

# E-Passport Threats

In 2004, the International Civil Aviation Organization (ICAO) standardized e-passports by specifying how to implement and protect machine-readable travel documents (<http://mrtd.icao.int>).<sup>1,2</sup> However, many countries had to generate their e-passports in a rush,

quire privacy protection.

After solving collisions, a reader can either dump the memory or go through an access control protocol (if such a feature is implemented). As far as my colleagues and I know,<sup>3,4</sup> every country has implemented Basic Access Control, a protocol that ensures the reader already knows to which e-passport it is “talking,” and in particular, that it knows the passport’s number, its expiration date, and the holder’s date of birth. The reader optically scans this information from the machine readable zone (MRZ) inside the passport, which is why some people think that the chip can’t be accessed when the passport is closed, although this clearly isn’t true. The chip *can* be read when the reader knows this information, whether it’s from reading it when the passport is open, “remembering” it, or guessing it because the entropy isn’t high.<sup>5-7</sup> Anyone can easily build an e-passport reader, and if you’re okay with using it at a distance of 5 centimeters, you can find equipment that costs even less than the e-passport itself (see [www.rfidiot.org](http://www.rfidiot.org)). A metallic shield in the e-passport’s cover prevents the chip from being read when the passport is closed. This shield forms a Faraday cage around the chip, and to the best of our knowledge, only US passports use it.

## Crypto from the 1980s

Figure 1 shows an example of the text found in a typical MRZ. From this segment, we can discern the document type (P for passport), the issuing country code (CHE for Switzerland), the holder’s name (Alice Smith), the document number (74HK8215), the holder’s

SERGE  
VAUDENAY  
Ecole  
Polytechnique  
Fédérale de  
Lausanne

under pressure by a US visa-waiver policy change that mandated all foreign passports be machine-readable. Ideally, e-passports will substantially improve border security, but at what cost to passport-holder privacy?

E-passports have an embedded contact-less chip that can be read by radio from up to a few centimeters away (although boosted readers can scan them from a few meters). The ICAO chose this technology over magnetic strips and 2D barcodes because it provides reliable connection, large memory capacity, random access, and rewritable memory.

However, an open question remains—what happens if the chip doesn’t respond at border control? Chips can malfunction, especially if they’re grilled by electromagnetic waves either by accident or an active attack. In theory, an e-passport remains valid even if the chip doesn’t respond, but the holder is likely to waste a lot of time at immigration offices. Some people have opted to break the law to protect their privacy by destroying their passport chips with a hammer, a microwave, or a photograph flash. But let’s assume for a moment that people can peacefully live with their e-passports: what sort of cryptography technology

is involved here? Can e-passport holders protect their privacy without resorting to subterfuge?

## RFID for dummies

As with many other RFID devices, the chip in e-passports uses a 32-bit number for collision avoidance. (Indeed, if we give two e-passports to a reader simultaneously, it should be able to select which one to scan first.) Some countries (such as New Zealand and Italy) use a constant number, so that any scanner can easily track e-passport holders. Other countries use a constantly changing random number for privacy protection. The ISO 14443 standard specifies that random numbers should start with byte 08, but some people claim that starting with this byte clearly indicates that the device reveals itself as a potential target. For this reason, some countries (such as Australia) have opted to use a random byte, but this doesn’t always give the intended protection—a constantly changing number that doesn’t start with byte 08 might implicitly indicate that the chip belongs to, say, an Australian passport. This type of privacy protection mechanism is effective only when it’s universally and uniformly implemented, even in RFID tags that don’t re-



## Proving knowledge of a valid signature

Let's assume that an e-passport holds an RSA signature  $x$  for the formatted message  $X$ .<sup>1</sup> The signature is from an issuing agency that uses a public key with modulus  $N$  and exponent  $e$ . The e-passport can prove to the reader that it holds a valid  $x$  without revealing it by using the GQ zero-knowledge proof. For that, the reader first commits to a random value  $c$  and sends the commitment  $\gamma$  to the chip. The chip encrypts a random value  $y$  with RSA and sends the ciphertext  $Y$  and a random  $c'$  to the reader. The reader then opens its commitment and reveals  $c$ , which means the chip and the prover can now compute the GQ challenge  $c + c'$ . Finally, the chip sends  $z = yx^{c+c'} \pmod N$ , and the reader can check that  $z^e$  and  $YX^{c+c'}$  match modulo  $N$ .

E-passport		Reader
formatted message: $X$	public key: $N, e$	Formatted message: $X$
private signature: $x$		
	$\xleftarrow{\gamma}$	pick $c, \delta; \gamma = H(c \parallel \delta)$
pick $c', y$		
$Y = y^e \pmod N$	$\xrightarrow{Y, c'}$	
check $\gamma = H(c \parallel \delta)$	$\xleftarrow{\delta, c}$	
$z = yx^{c+c'} \pmod N$	$\xrightarrow{z}$	check $z^e = YX^{c+c'} \pmod N$

Depending on a secure commitment scheme, this protocol is a zero-knowledge proof of knowledge about  $x$  satisfying  $x^e \pmod N = X$ . A pragmatic choice for the commitment would be to use  $\gamma = H(c \parallel \delta)$  with a hash function  $H$  and a random value  $d$ . By using small  $c$  and  $c'$ , the protocol hardly requires more than two RSA encryptions, which might still be faster than the Active Authentication protocol. The proof is further nontransferable after completion—that is, after the protocol completes, a malicious reader can't prove that the issuing agency ever released  $x$ . The only way to prove it to a third party would be to run a Mafia fraud attack online.

### Reference

1. J. Monnerat, S. Vaudenay, and M. Vuagnoux, "About Machine-Readable Travel Documents: Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication," to be published in *Proc. RFID Security Workshop*, 2007.

can suffer from semantic challenge attacks: any reader can ask a chip for a transferable proof that it was scanned at some given place at some given time by using regular time-stamping techniques.<sup>8,9</sup> Relay attacks can also defeat the protocol.<sup>10</sup>

The current default biometric is the facial image, but the ICAO standard makes it possible to use finger and iris prints as well. However, most countries don't go this far because such technology isn't easy to deploy and leads to privacy issues. The EU considers biometric data to be more privacy-sensitive, so its countries use Extended Access Control to protect them. The chip uses a static key to authenticate itself to the reader, and the terminal authenticates itself via a protocol that looks like Active Authentication with an extra PKI for readers.<sup>8</sup> One reported problem with this is that e-passports aren't online and have no reliable clock, thus they can't get a revocation list or reliably check that a certificate is still valid.<sup>9</sup> In other words, the

reader could say, "here's my public key...it's valid until 1995, but we're currently in 1990," and the e-passport would believe it. Another challenge for chips is to maintain an up-to-date list of PKIs belonging to those countries that have signed the appropriate agreement to access privacy-sensitive data. So far, readers must help e-passports figure out whether their countries have been granted access through an as-yet-unspecified protocol.

Extended Access Control suffers from an additional problem—it can leak the digest of every privacy-sensitive data group because the reader can read the SOD without passing through Extended Access Control. Someone who isn't authorized to read a private data group but who already knows its content will get a confirmation that his or her guess is correct and can publish a proof of it. Someone who, say, knows most of the content of data group 11 except for the secret telephone number can find it by brute force.

Despite all this poor cryptographic quality, can anyone still have a private life with an e-passport? Well, most attacks are hardly practical and the motivation for doing so doesn't seem especially clear. Nevertheless, these flaws should be addressed in future versions—especially the potential threat of abuse after authorized access. E-passports can definitely improve security at the border, but they could also do it without ruining our privacy. □

### References

1. *Development of a Logical Data Structure for Optional Capacity Expansion Technologies*, v1.7, Int'l Civil Aviation Organization, 2004.
2. *PKI for Machine Readable Travel Documents Offering ICC Read-Only Access*, v1.1, Int'l Civil Aviation Organization, 2004.
3. J. Monnerat, S. Vaudenay, and M. Vuagnoux, "About Machine-Readable Travel Documents: Privacy Enhancement Using (Weakly) Non-Transferable Data Authen-

- tication,” to be published in *Proc. RFID Security Workshop*, 2007.
4. S. Vaudenay and M. Vuagnoux, “About Machine-Readable Travel Documents,” *J. Physics: Conf. Series*, vol. 77, no. 012006, 2007; [www.iop.org/EJ/article/1742-6596/77/1/012006/jpconf7i77012006.pdf](http://www.iop.org/EJ/article/1742-6596/77/1/012006/jpconf7i77012006.pdf).
  5. D. Carluccio et al., “E-Passport: The Global Traceability or How to Feel Like a UPS Package,” *Proc. RFID Security Workshop 2006*, 2006; <http://events.iaik.tugraz.at/RFIDSec06/Program/papers/015%20-%20E-Passport%20Global%20Traceability.pdf>.
  6. G.P. Hancke, “Practical Attacks on Proximity Identification Systems (Short Paper),” *IEEE Symp. Security and Privacy (S&P 06)*, IEEE CS Press, 2006, pp. 328–333.
  7. A. Juels, D. Molnar, and D. Wagner, “Security and Privacy Issues in E-Passports,” *Proc. 1st Int’l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm 05)*, IEEE CS Press, 2005, pp. 74–88.
  8. *Advanced Security Mechanisms for Machine Readable Travel Documents—Extended Access Control (EAC)*, v1.01, tech. guidelines TR-03110, Federal Ministry of the Interior (Bundesamt für Sicherheit in der Informationstechnik), 2006.
  9. J.-H. Hoepman et al., “Crossing Borders: Security and Privacy Issues of the European e-Passport,” *Advances in Information and Computer Security, First Int’l Workshop on Security (IWSEC 06)*, LNCS 4266, Springer-Verlag, 2006, pp. 152–167.
  10. M. Hlaváč and T. Rosa, “A Note on the Relay Attacks on e-Passports: The Case of Czech e-Passports,” tech. report 2007/244, Int’l Assoc. for Cryptologic Research, 2007; <http://eprint.iacr.org/2007/244>.

*cryptography from the University of Paris 7. Contact him at [serge.vaudenay@epfl.ch](mailto:serge.vaudenay@epfl.ch).*

**Serge Vaudenay** is a professor at EPFL. His technical interests include cryptography, communication security, and security analysis. Vaudenay has a PhD in