

e-Passports

September 20, 2005



Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Agenda

- e-Passport Overview
- Protecting Privacy
- Current Progress and Initiatives
- Future Possibilities



Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

e-Passport Overview

What is an e-Passport?

- A passport with an integrated circuit chip embedded somewhere within the document.
 - The chip contains certain data elements visible on the face of the passport. The data is encrypted and must be unlocked to be read.
 - The chip is “contactless” – it does not need to be physically connected to or touched by anything to be read.
 - The chip can be embedded into the following places within the passport: front page, back page or middle page.



Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

e-Passport Overview

Benefits of an e-Passport

- It is tamper proof
 - The data stored on the chip is protected against passport tampering or photo substitution.
- Legitimately issued
 - The digital signature on the e-Passport verifies that the passport was issued by the country claimed.



Homeland
Security



e-Passport Overview

What is a “digital signature?”

- E-Passports’ will often have a “digital signature.” This feature helps to ensure that the chip was manufactured by the issuing state or country.

Digital Signature

- A digital signature can be verified in two ways: passive or active authentication.
 - **Passive Authentication** – The e-Passport reader checks the contents of the chip to ensure that it was issued by the country claimed. It cannot, however, protect against perfect duplications of the chip or chip substitution.
 - **Active Authentication** – Consists of computations and communications between the reader and the chip. It can ensure that the chip is legitimate and issued by the country claimed.



Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Protecting Privacy

Privacy protections can be ensured in many ways, most commonly:

- Thin metal shields can prevent the e-Passport from being read by readers while the document is closed.
- Many e-Passports include “Basic Access Control.” This means that the e-Passport cannot be read by an electronic reader until the machine-readable zone is read first.
- Each of these features protect against “skimming,” or unauthorized reading of the e-Passport.
- The U.S. government is seriously considering these features.



Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Current Progress and Initiatives

**Late
1990s**

International Civil Aviation Organization (ICAO) began setting e-Passport standards.

2002

The digital facial image was the mandatory biometric for e-Passports. Fingerprints were considered optional.

**Nov.
2004**

The U.S. hosts “mock” port of entry tests at Baltimore/Washington International Airport.

- The goal of the test was to determine operational impact of using new equipment capable of reading e-Passports.
- Findings indicated that ergonomics played a critical role in the e-Passport reader process.

**June
2005**

The U.S., Australia and New Zealand began a test of e-Passports at actual ports of entry.

- e-Passports were given by each government to airline crews of United, Qantas and Air New Zealand airlines. e-Passport reader stations were set up in Los Angeles International Airport and Sydney International Airport.
- The test concluded on September 15, 2005 and the results are pending.



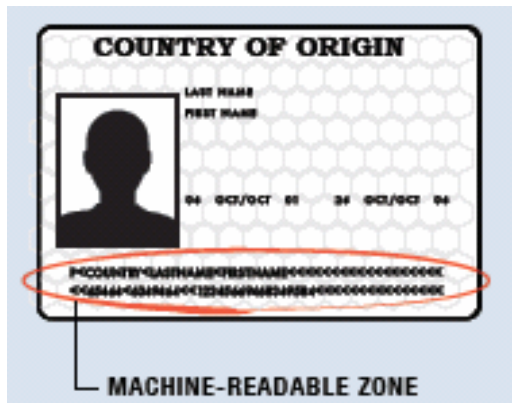
Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

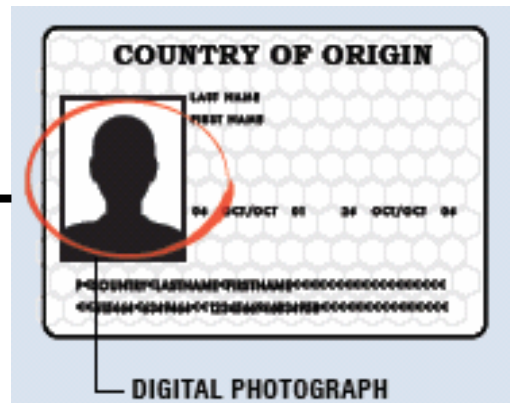
Current Progress and Initiatives

This timeline shows important deadlines for passports required by the United States for countries participating in the Visa Waiver Program.

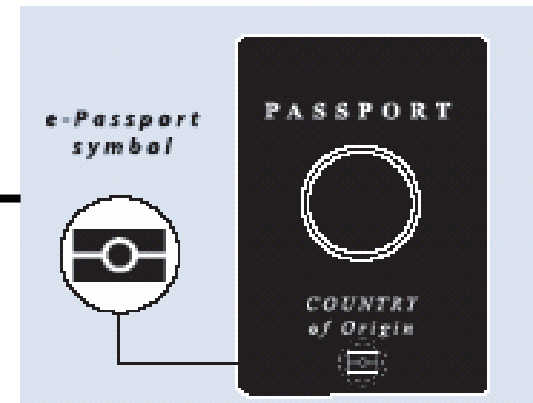
June 26
2005



October 26
2005



October 26
2006

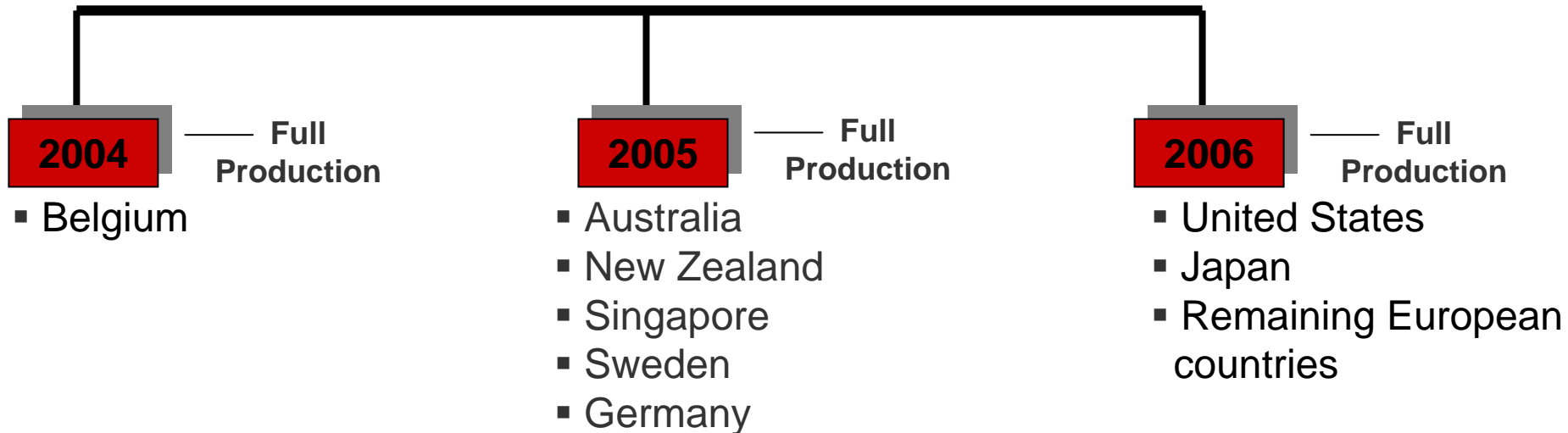


Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Current Progress and Initiatives

Development of e-Passports by country



Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Visa Waiver Program Conference

On Friday, September 23 the DHS will co-host with DOS a conference between the United States and all 27 Visa Waiver Program countries.

- The discussion will be partially about e-Passport and reader interoperability.
- Throughout late 2005 and 2006, the United States will work with each VWP country's passport division to ensure that the passports can be read with U.S. readers.
- DHS Secretary Michael Chertoff has determined that by October 26, the United States will have compatible readers at all ports of entry in the United States.



Homeland
Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Future Possibilities

Currently, most countries will use the digital facial image as the primary biometric in e-Passports; however there are some other technologies to enhance the e-Passport such as:

- **Facial Recognition Technology**

- Facial recognition technology would electronically compare the face of the person seeking admission to the photograph stored on the chip to ensure that they match. Current technology shows that this is difficult in the existing POE environment due to inconsistent lighting, backgrounds and other factors.

- **Fingerprint Technology**

- Some countries are placing fingerprints on the chips. The EU will require its nations to have fingerprints in e-Passports by 2009. Depending on international cooperation, a system could be created where fingerprints stored on the chip are compared to the person seeking admission (similar to US-VISIT now).



Homeland
Security

