



Biometric passports

Standard Note: SN/HA/4126
Last updated: 25 May 2010
Author: Melanie Gower
Section: Home Affairs Section

The UK has been issuing “biometric” passports (also known as “ePassports”) since 2006. The passports include a microchip which stores a digitised image of the holder’s passport photograph as well as the biographical details printed on the passport. Non-biometric passports continue to be valid until they expire.

In recent years many countries have been moving towards the use of biometric technology in passports (and other immigration documents). International Civil Aviation Organization recommendations for biometric standards include a digitised photograph embedded on a chip in the passport. Countries wishing to stay in the US visa waiver programme have had to start issuing biometric passports in line with these international recommendations.

The EU has set minimum standards for passports which include the use of facial and fingerprint biometrics. The UK is not covered by the regulations. The previous government had intended to introduce “second generation” ePassports, which would have included fingerprint data, in order to keep pace with the EU regulations. However, the Coalition Agreement of May 2010 confirmed that these plans have now been halted.

The [passport section](#) on the DirectGov website gives a lot of information about the passport application process. Some more detailed information is available in the [passport policy](#) section on the Identity and Passport Service website.

This information is provided to Members of Parliament in the performance of their parliamentary duties, and may not fully address the specific circumstances of any particular individual. It should not be relied upon by either Members or others as legal or professional advice, or a substitute for it. If specific advice is needed, a suitably qualified professional should be consulted. The website of the [Office of the Immigration Services Commissioner](#) explains about the regulation of immigration advisers and includes a useful online ‘adviser finder’. The [Immigration Law Practitioners' Association](#) may be able to suggest someone with experience in this area from its list of specialist practitioners. The [Immigration Advisory Service](#) provides advice and representation (which, if eligibility criteria for publicly funded legal services are fulfilled, may be free of charge), and the [Community Legal Service](#) website may also be helpful.

This information is provided subject to [our general terms and conditions](#) which are available online or may be provided on request in hard copy. Authors are available to discuss the content of this briefing with Members and their staff, but not with the general public.

Contents

1	Biometric passports in the UK	2
2	Why have they been introduced?	2
3	Fingerprint biometrics	4
4	NAO report	4

1 Biometric passports in the UK

The Identity and Passport Service (IPS) – an Executive Agency of the Home Office – began issuing “biometric” passports in March 2006. They are also sometimes known as ePassports. All new passports issued since September 2006 have been biometric. Non-biometric (digital) passports nevertheless remain valid until their expiry date.

Passport fees are set on a full cost recovery basis. There is a [table of current passport fees](#) on the passport pages on the DirectGov website.

The UK’s biometric passports contain a microchip with what is known as a “facial biometric”. This is simply a digitised image of the holder’s photograph. Various features on the face, for example the distances between eyes, nose, mouth and ears, are digitally coded from the photograph and the information stored on the electronic chip secured in the passport page.

The chip also stores electronically the biographical information which is printed in the passport. It does not contain any information which is not also on the face of the passport. The information printed on the passport can be checked against the information on the chip, which is intended to be harder to forge; and the chip can also be checked against information stored centrally by the IPS. The information on the chip is encrypted so it can be read only by special biometric passport readers (sometimes called eReaders). Passport-holders can use eReaders in any of the seven IPS regional offices to check the information contained on their passport chip.¹

Since July 2007, all adult first-time passport applicants have had to attend a personal interview as part of the passport application process.² The IPS established a network of passport interview offices across the UK for this purpose. In areas where the travelling time to the nearest interview office would be more than one hour, arrangements will be made for interviews using video-conferencing facilities.³

2 Why have they been introduced?

Some of the perceived benefits of ePassports were set out in response to a Parliamentary Question in October 2009:

¹ IPS, *Passport policy Biometric passports and Passport Readers* (accessed on 26 March 2010)

² See DirectGov website, [Passport interviews](#) for further background information (accessed on 26 March 2010)

³ [HC Deb 7 March 2007 c2040-1W](#)

Bob Spink: To ask the Secretary of State for the Home Department what evidence his Department used to evaluate the effectiveness of e-passports on (a) security and (b) efficiency of border immigration arrangements; and if he will make a statement.

Mr. Woolas: The introduction by the UK of the e-passport containing the holder's personal details and facial image on a contactless chip was part of a major international drive to make travel documents more secure. The UK e-passport's physical and electronic security features are a significant impediment to forgers and counterfeiters. The UK e-passport is recognised as a high integrity document, and there is no evidence that anyone has modified or changed the data within the chip on the e-passport in a way that would pass through the checks made at UK border control.

In terms of security, if the UK had not introduced the e-passport then there was a risk that the UK passport would have received greater attention from fraudsters and counterfeiters. Also, UK nationals would have been treated less favourably than those of other nations at border controls and not have been able to travel visa free to the United States.

The greater assurance and integrity offered by the e-passport enables border control authorities worldwide to spend more time dealing with higher risk passengers. Accessing the data held on the e-passport automatically, enables UK Border Force officers to use their time more efficiently on improved security and fraud checks, making our border even more secure. Additionally, the UK Border Agency is encouraging e-passport holders to use the facial recognition gates currently being trialled in the UK, providing the travelling public with an easier passage through the controls.⁴

The International Civil Aviation Organization (ICAO) began research on biometric passports in 1995, and has developed a set of international recommendations for the development and specification of globally interoperable biometric standards. These simply require the inclusion of a digital (or digitised) photograph embedded on a chip in the passport. Other biometric data are optional, and there is no requirement for databases of biometric information behind the passports.⁵

The USA-PATRIOT Act, passed in response to the events of September 11 2001, signalled new requirements for biometric information to be provided by those seeking to go to the US. In particular, countries wishing to stay in the visa waiver programme have had to start issuing biometric passports in line with the ICAO recommendations (i.e. with a digital photograph embedded on a chip). The US will continue to accept most British passports issued before September 2006 as long as they are machine-readable and contain a digital image rather than a pasted-in photograph.⁶

The EU has decided to standardise all EU passports, so that all Member States' passports contain a digitalised facial image and fingerprint data.⁷ This goes beyond requirements of the US and the ICAO. The UK was not able to take part in this regulation, which comes under the Schengen *acquis* (however, see following section).

⁴ [HC Deb 12 October 2009 c576W](#)

⁵ ICAO, [Doc 9303 Machine Readable Travel Documents](#), 2006

⁶ For more information see the US State Department website, [Visa Waiver Program](#) (accessed on 26 March 2010)

⁷ Council Regulation (EC) No 2252/2004 of 13 December 2004 *on standards for security features and biometrics in passports and travel documents issued by Member States*. See [Europa website summary](#) for further information.

3 Fingerprint biometrics

The previous government intended to introduce a “second generation” ePassport in 2012. This would have incorporated fingerprint data (considered to be a ‘true’ biometric), in line with the EU’s minimum standards. Passport applicants would have had their identity details and biometrics stored on the National Identity Register.⁸ It argued that keeping pace with the EU standards would prevent UK passports from becoming regarded by other countries as “second-class” and consequently more vulnerable to fraud and onerous checks overseas.⁹

However, the Coalition Agreement of May 2010 indicated that the Government does not intend to proceed with these plans.¹⁰ [Comparative information](#) on the cost, validity and type of passport issued for 47 countries is available on the IPS website. Australia, Canada, Ireland, New Zealand and the USA are amongst the countries which are not issuing ePassports with fingerprint data.

4 NAO report

On 7 February 2007 the National Audit Office published a report on the *Introduction of ePassports*.¹¹ This found that the implementation project had been delivered on time and within budget, and that the ePassports meet international standards on ePassport design, but it also raised some serious concerns:

- Although it has been tested in laboratory conditions, the ability of the chip unit2 to withstand real-life passport usage is unknown. The chip units have a two year warranty but British ePassports are intended to last ten years. The Identity and Passport Service is keeping this issue under review.
- With the right equipment, technical experts have shown that it is possible to read and clone ePassport chips. To access the data on a chip, prior knowledge of the information contained on the passport data page is required. But if the information on the data page can already be seen (or is known from another source) then there is no need to read the electronic chip since it contains no more biographical information other than that visible on the data page with the naked eye. New security features in the ePassport design are intended to render impractical the creation of a faked ePassport in which a cloned chip could be inserted. The Identity and Passport Service told us that any alteration of the data on cloned chips would be detected when the ePassport is read by an electronic reader at border control.
- Future liabilities may arise from intellectual property rights relating to the design of electronic components which are held by contractors.
- The Identity and Passport Service spent £4.9 million on consultants during the project. The Identity and Passport Service recognises the need to reduce its reliance on consultants and interim staff and to devote greater attention to knowledge transfer. Using civil servants in non-technical roles within the future passport development project could save £3.5 million over the next five years and help retain organisational memory.

⁸ [HC Deb 26 January 2010 c819-20W](#)

⁹ [HC Deb 10 July 2008 c1770W](#)

¹⁰ HM Government, ref 401238/0510, *The Coalition: Our programme for government*, May 2010, p.11

¹¹ Report by the Comptroller and Auditor General, *Identity and Passport Service: Introduction of ePassports*, HC 152 Session 2006-2007, 7 February 2007

- There was insufficient liaison between the Identity and Passport Service and the Immigration and Nationality Directorate about how ePassports would be read at border control.
- The Immigration and Nationality Directorate began testing the ability of electronic readers to cope with high volumes of ePassport checks in late November 2006. If readers cannot cope, the full benefits of ePassports may not be realised.

The report made the following recommendations:

1 To manage the risks to value for money, the Identity and Passport Service should:

- analyse the costs and benefits of a negotiated increase in the chip unit warranty and revisit this issue, and the question of passport validity, as more evidence of durability emerges;
- test the market as soon as possible for potential suppliers to compete for the new contract for ePassport production which will begin in October 2010;
- clearly document the basis for claiming any future exclusion from procurement regulations;
- reduce expenditure on technical consultants by using alternative methods of remuneration such as fixed-price contracts and bonuses for work delivered, rather than paying daily rates; and
- reduce expenditure on non-technical consultants in project teams by: developing a sustainable core of in-house project management skills to be supplemented with external specialists when required; and employing permanent staff rather than consultants to perform business analysis and administrative functions.

2 To increase effective working between government departments, the Home Office should:

- oversee the sharing of technical expertise between the Identity and Passport Service and the Immigration and Nationality Directorate to ensure the forthcoming upgrade of readers at UK Immigration is timely and enables prompt reading of ePassports;
- aggregate the purchase of biometric consultancy, readers and other equipment across the Home Office, appointing a lead purchaser who could also act on behalf of the Foreign & Commonwealth Office to secure better prices; and
- manage any future upgrades to ePassports as a cross-agency project encompassing the Identity and Passport Service, the Foreign & Commonwealth Office and the Immigration and Nationality Directorate with a Senior Responsible Owner, a single project plan and project board.