Biometric Passports

Security and Privacy

William Henderson

University of Cambridge

Wednesday 11th October 2023

What is a biometric passport?

- A passport with an embedded chip containing biometric data
- Also known as an e-passport or digital passport
- Standardised by the International Civil Aviation Organisation (ICAO) as Document 9303 [1]
- Identified by this symbol:

What data does it contain?

All biometric passports contain a chip with the following data:

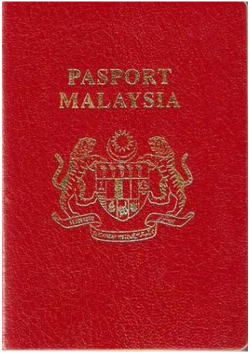
- A copy of the information printed on the passport
- A digital photo of the passport holder
- Digital signatures from the issuing country

Issuing countries may optionally include additional data:

- Fingerprints
- Iris scans
- Additional personal information (e.g. address)
- Additional document information (e.g. observations)

A Brief History

- 1968: Development begins
- 1980: Machine-readable passport first standardised
- 1988: Work begins on biometric systems
- 1998: First biometric passport issued by Malaysia [2]
- 2006: Biometric passport standardised



How is the data used? [3]

When the passport is scanned:

1. The machine-readable zone (MRZ) is read

```
P<GBRHENDERSON<<WILLIAM<EDWARD<HASWELL<<<<<<
0123456789GBR0409061M231011<<<<<<<<<<<<<<<02
```

2. The scanner and chip derive keys to establish a secure channel
3. The scanner reads the chip and verifies the digital signatures
4. The photo (and possibly other biometrics) are compared to the passport holder
   - by an e-gate using facial recognition
   - or by a human officer
5. The system checks the holder against watchlists
6. The holder is allowed into the country (or not)

Live Demo

- Reading the passport chip with an NFC-enabled phone
- Written in TypeScript (big mistake)

Basic Access Control (BAC)

- The data in the passport chip cannot be accessed without first establishing a secure channel
- One way of doing this is with Basic Access Control (BAC)
- We will call the scanner the interface device (IFD) and the chip the integrated circuit (IC)

- The hash function **H** is SHA-1
- The encryption function **E** is Triple-DES
- The MAC function **M** is ISO 9797-1 MAC algorithm 3

UNIVERSITY OF CAMBRIDGE

Step 0: Document Access Key Calculation

$$P = \text{passport number}$$
$$D = \text{date of birth}$$
$$E = \text{date of expiry}$$

$$\text{MRZ} = P \,\|\, D \,\|\, E$$
$$K_{\text{seed}} = \mathbf{H}(\text{MRZ})_{0,\ldots,15}$$
$$\mathbf{KDF}(K, c) = \mathbf{H}(K \,\|\, c)_{0,\ldots,15}$$
$$K_{\text{Enc}} = \mathbf{KDF}(K_{\text{seed}}, 1)$$
$$K_{\text{Mac}} = \mathbf{KDF}(K_{\text{seed}}, 2)$$

$\|$ denotes concatenation

$X_{a,\ldots,b}$ denotes the bytes a to b of X

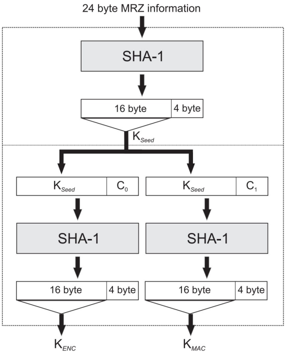


Figure 1: BAC key derivation [4]

Step 1: Basic Access Control

Inspection System (IFD)		**Passport (IC)**
		$\mathrm{RND_{IC}} \in \{0,1\}^{64}$
	$\xleftarrow{\mathrm{RND_{IC}}}$	
$\mathrm{RND_{IFD}}, K_{\mathrm{IFD}} \in \{0,1\}^{64}$		
$X \leftarrow \mathrm{RND_{IFD}} \parallel \mathrm{RND_{IC}} \parallel K_{\mathrm{IFD}}$		
$E_{\mathrm{IFD}} \leftarrow \mathbf{E}_{K_{\mathrm{Enc}}}(X)$		
$M_{\mathrm{IFD}} \leftarrow \mathbf{M}_{K_{\mathrm{Mac}}}(E_{\mathrm{IFD}})$		
	$\xrightarrow{E_{\mathrm{IFD}} \parallel M_{\mathrm{IFD}}}$	
		Decrypt and verify $E_{\mathrm{IFD}} \parallel M_{\mathrm{IFD}}$
		$K_{\mathrm{IC}} \in \{0,1\}^{128}$
		$Y \leftarrow \mathrm{RND_{IC}} \parallel \mathrm{RND_{IFD}} \parallel K_{\mathrm{IC}}$
		$E_{\mathrm{IC}} \leftarrow \mathbf{E}_{K_{\mathrm{Enc}}}(Y)$
		$M_{\mathrm{IC}} \leftarrow \mathbf{M}_{K_{\mathrm{Mac}}}(E_{\mathrm{IC}})$
		$\mathrm{KS_{Seed}} = K_{\mathrm{IFD}} \oplus K_{\mathrm{IC}}$
	$\xleftarrow{E_{\mathrm{IC}} \parallel M_{\mathrm{IC}}}$	
Decrypt and verify $E_{\mathrm{IC}} \parallel M_{\mathrm{IC}}$		
$\mathrm{KS_{Seed}} = K_{\mathrm{IFD}} \oplus K_{\mathrm{IC}}$		

Step 2: Session Key Derivation

Once the shared secret $\mathsf{KS}_{\mathsf{Seed}} = K_{\mathsf{IFD}} \oplus K_{\mathsf{IC}}$ is established:

$$\mathsf{KS}_{\mathsf{Enc}} = \mathbf{KDF}(\mathsf{KS}_{\mathsf{Seed}}, 1)$$
$$\mathsf{KS}_{\mathsf{Mac}} = \mathbf{KDF}(\mathsf{KS}_{\mathsf{Seed}}, 2)$$

The send sequence counter (SSC) is further initialised:

$$\mathsf{SSC} = (\mathsf{RND}_{\mathsf{IC}})_{4,\ldots,7} \parallel (\mathsf{RND}_{\mathsf{IFD}})_{4,\ldots,7}$$

Step 3: Secure Messaging

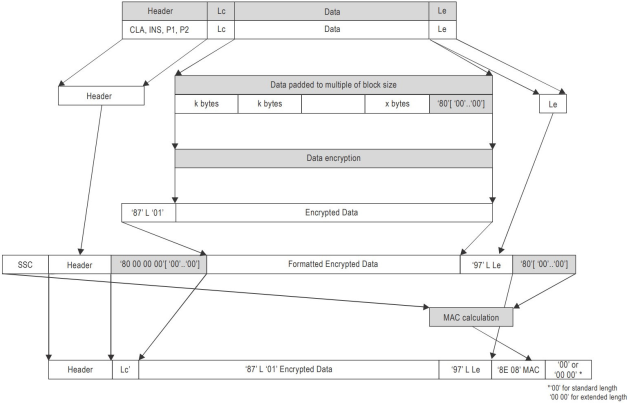


Figure 2: SM command APDU structure [1]

Passive Authentication

With Secure Messaging enabled, the IFD can read the holder's data from the IC and verify its authenticity and integrity using Passive Authentication.

- Each issuing country has a Country Signing Certificate Authority (CSCA) which issues certificates for national Document Signers (DS)
- CSCA certificates must be acquired from a trustworthy source (e.g. ICAO PKD)
- The Document Security Object (SO_D) contains digital signatures over hashes of the data in the passport, as well as the DS certificate
- The inspection system builds and validates a certificate chain from a Trust Anchor to the DS certificate
- The inspection system finally verifies the digital signatures in SO_D

Attacks

- **E-Passport: Cracking Basic Access Control Keys**, Liu et al. (2007)
  Due to the low entropy of the MRZ, the BAC keys can be cracked in a matter of seconds using specialised hardware.
- **A Traceability Attack Against e-Passports**, Chothia et al. (2010)
  By measuring the time taken for the IC to respond, the movements of an individual passport can be traced.
- **ePassport: Side Channel in the Basic Access Control**, Sportiello et al. (2014)
  Further timing analysis can be used to recover the MRZ without eavesdropping.

UNIVERSITY OF CAMBRIDGE

E-Passport: Cracking Basic Access Control Keys [4]

- Eavesdrop $\mathrm{RND}_{\mathrm{IC}}$, $E_{\mathrm{IFD}} \parallel M_{\mathrm{IFD}}$, $E_{\mathrm{IC}} \parallel M_{\mathrm{IC}}$ and the entire subsequent communication C
- Run a key search on the MRZ information to match the most significant eight bytes of E_{IC}.
- C can then be decrypted.

This becomes feasible if the MRZ has low entropy, due to:

- Passport numbers that are sequential, structured, include a checksum, or are otherwise predictable
- Passport expiry dates having a small range
- An attacker being able to narrow down the date of birth

UNIVERSITY OF CAMBRIDGE

E-Passport: Cracking Basic Access Control Keys [4]

- At the time, a lot of passports had these issues!
- **Germany**: 4 digits for local authority (of which there are 295), remaining 5 digits sequential
- **Netherlands**: Begins with fixed character "N", ends with a check digit, remaining 7 digits sequential

The authors demonstrated that, with just a photo of the passport holder and some knowledge about the dependency between passport numbers and expiry dates, the keys for a German passport could be cracked in ≈ 22 seconds and a Dutch passport in ≈ 10.3 seconds.

UNIVERSITY OF CAMBRIDGE

A Traceability Attack Against e-Passports [5]

- Eavesdrop $E_{\mathrm{IFD}} \| M_{\mathrm{IFD}}$ during a legitimate BAC exchange
- Initiate a BAC exchange with the IC and send it random data
- Initiate a BAC exchange with the IC and send it the recorded message
- Compare the time taken for the IC to respond

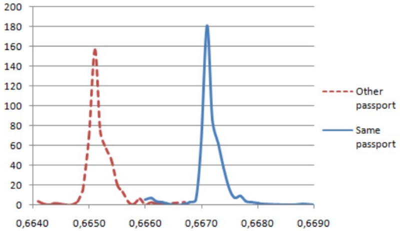


Figure 3: Sampled response times (British passport) [5]

UNIVERSITY OF CAMBRIDGE

A Traceability Attack Against e-Passports [5]

- IC checks the MAC before comparing nonces
- If the MAC is invalid (i.e. K_{Mac} is wrong), the IC will not compare nonces, and the response time will be shorter
- Could be used to, for example, build a bomb that detonates in the presence of a specific person [6]
- All 10 passports from 6 countries that the authors tested were vulnerable
- The French passport was even worse: it went against the spec and explicitly gave a different error code!

UNIVERSITY OF CAMBRIDGE

ePassport: Side Channel in the Basic Access Control [7]

- Set a generic E_{IFD} and a random M_{IFD}.
- Vary the ith byte of M_{IFD} and measure the time taken for the IC to respond.
- The value that causes the longest mean response time is the correct value of the ith byte.
- Work through the bytes to find the valid MAC for E_{IFD}.
- Use specialised hardware to crack the MRZ.

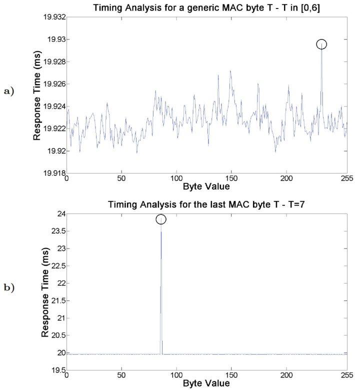


Figure 4: Timing analysis [7]

UNIVERSITY OF CAMBRIDGE

ePassport: Side Channel in the Basic Access Control [7]

- Requires an interaction of $\approx$ 85 hours with the IC
- The authors suggest that this could be achieved by performing the attack from malware on the target's phone:
  - Phone and passport are kept in the same pocket or bag
  - Malware uses the phone's NFC reader to communicate with the passport
  - Once the keys are cracked, the malware can extract further data from the passport and send it to the attacker
  - Alternatively the passport could be used remotely through a relay attack

UNIVERSITY OF CAMBRIDGE

Mitigations

- Ensure that the IC does not leak information through the timing of its responses
- Improve the entropy of the MRZ (e.g. by using a random passport number)
- Shield the chip so it can only be read if the passport is open
  - The US passport has a thin metal mesh in the cover [8]
- What to do about the fundamentally insecure DES encryption?

Password Authenticated Connection Establishment (PACE)

- PACE is an alternative to BAC that uses asymmetric cryptography
- Generates strong session keys independent of the strength of the password (in this case, the MRZ)
- Based on Diffie-Hellman key exchange
- Further communication is encrypted using AES
- See ICAO Doc 9303 Part 11, Section 4.4 [1]

Cryptographic Weaknesses

- EU passports since 2014 have been required to use PACE [9]
- Until 2018 it was still required to support BAC [1]
- PACE prevents eavesdropping but if BAC is still supported, the MRZ can still be cracked

UNIVERSITY OF CAMBRIDGE

LDS2 Applications

- In 2021, the ICAO introduced Logical Data Structure 2 (LDS2), which allows for additional data to be stored
- This includes travel history, visa records, and additional biometric data

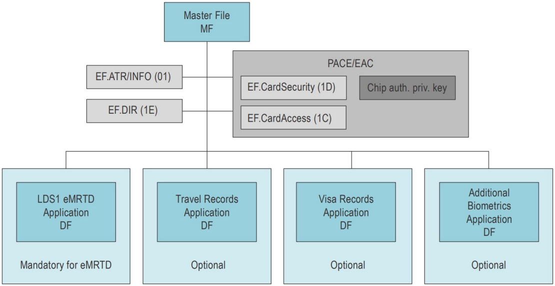


Figure 5: Applications for LDS1 and LDS2 [1]

Mandatory recording of travel history

- Up to the issuing country whether to enable this feature
- If enabled, it is mandatory for all countries to record the holder's travel history
- Currently, countries that don't want visitors stigmatised can issue visas and record entries and exits on separate documents

Tag	Tag	Content	Mandatory /OPTIONAL	Format	Example
'5F44'		Embarkation/Debarkation State (copy for SEARCH RECORD)	M	F (3) A	USA
'73'		Entry / Exit Travel Record (signed info)			
	'5F44'	Embarkation/Debarkation State	M	F (3) A	USA
	'5F4C'	Visa approvals, refusals, and revocations	O	V (50) A,N,S,U	Free-form text
	'5F45'	Travel date (Date of entry/exit)	M	F (8) N	20120814 (yyyymmdd)
	'5F4B'	Inspection authority	M	V (10) A,N,S	CBP
	'5F46'	Inspection location (Port of Entry/Exit)	M	V (10) A,N,S	SFO
	'5F4A'	Inspector reference	M	V (20) A,N,S	SFO00001234
	'5F4D'	Result of inspection	O	V (50) A,N,S,U	Free-form text
	'5F49'	Mode of travel	O	F (1) A	A (Air), S (Sea), L (Land)
	'5F48'	Duration of stay (days)	O	V (2) B	'00FF' (255 days)
	'5F4E'	Conditions holder is required to observe while in the issuing State	O	V(50) A,N,S,U	Free-form text
'5F37'		Authenticity token (Signature)	M	V (140) B	'5F' '37' Len {Signature}
'5F38'		Reference (record number) to LDS2-TS Signer certificate in Certificates Store	M	F (1) B	'01' …'FE'

Figure 6: Entry/Exit Record [1]

Irremovable messages

- Countries can add irremovable messages to the passport
- For example, a country could mark a person as “suspicious” with no reason given and no way to remove it
- This would make it difficult for the holder to travel [10]

Conclusion

- Biometric passports allow for much faster border control without compromising security
- Most of the security issues are fixed and just need time to be rolled out
- The privacy issues are just getting started...

UNIVERSITY OF CAMBRIDGE

References I

[1] International Civil Aviation Organization.
Machine Readable Travel Documents.
Doc 9303, Eighth Edition, 2021.

[2] Mohd Jamal Kamdi.
The Malaysian Electronic Passport, 2004.

[3] Frontex.
Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, 2015.

[4] Y. Liu, T. Kasper, K. Lemke-Rust, C. Paar.
E-Passport: Cracking Basic Access Control Keys, 2007.

[5] T. Chothia, V. Smirnov.
A Traceability Attack Against e-Passports, 2010.

UNIVERSITY OF CAMBRIDGE

References II

[6] A. Juels, D. Molnar, D. Wagner.
Security and Privacy Issues in E-Passports, 2005.

[7] Luigi Sportiello.
ePassport: Side Channel in the Basic Access Control, 2014.

[8] Kurt Kleiner.
Metal shields and encryption for US passports.
New Scientist, 2005.

[9] European Commission.
Commission Decision C(2011) 5499 of 4 August 2011 amending Commission Decision C(2006) 2909 final laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.

UNIVERSITY OF CAMBRIDGE

References III

[10] Edward Hasbrouck.
ICAO expands travel tracking and control through RFID passports, 2022.

UNIVERSITY OF CAMBRIDGE