



# Safer Travel with Smart Card Technology

Gemalto supplies its Sealys™ ePassport solutions to the U.S. Department of State

FINANCIAL SERVICES & RETAIL

ENTERPRISE

INTERNET CONTENT PROVIDERS

**PUBLIC SECTOR** & TRANSPORT>CASE STUDY

TELECOMMUNICATIONS



# Safer Travel with Smart Card Technology

## Gemalto supplies its Sealys ePassport solutions to the U.S. Department of State

### > The context

The International Civil Aviation Organization (ICAO), an agency of the United Nations, defines and adopts standards for international civilian air travel. Over 180 countries are members of ICAO. ICAO's goal with machine readable travel document specifications is to provide interoperable specifications, implemented world wide, that increase national security while speeding the border control process for travelers. ICAO issued their revised Machine Readable Travel Document specifications for ePassports as part of the initiative to further increase the passport document integrity. The United States of America adopted these specifications as part of their requirements for accepting ePassports from Visa Waiver Program nations under the Enhanced Border Security and Visa Entry Reform Act of 2002.

### > The challenges

To better protect travelers, streamline immigration processes and improve the security of the passport booklet, the U.S. Department of State (DoS) and the Government Printing Office (GPO), which assembles all U.S. passports, set a program in place to issue electronic passport

booklets to U.S. Citizens, in accordance with the standards developed by ICAO.

The use of chip-enabled passports was initially of concern to privacy and civil liberty organizations around the world. Whilst ICAO specifications recommended a minimum level of security, it was clear that additional security was required to protect the privacy of the ePassport's electronic credential.

Gemalto lead a global initiative to enhance the ePassport's security features to fully protect the privacy of the electronic credential by adopting Basic Access Control. Basic Access Control ensures the privacy of the electronic credential is preserved over the communication to external readers and protects against any attempts to skim, eavesdrop or modify any information. The use of Basic Access Control now forms the new baseline implementation for ePassport implementation worldwide.

### > The solution

In August 2006, U.S. GPO placed its first production order with Gemalto after evaluating the Gemalto's Sealys ePassport solution and confirmed it fully satisfied the agency's

requirements for privacy protection, security, durability, manufacturing yield, transaction speed and communications performance. Gemalto is one of only two vendors to be selected for the supply of the U.S. ePassport program.

Gemalto's ePassport technology includes Sealys eTravel, the company's ePassport operating system software running in a large capacity, secure, contactless microprocessor chip. The microprocessor is embedded in a module and then integrated with the antenna into the passport booklet back cover. The same personal information that is printed in the ePassport data page, including a high-quality digital photo, is stored securely in the chip.

Not to be confused with insecure RFID, Gemalto's contactless smart card technology has built-in security and encryption technology to protect unauthorized access to the credential contained in the chip.

### > The results

The new ePassport being issued to U.S. citizens is perhaps the most visible aspect of the U.S. government's investment in digital technology for enhancing border security.

## What Happens at Passport Control

1 The officer swipes the data page through a special reader to read the two lines of printed characters on the bottom of the data page. This provides a key that's unique to the passport and lets the checking proceed.

2 The officer holds your open passport over another reader, then checks that you (a) match the photo in your passport (b) and also the data from the passport's chip (including your photo) which is shown on the monitor. (c)

The data on the monitor also verifies that your passport was issued by a legitimate authority, and that it has not been altered.



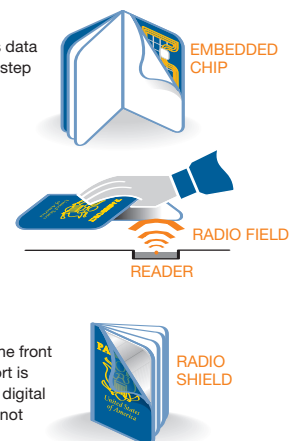
## Details, details

3 A chip is embedded into the passport. It contains data that cannot be read without the security key shown in step 1 above.

4 When the passport is held over the reader (no contact is necessary), a radio field from the reader wakes up the chip, and the encrypted data is transferred to the reader, allowing the officer to conduct the visual check.

## Privacy protection

5 A thin radio shield can be sandwiched between the front cover and the first page. So that whenever the passport is closed - for instance, in your pocket or briefcase - the digital information in the chip cannot be read. The shield will not set off airport metal detectors.



Gemalto, a world leader in digital security

www.gemalto.com

**gemalto**  
security to be free