencrypted format;
- Inherent threats to privacy and security in RFID technology.

We cannot emphasize enough that the creation of an RFID passport is not a merely internal, administrative matter. "[T]he passport's electronic chip would duplicate the data that appears on the visible data page of the passport: the bearer's name, date of birth and place of birth, the passport number, the dates of issuance and expiration, the issuing authority, the document type, the passport application reference number, and the photo in digitized format. It would also contain a unique chip identification number." 70 Fed.Reg. at 8306. Because the State Department has (for now) decided to use RFID technology without confidentiality protection for passport data, the proposed RFID passport will indiscriminately expose Americans' personal

information to others. Under informational privacy cases like *Whalen v. Roe*, 429 U.S. 589, 605 (1977), the government arguably has a constitutional duty "to avoid unwarranted disclosures" of personal information collected and used for public purposes.

Furthermore, because this exposure can occur whenever and wherever a person carries the RFID passport, unauthorized persons – from government or the private sector – could link passport holders to their activities in particular places. If government officials equipped with RFID readers scanned all persons entering abortion clinics, a woman who carried her RFID passport could be identified against her will. Cf. *Aid for Women v. Foulston*, 327 F.Supp.2d 1273, 1285 (D. Kan. 2004) (finding that minors have right to informational privacy concerning personal sexual matters that might be revealed through mandatory reporting).

Finally, beyond the questions and issues created by the use of RFID in passports, the proposed rules raise other issues of fairness, privacy, and security. For example, the new grounds for invalidating a passport based on chip-tampering or non-payment are problematic in multiple respects. Handling of source documentation for the passports was poorly defined in the NPRM; handling source documents such as original birth records is an area that is already recognized as highly sensitive by the U.S. government and was recently addressed by the guidance for implementation of HSPD-12 in relation to the Federal ID "smart cards." Additionally, we believe the government's analysis of the cost burden of the proposed RFID passport is significantly understated, which further threatens successful implementation.

I. The RFID passport is ultra vires

There is no statutory authority for the RFID passport. Under § 303 of the Enhanced Border Security and Visa Entry Reform Act of 2002, nations whose citizens are allowed to enter the United States under the provisions of the Visa Waiver Program must by October 26, 2004 have a program in place to "incorporate biometric and document authentication identifiers that comply with applicable biometric and document identification standards established by the International Civil Aviation Organization."

This statute neither requires nor authorizes the U.S. government to comply with International Civil Aviation Organization (ICAO) standards; as the State Department itself has admitted, "the United States is not mandated to comply with the requirements of section 303." U.S. Department of State, *Abstract of Concept of Operations for the Integration of Contactless Chip in the U.S. Passport*, Abstract of Document Version 2.0, April 26, 2004, at 1 <http://www.statewatch.org/news/2004/jul/us-biometric-passport-original.pdf> ("Abstract"). In short, had Congress intended to authorize the State Department to issue passports that comply with § 303, "it knew how to do so." *Custis v. United States*, 511 U.S. 485, 492 (1994). Congress did not.

Nor do any other statutes cited by the State Department delegate authority to issue RFID passports. 22 U.S.C. § 211a generally authorizes the Secretary of State to grant, issue, and verify passports. One would have to interpret this statute extremely broadly to conclude that it authorizes the Department to issue these radically altered passports without further specific legislative authority. The same is true for 22 U.S.C § 2651a, which sets forth the broad

administrative authority of the Secretary of State, along with some exceptions. 22 U.S.C. § 2651a(B)(4) (authorizing Secretary "to promulgate such rules and regulations as may be necessary to carry out the functions of the Secretary of State and the Department of State."). In promulgating such rules, however, it is implicit that the Secretary must adequately justify the necessity and benefit of those rules with supporting evidence. The Secretary has not done so here.

Administrative agencies may only exercise powers delegated to them by Congress. Until Congress delegates authority to the State Department to issue RFID passports, the State Department may not do so.

II. The proposal for an RFID passport is not adequately supported by substantial evidence or reasoned articulation.

Under the Administrative Procedure Act (APA), a court must "hold unlawful or set aside agency action, findings, and conclusions" that are found to be "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with the law ... [or] unsupported by substantial evidence." 5 U.S.C. § 706(2)(a), (e).

In reviewing agency action under the "arbitrary and capricious" standard, a court must ensure that the agency examined the relevant data and articulated a "rational connection between the facts found and the choice made." *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (internal quotation marks and citation omitted). In general, a court may find an agency rule is arbitrary and capricious where "the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise." Ibid. (citation omitted).

Moreover, an agency that departs from its "former views" is "obligated to supply a reasoned analysis for the change beyond that which may be required when an agency does not act in the first instance" in order to survive APA scrutiny. Id. at 41-42 (noting presumption "*against* changes in current policy that are not justified by the rulemaking record") (emphasis in original). Because the proposed RFID passport is clearly a departure from the current U.S. passport, the State Department must, in order to survive APA scrutiny, "supply a reasoned analysis." The State Department has not done so, and the NPRM is accordingly deficient in several crucial respects.

We will briefly outline these deficiencies here, and discuss them in more detail in our technical comments below.

A. The NPRM presents no facts to support the assertion that there is a need to enhance the U.S. passport.

First, the NPRM provides no factual basis for its assertion that security needs require incorporating RFID technology into U.S. passports. As discussed in more detail below, there are

significant privacy and security issues associated with the use of RFID technology. The NPRM mentions these issues, but contains no actual information – or even references to such information – that would support a finding that RFID passports would actually be, on balance, beneficial.

More important, the NPRM contains no discussion whatsoever of the alleged problem to be solved by the use of RFID technology in the U.S. passport. Instead, it assumes the existence of problems such as lack of security, without ever demonstrating that these problems actually exist. If there is any factual record evidence that current U.S. passports are insecure, it is neither presented nor cited here. It must be remembered that identity verification – knowing who someone is – does not by itself provide security. Many of the 9/11 hijackers used their true names and presented authentic identification credentials. The fundamental problem is that the system had no reason to treat, for example, Mohammed Atta differently from anyone else.

For instance, the NPRM states that:

"Using an embedded electronic chip in the passport to store the information from the passport data page will enhance the security of the document and is expected to benefit travelers by improving the ability of border officials to verify personal identities. The Department plans to use this format because of the enhanced security features and improved port of entry performance provided by the electronic chip technology."

But the NPRM does not back up any of these assertions. There are no factual findings or "reasoned analysis" offered to support the fundamental premises that security needs to be enhanced, or that border officials today cannot adequately verify personal identities.

Nor is there is any evidence that the proposed RFID passport will in fact improve document security, better enable border officials to verify personal identities, benefit travelers, or improve port of entry performance. Indeed, the NPRM strongly suggests that these supposed benefits are speculative. 70 Fed.Reg. at 8306 (referring to "pilot programs" for "reader technology" to be implemented by the Department of Homeland Security "by the end of the year.").

Nowhere does the State Department state for the public record that it has researched the costs and benefits of the RFID passport. The main body of the NPRM says nothing about the costs of the proposed RFID passport. Only in its discussion of "Regulatory Findings" does the Department state that "[t]his rule would not result in an annual effect on the economy of $100 million or more." 70 Fed.Reg. at 8307. But there is no explanation of how the Department arrived at this number; we therefore do not know whether the Department considered the costs of privacy invasion or identity theft likely to be associated with the proposed RFID passport, much less whether the system will even work. Recent media reports suggest that the system has failed tests so far. See *Vendors taken to task over e-passport flaws* (Feb. 3, 2005) <http://www.securityinfowatch.com/article/article.jsp?id=2941&siteSection=304> ("Three of the readers tested could successfully read the chips only 58%, 43% and 31% of the time, respectively, according to a U.S. government report.").

It therefore appears that the State Department wishes to implement RFID passports before their efficacy has even been established. (We are aware that various bodies, ranging from the congressional joint inquiry into 9/11 to the 9/11 Commission have made findings and expressed opinions about the need to improve travel document security. But the State Department has not relied on any of these materials in the NPRM, even assuming for the purpose of argument that such materials could be part of the agency record here.)

The importance of analyzing these purported benefits cannot be emphasized enough. Recent headlines about the FBI's information technology (IT) procurement problems with respect to its Trilogy program and Virtual Case File management system prove beyond a doubt that it is easy for agencies to waste enormous sums of taxpayer money on IT systems that do not work. See *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project* at 78, U.S. Department of Justice, Office of Inspector General, Audit Division, Report No. 05-07 (February 2005) ("the FBI has not succeeded in its goal to replace the antiquated ACS [Automated Case Support] system with a fully functional and effective case management system, despite more than 3 years in development and $170 million.") <http://www.usdoj.gov/oig/audit/FBI/0507/final.pdf>.

Sadly, procurement problems and inadequate cost-benefit analysis appear especially common when agencies claim benefits relating to homeland security, fighting terrorism, or intelligence and law enforcement needs, because most people accept that these goals are important and do not ask hard questions about the agency's plans to achieve those goals.

For example, the NPRM states that "[t]he technology selected for the electronic passport . . . . is compatible with standards and recommendations of ICAO." 70 Fed.Reg. at 8305. But there is no reasoned analysis or information about why the ICAO's standards and recommendations are themselves reasonable, or why following the ICAO's standards and recommendations is in the public interest. Are we to assume without explanation that ICAO decisions set U.S. policy?

Furthermore, as we discuss below, the ICAO guidelines provide numerous options about how to implement privacy and security in machine-readable travel documents – and implementing more sophisticated privacy and security features will still be compatible with ICAO standards and recommendations. See ICAO, PKI Task Force, *PKI for Machine Readable Travel Documents offering ICC Read-Only Access* at 18, Version 1.1 (Oct. 2004) ("MRTDs issued by States choosing to use advanced security methods will be fully ICAO compliant and deem [sic] to meet global interoperability standards.") (hereinafter "ICAO PKI MRTD Report"). But the State Department has failed to explain its choices among the various options, in particular the choice to use the weakest possible security under the ICAO guidelines.

The NPRM also states that "[a]s biometric technology is rapidly advancing, the inclusion of facial image data in U.S. passports is considered a first step in ensuring that an effective biometric system is incorporated into the U.S. passport system." 70 Fed.Reg. at 8305. But the NPRM does not offer any explanation for why an effective biometric system should be used in the U.S. passport system in the first place, or even what the State Department means by "an effective biometric system."

Note also that the proffered assertions about the "need" for security are entirely neutral as to the issue of using RFID technology. The decision to use RFID only relates to how passport data is communicated. Thus, even assuming that electronic storage, biometrics, and machine-readability produce benefits, these assumptions do not themselves justify the use of RFID.

B. The NPRM fails to provide reasoned analysis or substantial evidence justifying the State Department's proposal to use a contactless technology in the new passports.

Perhaps the most important choice being made by the State Department in this proposal is the choice of a contactless rather than a contact technology under which the passport can be read through the air rather than being "swiped" through physical contact with a reader. As discussed below, contactless technology creates numerous risks because it exposes passport information, which is sensitive personal information, to clandestine access. We are not aware of any mechanism in the proposed passport that would alert the passport holder to data access events.

U.S. passports could be machine-readable via a contact technology such as the familiar magnetic stripe used by many states for their driver's licenses and by credit card companies for credit cards, debit cards, and ATM cards, or more sophisticated contact smart cards that can store more data than current magnetic stripes. Contact technologies eliminate the risk of clandestine data access associated with wireless data transfer mechanisms. Moreover, given the widespread use of contact technologies, people generally understand how to protect themselves against their privacy and security risks. We note that the ICAO has moved to standardize the use of contact smartcards in MROTDs (machine-readable official travel documents) (TD-1 size). See Annex I, *Use of Contactless Integrated Circuits in Machine Readable Travel Documents* at 9 (version 4.0) (May 5, 2004).

Yet the State Department never discusses the possibility of contact technology for electronic passports. Instead, it assumes without analysis or evidence that the passports must use contactless rather than contact technology.

C. The NPRM fails to provide reasoned analysis or substantial evidence justifying the State Department's proposal to use RFID technology in the new passports

The State Department's second crucial choice is to use RFID technology (ISO 14443) as the contactless technology in the proposed passports. Here again, there are other options with less risk to privacy and security. So-called "2D barcodes" can be read at a distance and are used in driver's licenses in 39 states. Datastrip, a UK and US company, produces a compact 2D barcode that can store photographs, text, and biometrics in an area the size of a conventional magnetic strip. Airport Aviation Services (Sri Lanka) Ltd. has implemented a digitized photo ID system using Datastrip ID card technology. Indeed, the State Department itself uses 2D barcodes in its visa application process. See *New Online Visa Application Form*, at <https://www.usembassy-china.org.cn/shanghai/visa/#6>.

Similarly, optical memory stripe cards do not require direct physical contact with a reader; they can be read by presenting the card to a reader at a fixed distance and orientation. In 1998, the U.S. government assessed available technologies for a Personal Information Carrier (PIC) that

would store one person's medical records. The key criteria were reliability under repeated use and extreme conditions (waterproof, dust-proof, shockproof). The LaserCard optical memory card was tested along with five other data carriers, and was the only one to pass successfully.

In fact, the State Department currently uses the LaserCard optical memory card for its Border Crossing Card. Used as a multiple-entry visa, the "Laser Visa" allows border officials to verify the holder's identity biometrically (fingerprint) in less than five seconds and simultaneously reads from the card and displays a color photograph of the holder. The same technology is used in U.S. and Canadian permanent resident cards. It would seem clear that this technology is acceptable to the State Department for identification and security purposes.

By contrast, the durability of the RFID passport is an open question. See *Vendors taken to task over e-passport flaws* (Feb. 3, 2005) <http://www.securityinfowatch.com/article/article.jsp?id=2941&siteSection=304> (quoting ICAO official as saying "Durability is probably the single most critical unknown. The vendors do not know how long a contactless chip will last.").

Yet the State Department neither discusses the possibility of 2D barcode or optical memory stripe technology for electronic passports, nor justifies the use of RFID technology rather than these optical technologies. This lack of reasoned analysis is especially surprising given that the U.S. government has actually tested and currently uses optical memory cards in several applications. Reasons may exist for not using optical memory cards for the new passport, but they have not been made public; one would not even know from reading the NPRM that these options exist.

D. The NPRM fails to provide reasoned analysis or substantial evidence justifying the State Department's decision not to encrypt or otherwise safeguard the sensitive personal information exposed to the public by the RFID device.

The State Department's third crucial choice is to not encrypt or otherwise safeguard the sensitive personal information exposed to the public by the RFID passport. The NPRM recognizes that there has been public concern about the lack of encryption. 70 Fed.Reg. at 8306 ("Recent press stories about the use of this technology have noted that the information will not be 'encrypted' and mention the concern about identity theft by unauthorized persons through either skimming (the surreptitious reading of the electronic information without the holder's knowledge) or eavesdropping (intercepting information from the electronic chip while it is being read at an official port of entry station).").

Here, the State Department at least offers some reasons for its decision: "The United States does not intend to encrypt the data for the following reasons: the personal data stored on the passport's electronic chip consists simply of the information traditionally and visibly displayed on the passport data page; encrypted data takes longer to read, increasing port of entry processing time; and in order to be globally interoperable, encryption would require a higher level of technology and more complicated technical coordination with other nations." 70 Fed.Reg. at 8306. (The NPRM also asserts that skimming and eavesdropping are technically difficult. Ibid. We discuss this claim in the next section.)

Unfortunately, these reasons are either specious or without factual support. The first "reason" – that the personal data is the same as the information "traditionally and visibly displayed on the passport data page" – is a fact, not a reason. And in asserting this fact as a reason not to secure this information, the State Department fails to grasp a basic point of privacy: control over who can access personal information. No one can gather information from the paper passport data page without physically obtaining the passport. But once that data is available via RF technology, which can extract data through a person's wallet or clothing, the contingencies of information control are entirely different.

Moreover, the State Department entirely ignores the fact that this data can be accessed any time and anywhere that a person carries the RFID passport. One's name may be public; one's face may be public; but it is an entirely different matter from a privacy perspective if a passport holder's identity can be ascertained by anyone with the right equipment when he or she is at a doctor's office, place of worship, or anti-war demonstration.

The second reason, that encrypted data takes longer to read, also is not supported by any factual evidence or reasoned analysis. The NPRM merely asserts without any evidence that encrypted data takes longer to read. There is good reason to believe that this is not true: under the scheme of the NPRM, the readers must already verify a digital signature, and verifying a digital signature is at least as computationally intensive as decrypting with a key. Indeed, Juels, Molnar and Wagner suggest that the only reason for increased processing time is due to the optical scanning requirement under the ICAO's Basic Access Control (BAC) confidentiality option. See Ari Juels, David Molnar, and David Wagner, *Security and Privacy Issues in E-passports*, at 8 n. 3 (2005) (prepublication draft available at < http://eprint.iacr.org/2005/095>) (attached as appendix) (hereinafter "JMW").

Nor has the State Department explained how much any supposed increase in reading time would actually affect operations. Would a one-second increase matter? If it did, would it matter enough to outweigh the clear privacy benefits of encryption? These issues are simply ignored by the NPRM.

Note also that contact or optical-stripe technologies arguably make it unnecessary to encrypt the data, because they are not vulnerable to eavesdropping or sniffing. In essence, the State Department defends its refusal to encrypt data for privacy in the RFID passport on the basis of its logically prior refusal to use a technology that would make encryption unnecessary. Put another way, the State Department has made a series of apparently deliberate choices to expose, rather than protect, passport information.

Nor is the third reason – that encryption is inconsistent with global interoperability – supported by factual evidence or reasoned analysis. Indeed, the ICAO guidelines specifically include three different cryptographic features. One such feature, "Basic Access Control" (BAC), uses encryption for data confidentiality, with the intent that the ability to read the passport contents should only be available when a passport holder intends to show his or her passport. Indeed, the ICAO document authors were well aware of the privacy issues and enumerated privacy risks if BAC is not used.

Unfortunately, the State Department is using a different feature, "Passive Authentication," which provides no privacy or confidentiality and demonstrates only that the data is authentic (via digital signature). (As we will later discuss, Passive Authentication does not even authenticate the data "container," and thus does not prevent cloning.) The crucial point here, however, is that even Passive Authentication requires that readers be cryptographically capable. No facts or explanation support the implication that encryption under BAC would demand a higher level of technology than required by Passive Authentication.

Eurosmart, an European smart-card industry association, has recommended that the European Parliament "adopt[] the Basic Access Control security scheme to protect privacy." Eurosmart Contribution to European Union regarding ePassports and eVisa (Oct. 2004) <http://www.eurosmart.com/Update/ Download/November04/ES_eVisaPassport.pdf> This report states:

"Privacy is a key concern for European citizens. In particular, citizens do not want a non-authorized person to access the data in their passport (nationality, name, address . . .) by just walking by with handheld contactless reader equipment. . . . This risk exists with ePassports relying on the ICAO Passive Authentication security scheme. The ICAO Basic Access Control (BAC) scheme dramatically reduces this risk: the ePassport must be physically open and visible to the passport OCR reader so processes of authentication and encrypted communication can take place using a key stored in the Machine Readable Zone (MRZ) of the ePassport. Hence surrounding and non-authorized equipment are not able to access the passport information. EU must mandate Basic Access Control on European ePassport. EU must install Basic Access Control-compliant readers at its borders. EU must ensure that its partners, in particular the US, equip their own borders with Basic Access Control-compliant readers too."

Comments already submitted on this issue claim that encrypted passports would mean a global key management scheme to determine the circumstances in which the RFID passport would be unlocked by a reader, reflecting the NPRM's statement that "in order to be globally interoperable, encryption would require a higher level of technology and more complicated technical coordination with other nations." 70 Fed.Reg. at 8306.

As we understand the technology and ICAO specifications, this claim is false. The Basic Access Control standard explicitly specifies a mechanism for key management that does not require a global key management scheme: the key to unlock the chip is derived from the information on the front cover of the passport. Therefore, a reader cannot read the RFID passport data unless the entity that owns the reader has optically scanned the passport cover. No global key management scheme is required, while a large class of skimming attacks is prevented.

In sum, the NPRM completely fails to justify the State Department's three crucial decisions about the proposed RFID passport: to use contactless, not contact, technology; to use RFID as its contactless technology; to refuse to protect the confidentiality of information on the RFID passport.

III. The RFID passport presents a host of privacy and security threats.

Passports contain sensitive personal information such as name, birthdate, and nationality. The RFID passport poses many privacy and security risks, all of which ultimately stem from the State Department's decision to use a technology (RFID) that enables covert and remote reading of this stored data. These threats include:

- clandestine skimming (surreptitious reading of or access to the stored passport data)
- clandestine tracking of the passport holder via a unique number on the passport
- cloning of the passport
- eavesdropping on authorized transactions
- biometric data leakage

A. Clandestine skimming

By their very design, RFID devices – whether "dumb" RFID tags or "smart" contactless integrated circuits – are remotely and secretly readable. As security expert Bruce Schneier has said, "Unfortunately, RFID chips can be read by any reader, not just the ones at passport control. The upshot of this is that travelers carrying around RFID passports are broadcasting their identity. Think about what that means for a minute. It means that passport holders are continuously[1] broadcasting their name, nationality, age, address and whatever else is on the RFID chip. It means that anyone with a reader can learn that information, without the passport holder's knowledge or consent. It means that pickpockets, kidnappers and terrorists can easily -- and surreptitiously -- pick Americans or nationals of other participating countries out of a crowd." <http://www.schneier.com/blog/archives/2004/10/rfid_passports.html>

When the capacity for clandestine skimming is combined with freely available and customizable software for reading the contents of an unencrypted passport and running realtime queries against demographic databases provided by commercial data brokers like ChoicePoint, Axciom, and Lexis/Nexis, the accuracy and efficacy of attacks targeted against carriers of RFID passports is greatly enhanced. See <http://www.rf-dump.org> (Lukas Grunwald's RFID reading software); Mark Willoughby, *Securing RFID information: Industry standards are being strengthened to protect information stored on RFID chips* , Computerworld (Dec. 20, 2004) (quoting Bruce Schneier as saying that Grunwald "is doing what RFID is supposed to do. This is serious. He didn't hack anything. RFID technology originally was designed to be completely open; that's its problem. He went to the spec, read it and followed it. If you query the chip, you will get this info. If there were security countermeasures on the chip that were thwarted, then we could talk about hacking."). Furthermore, as Juels, Molnar and Wagner note, "[a] photograph, name, and birthday give a head start to a criminal seeking to commit identity theft." JMW at 4.

Without explanation, the State Department minimizes the skimming threat, claiming that skimming is "technically very difficult." The ICAO itself has stated: "Compared to paper-based MRTDs copying the signed data stored on the RF-Chip is easily possible in general." ICAO PKI MRTD Report, at 55.

[1] We recognize that RFID devices only emit data in response to a signal from the reader, but the general point is that the RFID passport will broadcast data to any entity armed with a reader.

One reason may be that the ISO 14443 standard specifies a limited (10 cm.) distance for authorized reading of compliant devices. But there is no public record to establish that the authorized readers cannot in fact read the proposed RFID passport from a greater distance. As Schneier notes, the claim that RFID passports can only be read from a distance of a few centimeters is "spectacularly naive," because "[a]ll wireless protocols can work at much longer ranges than specified." <http://www.schneier.com/blog/archives/2004/10/rfid_passports.html>

Nor is there any public evidence that hostile attackers cannot design unauthorized readers capable of reading at a greater distance, unfettered by FCC or other regulations that limit device power. Axalto spokesperson Neville Pattinson has been quoted as saying that skimming occurred from about 30 feet away during a NIST trial. Junko Yoshida, *Tests reveal e-passport security flaw*, EE Times Aug. 30, 2004 <http://tinyurl.com/46vml>. Although the above-mentioned attack may have involved eavesdropping, not skimming,[2] the State Department should formally clarify the official public record by publishing all information relating to the known skimming and eavesdropping threats associated with ISO 14443 devices; it should also extend the comment period for this docket to permit public comment based on accurate information.

Indeed, available public information indicates that the risk of long-distance reading is significant; Bluetooth radio communication protocols, which were originally designed for close-range communications (30 feet) have been successfully augmented for use in skimming activities taking place more than a mile away. Kim Zetter, *Security Cavities Ail Bluetooth* (Aug. 6, 2004), <http://www.wired.com/news/print/0,1294,64463,00.html> (BlueSniper "rifle" created by John Hering and colleagues at Flexilis "attack[ed] a Nokia 6310i phone 1.1 miles away and grabb[ed] the phone book and text messages"). Equally important, the results of this research have led to the creation of a step-by-step tutorial so well written that virtually anyone can read and replicate these modifications. <http://www.tomsnetworking.com/Sections-article106.php>

The NPRM adds, "the Department is taking measures to prevent skimming of the unencrypted data" and "intends to place an anti-skimming feature in the passport." NPRM at 8306. Yet there is no discussion of what that anti-skimming feature might be. Media reports suggest that the Department is considering some form of shielding inside the passport; the problem is that such physical shielding will not protect the data when the passport is opened.

Furthermore, in its discussion of the related threat of eavesdropping, the NPRM seems to believe that eavesdropping is infeasible because in a secured port-of-entry environment, "the equipment needed to eavesdrop would be obvious and detectable to authorities managing the port of entry." Here again there is no public record evidence that devices used for skimming or eavesdropping are "obvious and detectable."

---

[2] See Smart Card Alliance, <http://www.smartcardalliance.org/alliance_activities/rfid_FAQ.cfm> (item 17) ("In the NIST experiment, a card was placed on a reader (within the 4 inch/10 centimeter reading range). Under these normal work conditions, the card and the reader started communicating. NIST set up a sophisticated antenna with sensitive radio-receiving equipment some 30 feet (approximately 9 meters) away to capture the communication stream and was successful in doing so.").

Lukas Grunwald used his RFDump software on a PDA equipped with an RFID reader to read and write to RFID tags in a German grocery store. Arik Hesseldahl, *A Hacker's Guide to RFID* (July 29, 2004) <http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html>. There already exist SD cards for Palm-compatible handhelds that can convert popular PDAs like the Treo into RFID readers. <http://www.engadget.com/entry/1234000257034127/> Nokia last year unveiled a cell phone that can read RFID tags. RFID Journal, *Nokia unveils RFID phone reader* (March 17, 2004) < http://www.rfidjournal.com/article/articleview/834/1/13/> Given that U.S. passports are intended to last for five to ten years, there is every reason to believe that more sophisticated handheld readers will be created during the life of the proposed RFID passport.

But while the majority of public concern about RFID data insecurity has focused on remote reading over long distances, Americans should probably be more concerned about short-range reading. If RFID technology continues to proliferate, the most practical threat to the average person may well be RFID readers built into stores, shopping malls and office buildings. The ICAO standards clearly contemplate the rise of "walk through" RFID reader gates for covert surveillance. ICAO, *Use of Contactless ICs in Machine-Readable Travel Documents*, Annex I, at 23, Version 4.0 (May 5, 2004) (defining "walk through" as "where the holder is inspected remotely without any specific action being required of the holder").

B. Clandestine tracking and hotlisting

RFID technology generally presents a second class of threats: clandestine tracking and hotlisting. Virtually every type of RFID tag we know about contains some form of unique ID number – designed in by the manufacturer, used in collision avoidance protocols, or added as part of the intended application (such as a passport number). So long as the RFID tag or chip broadcasts its information in the clear, the person carrying that tag can be distinguished from any other person carrying a different tag.

A static identifier also enables hotlisting, where the attacker builds a database matching identifiers to persons of interest. An out-of-band information gathering mechanism can be used to associate the static identifier with a person's true identity whether or not ID information can be accessed from the RFID device directly.

The RFID passport is no exception: as Juels, Molnar and Wagner observe, the ISO 14443 standard "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 cannot be read." JMW, at 2. Moreover, "e-passports might enable the construction of 'American-sniffing' bombs, since U.S. e-passports will not use encryption to protect confidentiality of data." JMW, at 4.

C. Eavesdropping

The RFID passport also presents an eavesdropping threat. With eavesdropping, the attacker need not supply power to the RFID chip itself; the attack consists of listening to an authorized transaction between passport and reader. Here again the State Department seems to believe that the threat is small.

But the ICAO, which developed the standards that the State Department relies on, recognized eavesdropping as a significant privacy threat: "eavesdropping on an existing communication between a chip and reader is possible at a longer distance" than for reading the chip directly. The ICAO thus provided a "Basic Access Control" option to authenticate readers and to encrypt the link between the chip and the reader, saying that "States wishing to address this threat SHOULD implement Basic Access Control." ICAO PKI MRTD Report, at 56 (Sec. G.3.2) (emphasis in original). Unsurprisingly, Juels, Molnar and Wagner say that "passive eavesdropping during legitimate read sessions is likely to constitute perhaps the major vulnerability to data leakage." JMW at 9.

Researchers have described an eavesdropping "relay attack" using two devices: a "leech" that can be as far as 50 centimeters from the RFID passport, and a "ghost" that can be up to 50 meters away from the authorized passport reader. Ziv Kfir and Avishai Wool, *Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems* (2005), Cryptology ePrint Archive, Report 2005/052 <http://eprint.iacr.org/2005/052>.

Curiously, the NPRM states that "[e]avesdropping can only occur while the electronic chip is being read using a specially designed reader furnished with the proper public key." NPRM at 8306. Yet the ICAO clearly states: "Everyone who has the appropriate equipment is able to read the chip contents of the MRTD, but only the parties that are provided with the appropriate public key certificates and certificate revocation lists will be able to verify the authenticity and integrity of the chip contents." ICAO PKI-MRTD Report at 15 (Sec. 2.2.4).

D. Biometric data leakage

The use of a biometric – currently facial image – raises biometric leakage issues. "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 biometrics important." JMW, at 2. These concerns are enhanced by the fact that the NPRM speaks of "[a]dditional biometric information that may be required in the future." 70 Fed.Reg. at 8309 (proposed 22 C.F.R. § 51.1(j)).

There is already a visible trend in e-passport applications toward less human oversight. JMW at 5 (giving examples of unattended authentication at Kuala Lumpur International Airport and planned "SmartGate" in Australia). This creates more opportunities for spoofing or deceiving biometric authentication systems. JMW at 5 (noting that fingerprint recognition systems can be fooled by gelatin "fingers" inscribed with ridges creates from pictures of fingerprints). Moreover, the ICAO itself contemplates such developments: "The use of a Contactless IC in an MRTD lends itself to the self-service processing application." ICAO, *Use of Contactless ICs in Machine-Readable Travel Documents*, Annex I, at 24, Version 4.0 (May 5, 2004).

Second, biometric leakage may spill into other environments. The more popular that biometric authentication becomes, the more important it becomes to secure biometrics. In particular, if the passport facial image becomes a standard biometric outside the passport context, the insecurity

of the RFID passport will make it an easy target for obtaining a person's official biometric "identity." See generally JMW at 5.

E. Passport cloning

From a security standpoint, there are significant concerns about passport cloning. Axalto has noted that a dangerous feature of the RFID passport is that "[t]here is no logical link between the data page information and the electronic chip which is transporting it," which allows not only replay attacks but also "signal emulation, by invalid or illicit devices representing the previously collected data from a legitimate ICC from another passport, having permanently disabled the authentic ICC." Axalto White Paper, *Securing and Enhancing the Privacy of the E-Passport with Contactless Electronic Chips* at 3 (May 24, 2004) (attached as exhibit); see generally National Academy of Sciences, Computer Science and Telecommunications Board, Committee on Authentication Technologies and Their Privacy Implications, *IDs—Not That Easy: Questions About Nationwide Identity Systems* 37-41 (2002) (discussing architectural and technological difficulties of "binding persons to identities") (hereinafter "IDs—Not That Easy").

The ICAO guidelines include an anti-cloning feature called Active Authentication. But as Juels, Molnar and Wagner note, the public key used in Active Authentication must be bound to the specific RFID passport and biometric data being 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." JMW, at 7.

Under the ICAO specifications, Active Authentication must involve an optical scan of the machine-readable zone of the RFID passport by the authorized reader. JMW, at 7. It is unclear whether the State Department will use Active Authentication, although in an earlier document the State Department specified that compliant readers should support Active Authentication. Abstract, Appendix D.

F. Time, scale and other issues

Finally, we are generally concerned that the State Department has framed the security and privacy issues in a narrow and short-sighted way. We highlight three issues here.

First, the State Department seems to view the privacy and security issues purely in terms of the passport control context. In the real world, U.S. citizens traveling abroad may carry their passports with them at all times, putting them at risk of clandestine skimming and tracking outside of government-controlled ports of entry. Moreover, there is a danger of function creep: "passports might come to serve as authenticators for consumer payments or as mass transit passes." JMW at 10.

Also, the adoption of RFID technology for passport control cannot be viewed in isolation from the potential, later uses of RFID technology in other applications. For instance, the federal Personal Identity Verification (PIV) card will likely "include the same blend of technical mechanisms as e-passports: a combination of RFID and biometrics." JMW at 1. They also note that the REAL ID Act now pending in Congress may stimulate demand for both biometrics and

RFID in state ID cards and driver's licenses. JMW at 1. Thus, the State Department's policy choices will likely harm privacy outside the passport context.

Second, it is not obvious that the State Department has evaluated the privacy and security issues in light of the intended ten-year lifetime of the RFID passport. Technology is continually improving. Even if the State Department were correct that the privacy and security threats are not significant today, which we dispute, any meaningful analysis must attempt to address threats throughout the passport's ten-year life.

Third, we question whether the State Department fully appreciates the privacy and security problems of mass RFID applications. Under the NPRM, there will be millions of RFID passports (and passport holders) and thousands upon thousands of authorized passport readers around the world. Each authorized passport reader is itself a threat to the privacy of passport holders and must be secured. Because the technology will be so widespread and persistent over time, the likelihood of reverse engineering and thus security compromise will be high. At the same time, because so many people will be carrying RFID passports, the magnitude of harm associated with security compromise will be large – and it is unclear how well the system will recover once it is compromised.

A good example here is the recent demonstration by Prof. Avi Rubin and his team of security researchers at Johns Hopkins University of the inadequate security on the Texas Instruments Digital Signature Transponder used in the Exxon/Mobil SpeedPass and common automobile anti-theft devices. See S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, *Security analysis of a cryptographically-enabled RFID device*, (2005), <http://rfid-analysis.org/DSTbreak.pdf>.

All of these concerns also apply, of course, to the databases and information systems that support the implementation of RFID passports, which are beyond the scope of these comments. See generally *IDs—Not That Easy*, at 41-44 (discussing issues and complications of "backend systems").

IV. The E-Government Act of 2002 mandates a privacy impact assessment before RFID passports can be issued

Section 208 of the E-Government Act of 2002, which became effective on April 17 2003, requires an agency that develops a new information technology (IT) system to handle the collection of personally identifiable information (PII) to take the following steps:

1. Conduct a privacy impact assessment (PIA) for electronic information systems and collections and, make it publicly available by posting it to the agency's web site.
2. Post a privacy policy on the agency's web site.
3. Report annually to the Office of Management and Budget (OMB) on compliance with section 208 of the E-Government Act.

The requirement for a PIA must apply to the creation of a major data collection system such as the State Department intends to establish by requiring all personally identifiable information in U.S. passports to be stored in a world-readable RFID chip:

> *Major information system* - embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.[3]

According to the OMB Guidance, a privacy impact assessment should be conducted *before* an agency develops or procures an IT system, such as the proposed RFID passport system, that collects, maintains or disseminates information in identifiable form from or about members of the public.[4] This is especially important given that the proposed RFID passport is deliberately designed to disseminate personal information to any entity with a compatible RFID reader.

The PIA must also be updated whenever changes that impose new privacy risks are made to the system. For example, if the State Department modifies the RFID passport or develops significant new uses for information collected from reading RFID passports, it must update its PIA.

The privacy impact assessment for RFID passports should include an explanation and analysis of

- Less intrusive technologies that could serve the same purposes.
- What information the IT system will collect.
- Why it is being collected.
- What its intended use is.
- With whom the information will be shared.
- Whether individuals may decline to provide information or consent to particular uses of it.
- How the information will be secured.
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.[5]

The PIA must also identify the choices made by the agency regarding an IT system or collection of information as a result of performing the PIA. Given the privacy and security risks posed by the RFID passport, we believe that it is essential to undertake a PIA before deploying the technology.

---

[3] See OMB M-03-22, Memorandum for Heads of Executive Departments and Agencies, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, http://www.whitehouse.gov/omb/memoranda/m03-22.html.

[4] Id.

[5] E-Government Act, Sec. 208(2)(B)(ii)

V. Comments on other issues raised by the NPRM

A. "Damaged, Defective or Otherwise Nonfunctioning Electronic Chip"

The NPRM states: "a damaged, defective, or otherwise nonfunctioning electronic chip may be grounds for invalidating a United States passport. A passport with an intact data page but a nonfunctioning electronic chip would still be used as a travel document. However, detected attempts to alter chip data or to substitute a different electronic chip would result in invalidation." 70 Fed.Reg. at 8306.

Unfortunately, the NPRM neither establishes nor recognizes the need for a neutral, consistent process for determining whether a chip is deemed to be damaged, defective, or nonfunctioning. New language needs to be inserted that would define and set out a pre-determined and evenly applied process for testing nonfunctioning chips as to whether or not the chips had been tampered with. This is particularly important in light of the consequences associated with actively tampering with a chip.

For example, an individual may be carrying a passport with an inadvertently damaged chip. This individual may well be successfully accused of intentionally damaging the chip due to a lack of concrete, fair and evenly applied guidelines for distinguishing deliberate tampering from inadvertent damage. This is a potential area for substantial abuse of individuals. We cannot emphasize enough that there must be a pre-set, fair process with built-in checks and balances that is used to determine accidental or intentional chip damage, and provide clear mechanisms for recourse/refutation of tampering charges.

Regarding the specifics of any recourse mechanisms, there needs to be a very clear and speedy mechanism set down in writing that determines how, when, and where an individual may pursue recourse that is free to the individual who is charged with tampering with a chip in a passport. Not providing such a mechanism will have a long-term negative impact on potentially many individuals. This recourse mechanism should be made available for public comment prior to any launch of the new RFID passports.

B. "New Ground for Invalidating a Passport"

We are concerned about the NPRM's statement that unpaid fees will be a sufficient ground for invalidating a passport. Unpaid fees include bounced checks or disputed credit card charges. 70 Fed.Reg. at 8307. Before instituting this New Ground, there must be a system of checks and balances that protects the individual from bad actors and from bad luck before a decision of invalidation is made.

First, too much can go wrong with the section (h)(3) plan of sending notice to the "last address." We have all experienced mail problems and transitional times. If a person is in between residences, this notification plan is highly problematic. And if something goes wrong with a single mail delivery, a person's passport can be invalidated and they would never know about it until they arrived at the airport.

Additionally, the NPRM does not make allowances for possible bank or credit company error. Further, identity theft is a horrific problem for individuals, and may lead to a denied or disputed credit card charge that the affected individual does not understand or hear about until they attempt to travel. These issues must be carefully considered in developing a plan to invalidate a U.S. passport merely for unpaid fees.

We recommend that there be multiple notices and a much greater effort made to contact the individual prior to invalidation. We also recommend that the financial institution involved with the rejected or disputed payment be contacted to see if there is a fraud alert on the account or any indications of foul play due to identity theft, or a potential mix-up that is not the fault of the individual in question.

Again, it is a matter of instituting checks and balances. For example, there should be a minimum of two notices to the last known address, and there should be a minimum of two phone calls to the last known phone number, as well as contact with the relevant financial institution. It is likely that there are additional means of arriving at a fair system that will not discriminate against those who due to their jobs or schooling must move frequently. And we must remember that with 10 million identity theft victims, the financial impact and ensuing chaos is substantial and requires special consideration prior to instituting this New Ground.

It is imperative that alternatives to sending notice only to the last known address be explored. Invalidation of a passport is no small matter, and a single notice to the last known address is inappropriate given the serious consequences that can arise from not receiving notice through no fault of one's own.

C. Added Cost Burden

The added cost burden for replacement passports appears to be grossly understated in the proposed rule. The NPRM states: "The electronic chip is designed to be very durable. If an electronic chip fails, the bearer may apply for a no cost replacement passport issued for the balance of the original validity period. However, given the durability of the chip and the fact that an electronic passport with a nonfunctioning chip may continue to be used if the data page is not damaged, we do not anticipate receiving many such applications." 70 Fed.Reg. at 8308.

The NPRM, however, offers no factual basis for the assertion that the chip is durable in passport use. On the contrary, research shows that some percentage of the chips may be corrupted or malfunction quite easily due to a number of factors, which would greatly change the estimated cost burden of the RFID passport. See e.g. Rich Fletcher, *Packaging and RFID special interest group presentation* (March 10, 2004), <http://web.mit.edu/auto-id/www/SIG/Packaging/Members/031004/Auto-ID-Labs-PackSIG-March-2004.pdf>.

The NPRM estimated that the number of individuals that would need to order a free replacement passport was 20,000 per year. 70 Fed.Reg. at 8308. According to the Bureau of Consular Affairs, U.S. Department of State, 8,825,410 passports were issued in 2004. <http://travel.state.gov/passport/services/stats/stats_890.html>. Given that more than 8 million passports were issued in 2004, how was a low number of 20,000 people needing replacement

passports arrived at? This number seems remarkably low, particularly since it is based not upon any trial study, but upon the assertion that the chips "are sturdy" and therefore would not need to be replaced.

Yet media reports from the smart card industry indicate that no one knows how durable the RFID passports will be. Barry Kefauver, a former U.S. State Department official who heads the main committee of the International Organization on Standardization assisting ICAO has publicly stated that: "Durability is probably the single most critical unknown. The vendors do not know how long a contactless chip will last." See *Vendors taken to task over e-passport flaws* (Feb. 3, 2005) <http://www.securityinfowatch.com/article/article.jsp?id=2941&siteSection=304>

Accordingly, a thorough cost burden analysis based on actual studies and thorough, unbiased documentation and testing should be conducted before the government's plan to institute RFID goes into effect – and these results should be released fully to the public. Finally, if the government introduces a passport error, all charges for replacement passports after one year or at any time need to be paid by the government, not by the individual.

D. New forms and handling of source documents

Unfortunately, copies of the new forms were not made available to us prior to the comment deadline. However, the new forms must comply with the Privacy Act of 1974 and must contain sufficient notice of how source documents are handled and provide detailed explanations about source documentation handling, storage, access, and deletion.

Due to the high incidence of identity theft, it has become more important than ever to safely handle and store documents such as birth certificates and any other documentation containing a unique identifying number of any kind, including a passport number. It is not clear from the NPRM how individuals may get a copy of their passport files, stored documentation, and forms. It is also quite unclear how long the original source documentation will be stored, under what circumstances (encrypted or not?) and for how long. It is crucial that individuals are given this information prior to providing source documentation to the U.S. government.

We contend that passport source documentation should be handled at least as carefully as the documentation for the new "smart card" Federal ID pursuant to Homeland Security Presidential Directive 12 (HSPD-12_. Guidance for this ID card was recently established, providing that source documents themselves are not stored due to the high risk such storage presents to the individual. Instead, the information is taken from the source documents and put in a new form where it will be much more difficult for malicious actors to re-create a person's identity fraudulently. <http://www.whitehouse.gov/omb/inforeg/hspd-12_guidance_040105.pdf>.

In short, storing source documents such as original birth certificates in a large database is highly problematic and must be avoided. And finally, we reiterate that all forms associated with the new passport contain a robust Privacy Act notice and appropriate discussion of the privacy and security of the highly personal information that is being entrusted to the U.S. Government.

Conclusion

The decision to build tracking technology into government identification documents raises significant privacy and civil liberties issues. Unfortunately, the State Department has not addressed these issues in any meaningful way. Accordingly, we believe that the State Department's proposal is fatally flawed. First, there is no proper delegation of legislative authority to the Department for the RFID passport given its many privacy risks. Second, the Department has failed to present substantial evidence to support any of the policy choices associated with the RFID passport. Third, the Department has failed to conduct a meaningful technology and privacy assessment for the use of RFID technology on such a large-scale basis despite the obvious privacy risks.

We urge the State Department to abandon its plans for the RFID passport.

[Attachments:
1. Juels, Molnar and Wagner paper on e-passport security
2. Axalto white paper on e-passport security]

Respectfully submitted,

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Tel: (415) 436-9333 x 102
tien@eff.org
http://www.eff.org

Cédric Laurant
Policy Counsel and Director, International Privacy Project
Electronic Privacy Information Center
1718 Connecticut Ave., N.W., Suite 200
Washington, DC 20009 - U.S.A.
Tel: +1 (202) 483-1140 (x114)
Fax: +1 (202) 483-1248
chlaurant@epic.org
http://www.epic.org

Linda Ackerman
Staff Counsel
PrivacyActivism
lga@privacyactivism.org
http://www.privacyactivism.org

Beth Givens
Director
Privacy Rights Clearinghouse
3100 - 5th Ave., Suite B
San Diego, CA 92103
Voice: 619-298-3396
Fax: 619-298-5681
bgivens@privacyrights.org
http://www.privacyrights.org

Pam Dixon
Executive Director
World Privacy Forum
San Diego, CA
Voice: 760.436.2489
pdixon@worldprivacyforum.org
http://www.workprivacyforum.org

Bill Scannell
Independent privacy activist
Washington, D.C.
bill@scannell.org
http://www.rfidkills.org

Attachment 1

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.**

I. 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 2005 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. 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 [14]. 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. 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 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 [21].

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

RSA Laboratories, ajuels@rsasecurity.com
UC-Berkeley, dmolnar@eecs.berkeley.edu
UC-Berkeley, daw@eecs.berkeley.edu

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.[1] 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 [27].
   - *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 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.[2]

   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., [24], have recognized the first three. 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 [23]. Pattinson also points out the need for a direct link between

[1] 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.

[2] 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.

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.

Organization

In section II, we provide some basic technical background on RFID and biometrics. We turn in section III 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 IV, illuminating some potential weaknesses and discussing the selection of features the United States has made for its US-VISIT program. In section V, 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 VI. We conclude in section VII with summary recommendations for improved e-passport deployment and with pointers to ID projects with similar underpinnings.

II. Technical Background

A. 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 showed the possibility of eavesdropping from a range of 30 feet [27]. Others have shown how relay devices can be used to read ISO 14443 chips, the kind used in e-passports, from even greater distances [19].

B. 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.

III. E-passport Threats

A. 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 [13]. 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.

B. 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 [15]. 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 [18]. 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 [22]. 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 [25].)
   Also, multiple enrollments of the same biometric can cause subtle security problems, even if none of the biometric data is "compromised." Recently, Barral, Coron, and Naccache proposed a technique for "externalized fingerprint matching" [8], now sold to the global ID card market by GemPlus under the name BioEasy. The goal is to enable storing a fingerprint template on a low-cost chip, without requiring the overhead of traditional cryptography. In their scheme, a chip stores a fingerprint template $f(D)$ of a fingerprint D together with a set of randomly chosen fingerprint minutae r. When queried, the chip returns $t := f(D) \cup r$ and challenges the reader to determine which minutae belong to $f(D)$ and which belong to r. The authors argue that even if an adversary queries the chip remotely and learns t, recovering the template $f(D)$ without access to the fingerprint D is difficult because of the additional minutae r.
   If the same user enrolls in two different organizations A and B with the same finger, however, these organizations will give the user cards with $t_A = f(D) \cup r_A$ and $t_B = f(D) \cup r_B$ (we assume that the template algorithm can tolerate some fuzziness in the fingerprint reading and obtain the same or very similar f(D)). If the adversary scans the user, then it will learn both t_A and t_B. Then the adversary can compute $t_A \cap t_B = f(D) \cup (r_A \cap r_B)$. If r_A and r_B were chosen independently, we expect their intersection to be small, so the adversary can gain an advantage at determining the fingerprint template not envisioned in the original design of the system. This vulnerability illustrates the issues that could arise when fingerprints are used both for e-passports and for other forms of identification.

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 [9].
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 [20].

IV. Cryptography in E-passports

A. 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 [14], [15]:

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

Fig. 1. Summary of ICAO security features.

Passive authentication: The data stored on a e-passport will be signed by the issuing nation [15]. 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:

Reader		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" [16]. 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 [15].

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 has elected not to include Basic Access Control in its e-passport deployment.

"Active Authentication": The ICAO spec urges use of 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.

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. Be-

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	Unknown	Photo

Fig. 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. "Unknown" indicates a lack of reliable public information.

cause 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.

B. 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 [25]. 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[3]; 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 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.

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 [26]. 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].

V. Strengthening Today's E-passports

A. 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 radio waves 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

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

shown in a discussion of "physical measures" in Section 2.4 of [15]. 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" [17] 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.

B. 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.

C. 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].

D. 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.

We can address both problems by the JFKr Diffie-Hellman based key agreement protocol of Aiello et al. [6], which allows a responder (in this case, the e-passport) to hide its identity until a reader has proved it is authentic. As we are not concerned with protection of the identity of an e-passport reader, such asymmetric anonymity is well-suited to our situation. Because each session derives a new key, reader cannot re-use keys from an old session to eavesdrop on a new session. While the JFKr protocol requires public-key cryptography, operations of similar complexity must be supported by any passport performing Active Authentication. Therefore we believe JFKr will be reasonable for many deployments. A remaining question for future work is how the e-passport can recognize that a reader is no longer authorized to read the e-passport, given that the e-passport has limited storage and no clock.

VI. Future Issues in E-passports

A. 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.

B. 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.

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.

VII. 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.

VIII. 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.

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] Andy 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. Social Security Administration. Passports as evidence, 2005. http://policy.ssa.gov/poms.nsf/lnx/0302640050?OpenDocument&Click=.

[6] William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Just fast keying: Key agreement in a hostile internet. *ACM Trans. Inf. Syst. Secur.*, 7(2):242–273, 2004.

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

[8] Claude Barral, Jean-Sébastien Coron, and David Naccache. Externalized fingerprint matching. Cryptology ePrint Archive, Report 2004/021, 2004. http://eprint.iacr.org/.

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

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

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

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

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

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

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

[17] Ari Juels, Ronald L. Rivest, and Michael 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.

[18] Dato' Mohd Jamal Kamdi. The Malaysian electronic passport, 2004. Presentation to ICAO, http://www.icao.int/icao/en/atb/fal/fal12/Presentations/Malaysia.ppt.

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

[20] Tsutomu Matsumoto. Gummy and conductive silicone rubber fingers. In *ASIACRYPT 2002*, 2002.

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

[22] Will Ness. Microsoft optical desktop comes with fingerprint reader, January 2005.

[23] Neville Pattinson. Securing and enhancing the privacy of the e-passport with contactless electronic chips, 2004.

[24] 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.
[25] "Architecture Team". IC embedded passport PKI requirements, 20 October 2003. http://www.aclu.org/passports/PKIRequirements.pdf.
[26] Chas Hock Eng Yap and Foong Mei 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.
[27] Junko Yoshida. Tests reveal e-passport security flaw, August 2004. *EE Times*.

Attachment 2

24th May 2004

WHITE PAPER

Title: Securing and Enhancing the Privacy of the E-Passport with Contactless Electronic Chips.

Introduction to the E-Passport

A new generation of US passport was mandated as part of the Enhanced Border Security and Visa Entry Reform Act 2002, requiring the Department of State to support machine readable biometric identifiers. ICAO is the body responsible for picking the technology and setting the standards for the deployment of the e-passport program. While a chip based solution for the program will enable biometric to easily and securely be incorporated into the passport, the policy decision surround security must be addressed. This paper details the problems with the ICAO specification and measures that must be taken to protect the privacy and security of all passport holders.

Background

The International Civil Aviation Organization (ICAO) is developing draft specifications for embedding contactless electronic devices in its 140+ member countries' passport documents, which will contain information regarding the holder of the passport. The electronic chip must, at a minimum, include the same information that is on the current printed 'data page' of the passport and also include a digital image of the scanned facial photo.

The US Department of State is presently mandated to begin issuing these machine-readable passports by October 26, 2004. Recently, the Department of State and the Department of Homeland Security requested a two-year extension to this timeframe for various reasons that were presented at a hearing of the House Judiciary Committee on April 21 2004. To enable the Department of State program, the GSA published an RFP on November 21, 2003; this RFP was eventually cancelled in March 2004 due to a complaint submitted by Anteon Corporation.

The ICAO specifications defining the use of contactless electronic chips allows for additional *optional* biometric identifiers such as fingerprint images, iris scans, palm scans etc. While this data can be useful in security schemes, ICAO has paid only very limited attention to the security of this biometric data and to privacy concerns regarding its use. ICAO's position is to leave the implementation of these optional items up to individual countries, and for the

countries to make their own bilateral agreements regarding their usage. ICAO's view is that the responsibility for the security and privacy of these items is outside of their scope.

Present Situation

The Department of State's original e-passport RFP required the existing passport document's data page information to be digitally signed by Department of State and loaded into embedded electronic chips in issued passports. The scope of the Department's initial implementation did not contain the highly controversial, optional raw biometric images, other than the digitally signed scanned facial photo that ICAO outlined. Care must be taken here with regard to a potential international privacy crisis and in case of potential "function creep" in the event that the additional biometrics are introduced without significant planning and clear usage policies. Clearly if significant personal information (e.g., in the form of raw biometric images) is stored within the chip and securing access to this information is not considered at the outset, unlawful or illicit use of this personal data could be easily obtained.

We understand that the Government Printing Office intends to release a new RFP in very soon, seeking bids for e-Passport covers that will include contactless electronic devices supporting a minimum of 64Kbytes of non-volatile storage memory. The GPO RFP is currently expected to require only the minimal mandatory ICAO specification.

Given that the ICAO remains the authority on the mandatory e-passport data content and interoperability requirements, the Department of State and the GPO defer to ICAO for the interoperable specification.

If the US implementation of e-passport follows the minimal mandatory sections of the ICAO specifications (i.e. data page information only), several concerns remain:

1. Unprotected Data. The digitally signed data page information contained within the electronic chip is freely available to any suitably equipped device with potentially no specific access security, encryption scheme or restrictions.[1] Such an approach may be convenient and interoperable, but is

[1] The ICAO specifications include an optional provision to have the passport document physically swiped to read the machine-readable printed characters. An encrypted password can be collected at that point and be used to electronically unlock the contactless chip and its data payload for reading over the contactless RF interface. This would limit the ability to 'skim' the data contained with the chip without the user's conscious awareness. Even this optional scenario is weak, in so far as a simple brute force attack on the password is possible given sufficient time

prone to several attacks (see point #3 below), as the data is static in nature and has no dynamic element.

2. Unprotected Wireless Transmission. There is no mechanism to notify the passport holder when data is wirelessly transmitted to a requesting party. The data is transmitted from the E-Passport over a low power 13.56Mhz radio frequency [contactless] interface and nothing would prevent a third party from intercepting this data. The information is also transmitted in the clear (not encrypted) with a State Department issued digital signature to attest to data integrity and issuer authentication. There is no requirement to encrypt the data during transmission, therefore leaving the data vulnerable to interception and eavesdropping during transmission.

3. No Connection between Chip and Paper. There is no logical link between the data page information and the electronic chip which is transporting it; without such a link, the data is vulnerable to several common attacks, such as skimming[2] or replay attack and even signal emulation, by invalid or illicit devices re-presenting the previously collected data from a legitimate ICC from another passport, having permanently disabled the authentic ICC.

Using cryptographic challenges to achieve mutual authentication between trusted devices (both chips and terminals) would address many of these potential attacks.

Conclusion

Under the current strategy, the electronic chip's role in the e-passport has been reduced to that of a relatively insecure data carrier and transmitter. This position will do little to inspire confidence among e-passport holders that the correct security and privacy practices have been considered to protect their data and identity information. However, the electronic chips being used *are* capable of providing the necessary and more appropriate security commensurate with this application. It would be a political and technological travesty to continue without reconsidering the correct use of the technology with respect to the needs of the application.

Summary:

We are deeply concerned about the very weak use (mere transportation and transmission of data) of the e-passport's electronic smart card chip, because it may facilitate the undermining of e-passport programs from a security and

---

and proximity to the document. Furthermore, this approach defeats many of the benefits of using contactless technology in the first place.

[2] i.e. Skimming: The subtle, non-obvious illicit reading of the chip's data by a third party when being distributed via the mail or carried around in pockets etc.

privacy perspective. Digitally signing data is a good method for ensuring data integrity, but does nothing for confidentiality. Without ensuring a strong chain of trust from the chip to terminal the transported data is vulnerable to misuse (collection) and potentially false presentation.

Offering minimal protection of personal security and privacy the e-passport implantation as it stands now could create a data management crisis on a global scale. With minor changes to the project's requirements, the e-passport can be implemented without creating a significant privacy concern, at the same time respecting the information usage. Where ICAO indicates the optional use of other biometrics beyond that available on the printed data page, there is also significant need to ensure that appropriate security is used to protect this information from misuse.

Smart card, biometric and encryption technologies securely, effectively and privately provide the nation's main defense against electronic attacks by terrorists and criminals. The proper use of such technologies in the e-passport program would lead to more widespread adoption of such defenses, which would ultimately make the our nation, international travelers and the world more secure. On the other hand, a loss of public confidence if the technology is incorrectly and inadequately deployed within the e-passport program would risk leaving our nation's data systems vulnerable to attack.

The combination of smart card and biometrics technologies provide a powerful multi-factor authentication mechanism which, on behalf of the issuer, ensures the authenticated identity of the card holder at the point of usage. Smart cards also offers privacy enhancing technology in so far as they can ensure the confidentiality and integrity of information disclosed whilst determining the appropriate sub set of information to be released according to the requesting parties access rights.

Recommendations and Actions Needed:

To prevent a loss in public confidence in the e-passport program amidst heightened awareness of security risks and privacy concerns, a public debate and review of the expected implementation of e-passport's electronic information and the important role of the electronic chip is required. The outcome of these discussions should be recommending or establishing a set of additional required security and privacy related practices for the implementation of the US e-passport program. This review should encompass how the security and privacy enhancing capabilities of the embedded electronic chips can be utilized to improve the implementation and address potential highly damaging and embarrassing privacy and security concerns. We would then strongly recommend that the role of the embedded chip be extended to ensure a "chain of

trust” for the data page information and to consider a mechanism to indicate to the chip that it may release the information only to "trusted" devices requesting its content in a secure manner.

A technical perspective of how to make significant improvements to the entire chain of trust for the e-passport document is laid out on the following pages. Attention to a few simple recommendations within the capabilities of the technology is outlined. These specific suggestions address both security and privacy improvements.

Improving the Chain of Trust, Enhancing Security and Privacy for the E-Passport Program.

With the incorporation of an Integrated Circuit chip (ICC) within the passport document, a convenient, automated, machine-readable mechanism will allow the extraction of the credential information by immigration officers upon presentation of the document. This can then be compared to the printed information and the person presenting the document.

At present the latest draft ICAO NTWG LDS v1.6 document clearly specifies the inclusion of the passport number within the logical data structure (LDS). This creates a trusted link between the passport document, bearing the passport number, the printed data page and the electronic credential held within the ICC. However there is *no* direct link between the credential and the ICC. Axalto continues to strongly recommend to ICAO that the ICC serial number be made *mandatory* and included in both the file system maintained on the ICC and also with the digitally signed LDS. This simple incorporation has the ability to significantly increase the chain of trust of the credential and to enable several cryptographic operations to verify the relationship between that of the ICC and the credential being presented.

Potential Enhanced Security Benefits

Some of the benefits that would potentially be enabled by incorporating on a mandatory basis the ICC serial number are as follows:

a) **Consistency Check**. The ICC serial number can be optionally cross verified locally by performing a SelectFile and ReadBinary operations to ensure that the LDS is indeed being presented by the device specified within the issuer's digitally signed LDS payload. This is still subject to replay attack and emulation, however it is a basic consistency check between the LDS and ICC serial number.

b) **Mutual Authentication**: For a higher level of authentication, the ICC can optionally be verified by a cryptographic challenge response mechanism to ensure it is an authentic ICC and is knowledgeable of a secret unique key and is entitled to present an LDS issued to it. This technique requires the external equipment to send the ICC a challenge. The ICC then encrypts the challenge using a unique secret only known to the particular ICC and the issuer. The resulting response to the challenge is then sent to

the external equipment where it is relayed in real time back to the issuer for verification. The issuer is then able to compare the answer to the challenge along with determining that the ICC knows the unique secret given to it at issuance. Variations of this scheme can be implemented where no on-line or real time communications are necessary and the local equipment can perform the necessary checks.

c) **Confidentiality**. Again the use of the ICC number can allow a secure channel to be established between the ICC and the reader/host application to ensure confidential transmission (data is encrypted) over the contactless interface and potentially beyond. This technique can utilize diversified keys maintained with the ICC to create session keys for secure communication externally.

d) **Accessibility/Privacy**. The ability to detect the ICC serial number outside the LDS can also lead to the ability for the terminal equipment to present one time passwords via the VERIFY command to authenticate its validity to receive the LDS. Without the ICC being available the external equipment cannot establish the ICC's identity and thus cannot present a suitable one-time password.

Operational Impact

By adding the ICC serial number information *as a mandatory item* to the LDS, the passport issuance process is directly affected because a specific issuer Digitally Signed LDS must now be loaded into a specific passport document. We believe this should be considered a necessary additional measure of credential trust assurance. Accordingly the LDS data must now be constructed with advanced knowledge of the target document it is to be loaded into. When the passport Document is to be printed/ programmed at issuance, the correct card stock document must be located and used. This practice is in line with the passport booklet document's stock serial number being used as the passport number. In the event of Issuance failure and a new target passport booklet having to be used, the LDS block will need to have both the new passport booklet serial number and the new ICC serial number included in replacement of the originals and then digitally signed by the issuer once again prior to being issued into the new passport document.

When the manufacturer of the passport documents supplies the stock, an additional data file must be provided to the issuer. The data file should include a list of passport document stock numbers along with the specific ICC that has

been embedded within the document. This information will then be used to form the Digitally Signed LDS information prior to loading onto the ICC.

Use of the VERIFY Command

The Verify command could be used to inhibit the unauthorized extraction of the electronic credential. In order to ensure authorized access to extract the credential from the ICC the correct presentation of a specific key must be presented to the ICC. As suggested by ICAO, this key can be transported within the Machine Readable Characters on the data page and extracted by the terminal equipment and presented by the terminal to the specific ICC. The Issuance process would also be responsible for encoding the Verify key within both the ICC and the printed Machine Readable Characters on the data page.

White Paper Author:
Neville Pattinson CISSP
Director of Business Development, Technology and Government Affairs.
Public Sector
Axalto, Austin, TX.
Ph: 512 257 3982
Pattinson@axalto.com

About Axalto

Axalto Inc, an independent public company, formerly known as Schlumberger Smart Cards & Terminals, is the world's leading provider of microprocessor cards (Gartner 2003, Frost & Sullivan 2003) — the key to digital networks — and a major supplier of point-of-sale terminals. Its 4300 employees serve customers in more than 100 countries, with worldwide sales reaching 3 billion smart cards to date. The company has more than 20 years' experience in smart card innovation and leads its industry in security technology and open systems.

Among many achievements, Axalto was the first and has subsequently been a major supplier to the US Department of Defense for Common Access Cards (Smart ID Cards) that have been issued to over 4M service personnel.

Axalto continuously creates new generations of products for use in a variety of applications in the telecommunications, finance, retail, transport, entertainment, healthcare, personal identification, information technology and public sector markets. Smart card solutions provide convenience, security and privacy to public and private services operators, their customers and end users. For more information, visit us at www.axalto.com