

Biometric technology is increasingly becoming a part of daily life. Maturing technology, greater integration and plummeting costs have fueled greater biometrics adoption across nations and industries.

The BioLook series examines market and technology developments in behavioral and physiological biometric technologies, such as fingerprint, iris, retina, vein pattern, hand geometry, facial recognition, voice, signature and smart cards. Application know-how and solution design will complement systems in numerous sectors, including government, law enforcement, border control, travel, aviation, financial services, banking and health care.

A&S invites you to take advantage of the current trend and digest these special reports, which help foster a more comprehensive understanding of the ever-changing security industry.

P. 130

Biometric Technology in the U.K.: Friend or Foe?

P. 134

BioLook News

P. 136

BioLook Product Showcase

Biometric Technology in the U.K.: Friend or Foe?

Over the last two years, the U.K.'s Identity and Passport Service (IPS) has introduced a range of new procedures and systems to prevent identity and passport fraud. The International Biometric Foundation, based in London, talks us through biometric ID systems in the U.K.

BY TIM COCKERELL

In March 2006, the IPS launched one of its most important counter-fraud initiatives: the biometric passport to detect counterfeit or manipulated documents and to confirm the identity of individuals. The biometric e-passport came with a new design and additional new security features, including a smart chip and antenna, pages with intricate designs, and complex watermarks.

The increasing threat of identity fraud across the globe fuelled the introduction of increased security features in passports, with biometrics a key function. The International Civil Aviation Organization (ICAO) chose facial recognition as the primary biometric technology, with iris and fingerprint as backup (but not compulsory). Its conclusion that the use of biometric information to link a person to a passport helps to counter identity fraud means biometric verification can be used at border controls and to verify the image on a passport renewal application against images held on record.

As the security issue grew more prominent, the U.K. Home Office released "Managing Global Migration" in June 2007, a report outlining the country's plans to manage future migration to the

U.K. The plan detailed in the report includes strengthening borders, enforcing immigration laws, and fast-tracking asylum decisions. Five key objectives, which include securely identifying foreign individuals; working with allied nations to ensure compatible systems; collecting, analyzing, and sharing data; attacking organized immigration crime; and working with migration-route transit countries, have been put in place. All surround the implementation of new technologies, particularly biometric security checks on individuals attempting to travel to the country from their journey's starting point.

It is planned that biometric visas will be issued worldwide by 2008, and migrants from outside the E.U. will be issued biometric ID cards beginning in 2008 in an attempt to combat illegal employment. Meanwhile, at home in the U.K., the U.K. Identity and Passport Service (UKIPS) also needed to allow passport holders to view details held on their new biometric passports, through the provision of self-service biometric readers. Since the UKIPS started issuing biometric chip passports, there has been a legal obligation to enable the public to read the new passport chip. The first solution was an e-Passport reader

attached to a laptop, kept behind the counter at UKIPS offices and requiring a trained operator to use.

HELP YOURSELF

This created unacceptable delays at the counter, so the UKIPS issued a tender for the supply of self-service automated kiosks to be placed in public areas to meet their legal obligations. The final solution, provided by Datacard Group and due to be rolled out this year nationwide, is a kiosk-based solution which improves on the UKIPS' existing system by installing self-service, highly secure units capable of working in a public area.

FEATURES INCLUDE:

The 'Plug-in-and-Go' configuration, which requires no operator training. Kiosks are self-booting; and as they are networked, proper functioning of all kiosks is constantly monitored.

- No user confidential data is permanently stored or recorded in the e-Passport kiosk. Only statistical data is collected and transferred to the server.
- The kiosk runs a customized embedded system, secured against unauthorized access with anti-virus measures and firewalls as defenses against malicious attack.
- Access to the server is via secure password log-on; and application or driver software can be updated through the network, either individually or by kiosk group.



■ U.K. homeland security is serious business indeed.



■ The U.K. is eagerly prompting its citizens to go for ID cards with biometric features.

The kiosks can be configured to check e-ID cards, if and when they are introduced into the U.K. under the National Identity Scheme (NIS). The debate on the scheme's introduction is ongoing, with security and ID management issues on the one hand and civil liberty issues, costs, and the dangers of multiple identity registers on the other. A government body, the Public Private Forum on Identity Management, was set up earlier this year to explore this issue and has as its main thrust, identity assurance (or management). Its objective is to join the various sources of identity on 'the same wheel', drawing on knowledge and experience from both the public and private sectors.

This means managing information from sources including the property dwelling register; business and customer ID registers; and citizens' ID in public services such as the health service, schools and local authorities. The forum's main focus is the NIS, which, it says, would have a gradual inclusion of biometrics through the U.K.'s visa and passport programs. The plan is to issue ID cards by 2009 with three-quarters of the population covered by 2020.

The cards would incorporate an IC chip with personalized data and a digitized biometric template, which in the future could contain face, 10 fingerprint, and possible iris patterns. The biometric elements would be for various controls, including border crossings, law enforcement and anti-fraud in public services. The card is intended to be evolutionary in order that a suite of

services can be built around the initial non-biometric scheme.

BIOMETRIC TRIALS

U.K. public perception surrounding biometrics has also been taken into account and a recent survey conducted by CPP, a card protection company, with 4,000 members of the public, revealed a number of concerns regarding risks surrounding the resourcefulness of fraudsters, privacy issues, and the effectiveness of biometrics. These included surgery, which can alter facial imagery and wear-and-tear of fingerprints.

Biometrics in the home sector are also raising concerns, and a recent Liberal Democrat survey of Local Education Authorities (LEAs) in England has revealed that at least 285 schools are fingerprinting children, but claims they are doing so without any guidance from the government. The survey claims that only a quarter of LEAs had details about the use of fingerprinting in schools, while education authorities did not have information regarding whether parental consent had been obtained in four-fifths of the schools that collect fingerprints. However, the government has said that officials were working with the education technology agency Becta and the Information Commissioner to update guidance on the use of fingerprints.

Campaigners claim the move does not go far enough and are demanding a change in the law to abolish biometric scanners completely from school premises. The Leave Them Kids Alone group said the schools had purchased

the technology from two DFES-approved (Department for Education and Skills) suppliers, suggesting the true figure could be even higher. The collecting of children's fingerprints has also raised fears that children could become accustomed to giving out data about themselves, losing even more of their privacy. Protesting groups also warn that youngsters would be compromised for the rest of their lives if biometric data were to fall into the wrong hands. Unlike compromised PIN numbers, which can swiftly be changed, stolen fingerprint data will be in existence for life.

Elsewhere, on a positive note, the U.K.'s miSense Airport Biometric Security Trials have been completed with favorable results. The trials at Heathrow Airport that used encryption and database security technology have received a positive response from passengers. According to a report released in June, the vast majority of people who participated in the trials would recommend the service

to their fellow travelers. The comprehensive report evaluated the experiences and feedback of the 3,166 passengers who took part in the voluntary trials at Heathrow's Terminal 3 during a 16-week period. The trial is widely regarded as one of the largest and most comprehensive ones of biometrically-enabled access control ever to be conducted in an operational transport environment.

The report found passengers not only accept the need for biometric technology as a means of providing increased levels of security, but also believe it can significantly improve their journey through the airport. The quantitative and qualitative research found that passengers thought that the biometric technology was easy to use and reduced waiting times at security screening and passport control.

Hardware security modules were deployed in the system to generate and protect the unique cryptographic keys that were used to identify and validate each traveler, based on their biometric

information. In addition, the solution's database encryption was used to protect stored passenger information and passport details in order to ensure compliance with data protection legislation. Since passengers want better airport security, but also want to avoid the long delays that may result from increased scrutiny of passengers, the trials have shown that an effective and well-implemented biometric solution can increase protection and also improve passenger experience.

A TASTE OF THINGS TO COME

The jury is still out on the use of biometrics in various schemes across the board in the U.K. public sector. Border security and internal security are a priority and a growing concern; so it seems inevitable that biometrics will feature, in the not too distant future, in key areas such as e-passports and ID cards, once they are introduced.

AS


OFIS

Online Fingerprint Identification System

Ofis can be integrated into Windows-based and Web-based applications. Sample applications written in Visual C++, Visual Basic 6.0, Borland Delphi 7.0, and Active Server Page are provided.

With Ofis technology, you can prevent illegal and unauthorized access to your system by deploying biometrics identification technology.

- ✓ **System Developer**
 - Enhance security of your existing solution
 - Offer fingerprint security as option for your clients
- ✓ **End User**
 - Secured access to server system
 - Easy use without the need for password