

Biometric Technology Today

March 2005

ID

Seafarer's biometric ID card sets sail

One of the first global biometric identification systems is about to roll into action in a bid to enhance security in the international shipping industry. Up to 1.2 million seafarers will potentially be affected by the new scheme, which will see a biometric-based card being issued to enable the positive identification of seafarers.

The International Labour Office (ILO) said that the *Seafarers' Identity Documents Convention, 2003 (No. 185)* has so far only been ratified by France, Jordan and Nigeria, but that this number of countries exceeded the minimum of two that were needed to

ratify the convention before it could come into force.

The ILO is a group that formulates international labour standards in the form of conventions and recommendations. The negotiations that concluded with the adoption of Convention No. 185 were held in response to the need for greater global security, while guaranteeing the rights of workers in the shipping fleet, which handles nearly 90% of world trade.

In March 2004 the Governing Body of the ILO approved standards for converting two fingerprints into a biometric template to be stored in an internationally

standardised 2D barcode, which would be printed on the Seafarers' Identity Document (SID).

One basic requisite for the SID's biometric identification system was global interoperability, meaning that the fingerprint information issued in one country can be read correctly by equipment used in another. The ILO announced in December 2004 that after a six-week test involving 126 volunteer seafarers from 30 countries, two biometric products have already met the requirement of global interoperability and thus can be used to issue the new SIDs.

Continued on back page...

3D FACE

A4 Vision adds additional high-profile strategic investors

3D facial recognition technology company A4 Vision has announced two more high-profile strategic investors, boosting total investment in the company to well over US\$28 million.

In-Q-Tel and Motorola have been named by the company as the latest investors, following on from a long list announced late last year, including Logitech, TAKO Ventures; FusionTech, a subsidiary of Singapore Technologies Engineering; NTT Leasing; and Stanford University. Following the funding round in the latter half of 2004, investment in A4 Vision was boosted by US\$17.6 million to reach a total of US\$23.3 million. This latest news sees In-Q-Tel add another 'couple of

million' and Motorola pump in US\$4 million.

Grant Evans, CEO of A4 Vision told *Btt*: "This isn't just about money. We are looking for a go-to-market strategy. Each of our strategic investors is in some way involved with A4 Vision, whether that's through a product development relationship or a licensing agreement. We expect many developments to come to fruition in 2005."

In-Q-Tel is a private, non-profit enterprise funded by the United States' Central Intelligence Agency (CIA). Its role is to connect with technology companies,

Continued on page 2...

Contents

Application news	5
Product news	4
Company news	6
Feature:	7
Security technologies to the fore	
Survey:	9
Sizing up silicon sensors	
Regulars	
Events	5
Business Watch	6
Comment	12

ISSN 0969-4765/05 © 2005 Elsevier Ltd. All rights reserved.

This journal and the individual contributions contained in it are protected under copyright by Elsevier Ltd, and the following terms and conditions apply to their use:

Photocopying

Single photocopies of single articles may be made for personal use as allowed by national copyright laws. Permission of the publisher and payment of a fee is required for all other photocopying, including multiple or systematic copying, copying for advertising or promotional purposes, resale, and all forms of document delivery. Special rates are available for educational institutions that wish to make photocopies for non-profit educational classroom use.



Copyright Notice

This newsletter and the individual contributions contained in it are protected under copyright by Elsevier Ltd, and the following terms and conditions apply to their use:

Permissions may be sought directly from Elsevier Rights & Permissions Department, PO Box 800, Oxford OX5 1DX, UK; tel: +44 (0)1865 843830, fax: +44 (0)1865 853333, e-mail: permissions@elsevier.com. You may also contact Rights & Permissions directly through Elsevier's home page (<http://www.elsevier.com>), selecting first 'Support and contact', then 'Copyright and permission'.

In the USA, users may clear permissions and make payments through the Copyright Clearance Center, Inc, 222 Rosewood Drive, Danvers, MA 01923, USA; tel: 978 7508400, fax: +1 978 7504744, and in the UK through the Copyright Licensing Agency Rapid Clearance Service (CLARCS), 90 Tottenham Court Road, London W1P 0LP, UK; tel: +44 (0) 207 436 5931; fax: +44 (0) 207 436 3986. Other countries may have a local reprographic rights agency for payments.

Derivative Works

Subscribers may reproduce tables of contents or prepare lists of articles including abstracts for internal circulation within their institutions. Permission of the publisher is required for resale or distribution outside the institution.

Permission of the publisher is required for all other derivative works, including compilations and translations.

Electronic Storage or Usage

Permission of the publisher is required to store or use electronically any material contained in this journal, including any article or part of an article. Contact the publisher at the address indicated.

Except as outlined above, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publisher.

Address permissions requests to: Elsevier Rights & Permissions Department, at the mail, fax and e-mail addresses noted above.

Notice

No responsibility is assumed by the publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made.

Although all advertising material is expected to conform to ethical (medical) standards, inclusion in this publication does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

02265 Printed by Mayfield Press (Oxford) Ltd.

Continued from front page...

such as A4 Vision, in an attempt to develop technologies that could pay out in superior intelligence capabilities. Evans told *Btt* that A4 Vision is already actively involved in development of special products for the CIA.

Motorola, meanwhile, is the owner of Printrak, a company heavily involved in the production of automated fingerprint identification systems (AFIS). The combined use of 3D facial and AFIS systems is something that would not come as a surprise, with a variety of ideal scenarios, from law enforcement to civil ID. Announcements between A4 Vision and its remaining investors remain the subject of speculation, with Logitech being a leading supplier of video conferencing cameras, and NTT Leasing being the main investment arm for NTT.

A4 Vision is upbeat about the prospects for 3D facial recognition. It says that many traditional 2D vendors are now being pushed to look at 3D, the US government is putting massive funding into researching the technology and there is a trend towards fusing two-dimensional face engines with 3D capabilities.

A4 sees its strengths in being able to provide all of the system, from cameras to algorithms and applications. The company also believes that the cost of its cameras are now highly competitive, selling for between US\$1,000-2,000.

Contact: Suzanne M. Matick at A4Vision, Tel: +1 831 479 1888, email: smatick@earthlink.net

More 3D face news

As well as A4 Vision's funding announcements there has been a spate of other news during the last month, such as the introduction of new 3D standards (see p4) and the acquisition of Genex Technologies by Markland Technologies (see p6).

Meanwhile, Geometrix has announced the launch of its *ActiveID Biometric Identity System*, featuring its *FaceVision* 3D facial recognition technology. The supplier says that the system includes a passive 3D biometric camera, plus a scalable and customisable set of software products for identity management including multi-biometric enrollment, verification against a claimed identity, and identification of an individual within a database.

PASSPORTS

Belize passport authorities make biometric checks

Citizens of Belize in South America are being asked to undergo biometric checking procedures before being issued with new machine-readable passports. The Belize Ministry of Home Affairs, in cooperation with the International Organization for Migration

(IOM), said that the new system, which has been under development for around two years, is now operational and requires citizens to provide fingerprint and facial images to ensure they are not attempting to fraudulently obtain more than one passport document.

German face recognition technology provider Cognitec Systems and Bioscrypt, a US fingerprint technology company, along with systems integrator 3M announced that they are working together to provide the passport issuance system for the Government of Belize.

According to Gareth Murillo, senior immigration officer and acting director, Immigration and Nationality, Belize: "We are pleased to be deploying a state-of-the-art system for the issuance of our passport. We believe the strong security that is built into our issuance process will ensure our document is trusted at borders around the world."

The system will be built using the web-based *Identity Document Issuance System* from 3M. Data capture will be decentralised, taking place at seven sites across Belize as well as in seven Belizean Consulate locations. Document personalisation and issuance will be centralised at two sites, and the passports will be produced using the *Personalization Solution* from 3M.

Cognitec's facial recognition and fingerprint matching technology from Bioscrypt is being used to check each new applicant against all applicants in the passport database to ensure they have not previously applied for a passport under a different identity. The combination of the face and two fingerprints allows rapid automated searching, and a very small chance of an incorrect match. The issuance system operator will be provided with the results of the search, and will make the final decision on whether two identities in the database represent the same person.

The new system is not producing biometric ePassports. As Murillo pointed out in a local media report: "There will be nothing stored on the passport. The passport has only printed information, which most currently do, and the information will be stored in a database. The sole purpose of storing that information is preventing an applicant from getting a passport under different identities."

According to a Cognitec source this is just one of many passport projects the company is involved in. The facial recognition technology company's capabilities include:

- acquisition of ISO standardised facial photographs for ID documents;
- search for fraudulent duplicate entries in large databases for visa, passport, or drivers' license issuance;
- identity verification at the border using new biometric passports;

- background checks at the border, comparing facial images against unwanted lists.

Contact: Jürgen Pampus at Cognitec Systems,
Tel: +49-351-862-920, Fax: +49-351-862-9210,
Email: pampus@cognitec.com

FACE RECOGNITION

Identix smiles at the camera

Multi-biometric company Identix has announced that a part of its facial recognition software is to be integrated into a range of cameras from one of the world's leading suppliers, Nikon. The deal will potentially see the face-finding capabilities of the supplier's FaceIt engine being deployed in millions of COOLPIX camera units, in what Identix describes as the largest deployment of its technology in a commercial application to date.

Nikon and Identix worked in partnership to develop *Face-priority AF* (Autofocus), a photography feature that uses the face finding technology embedded within Identix's FaceIt engine to automatically detect human faces in the scene, and to automatically adjust camera settings – such as focus and gain – to produce optimal images of the faces irrespective of background, lighting or other viewing conditions.

The feature will initially be available with Nikon's *COOLPIX 7900*, *COOLPIX 7600* and *COOLPIX 5900* models, although the licensing agreement covers production for the entire COOLPIX camera line, which is expected by Nikon to run into many millions of camera units.

According to Identix president and CEO Joseph Atick, the face finding technology works in real time and it is able to control the auto-focus even if the person moves or the photographer recomposes the picture. He commented: "With this feature photographers are able to automatically adjust camera settings faster than any human capability allows."

Financially the deal is expected to generate significant revenue. Atick commented: "We believe our agreement with Nikon, which will generate meaningful US dollar royalties for Identix, represents the opening of an entirely new frontier – the licensing and integration of our enabling biometric technologies for mass market consumer applications. We expect to continue to see similar unique and totally new applications with commercial appeal begin to generate meaningful opportunities for the potential generation of material revenues in the commercial and consumer vertical sectors."

Contact: Frances Zelazny at Identix,
Tel: +1 201 332 9213, email:
frances.zelazny@identix.com

DSV

Sign here for insurance and your coffee

Israeli dynamic signature verification company WonderNet has announced a number of new projects using its Penflow technology.

The first project is being implemented in Israel by insurance broker Maalot. It has installed more than 130 kiosks in a variety of locations, predominantly banks, which allow new customers to connect via an integrated handset to its call centres and instantaneously take out an insurance policy. Each kiosk is equipped with a signature tablet that allows the customer to sign insurance documents in a legally binding transaction.

Alex Herman, vice president of sales and business development at WonderNet told *Btt*: "This is an ideal solution in the banking environment. For instance, when a customer decides to take out a mortgage, they also need insurance. Now this process can be made almost instantaneous by allowing customers to move over to the in-branch insurance kiosk and instantaneously sign insurance forms using the biometric technology."

Herman said that most of the banking locations are within Bank Leumi branches – a company with which WonderNet already has a large electronic signature project. The project went live at the start of the year.

The project does not perform real-time verification, although the dynamic properties of the customer's signature are stored in case verification is needed at a later date. However, Herman said that another project about to go live in Hong Kong does use the dynamic properties of the signature in a true verification application.

In this instance the trial project is being implemented in a popular coffee shop. The idea is that customers will be able to leave their cash, or special coffee shop payment card, behind, and instead simply sign their name in order to pay for their coffee. According to Herman, this web application connects the coffee house to a central system, which verifies the validity of the signature and deducts the appropriate amount from the customer's dedicated account.

Although this is a trial in a single location, Herman said the feedback has been positive and the business model could be attractive enough to warrant a wider scale roll out.

Contact: Alex Herman at WonderNet,
Tel: +972 3 9036860, Fax: +972 3 9304925,
Email: alex@penflow.com

Application news

- North Carolina-based **Lowes Food Stores** is to begin offering a biometric payment option to its customers using technology from **BioPay**. To enrol, the customer gives the clerk their driver's license information, which is entered onto BioPay's database. The customer's index fingers are also scanned. The customer's preferred bank account is recorded, as well as rewards card and age information. Once enrolled, the customer can pay at any BioPay-enabled retailer in the USA. **Lowes Foods** customers in the North Carolina market have already begun using BioPay's *Paycheck Secure* product to cash payroll cheques.

- **General Dynamics Advanced Information Systems** has selected the *IWS Biometric Engine* from **ImageWare** as the platform for a federal biometric pilot project that will test the viability of increased accuracy when using multiple biometrics, including face, finger and iris, within a single integrated environment. The *IWS Biometric Engine* is technology agnostic, so enabling users to employ biometric devices and algorithms from any vendor.

- **BIO-key International's** technology is being used in a biometric-based identification solution that automates various activities at **Visitation BVM Catholic School** in Philadelphia, PA. The school has installed **identiMetrics'** software platform, *identiFi*, which uses BIO-key's *WEB-key* technology. In order to identify students and take daily attendance, a fingerprint reader scans the students entering the classroom at the start of the day. The school has also linked attendance to its cafeteria to allow it to plan its food service more efficiently.

Product news

- **Datastrip** has added three swipe-style models to its *DSVII* family of handheld ID card/biometric readers. The new models add decoding of swiped 2D bar codes, OCR-B data, and/or partial or full-page passports to the functions previously available, including the ability to read both contact and contactless smart cards and to instantly match a live fingerprint to a biometric template with the same unit.

- **Bird**, one of China's top mobile phone manufacturers will launch a phone with an integrated fingerprint verification system, designed to allow internet-based transactions. The manufacturer purchased the technology from a research team at the **Chinese Academy of Sciences (CAS) Institute of Automation**. Costing only about US\$6 to add to the phones, the company will reportedly begin equipping its high-end products later this year.

- **Aprilis** has launched a range of AFIS fingerprint capture devices with improved moisture-discrimination. The three new imagers – *HoloSensor HS-500*, *HoloSensor HS-500L* and *HoloSensor HS-1000* – are designed to acquire fingerprint images at 500 and 1000dpi with image areas up to 2 x 2 inches. The **Massachusetts State Police Crime Lab** recently took delivery of an Aprilis system, the company claims.

- Israeli company **i-Mature** has announced technology that could verify whether a user is a child or an adult by analyzing the bone in a person's finger. Ultrasound waves are used to check more than a dozen biometric attributes. I-Mature has a prototype and recently entered a partnership with **RSA Security**.

3D FACE/STANDARDS

3D face standard finally on the way?

An international standard for three-dimensional facial recognition has moved one step closer with the news that a proposal to amend the existing US national standard for facial recognition has been accepted by the International Committee for Information Technology Standards' (INCITS) M1 Committee on Biometrics.

The new draft standard was prepared by A4 Vision and supported by a sizeable alliance including ID Technology Partners, Unisys Corporation, Logitech, Oracle and Motorola.

The M1 committee voted in favour of the proposal to amend the existing US standard and agreed to submit the proposal to the International Standard Organization (ISO/IEC JTC 1 /SC37/WG3) for acceptance as an amendment to the corresponding international standard. A4Vision's CTO Artiom Yukhin and Identix's CTO Paul Griffin were nominated as co-editors of the amendment.

The creation of a 3D facial recognition standard is expected to stimulate demand for the technology, particularly in the area of immigration, where there could be great advantages to using 3D images in terms of increased accuracy (especially if fused with a 2D face engine, so as to allow the handling of legacy database images). However, there has been a reluctance to do this so far, in part because of a lack of standardisation.

According to Yukhin, who developed the original proposal: "Because 3D hasn't been defined for vendor implementation, adoption of 3D facial imaging has been impeded. Though the past 12 months have seen global interest in 3D face recognition technology for security applications and in models which use 3D information with traditional 2D images or photos to achieve greater accuracy, lack of standards has delayed potential growth."

The standard provides a great deal of information for vendors wanting to use 3D face systems. For example, the standard gives the formula on how to create a wire mesh of a person's face in VRML format, and crucially it also divulges how to take the resulting 300 KB image and compress that down to a 3-5 KB image - comparable to the template size of a fingerprint image. This is without any compression loss and at a precision of 0.1 mm, the supplier claims.

Contact: Suzanne M. Matick at A4Vision,
Tel: +1 831 479 1888, email: smatick@earthlink.net

ASSOCIATION NEWS

EBF and TeleTrusT to partner

The European Biometrics Forum (EBF) has signed a partnership agreement with TeleTrusT, a German-based information security body. The agreement will see the two partners work together on goals such as the protection and security of information and the creation of excellence in the use of biometrics in Europe and beyond.

The organisations will also examine the use of biometrics as a means of enhancing information security and as a way to prevent some of the problems now facing European governments, such as identify theft and fraud.

The EBF and TeleTrusT will now hold discussions with regard to finalising a common strategy and clearly defined tactical activities which will be announced this Spring. Furthermore, they are co-ordinating a meeting with the heads of the various National Biometric Forums.

This agreement builds on other partnership agreements announced in the last year, including the iAfB (International Association for Biometrics, UK), KISA (Korea Information Security Agency) and the BSC (Biometrics Security Consortium of Japan).

Following the departure of the EBF's managing director towards the end of last year, the organisation has been working on a fundamental review of its operations. A new strategy document is expected to be published in the coming weeks and will concentrate on four key themes – education, user acceptance, research and development and standards and testing.

NETWORK ACCESS

London Drugs prescribes fingerprint solution

Canadian-based retailer, London Drugs, is to implement a biometric-based enterprise solution for improving employee password management. Supplied by fingerprint technology company, DigitalPersona, the system will allow London Drugs' employees to sign-on to the corporate network using their fingerprint. The company hopes that the move will reduce the cost, time and effort associated with password resets and other IT management issues.

London Drugs employs more than 7,000 people and has 62 stores. According to Nick Curalli, the company's general manager of IT, "In order to consistently deliver the best possible shopping experience to our customers, we need to be highly efficient. DigitalPersona's one-step fingerprint

authentication solution protects our corporate network and allows our employees to focus on processes and productivity, not passwords.”

DigitalPersona's server software uses Microsoft Active Directory to store passwords and set policies for users, while the workstation client software and reader enable employees to log on to the network and various applications.

DigitalPersona recently announced it was supplying its software to Microsoft, to help with the roll out of Microsoft's new series of biometric PC peripherals.

Contact: Harvey Bondar at DigitalPersona,
Tel: +1 650 261 6070,
email: harveyb@digitalpersona.com

SV

BT adds sv technology to combat identity fraud

British Telecom (BT) is to add a speaker verification facility to its online identity verification service, URU. The UK's biggest telecommunications company chose to integrate technology from Israeli supplier Persay, following a competitive tender.

According to BT, identity fraud is estimated to cost the UK at least £1.3 billion per year. URU is designed to reduce the time and cost of verifying the identity of customers and employees, automate the process, and help detect false identity and impersonation fraud. An important feature of URU is that it enable financial institutions and other enterprises to select verification checks that are deemed proportional to the transaction risk. BT hopes that its URU Identity programme will become a universal system for securing call centre and web transactions.

BT selected Persay's new .NET-based speaker verification platform *VocalPassword 5.0*, making use of its web service interface.

Chris Gahan, BT's authentication capability manager commented: "Speaker verification adds another option to the choice of online checks that our customers can request. Passwords are increasingly vulnerable and not always easy to remember. Phishing attacks and keystroke viruses are driving businesses to use two-factor authentication. Voice is the 'verification' biometric. You can register it remotely, check it remotely, the infrastructure already exists and most people are used to using a phone."

Contact: Shira Lotto,
Tel: +972 3 767 8690, email: shira.lotto@persay.com

In brief

- The biometric ID card scheme in the UK could be jeopardised following the withdrawal of support from the UK's main opposition party – the Conservatives. The Labour Party admitted the Bill would find it tough to pass through the House of Lords, if the Conservatives removed their backing. The UK's other main political party – the Liberal Democrats – has already voiced its opposition to the cards. Despite the opposition, the latest vote on the Bill in the Houses of Parliament sailed through by a vote of 224 to 64.

- The West African state of Senegal has said that it wants to start issuing biometric-based identity cards. The cards will be used primarily as voter cards for the country's 2006 presidential and general elections. Approximately 174 registration centres will be set up around the country before the scheme is launched in April 2005.

- **Pay By Touch** has acquired a patent portfolio with issued US patents for additional biometric payment solutions. The portfolio includes a patent for biometric authentication when cheque cashing and adds to the supplier's existing patents, which are claimed to number more than two-dozen. The supplier also recently announced that **Piggly Wiggly Carolina Co.** is initiating a company wide launch of its biometric payment technology with full implementation expected by May 2005.

- **Liska Biometry** has filed for two patents surrounding its fingerprint "Biometric Identifier Number" (BIN) technology. The supplier is attempting to fast-track the patent applications under the **US Patent and Trademark Office's** anti-terrorism provision.

Events Calendar

11-14 April 2005
Las Vegas, NV, USA

CardTech/SecurTech

Now into its 15th year this major US event returns to Las Vegas, where its focus will be on transactions and security.

Contact: www.ctst.com

26-28 April 2005
Grand Hall, Olympia,
London, UK

Infosecurity Europe

Now in its 10th year, this exhibition typically attracts around 250 exhibitors and 10,000 visitors. The event brings together companies and organisations concerned about the security of their information with providers of technology and consultancy services.

Contact: Reed Exhibitions,
www.infosec.co.uk

27-29 April 2005
Singapore

Biometrics World Asia 2005

This conference and exhibition will address a broad range of practical biometric issues and is co-located with Cards Asia and RFID World Asia.

Contact: Stella Tan at Terrapinn,
Tel: +65 6322 2756,
email: stella.tan@terrapinn.com

7-9 June 2005
Marseille, France
Identech 2005

This trade fair covers all the major identification techniques. This year it will have a series of 12 conferences, with 110 papers.

Contact: Charles Copin,
Tel: +33 01 53 40 97 00, Email: charles.copin@wanadoo.fr
Web: www.identech-online.com

10 June 2005
Sydney, Australia

Biometrics Institute Conference

This is the main event in Australia discussing the area of biometrics.

Contact: The Biometrics Institute,
Tel: +61 2 9413 1400, Email: admin@biometricsinstitute.org,
Web: www.biometricsinstitute.org

20-26 June 2005
San Diego, CA, USA

CVPR2005

Run by the IEEE Computer Society this is an academic event looking at computer vision and pattern recognition.

Contact: Web: www.cs.duke.edu/cvpr2005

20-22 July 2005
New York, USA

AVBPA 2005

The Audio- and Video-based Biometric Person Authentication (AVBPA) 2005 conference is designed to provide a scientific forum for researchers, engineers, system architects and designers of biometric systems and related technologies.

Contact: <http://biometrics.cse.msu.edu/avbpa2005.html>

**Company
news**

• Silicon fingerprint sensor manufacturer **AuthenTec** has named Marc Gebert as director of marketing and sales in Europe, announcing plans to expand its presence to meet the demand for biometrics. Gebert will be based in Germany and will oversee the European marketing and sales operations, including direct sales, dealers and representatives. During 2005, AuthenTec also expects to hire additional staff to provide support for the company's customers throughout Europe. Previously, Gebert was CEO of **AD-Vision Technologies** in Munich.

• **Smiths Heimann Biometrics** (SHB) has signed a Memorandum of Understanding (MoU) with New Hampshire firm **AssureTec Systems** (ATS). SHB manufactures forensic quality fingerprint and palm print capture equipment, as well as full-page passport readers, while ATS operates in the document authentication market with products including document classification software. The MoU will see the two companies cooperate in product development and solutions that aim to solve government requirements for performing checks at border crossing points. This includes the use of ePassports with integrated RFID chips as defined by ICAO, the companies said.

• **Sequiam Corporation** has announced a technology, marketing and sales agreement with **BioMetAccess Company**, under which BioMetAccess will serve as a 'Master Distributor' of Sequiam's products and technology throughout its network of more than 250 resellers across the world. Sequiam's off the shelf products include *BioVault*, *BioLock* and the upcoming *BioVault II*.

ACQUISITION

Markland Technologies snaps up 3D player

Markland Technologies, a company focusing on homeland security products and services, has purchased Genex Technologies for US\$3 million in cash and US\$7 million in stock. Markland hopes the acquisition will provide it with capabilities in a range of technologies, including surveillance, biometrics and disposable sensors as well as research and development.

The acquisition was a multi part transaction, which included the purchase of a majority ownership in **Technest Holdings** (a company that prior to this acquisition had no operations but was traded on the OTC bulletin board) and the subsequent purchase by Technest Holdings of all of the stock of **Genex Technologies**.

Genex's revenues derive principally from 20 ongoing contracts to supply imaging and surveillance sensor technology to government customers. It has also been active in developing three dimensional facial recognition products.

The company has 32 employees and had revenues for the fiscal year ended 31 December 2004 of approximately US\$5.5 million.

Within Genex's biometric technologies division, its 3D facial recognition group has been developing tools for enhancing existing two-dimensional facial recognition systems, while advancing progress towards total 3D systems. In particular, the company's tools allow for capabilities, such as 2D-to-3D face conversion and compensation for pose, lighting, expression, aging and weight, the company claims.

Markland Technologies has four business segments set up to address the needs of the homeland security marketplace:

- remote sensor systems for military and intelligence applications;
- chemical detection systems;
- border security;
- advanced technologies

Contact: Robert Tarini at Markland, Email: marland@marklandtech.com

FINANCIAL RESULTS

Precise doubles sales

Swedish fingerprint and smart card technology company Precise Biometrics managed to more than double its sales revenue in 2004 reaching SEK 30 million (US\$4.3 million) compared with SEK 13.6 million (US\$1.95 million) in 2003. The company failed to make a profit, but managed to rein in its net losses from SEK54.1

million (US\$7.8 million) in 2003 to SEK38.1 million (US\$5.46 million) in 2004.

Christer Bergman, president and CEO commented: "It was a year when our Precise Match-on-card technology started to become a natural part of companies' security systems and a feature in travel and ID documentation."

Bergman said that the acquisition of Swedish IT consultancy **Fyrplus Teknik** in January this year puts the company in a strong position to meet the challenges being presented in the travel document area, as well as the national ID card sector, where numerous countries are planning biometric-based cards, such as Finland, Thailand, Italy, Malaysia and South Africa.

By the end of 2004 Precise Biometrics had 35 employees (raised to 60 with the Fyrplus acquisition) and liquid funds of SEK 37.6 million (US\$5.39 million).

Contact: Christer Bergman at Precise Biometrics, Tel: +46 730 35 67 26, email: christer.bergman@precisebiometrics.com

FINANCIAL RESULTS

Identix's record revenues

Identix reported its best-ever biometric revenues in its fiscal 2005 second quarter and first half financial results ended 31 December 2004.

Fiscal 2005 second quarter revenue was US\$18.6 million, up 54% when compared to US\$12.1 million in the same quarter last year. From this revenue Identix made a second quarter loss of US\$2.8 million compared with a loss of US\$5.5 million in the same year-earlier quarter.

President and CEO Joseph Atick commented: "I am very pleased to report that this was the fifth consecutive quarter of top line growth for Identix. As demonstrated by our record biometric revenue this quarter, which drove the second quarter's 54% year-over-year revenue growth, we continue to see strong opportunities for biometric solutions throughout the world."

Revenue for the first six months of fiscal 2005 was US\$35.2 million, with a loss from continuing operations of US\$7.6 million. This is up 44% compared to the same period of fiscal 2004, where revenue reached US\$24.5 million and a loss from continuing operations of US\$10.5 million.

The company reaffirmed its expectations for the remaining two quarters of its fiscal 2005 year. For the third quarter ending 31 March 2005, the company predicts revenue of between US\$19-US\$21 million and for the fourth quarter ending 30 June 2005 revenue is expected to be between US\$20.5-US\$23 million.

Contact: Damon Wright at Identix, Tel: +1 952 979 8485, email: damon.wright@identix.com

Security technologies to the fore

Scott Greiper, senior research analyst at C.E. Unterberg, Towbin, discusses the security industry post 9/11 and analyses some of the leading biometric companies in this sector.

Q: Would you begin with a quick overview of your coverage in the security space?

Mr. Greiper: I concentrate solely in the homeland security/global security space...

This is a relatively new sector for the Street. The whole sector has been reinvigorated by 9/11, unfortunately. I cover the security technologies that are driving much of the product deployment in the market today. Those are digital video surveillance and secure ID (being able to identify that a passport or driver's license is authentic and that you are the person in the ID photo). I cover the RFID space...as applied to tracking and monitoring something like cargo containers or vehicles in an airport. I cover wiretapping, intelligence gathering and, lastly, the area of access control – who's coming in and out of a building, are they presenting the right credentials to get in that building, etc. None of these technologies are new, by the way; they've all been around for a number of years. What is new is how they're being applied to the security space specifically. The cost of many of these technologies and products has come down as demand has increased. So much of what I do is following the money in security.

The creation of the Department of Homeland Security in 2002 was the biggest change in the US infrastructure since the development of the Department of Defense in World War II. There have been about 24 different agencies brought in under one umbrella, with about 180,000 different people. But if you look

at the federal initiatives in security, many of them are knee-jerk reactions to what went wrong on 9/11.

Let's start with the fact that we had 19 hijackers, eight of whom presented false or forged visas to the counter people at Logan Airport and got through. They were carrying with them up to 85 different driver's licenses from different states and countries, all of which were counterfeited. Obviously, the ability to authenticate a person's identity and authenticate that their ID is original is a prime source of funding for the Department of Homeland Security today because of the inability to check these people's IDs when they walked in.

Q: Is the government actually beginning to fund this?

Mr. Greiper: They are. The critical word is funding because the money has been allocated and budgeted for some time (the original Department of Homeland Security budget was around US\$22 billion, now it's closer to US\$40 billion), but the pace of spending has been disappointing. That really changed in the back half of 2004. We had the first contract given out for what's known as the ePassport program. All across the world, passports are going to be converted to electronic passports. They will have a chip embedded that will contain information about you...It's also going to contain a facial biometric template because these are mainly applied to photo IDs, so it made sense to use facial biometrics...They just

named the finalists for the passport award of about US\$250 million, and the award will actually be granted in 2005.

This was all mandated by a global aviation security group called the International Civil Aviation Organization (ICAO), which, after a year and a half study to improve the security of photo IDs and particular passports, mandated that the 27 visa waiver countries (countries whose citizens are able to come into the US without a visa) were now going to need ePassports in order to get access into the USA. The original date of deployment was supposed to be October 2004. That's obviously not happening. It has been pushed back to October 2005...It's probably a US\$2 billion project globally.

It's not only going to apply to passports, but it's also going to apply to driver's licenses. Part of the 9/11 bill that was just passed has several paragraphs devoted strictly to improving the security of the issuance of driver's licenses and the ability to authenticate the driver's license.

The problem is that it's very easy for your college age son or a terrorist in Afghanistan to counterfeit a driver's license. Each state manufactures and produces its own driver's license according to its own specs. There are no standards in the states. There was a directive that came out of the White House, the Senate and the House on 11 October mandating that the process of issuing a driver's license be tightened up.

It used to be that you could walk in with any kind of photo ID, even a student photo ID or work photo ID, and present a proof of address like a telephone bill, and

that would get you a driver's license. You could counterfeit that photo ID, and you could counterfeit that telephone bill. Now the IDs you offer as proof of identification to get the driver's license are going to have to go through that same authentication process to prove that they're legitimate. That is what was implemented as part of the 9/11 bill that was passed. The majority of the world uses photo IDs as proof of identity to do anything – to get a pack of cigarettes or to get into an airport – either a passport or a driver's license, and those are the two IDs globally that are going through an evolution to create a chip-based document that can be machine read and that has a biometric on it.

Q: Who are the winners?

Mr. Greiper: There are a number of people out there. Viisage Technology is the only manufacturer of passports in the United States under a long-term contract with the Department of State and is the number two manufacturer of driver's licenses.

Positioning is everything in the security industry, particularly when you're working with governmental agencies. Not only do you have to be able to be an approved vendor to the GSA, but experience of being able to work successfully with security agencies previously gets you in line to get more business as things roll forward. In terms of being the only manufacturer of passports and the number two manufacturer of driver's licenses and having a core technology in facial recognition, the company is extremely well-positioned to participate in the upgrade of security of photo IDs.

Identix makes fingerprint systems and facial systems. Cogent, a recent IPO, is a main player in the US-Visit program. If you're a foreign visitor coming into the US, you are fingerprinted and photographed as you cross customs. Cogent makes the devices that capture the fingerprints and does a quick database search to make sure you're not a bad guy, that you don't appear on a CIA watch list,

that you don't appear on a terrorist watch list and that you haven't given aliases before to get the passport. They do the database matching side of US-Visit, which is really where the value is because when you're processing a lot of people, either in an airport or customs, throughput is essential. You don't want people standing there for 45 minutes as you're searching the database. They have algorithms and software that allow very fast matching against very large databases. Those are some of the main players in the secure ID space.

The fastest growing part of the security market from a product perspective since 9/11 has been the video camera, where the old CCTV analogue cameras or some of the new digital cameras or new IP-based cameras are being offered in the market today. The old CCTV market prior to 9/11 was growing at 6%-7% a year. It was a mature business. Since 9/11 that market is growing 25%- 30% a year. It has just been turned on its head. The reason is because the simplest way in which you can remotely track people or objects is through video surveillance. If you walk in New York City today, you are tracked on video on average close to 120 times a day...In London, that number is close to 300. London is the most heavily deployed video surveillance city in the world.

In this space I like Verint Systems. Verint offers one of the highest quality best-of-breed solutions in digital video, not only bringing video to the network, but also bringing intelligence.

Q: You've recently picked up coverage of SuperCom?

Mr. Greiper: SuperCom is a company that I've known and worked with for about five years. For the past decade or so, the company has been making passports, visas and driver's licenses for countries like the UK, China, Hong Kong, the Philippines and the Ukraine. So within my overall coverage, one of the primary themes that I follow within the security industry is the

strong push toward secure IDs, which is essentially making sure that what happened on 9/11 won't happen again.

Q: You have written a lot about SuperCom's potential candidacy for the GPO contract for electronic passports?

Mr. Greiper: If you look at the structure of the initial four awardees [Note: since this interview four more awardees have been announced to bring the total to eight], SuperCom is a prime contractor and a subcontractor to BearingPoint. The two others are Schlumberger's affiliate called Axalto, which makes smart cards, and Infineon...Quite honestly, I have no call on how much of the award they could get or if they're even a final finalist. I do know that with the market opportunity throughout the world and the fact that since the announcement that the company was a finalist for GPO, they have signed on to be an eID vendor to two large European countries and one African country.

The opportunity for eID vendors in the rest of the world outside the US is much larger than the US, simply based on the fact that many more holders of passports and visas are outside the US just based on population.

My estimates are really based on how many eIDs the company will make this year and next, independent of whether it comes from the US GPO or from some of the other European and Asian efforts. With those numbers, I'm assuming the company will make 1.3 million eIDs this year, for which they will get paid about US\$5 per card, and they will make 2.4 million eIDs next year. When you look at solely the US project, which is 10 million eIDs per year, that one project could cover both of the assumptions for this year and next, but I'm really looking at a percentage of the global opportunity.

This article is excerpted, with permission, from an interview conducted by The Wall Street Transcript. To view the full text visit www.twst.com. Scott Greiper can be contacted on Tel: +1 212 389 8203

Sizing up silicon sensors

Silicon fingerprint sensor technology is moving forward in leaps and bounds, although its penetration into the marketplaces it is being targeted at is still low. Nevertheless, within the last two years many millions of fingerprint-enabled devices, such as laptops, PDAs and mobile phones, have been sold and this trend looks set to accelerate. Personal electronic goods manufacturers (and to some extent the suppliers of the fingerprint technology) are beginning to realise that fingerprint technology can be used in ways far beyond its original brief as an enhanced security tool.

In the space of just a few years the fingerprint market has undergone radical change. There are a number of different fingerprint sensor varieties (see [Figure 1](#)) with optical fingerprint sensors having traditionally led the way in terms of market share. In years gone by silicon-based sensors (including capacitive and thermal) were dogged by problems of performance, robustness and price. But in the last two years much of that has changed. Now, it seems, silicon technology is forging ahead at an unstoppable rate and has overtaken the optical fingerprint sensor market by some margin.

Taking a look at the volume of shipments released by the number one manufacturer in the silicon fingerprint sensor market – **AuthenTec** – graphically shows how the market is progressing. According to the company, since it was founded in 1998, shipments hit:

- one million by July 2003 – after 4.5 years in operation;
- two million by March 2004;
- three million by August 2004;
- four million by January 2005;
- an even greater rate from the start of 2005.

Figure 1. Fingerprint sensor options

Although not an exhaustive list, the following are the main fingerprint sensor types:

Optical	This technique is still widely used, especially for physical access control and in many PC peripherals. The finger is placed on a coated platen and exposed to a light source. In most devices a CCD (Charged Coupled Device) receives the image of the fingerprint, with dark ridges and light valleys.
Ultrasound	Acoustic waves are transmitted and distances are measured based on the impedance of the finger, the platen and the air. These distances are then converted into a representative image. Advantages of this type of sensor are its ability to work for long periods unattended thanks to its good performance in dirty environments. It is generally an expensive technology however.
Capacitive	This technology is based on measurements of the capacitance between the skin surface and the silicon sensor. The capacitance is then converted into a grayscale digital image. Delete Sentence from here
Thermal	This measures the temperature differential between the skin ridges and the air caught in the fingerprint valleys.

Other leading manufacturers, such as **Atmel**, also claim to have shipped significant quantities of fingerprint sensors (thermal sensors) – up to one million in its case.

There are a number of reasons for this acceleration in sales and hence the shift in dominance between silicon-based and optical-based sensors. First, there have been significant developments in mass consumer markets, such as the introduction of more value-added services and m-commerce opportunities in the mobile phone sector, which make the introduction of biometric technology more attractive. Second, the price of the fingerprint devices has plummeted to under US\$5 for many sensors on the market, when bought in quantity. This is less than half the price of typical sensors two years ago, and is a major driver for the technology. Third, the best silicon sensor manufacturers have been able to iron out some of the problems that have traditionally dogged the technology, such as robustness against physical scratching and the problem of electrostatic discharge (ESD). Fourth, the emergence of multi-functional fingerprint devices, which in addition to replacing PINs and passwords, also offer scroll functionality, navigational ability and phone personalisation options, are also making the fingerprint sensor more attractive. And finally, user perception of biometrics is now at an all-time high, with one recent survey showing that a high proportion of consumers would be willing to pay a premium to add fingerprint-based technology to their electronic devices, if it would make their lives easier and more secure (see [Figure 2](#)).

This certainly isn't to say that the optical sensor market is floundering. As Lennart Carlson, CEO of Swedish supplier **Fingerprint Cards** noted: "Look at the recent deal between **Microsoft** and **DigitalPersona**, which saw the launch of three optical-sensor based fingerprint PC peripheral devices. This was a significant deal. And in Asia there are countless optical sensors on the market."

Application markets

Without doubt the consumer electronics sector is the fastest growing market for fingerprint biometrics worldwide – primarily in Asia. According to some industry estimates, more than four million biometric-enabled mobile phones, PCs, laptops and PC peripherals are already in use. Other markets include flash USB memory drives, personal digital assistants (PDAs), physical access control and even the automotive market – although this is unlikely to take off within the next few years.

In the mobile phone sector, one of the biggest deals was announced between AuthenTec and leading Japanese mobile phone operator NTT DoCoMo. Tom Tombler, marketing manager at AuthenTec told *Btt*: “We’ve managed to sell them around 1.2 million sensors, alone.”

Elsewhere, UPEK (a spin-off from STMicroelectronics in 2004 and widely seen as the number two in the market) recently announced it had won a deal with IBM to incorporate its *TouchStrip* fingerprint sensor in the computer manufacturer’s *ThinkPad T43* notebooks to help protect user identity and data. According to the company, its *TouchStrip* and *TouchChip* solutions are used in more than a million notebook PCs and other applications.

Meanwhile, Atmel is continuing to provide its thermal fingerprint sensors to HP for use in certain models of its *iPAQ* range. The latest information is that Atmel will supply its *AT77C104B* FingerChip sensor for the new *HP iPAQ hx2700 Series Pocket PC*.

David Richard, Atmel’s worldwide biometrics marketing manager told *Btt*: “Although I cannot give exact numbers, there are a few hundreds of thousands of these fingerprint-enabled devices sold with our sensor each year. This latest 2700 model replaces four existing products, so we would expect the overall market for this fingerprint-enabled model to expand.”

One of the most recent mobile phone announcements came from another silicon fingerprint sensor manufacturer, Atrua Technologies, which teamed up with Yulong, a wholly-owned subsidiary of China Wireless Technologies Limited, to introduce the *Yulong CoolPad 858F GSM* mobile phone. It uses Atrua’s *Wings* swipe sensor solution.

Swipe dominates

As highlighted above, the price of silicon-based fingerprint technology has dropped dramatically in recent years. One of the main reasons for this trend is the increasing dominance of swipe style sensors, which are essentially thin rectangular stripes of silicon, over which a user must swipe their finger, rather than an area sensor, upon which a user would just place their finger. Bearing in mind that silicon represents the greatest material cost in a fingerprint sensor, it makes sense that the less silicon used the cheaper the sensor can be made.

As well as cost, there is another reason that swipe sensors are becoming so popular and that is the simple fact that devices such as mobile phones, where space is at a premium, demand the smallest sensor (including packaging) size possible.

Taking this further, even the size of swipe sensors themselves are coming down, as manufacturers develop sensors specifically for the wireless market. Atmel, for example, has just launched its *AT77C105A* sensor, which has a die size of 1.5x15 mm. This compares to an earlier model – the *AT77C101B* – which had a die size of 1.7x17.3 mm.

As note above, when looking at sensor sizes an important consideration is to look at the overall package size, as this, rather than just the exposed sensor, is what has to fit into the device. Atmel’s design is less impressive using this measurement, have an overall package size of 23x5 mm. One of the smallest package sizes on the market has just been announced by AuthenTec. It told *Btt* it is about to launch a completely new sensor for the mobile phone market – the *EntréPad 1500* – which has a complete package size of 12x5x1.85 mm and a frame capture rate of 1500 per second.

As well as Atmel and AuthenTec, many other manufacturers of silicon fingerprint sensors produce swipe-style sensors, including Atrua, Fingerprint Cards, Fujitsu, IDEX, LightTuning, Melfas, UPEK and Validity.

In total there are more than a dozen companies in the overall silicon sensor market, including swipe and area sensors (see [Figure 3](#)).

Enhanced functionality

There was a time when almost all of the sensor suppliers provided fingerprint sensors solely as a security and convenience devices. Replacing passwords or PINs with

a fingerprint sensor was not just more secure, the suppliers boasted, but they also meant the consumer didn’t have to spend time remembering them.

Now the market is changing. The use of fingerprint sensors in devices, such as mobile phones, often cannot be justified on security and convenience grounds alone, so some clever engineering has given the sensors a range of new *raisons d’êtres*. Everything from using the sensor as a touch pad to enable the user to click on items and scroll down a page, to its use as a navigational device (particularly in gaming

Figure 2. AuthenTec survey findings

A recent AuthenTec-sponsored survey, which polled more than 2,000 adults in the USA, has showed that:

- 63% of consumers would pay extra to add fingerprint verification to their PCs and notebook computers, while 71% would pay more to have this feature added to their mobile phones;
- most consumers said they would use the technology to replace their PC and Internet passwords, as well as to help transform their mobile phones into their personal wallets to conduct m-commerce and wireless banking;
- younger consumers (18-44) are the most interested and are willing to pay the highest price for a biometrically-enabled device;
- navigating the cursor and automatically starting favourite programs were other key capabilities consumers were interested in using;
- three in 10 (29%) said they would be willing to pay more than US\$25 for the additional feature;
- 60% said they would like to use biometrically-enabled mobile phones as a replacement for their debit/credit cards to conduct purchases or perform online banking. Nearly half of those said they would be interested in using a biometric cell phone to purchase items from a store, while 30% for wireless banking, 27% to gain access to mass transit, and 25% for wireless shopping.

applications) or as a device to personalise the set up of the device for different users. This additional functionality makes the fingerprint sensor a much more compelling option for device manufacturers.

An ideal application for suitably adapted sensors is to become the primary user interface for people playing games on handheld devices. As might be expected, this sort of application is of great interest to device manufacturers, but sensors need to be responsive enough to cope with the demands of ever-faster games. While navigational properties are not such a new feature for fingerprint sensors, with many of the manufacturers offering this capability, the ability to navigate at speed is one characteristic that can distinguish one sensor over another.

According to AuthenTec, for example, its latest sensor can operate at a swipe speed of 50 cm/sec, which according to the supplier is more than fast enough for even the fastest fingers. In fact a speed somewhat below this figure is most likely acceptable. For example, UPEK's *TCS3 TouchStrip* strip sensor has an acquisition speed of 20 cm/sec, similar to Atmel's *AT77C105A* fingerprint sensor.

Durability

With fingerprint sensors being used for much more than authentication, it is critical that the robustness of the sensor technology is adequate. In the past this has been a critical issue with mechanical scratching and susceptibility to electrostatic discharge (ESD) being constant problems.

To counteract mechanical scratching problems, coatings are used on the sensors

to form a layer of protection – and these coatings are another competitive differentiator between the suppliers in the market. As might be expected, most companies claim to have superior coating properties.

When considering coating, its thickness is a good parameter to consider, as is the material used. One potential problem with a thicker coating, however, is that the performance of the sensor can be affected. Different manufacturers have different ways of dealing with this issue.

Capacitive sensors measure the capacitance between the fingerprint contour and the sensor's plates. There are two ways of generating this capacitance:

- **direct capacitive measurement** – this technique is used by many sensor developers and involves an electrical charge being applied directly to the sensor plate.
- **active capacitive measurement** – with this technique electronic pulses are passed to the fingertip, potentially allowing for a strengthened signal communication between the fingerprint surface and the sensor plates, which in turn could allow for a thicker protective coating to be used. Companies such as Fingerprint Cards and AuthenTec use this method.

Some companies use special coatings, others stick to silicon nitrate, which is a standard coating and insulator.

One novel coating idea is adopted by thermal fingerprint sensor manufacturer, Atmel. Bearing in mind the 'trendy' markets that these sorts of sensors are being produced for, the supplier decided to introduce colour to the traditional sensor design. According to David Richard,

Atmel's Worldwide biometrics marketing manager: "Look and feel as well as brand identity are key features of today's consumer mobile devices, such as cell phones or PDAs. Manufacturers want their products to have great designs, as aside from the technical aspects of the device, the way it looks can greatly influence sales. As our technology permits it, we are adopting this trend by proposing matching colour options for the sensor. Our customers were limited by the availability of black or grey sensors."

The supplier says that virtually all colours are available for bulk orders, at no additional cost (the supplier's *AT77C104B SPI* sensors retails for less than US\$6 for high-volume orders).

Market penetration

As this survey demonstrates, robustness, price and functionality issues have largely been solved and this is why such a fast adoption of the technology is now taking place. However, the industry is starting from a very low base.

According to estimates by Fingerprint Cards, there were a couple of hundred thousand laptops sold with fingerprint sensors last year, and more than two million mobile phones. While this is a creditable performance, it barely scratches the surface when compared to the total number of devices sold.

According to the latest findings by market analysts **Strategy Analytics**, 2004 saw sales of mobile phones hitting 684 million units, 32.3% more than the 517 million shipped in the previous record year, 2003. This means that fingerprint phones represented 0.38% of the market in 2004.

Analyst group **Gartner** says that PC sales topped 183 million units in 2004, while mobile PC shipments will increase by 17.4% in 2005. Meanwhile, worldwide personal digital assistant (PDA) shipments, such as the iPAQ, increased 6.6% in 2004, to 12.29 million units, the analyst group commented.

Considering these figures, it is clear that the silicon fingerprint industry has made a good start, but that there is still a long way to go. However, the need for identity authentication technology is expected to increase as more and more sensitive transactions are performed using mobile devices, and that should enable the fingerprint sensor market to continue strongly on its upward curve.

Figure 3. A selection of players in the silicon-based fingerprint sensor industry

AuthenTec	www.authentec.com
Atmel	www.atmel.com
Atrua Technologies	www.atrua.com
Fingerprint Cards	www.fingerprint.se
Fujitsu	www.fujitsu.com
IDEX	www.idex.no
LighTuning	www.lightuning.com.tw
Melfas	www.melfas.com
NTT	www.ntt.com
Sony	www.sony.com
UPEK	www.upek.com
Validity	www.validityinc.com
Veridicom International	www.veridicom.com transit, and 25% for wireless shopping.

Seafarer's biometric ID card sets sail

All countries ratifying Convention No. 185 will now be required to issue new SIDs that conform to the requirements specified in the standard known as *ILO SID-0002*. According to information received by the ILO more than 50 countries have submitted the convention for consideration by their national parliaments. Many, including India, Philippines and Indonesia, which have large numbers of seafarers, are making plans for implementation.

Speaking of the convention, which came into force on the 9 February 2005, Cleopatra Doumbia-Henry, director of the ILO International Standards Department, said: "The convention puts in place a comprehensive security system that enables the first global implementation of biometric identification technology on a mandatory basis, thus enabling positive identification of the seafarer that holds the document"

Convention No. 185 replaces the *Seafarers' Identity Documents Convention, 1958 (No. 108)* that had been ratified by 61 ILO member States, representing more than 60%.

Sagem wins United Kingdom police identification contract

Northrop Grumman Information Technology has awarded Sagem an eight year contract to provide advanced biometric identification technology for a computer system linking more than fifty police forces and agencies in the United Kingdom.

The plan is to integrate and enhance the current Automated Fingerprint Identification System (AFIS) of England and Wales as well as the AFIS used by Scotland's police forces. The new system, called IDENT1, will enable these fingerprints and marks to be searched against a combined database of more than six million ten-print records and more than one million marks (latents) in minutes.

One of the first new developments will be the establishment of a national palm-print searching service. This service will enable forces, which already routinely collect palm prints from people that they arrest, to run national searches similar to

fingerprint searches. National palm-print searching can have a considerable impact on crime investigation and detection as nearly 20% of all marks obtained from crime scenes in the United Kingdom are from palms. Further developments will include mobile fingerprint checking, facial imaging and video identification.

According to Fred Preston, director of identification for the UK Police Information Technology Organization (PITO): "The UK has set the standard for identification technology in the police service, enabling the fingerprint bureau to complete complex national searches and comparisons. This contract award will enable us to continue the good work and to provide the police service with further national identification services they need to help fight the modern, sophisticated and mobile criminal."

Contact: Hervé Philippe at Sagem, Tel: +33 1 40 70 62 57, Fax. +33 1 53 23 20 47 email: herve.philippe@sagem.com



Comment

According to one of the industry's associations, biometrics is defined as: "Automatic identification or identity verification of an individual based on physiological or behavioural characteristics. Such authentication is accomplished by using computer technology in a non-invasive way to match patterns of live individuals in real time against enrolled records."

Is this definition still reflective of the industry, which has changed significantly over the last decade? If so, some companies that consider themselves part of the biometric family would not qualify.

Look at the dynamic signature verification market. Many of the best implementations are designed simply to eliminate ink signatures on official paper-based documents. Take the news from WonderNet this month, where technology

is being used to facilitate the electronic signing of insurance papers. There is no verification involved, simply the storing of a template, with no reason to believe it will be verified. Does this fit the definition ?

An automated fingerprint identification system is another example of a technology that is close to, but not quite a biometric system, as it does not involve matching a live biometric in 'real time'.

Identix also announced this month that it will provide its facial recognition engine to Nikon, in order to allow its cameras to detect (but not identify) human faces. Surely not a biometric process.

These systems are using biometrics, but not in the way that was originally conceived when the definition of biometrics was being formulated. Does this mean we should ignore them? Maybe now is the time to adopt them, and adapt our definitions accordingly.

Mark Lockie