

IDNewswire®

Trends in Personal Identification and Biometrics

www.cardtechnology.com

Vol. 3 No. 10 May 14, 2004

Eight U.S. Airports Testing New Access Control Technology Pg. 4
Biometrics will be tested at five airports as part of an eight-airport test of security technologies.

Viisage 1Q Revenue \$12M Pg. 4
Viisage Technology reported a loss of \$1.63 million for the first quarter of 2004 with revenue of \$12.26 million.

Cross Match Unveils Scanner Pg. 4

Identix Acquires Delean Pg. 4

Final Passport Specs Due Next Week From ICAO

Countries around the world are waiting for the final technical specifications for the new electronic passports set to be released later this month.

The meeting of the International Civil Aviation Organization's advisory group on machine-readable travel documents is set to convene next week in Montreal. This meeting could produce the technical specifications that would allow governments to begin issuing chip- and biometric-enabled passports.

It's been almost a year since ICAO first announced the choice of contactless chips and facial

recognition biometrics as standard technologies for the next generation of passports. While some of the difficulties involved in issuing the new documents have been identified, such as compatibility of microchips, there is still work to be done.

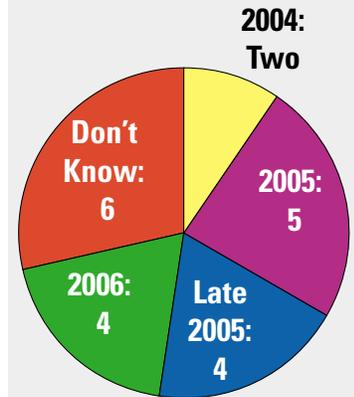
Several countries say they really won't be able to plan until they see the final guidelines, according to letters to the House Judiciary Committee from 21 of the 27 Visa Waiver countries. Some of the letters, which were released by the committee late last month, were also critical of the lack of communication from

the United States.

At the meeting next week, the ICAO committee is expected to approve the technical reports for biometrics, public key infrastructure and the logical data structure for the new passports, says Chuck Baggeroer, an advisor to ICAO who works for Minnetonka, Minn.-based Datacard Group. The logical data structure is how and where information is stored on the chip.

Baggeroer says the plans for the logical data structure have not significantly changed. But the reports on biometrics and PKI, > **Passports**, Page 2

When Countries Will Be Ready To Issue New E-Passports



Future Of Fingerprint Competition In Doubt



More fingerprint biometric vendors were tested in the Fingerprint Vendor Competition 2004, but results may be less useful because several vendors asked that their names be kept secret.

Eleven of the 18 vendors decided to remain anonymous when submitting their algorithms, the mathematical equations that match fingerprint templates, in the latest competition. This compares to eight of the 31 participants choosing to remain anonymous in 2002 and none of the participants in 2000.

In all 43 participants, comprised of vendors, academics and independent developers, submitted 67 algorithms to be tested for the latest competition, compared to 31 total participants and algorithms from the 2002 competition and 11 in 2000. The competition is run by the Biometric Systems Lab at the University of Bologna, the Pattern Recognition and Image Processing Laboratory at Michigan State University and the Biometric Test Center at San Jose State University. (For results, see *Bioscrypt Wins Again*, page 3)

But the future of this contest may be in question, says Davide Maltoni, with the Biometric Systems Lab at the

> **FVC**, Page 3

Transportation Worker ID Proposal Hits The Street

For months, when asked about the proposal for the final phase of the Transportation Worker Identification Credential, officials at the U.S. Transportation Security Administration would say it's "imminent."

Well, imminent arrived Monday as the bid documents were sent to BearingPoint, EDS, Maximus and Northrop Grumman Corp, the systems integrators on the General Services Administration's smart card contract.

Responses to the proposal are due by June 10 and those involved are being tight-lipped as they rush to put together their bids. The most significant aspect of the proposal document, one government official commented, was that it is finally on the street.

The oft-delayed proposal for the prototype phase was originally scheduled to be released in the 2003 holiday season. But it was pushed back due to questions about how the project would be funded, whether ID cards would be issued centrally, and how facilities would share worker data.

The prototype phase is a seven-month contract with a government option for an additional four months, according to the proposal. Various technologies will be tested with 16,805

> **TWIC**, Page 4



Biometrics In The United Kingdom

The UK government currently issues smart cards to asylum seekers that store two fingerprints. Consult Hyperion's John Elliott shows how biometric technology is set to further penetrate government operations.

> **Elliott**, Page 5

GAO Critical Of US-VISIT

The U.S. General Accounting Office released a report critical of some aspects of the first phase of Homeland Security's US-VISIT program.

> **VISIT**, Page 2

> **Passport, Page 1**

which will be used to secure the information stored on the chip, have evolved and are more detailed. Baggeroer doesn't expect any controversy at the meeting next weeks and says the final reports should be approved.

The delay of final specifications is one reason the U.S. State Department and Department of Homeland Security have asked Congress for the e-passport deadline to be pushed to November 2006. Nineteen of the 21 Visa Waiver countries surveyed by the U.S. House Judiciary Committee stated that they would not be able to meet the current Oct. 26, 2004 deadline, with many saying it would be late 2005 before they can issue the new documents.

Last month, Sen. Saxby Chambliss (R-Ga.), chairman of the Senate Judiciary Subcommittee on Immigration, Border Security and Citizenship, introduced legislation that would extend the biometric passport deadline to Nov. 30, 2006. No action has been taken on the bill since it was submitted on April 20.

From the reaction of congressmen at a House Judiciary Committee Hearing last month where Secretaries Colin Powell and Tom Ridge testified about the proposed deadline extension, it's likely the deadline will be extended (*IDNewswire 4/30/04*). To shore up potential security loopholes from the deadline extension all traveler to the United States will be enrolled in the US-VISIT program and submit two fingerprints and a digital photograph before being allowed entry to the country.

If the Visa Waiver countries choose not to participate in VISIT, their citizens would be forced to apply for visas. This is not an appealing option for the approximately 15 million Visa Waiver travelers that visit the United States each year. Nor is it an appealing option for the State Department which would have to add consular officers to staff U.S. embassies and consulates.

Many of the countries surveyed by the House committee stated that they were waiting for guidance from the European Union before starting an e-passport project.

A spokesperson for the EU's Justice and Home Affairs Commission says the newly elected European Union parliament, which

takes office in July, will start examining the passport issue in late August or early September. Some of the 25 members of the European Union will begin issuing the new documents in late 2005, he says.

The EU legislation proposes that the new passports store the passport holder's digital photo and two fingerprint images, the spokesperson says. The ICAO recommendation is for a photo to be stored on the chip, and leaves open the option for countries to add fingerprint or iris biometrics.

The EU is also planning on using contactless chips in its Schengen Visa. The chips will also store a digital image and two fingerprints of the visa holder, the spokesperson says. The Schengen Visa allows individuals to apply for one document and have access to the 15 countries that accept the document.

While it will be late 2005 before EU countries are ready with the new passports, Australia and New Zealand state that they could meet the Oct. 26, 2004, deadline. "Contracts are being finalized for the supply of chip-enabled passport books and we are in the design phase for the operational systems to support chip personalization," New Zealand Ambassador John Wood states in his letter to the committee.

But meeting the deadline would still be subject to the approval of technical reports next

week by ICAO, availability of chips and readers, and successful operational and durability testing of the new systems.

Australia stated that it would be ready to produce passports by the deadline, but was being held up "because the United States has not yet decided on its own passport reading/border infrastructure," the letter from Australian Ambassador Michael Thawley says.

Thawley's letter went on to say that Australia is "reluctant to proceed" until the United States has the technical infrastructure in place. "Especially as Australia has made a considerable effort to be able to abide by the new U.S. requirements, we would hope to avoid a situation where Australians were disadvantaged because of the failure of other countries to meet the U.S. deadline or because the U.S. agencies have not installed the infrastructure necessary to implement U.S. requirements," the letter states.

New Zealand was also one of two countries, Iceland being the other, which stated that the State Department and Homeland Security did not provide them with enough information about the new passport program. "We believe that appropriate United States authorities should have consulted Visa Waiver countries during the drafting of the legislation to ensure the full impact of the proposed changes were understood," the letter states.

Wood says that New Zealand was not officially informed about the 2002 legislation affecting passports until months after it was enacted, and says his country has received most of its information through ICAO. <

'Contracts are being finalized for the supply of chip-enabled passport books and we are in the design phase for the operational systems to support chip personalization.'

**- John Wood,
New Zealand Ambassador**

GAO Report Critical OF US-VISIT

The U.S. General Accounting Office released a report Tuesday critical of some aspects of the first phase of the Department of Homeland Security's US-VISIT program.

Homeland Security deployed VISIT at 115 airports and 14 seaports on Jan. 5. At that time it began collecting two fingerprints and a photo from all visa-carrying travelers to the United States and running them against a watch list. After Sept. 30, residents of the 27 Visa Waiver countries entering the country will have to enroll in the border control program.

Most reports on the first phase of VISIT have been positive. Several sources say the enrollment process adds some time to the entry procedure, but hasn't been unduly long. False match rates, travelers incorrectly identified as being on the watch list, have been

less than .1% and the system has netted 300 arrests.

The GAO report criticizes Homeland Security for inadequate testing and undisciplined management controls of the first phase.

But one industry observer says it's rare that a final test plan is ready before testing begins. "Usually, you're under tremendous time and budget constraints and you make do with the best you have at the time," the observer notes. "In any case, this sure seems like 'small change' considering how much DHS had to get up and running prior to (the deadline)."

In its reply to the GAO, Homeland Security noted that it is working to approve the management of the program. <

> **FVC, Page 1**

University of Bologna. If there is funding there will be a FVC 2006. However, the testing of biometric systems may be going in another direction. Also, some U.S. government officials and systems integrators says they pay only passing attention to these tests because of the anonymity of many of the vendors and the fact that they already perform their own tests.

Maltoni says the original goal of the competition was to trace the progress of fingerprint biometrics. "The aim of FVC is tracking the state of the art and not promoting or shaming any vendor or organization," he says. "I believe that in the future third-party evaluation will become mandatory for certain applications, and then every vendor will be obliged to (be named)."

Common Criteria testing is one direction biometrics vendors may be forced to go for testing. "Probably the future of biometric evaluation will be inside 'Common Criteria,' but nowadays the cost of a serious third-party evaluation is high

and the current market and players cannot afford it," Maltoni says.

The Common Criteria are international standards for evaluation of IT security products, and can be applied to products as varied as firewall software and smart cards. The testing makes sure that technology is evaluated using the approved methodology, and provides third-party verification of vendor claims. Common Criteria testing can cost \$50,000 for entry-level tests and up to \$500,000 for the more advanced testing, experts say.

The U.S. Department of Defense does its own biometric testing through the Biometrics Management Office and Biometrics Fusion Center and does not comment on tests the agency is not involved with, says a spokesperson for the Biometric Management Office. "While we are aware of such private industry testing initiatives, the BFC tests biometric products for DOD applications, so private industry testing guidelines do not necessarily correlate with those," the spokesperson says. "The DOD

has unique needs and requirements that often warrant more rigorous testing."

The agency, however, is not opposed to leveraging outside testing activities to reduce duplication of efforts, the spokesperson says.

One large government systems integrator, who did not want to be named, reviewed the results and says the lack of major vendor participation "doesn't make it too useful."

It isn't necessarily the device's algorithm that makes one product superior to another, the integrator says. The ease of integrating the device with other products and the ease of use for the end user is equally important.

"A poorly designed device with a good algorithm behind it will generally give poor results," the integrator says. For example, if it's not easy for the user to place a finger on the sensor the system won't work well. "Form factor and product design are very important. If they don't match up to what the application requires, then the products generally won't work so well." <

Bioscrypt Wins Again

The big winner in the Fingerprint Verification Competition 2004 is Toronto-based Bioscrypt Inc.

The fingerprint vendor, which was also the top finisher in the 2002 contest, which awarded eight gold medals, seven silver medals and two bronze medals in the latest competition's open category. Medals were awarded based on results in 20 categories, such as error rates, enrollment time and matching time.

Finishing second overall in the open category was Russian-based Sonda Ltd, followed by the Institute of Automation at China's Academy of Sciences. Lithuania-based Neurotechnologija Ltd. and South Korea-based Suprema Inc. round out the top five finishers. The open category has no limits on memory requirements or template size. For testing purposes, response time of algorithms is limited to 10 seconds for enrollment and 5 seconds for matching.

Bioscrypt also performed well in the light category, finishing third overall. The light category is intended for algorithms with low computing needs, limited memory usage and small template size. The maximum time for enrollment is 0.5 seconds and the maximum time for matching is 0.3 seconds.

Independent developer Ji Hui from China took first place in the light category with 10 gold medals, eight silver and six bronze. Suprema finished second, China-based fingerprint vendor Beijing HanWang Technology Co. Ltd took fourth and South Korea-based Testech Inc. was fifth.

One fingerprint vendor that had participated in previous FVC competitions and performed well was Sagem Morpho. The company decided not to participate this year because the company's customers are relying on testing from the U.S. National Institute of Standards and Technology. <

**What's the secret
to regaining control
of authentication?**

**Click
Here**

**Download
Datkey's Identity
and Access
Management
Success Kit**

> **TWIC, Page 1**

workers on both coasts. The ID card could eventually be issued to 12 million transportation workers across the country.

Locations in the East include the Delaware River and Bay areas near Philadelphia and MacArthur Field in Long Island, N.Y. In the West, tests will take place at Los Angeles International Airport and at ports in Oakland and Long Beach. Florida's 14 deepwater ports and the Florida Department of Highway Safety

and Motor Vehicles will also participate in the prototype phase.

This final testing phase will also evaluate contactless chip technology along with fingerprint and hand geometry, the documents state. After this phase concludes, the TSA has said it will start a full rollout of the TWIC.

Almost from the start, the TWIC program has been a political football. Sources say several political issues held up the ID, including which representative's district would get con-

tracts, a common source of time-consuming wrangles, and discussion of whether optical stripe or smart card technology should be used.

Another concerned group are the 12 million transportation workers. Each of them would have to undergo a background check to get the card, and workers without the legal right to live in the United States or those with criminal convictions could lose their jobs as a result. <

Eight U.S. Airports Will Test Security Technologies

Biometrics will be tested at five U.S. airports as part of an eight-airport test of security technologies, the U.S. Transportation Security Administration announced this month. Fingerprint biometrics will be tested at facilities in Boise, Idaho; Newark, N.J.; Fort Myers, Fla.; and Tampa, Fla. T.F. Green State Airport in Providence, R.I., will test iris biometrics. In some cases, the biometrics will be tested along with ID cards that use radio signals so cardholders can identify themselves by waving their cards past door controllers. Also to be tested are video surveillance and "anti-piggybacking" systems for preventing a second person from entering a secure facility behind an authorized individual. This Access Control Pilot Program is separate from similar tests of ID card technologies TSA is performing in preparation for issuing a smart card ID, known as the Transportation Worker Identification Credential, to some 12 million U.S. transportation workers. U.S.-based systems integrator Unisys Corp. is to perform the access control tests over a period of 20 months under a \$17 million contract awarded last fall. The eight airports announced last week are part of a first phase of tests

due to be concluded by December. Based on the results from this phase, Unisys will select technologies that will be piloted in the second phase. <

Viisage 1Q Revenue \$12M

Billerica, Mass.-based Viisage Technology Inc. reported a loss of \$1.63 million with revenue of \$12.26 million for the first quarter of 2004, the company reported this month. Revenue increased 33% from \$8.16 million while losses narrowed by 31% from \$2.37 million during the same period a year ago for the facial recognition and identification vendor. Viisage announced in February that it was purchasing Arlington, Va.-based Trans Digital Technologies, which provides passport production services to the U.S. State Department. Viisage's stock price has increased 43% since announcing the acquisition, from a close of \$5.36 on Feb. 17, when the buy was announced to Tuesday's close of \$9.33 a share. <

Cross Match Unveils New Scanner

Palm Beach Gardens, Fla.-based Cross Match Technologies Inc. last week released a new full handprint scanner based on requirements from the California law enforcement community, the company announced. Cross Match developed a sys-

tem with features specifically suggested by forensic examiners and identification officers. The ID 2500 has a curved sensor design that can capture a full handprint in one image, including the difficult to capture palm pocket without having to prepare or manipulate the subject's hand. Palm prints make up 30% of all crime scene prints that are lifted by law enforcement. Full hand and palm prints are increasingly being captured in the booking process for use in law enforcement criminal database matching and for scrutiny by forensic examiners, the company says. <

Identix Acquires Delean

Minnetonka, Minn.-based Identix Inc. last week announced the acquisition of Delean Vision Worldwide Inc., provider of skin biometric technology. Delean's technology uses surface texture analysis, which extracts a unique characteristic of the skin structure known as the "skinprint." The skinprint can be used on its own as a biometric identifier, or it can be fused together or incorporated with facial or fingerprint biometric templates to improve the accuracy of those technologies. Identix issued Delean 675,000 shares of stock, valued at approximately \$4.15 million, for the acquisition. <

Editor

Zack Martin

zachary.martin@thomsonmedia.com

Group Editor

Donald Davis

don.davis@thomsonmedia.com

Contributing Editor

Michael Fenner

michael.fenner@thomsonmedia.com

Advertising Sales

Jim Baker

james.baker@thomsonmedia.com

Publisher

Andrew Rowe

andrew.rowe@thomsonmedia.com

Group Publisher

Timothy Murphy

timothy.murphy@thomsonmedia.com

Thomson Media: Pres. & CEO: James M. Malkin; Pres./CEO Publishing & Conference Group: Bruce Morris; CFO: William Johnston; SVP, Operations: Celie Baussan; CTO: Raymond Ouellette; VP, Business Development and Strategy: Greg Mazzanobile; VP, Human Resources: Robert DeNoia.

IDNewswire® is published biweekly by Thomson Media. Visit our Web site at <http://www.cardtechnology.com>. The contents of IDNewswire are, and remain, the property of Thomson Media. Reproduction or forwarding of this publication is strictly prohibited. Individuals who infringe on these rights will be prosecuted to the full extent of the law. IDNewswire is a registered service mark used herein under license.

Subscribers who want multiple copies of IDNewswire should contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com for information. The annual subscription rate is \$695. For subscription, renewal or licensing information, please contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com.

For advertising information, contact Jim Baker at 312-983-6179 or james.baker@thomsonmedia.com. Editorial offices are located at 300 S. Wacker Drive, 18th Floor, Chicago, IL 60606. Telephone: 312-983-6168. FAX: 312-913-1365.

© 2004 The Thomson Corporation and IDNewswire. All rights reserved.

How Biometrics Will Penetrate UK Government Operations

John Elliott is a principal consultant with UK-based Consult Hyperion, an independent consultancy firm that specializes in secure electronic transactions. Consult Hyperion has helped a number of governments with the specification of and launch strategy for national ID systems.

Smart card and biometric technologies have been available individually for many years. We worked on our first smart card project over a decade ago and we have had biometrics systems in our laboratory for the last three years.

However, when used together, these technologies are showing great potential for ID applications. For example many national ID cards such as the one in Hong Kong being rolled out are storing biometrics on the smart card chip and the UK government Application Registration Card (ARC) being given to asylum seekers stores fingerprints on the chip.

All the things you are

The number of proposed biometric technologies increases daily. Starting with the well-established fingerprint systems to the more esoteric, such as ear print (commonly left at crime scenes in Switzerland, apparently), gait (the way you walk) and

body odor. How should you go about deciding the most appropriate technology for any given application?

Biometric technologies are useful means of identifying people against databases or verifying that they are who they say they are. A small number of technologies are good at the former function (e.g. iris and fingerprint), whereas many are capable of verification against a biometric template stored on a token, such as a smart card or travel document.

There are many different applications for these two functions within UK government, such as:

- Verifying that a document holder is the legitimate document holder by matching them against a biometric held within the document.
- Preventing duplicate applications for documents by searching against the database of currently issued documents.
- Preventing people holding different identities on different systems (e.g. driving license vs. passport) by sharing and cross-checking biometric data.

Ensuring that only legitimate members of staff have access to secure areas and systems.

The complexity of the individual require-



ments of each application coupled with the speed of advance of biometric technologies means that there is no single best biometric for all applications.

Who goes there?

Currently around 90 million passengers arrive at UK ports of entry each year and this is expected to increase by 5% each year. UK Immigration Service (UKIS) staff are under considerable pressure at the ports to both detect undesirables and at the same time facilitate the passage of bona fide passengers.

It is hoped that biometrics can be used to aid this effort and allow UKIS staff to be deployed where the risks are perceived to be highest. Identifying wrongdoers at the point of arrival is like looking for a needle in a haystack. Increasingly, the preferred approach is to push the borders abroad and prevent illegitimate travel to the UK before it begins. The idea is to process 'advance passenger information' so as to detect malefactors before they begin their journey to the UK.

The long arm of the law

Within the Home Office, the Immigration and Nationality Directorate (IND) runs the asylum screening units where asylum seekers apply after arriving in this country. In order to cope with the (until recently sharply increasing) numbers of applicants, IND have been collecting fingerprints at the point of application and automatically matching them against databases.

IND runs the highly successful Immigration and Asylum Fingerprint System that enables all UK asylum seekers to be recorded so as to track them during the period before either they become legitimate refugees or their claim is rejected and they leave the country. Checking against this database allows spotting of duplicate applications by those seeking to commit benefits fraud.

> Elliott, Page 6

UK Government Biometric Applications

- **Verifying that a document holder is the legitimate document holder by matching the individual against a biometric held within the document.**
- **Preventing duplicate applications for documents by searching against the database of currently issued documents.**
- **Preventing people holding different identities on different systems (e.g. driving license vs. passport) by sharing and cross-checking biometric data.**
- **Ensuring that only legitimate members of staff have access to secure areas and systems.**

> **Elliott, Page 5**

Fingerprinting is well known as a key tool in criminal justice activities. Traditionally it has been used by criminal justice organizations. The Police IT Organization (PITO) provides IT to UK Police forces. PITO runs the National Automated Fingerprint Information System (NAFIS) that allows the checking of fingerprint data by various law enforcement agencies.

The PITO fingerprint database can also be cross-checked in order to spot known criminals applying for asylum. Currently this checking is carried out with manual intervention, but a project is underway to automate cross-checking between IAFS and NAFIS. A European system (EURO-DAC) went live in January 2003 and allows EU states to exchange asylum seeker fingerprint data in order to detect 'asylum shopping'. Asylum seekers found to have previously sought asylum elsewhere in the EU can be returned to their first country of claim.

You have the right to remain...

The UK Home Office is currently considering introducing a national ID card. The decision to go ahead with a UK ID card has been taken. A ten-year road map was announced in November 2003. The recent Madrid bombing has led to an accelerated plan which could see voluntary cards rolled out by 2007 and a Parliamentary vote on compulsion taken soon after.

If the ID card scheme runs, there are likely to be three types of smart card: passport; driving license; and one for anyone with the right to remain in the UK who does not have one of the other two. The chip would contain a biometric for verification of the cardholder and this would be either fingerprint or iris since these are the only two currently capable of performing the one-to-many searches required to ensure that any given person is only allowed to enroll once.

A token gesture

It might seem like a two-horse race between fingerprint and iris for the majority of applications that require acceptable performance (speed and accuracy) when matching against large enrollment databases in the millions. However, an alternative way of addressing the problem is to

have the user carry a tamper-resistant hardware token (such as a smart card) containing their biometric template. Rather than identify people by matching against the whole database, instead you can verify their claimed identity against their token.

As already mentioned, IND's ARC being used with applications for asylum has proven this approach to be highly successful. But who else is going to go to the bother and expense of issuing these tokens, especially in the current economic climate? Interestingly enough, it is likely that the UK will have them in a couple of years in the form of travel documents such as passports, visas and ID cards.

The International Civil Aviation Organization (ICAO) is the main body making recommendations for travel document standards. After the September 11, 2001, terrorist attacks, the U.S. passed laws requiring nations with visa waiver agreements for entry to the U.S. to begin issuing travel documents containing biometrics and complying with ICAO standards.

In March 2003, ICAO passed the New Orleans Resolution stating that for verification purposes, standardized digital facial images are recommended as the globally interoperable biometric for machine-readable travel documents. In addition, standardized fingerprint and iris images may, optionally, be stored for identification and/or verification purposes.

ICAO encourages initial biometric travel document deployments to use contactless integrated circuits of sufficient capacity to store additional machine-readable data and biometrics. Alternative technologies such as 2-D bar codes and magnetic

stripes would not have the capacity to store facial images as well as fingerprint and/or iris images.

I'll show you mine if you show me yours

Data exchange is one of the major considerations when selecting which biometric to use for a given application. The only way to ensure interoperability of two biometric systems is for them to collect the same type of biometric data (fingerprint or iris or facial, etc.) and store it according to a common format.

At present standards relating to biometrics are few, and at the time of setting up a system, it is not possible to know who you might want to exchange data with in the future. For example, Police might exchange data with Immigration, but they might both wish to co-operate with

Customs in the future or the Prisons Service. Therefore many current systems prefer to store the complete biometric images captured at enrollment, rather than simply storing the templates derived to suit one particular system's matching algorithms.

For 'borders overseas' programs to be successful, it will be necessary to integrate and share data with both national governments for tracking of criminals and commercial enterprises, such as carriers (airlines, train and ferry companies, etc) and travel agents dealing with bookings.

The UK government recognizes the need for ID technologies and is moving quickly to stay at the leading edge – smart cards together with various biometrics will be the way forward, backed up by other biometrics such as fingerprint to allow for enrollment checks against existing criminal justice databases. <

'The UK government recognizes the need for ID technologies and is moving quickly to stay at the leading edge – smart card together with various biometrics will be the way forward, backed up by other biometrics such as fingerprint to allow for enrollment checks against existing criminal justice databases.'

For more information contact John Elliott at john.elliott@chyp.com, or +44 131 337 1379.