

# Mobile technology to ease problems of adoption for European ePassports

Modern worries about terrorism and identity theft are placing a heavy burden on national authorities to provide secure passports. This is a requirement that can be met by the use of biometric technology, says **Peter Hradek** of Datastrip, a company at the forefront of development

The market for electronic passport readers has grown steadily since 2003, when the International Civil Aviation Organisation (ICAO) agreed on biometric standards for machine-readable travel documents. To date, more than 20 European nations have integrated biometric facial images into their ePassports. However, the rate of adoption is accelerating: by February 2008, all ICAO member states are expected to have integrated fingerprint biometrics into their ePassports as well.

The ICAO's biometric standard has helped expedite the adoption of fingerprint biometrics in ePassports by clearly defining the requirements that will make them interoperable across all participating borders. For example, an ePassport's critical biometric information must be stored on a tiny RFID computer chip, much like the information stored on smartcards. Like some smartcards, the ePassport calls for an embedded contactless chip that possesses digital signature data to ensure the integrity of the biometric data it contains.

However, as with all new technologies, concerns and challenges surround fingerprint biometrics in ePassports. In addition to the ongoing public debate about personal privacy and security, there have been weak links in its operational effectiveness, specifically when it comes to biometric passport scanning technology – the single most important piece of equipment for points of entry.

## Point-of-entry problems

Though ICAO member countries have fully complied with the organisation's biometric passport standards, other nations are adopting the biometric



passport system at varying speeds and to varying security standards. Some use digital imaging without fingerprints while some use one fingerprint instead of two. Others have yet to implement biometric passports at all and continue to rely on ePassport identification verification based on optical character recognition (OCR).

The importance of passports as a primary form of identification also varies widely across the world. Although passports are growing in importance internationally, many nations still rely more heavily on visas, travel cards, driver's licenses, national ID cards and health cards for identification. As a result, governments need broad point-of-entry solutions that perform multiple functions.

There are also potential technological and operational drawbacks to this technology. A number of ePassport

scanners and readers are available, but not all are created equal. Some feature inferior components that threaten the integrity of the information that is stored and transmitted. For example, 'failure to enroll' is an issue for many fingerprint systems because fingers can be too worn, scarred, dry or moist for certain sensors to accurately read and transmit.

Mobile readers that aren't self-contained are prone to breakage, unreliable reads and other malfunctions. Other potential problems include 'false acceptance,' when unauthorised users gain access to a system, and 'false rejections,' when authorised users are kept out.

## Next-generation mobile solutions

Fortunately, point-of-entry technology has evolved. Mobile, multipurpose technology is paving the way for nations to easily accept

biometric passports, as well as other travel documents.

Self-contained, handheld units have been designed to be carried in person by the guard or border agent, so they go wherever the guard or border agent needs them. This reduces the need to

resolution scanners to accommodate full-page imaging of a passport; contact/contactless smartcard readers; high-resolution fingerprint scanners for instant biometric verification; and large, colour digital touch screen displays that are readable in direct sunlight or low-

**Because border agents, custom officials and travellers are often on foot, the technology needs to be transferable to all locations, and it needs to work reliably in any terrain and under all weather**

purchase multiple stationary units for border crossing, immigration and travel applications requiring 'on the spot' document verification. Handheld readers also provide access control for manned identity verification at entry points, gates, vehicle sides and other remote access areas.

Advanced ePassport readers can also connect wirelessly to back-end systems for biometric identity verification. If we can minimise the number of physical wired connections then mobility restrictions and line breakage can be reduced. Another important feature is extended battery life, which allows guards to carry a unit through a full eight-hour shift without recharging.

In addition, the readers provide identity verification and passport authentication for multiple forms of ID. They read 2-D bar codes, OCR-B, and contact and contactless chips found on identification documents such as visas, travel cards, driver's licenses and national ID cards. This reduces the need for potentially costly investment in multiple readers.

These readers are also designed to support evolving identification document specifications, including ICAO's standards, Border Crossing, US-VISIT, Common Access Card (CAC,) BIODEVII, Eurodac, and other ePassport and ID card scenarios.

The market-leading model features state-of-the-art components which protect the government's investment by ensuring that the technology will be applicable for the foreseeable future. These components include high-

light conditions.

Nations can maximise the return on their initial investment by purchasing mobile passport reader technology that meets the following requirements:

- **Rugged, flexible construction.** A mobile passport reader must be designed to withstand harsh weather conditions and unpredictable movements
- **Field-tested.** Because they perform such a critical function, mobile readers should be field-proven in mission critical environments
- **Long battery life.** Mobile readers that need to be recharged frequently create downtime, downtime which is associated with a backlog of traveller traffic and potential gaps in information security
- **Compliance with government specifications.** Mobile reader manufacturers should be able to provide verification that their products meet the most up-to-date requirements for biometric equipment
- **Easy integration with existing ID management systems.** Open platforms support biometric technologies from multiple ePassport providers
- **Expansion ready.** The ability to connect third-party options via USB, CF, serial and Bluetooth® allows expanded memory and global communications capabilities, increasing the life of the mobile passport reader's usefulness

## A final word

Technological needs and current political limitations add up to a big challenge for European nations making the transition to biometric passports.

As nations secure their borders amid global traffic carrying varying forms of identification, they're tasked with acquiring the technological means to accurately read and verify high-tech and low-tech IDs wherever travellers happen to enter the country. Because border agents, customs officers and travellers are often on foot, the technology needs to be transferable to all locations, and it needs to work reliably in any terrain and under all weather conditions.

Investing in new technology that meets all of these requirements can be a tall order, and one that could threaten the progress of biometric passport adoption. Ultimately, however, there is international agreement about the need for biometric passports, and moves towards their full implementation is inevitable. **ES**



Peter Hradek has over 30 years' experience in the IT industry with multi-national companies such as ICL, Xerox, Harris, Atari, Indigo, NBS and Datacard. During his six years at Datacard he established a CEE office based in Prague and developed a successful distribution network in the region. For the last seven years Peter has worked as Business Development Director for Datastrip Limited, with responsibility for Europe. In this role he has been instrumental in developing relationships with major systems integrators and at the highest levels in both government and the commercial sector. Peter can be contacted via e-mail at [peter.hradek@datastrip.com](mailto:peter.hradek@datastrip.com).