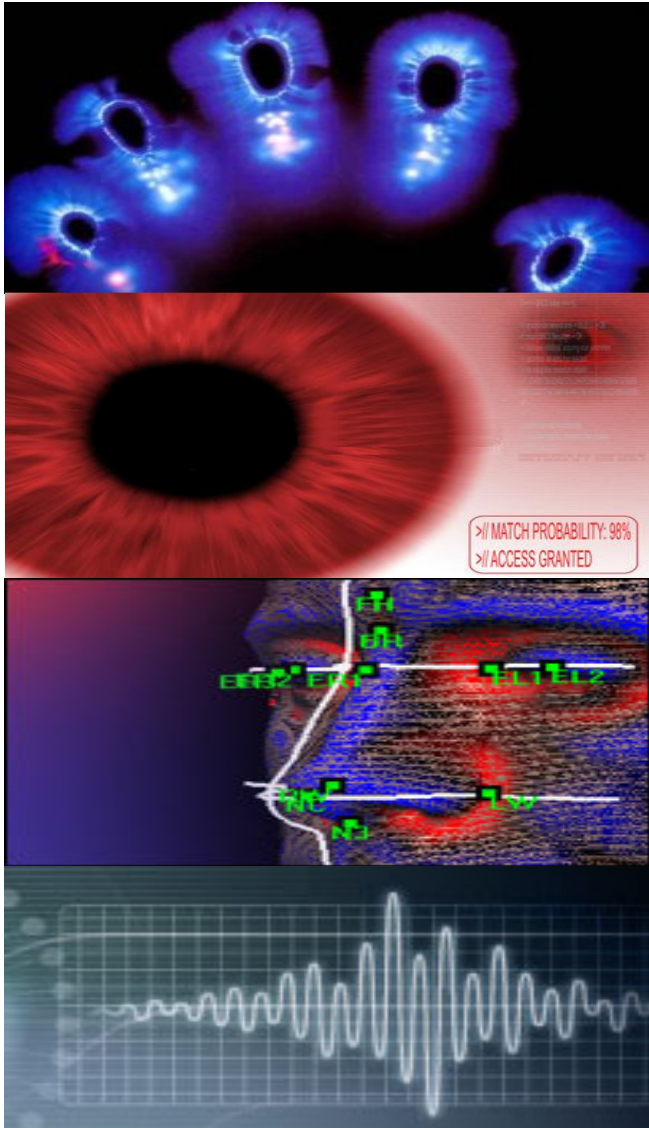




European Biometrics Portal



Biometrics in Europe

Trend Report

2007

UNISYS

Brussels, January 2007

Disclaimer

This report is copyrighted © European Community. Unisys (Belgium) is responsible for the content of this report which is based on a thorough desk-top study, on consultation of experts and on interviews with competent administration in concerned countries. The report does not necessarily reflect the view of the European Commission, nor does the Commission accept responsibility for the accuracy or completeness of information contained herein. Readers of this report will use it under their own responsibility. Neither the Commission, nor the authors may be liable for direct or indirect damages related to the use of this report.

Biometrics in Europe

Trend Report 2007

Patrice-Emmanuel SCHMITZ

Project Director

Ronald HUIJGENS

Chief biometric solution architect

Marc FLAMMANG

Business consultant

Thanks to:

Ed. SCHAFFNER

Roberto TAVANO

Director Integrated security programs

VP Justice & Public safety programs

Contact:

*patrice-emmanuel.schmitz
(@) unisys.com*

Contents

1. Management Summary	5
2. New business areas	7
2.1 Registered Passengers	7
2.2 Reducing welfare and identity fraud: saving €20 billion yearly?	12
2.3 Biometrics in Banking and Finance	14
3. Trends in biometrics technology	17
3.1 Evolving Markets	17
3.2 New and emerging products	19
3.2.1 True Single Sign-On	19
3.2.2 Biometric Security Card	19
3.2.3 Electro-physiological Signal recognition	20
3.2.4 Laser Surface Authentication™	21
3.2.5 Voice Verification and Analysis	21
3.2.6 Embedded biometrics	21
3.2.7 Fingerprint technology	22
3.2.8 Vascular Pattern recognition	23
3.2.9 Iris recognition	23
3.2.10 Face recognition	25
4. Recent developments in EU and Member States	26
4.1 EU	26
4.2 Relevant news in brief, by Member State	29

1. Management Summary

This second trend report is based on the output from the European Biometrics Portal (EBP) - www.europeanbiometrics.info.

The EBP is a project initiated by and belonging to the European Commission, DG Information Society, with the purpose to create and activate a Web Portal as a focal point for information exchange, coordination and community building activities between the main biometrics actors in Europe.

The EBP principle is based on volunteer contributions of authors, working according to a “Wikipedian” spirit. After 18 months of portal operation, the main trends are highlighted here. The Portal will now continue its information mission in the framework of the European Union Joint Research Centre (JRC) after March 2007, with a new focus on government interoperability and cooperation.

The development of Biometrics is an outcome of globalisation, which is not only technological, but also political and economic: the world is now a global place for commerce, migrations, trusted exchanges of all kind of information and values. This creates new opportunities as well as new risks, crises, frauds, illegal traffics or even terrorism. Measures to address these new risks are also questioned, mainly regarding the balance between privacy and security.

In the present report, we pinpointed three main development areas that will focus attention in Europe during the coming years. These are:

- ▶ Registered passengers (speeding up airport and other travel checks),
- ▶ Fight against welfare and identity fraud (where up to € 20 billion could be saved yearly),
- ▶ Biometrics to facilitate financial and commercial transactions.

In a second section, we discuss the technological trends, regarding true single sign-on, biometric security cards, electro-physiological signal recognition, laser surface authentication, voice verification and analysis.

We briefly explore embedded biometrics, new developments in fingerprint technology, vascular pattern recognition, Iris and face recognition.

Last, we updated our 27 Member States survey (for previous developments, please refer to the June 2006 Trend report): implementations of biometrics are accelerating and enter in operational phase in several Member States, especially as from the last months of 2006.

Biometric technologies still fascinate people. Many action movies and thrillers are illustrated with a lot of technology, from iris and retinal scanners to vein recognition, 3D face and palm hand print readers. Almost constantly, the scenarios of such movies try to demonstrate the hero's capacity to evade the most sophisticated detection methods, to authenticate in the most secret places, to succeed with fake signature, fingers or even bloodied, extracted eyeballs or face. Good or bad, humans won over machines and machines, incidentally, are unable to control processes and security according to their purpose.

Despite all the hype, biometric technologies have been slow to take off. Cost issues, instability, lack of portability, interoperability problems and multiple standards have made them a hard sell and consolidation, from demo prototypes to operational.

A part of the focus on biometrics still obviously results from Sept. 11, 2001, as an attempt to reach better security in the fight against terrorism. However the reality is both less ambitious and more tangible. Less ambitious because no biometric system will ever provide any guarantee against terrorist actions, which may be initiated at any time by legally established citizens, having all kind of legitimate documents. More tangible because convenient applications of biometrics will provide citizens with the "state of the art" best possible protection against identity fraud and will provide public authorities and enterprise a better protection against a series of abuses and fraud in daily transactional business: reducing these abuse by 70 or 80% in welfare could already save € 15 to 20 billion Euro yearly in Europe.

In that sense, we believe that biometrics may be seen as a complement to efficient citizen's rights management, daily transaction security and authentication processes. It can never be trusted blindly, and it cannot replace case by case verification and human responsibility, otherwise both security and privacy will be deteriorated. At the contrary, decision from responsible persons must stay in place and possibilities to escalate at higher decision level must be available at any time.

Together with established success and improved application, the technology still knows many developments and evolutions. At the same time, in several domains like passport delivery (under pressure from the US-Visa waiver programme), the delivery of biometric documents is now part of a daily routine.

2. New business areas

By Patrice-E. Schmitz,
Director EU consulting,
Unisys

They are numerous new business areas for biometrics. Coming years will see biometric applications for increased security in using cell phones (voice, face or iris recognition, small fingerprint), more biometrics for residential and business access control or biometrics integrated with video surveillance. For Europe, we rapidly present hereafter three of the most recent trends, where we foresee future large applications:

- ▶ Registered passengers,
- ▶ Fight against welfare and identity fraud,
- ▶ Biometrics to facilitate financial transactions

2.1 Registered Passengers

The events of September 11th 2001 forever changed the civil aviation landscape. In response to these attacks, Regulation (EC) No 2320/2002 was drawn up to lay down basic requirements for aviation security and has been in force since January 2003. It lays down procedures to be applied to all travellers without differentiation. The regulation sets common standards requiring, among other things, the screening of all passengers and baggage departing from airports in Member States. These rules treat all passengers and their baggage in the same way, although possibly some may present lower risks than others, as it may be the case for frequent flyer businessmen coming back at home every week or groups of elderly tourists organised by specialised travel agencies.

Obviously, such screening of large numbers of passengers and great quantity of baggage delays passengers, complicates operations and raises the cost of air transport. It has resulted in longer waiting times, more complex and thus lengthier security screening procedures, the need for more staff to be engaged in this activity and even an impact on airline performance (on time take off statistics etc.). Is this unavoidable? Could these problems and costs be reduced by simplifying the security checks on those passengers presenting low risks to aviation security? This is the purpose of a “Registered Passengers” system.

Various third countries, notably the United States, are already experimenting with “trusted traveller” schemes. In Europe, air transportation is an essential economic activity, open to competition.

European air companies and airports will look for maintaining their attractiveness and will try to propose their frequent flyers facilitation packages including the simplification of security checks, if this is possible according to the regulations and without compromising security.

One obvious approach is to lower or automate certain (manned) security activities aimed at those who are less “likely” to need the checks. By allowing passengers to declare themselves and allow themselves to be checked up on and authenticated as one presenting a low security risk, it is possible to target the speedier technology based measures at these persons and to “reserve” the more laborious procedures and the personnel required for them for the other passengers.

This concept has been tried and tested for somewhat different reasons (clearing immigration) serving as an example of the potential of such a programme for civil aviation security inside the “territory”. In the US, after testing at 5 airports, other airports have now started the process of procuring prior registration services. In the Netherlands (the Privium programme) or in U.K. (the Iris Recognition Immigration System - IRIS) paved the way for clearing immigration through deploying state-of-the-art biometric technologies for performing authentication.

A registered passenger scheme is one whereby interested passengers would apply to a national authority, be subjected to a risk assessment and, if that were successful, be registered as someone presenting a low risk to aviation security. When departing from an airport in the European Community, registered passengers would be subjected to lighter (or maybe even exempted from) certain security checks after identification or would be allowed access to an expedited process of security checks.

The objective of a registered passenger programme is to provide frequent travellers (or other interested passengers) with the means to expedite the screening experience and to thus facilitate air travel without compromising on security. The key words here are “without compromising on security” as any programme put in place to speed up procedures must never be implemented at the cost of security standards.

From the passenger point of view, the motivation is twofold:

- ▶ concrete and rational, if the system reduces waiting time significantly (e.g. more than 10 minutes) and reduces stress, by providing frequent fliers a quicker pass through security checkpoints;
- ▶ Emotional, with the feeling to be part of a privileged club of “first class / frequent travellers” with more control on the checking processes than others.

From the airport point of view, the motivation is:

Reinforce competitiveness and increase customer satisfaction
Reduce costs, of long security checks (impacting their productivity and personal costs too).

Issues and obstacles related to efficient registered passenger's schemes are multiples:

- ▶ **Legal:** Is such system in conformity with both security, privacy (data protection) and non-discrimination compulsory rules? Is it conform to international conventions (i.e. annex 17 to the Chicago Convention on International Civil Aviation)?
- ▶ **Economic:** Who will pay for it? How much could a passenger pay for it? Is the perceived or measurable value of system advantages high enough to attract a critical mass of customers? Will advantages be preserved if the critical mass is reached (without moving delays on registered passengers)?
- ▶ **Organisational:** how to ensure interoperability and avoid fragmentation or enrolment duplication in a "multiple operators" framework? How to maintain efficiency if the system is massively used?
- ▶ **Social:** is it acceptable from a "society" point of view? What could be the attitude of "non-pre-registered" passengers when they will be delayed or if they are checked with less priority? Are there risks of exclusion (passengers who will never be "accepted as secure" i.e. for cultural, social/educational or ethnic reasons, although they could be) ?

Although important, the biometric technology applied in the Registered Passenger scheme is therefore just one of the aspects. A successful project will have to deal with all other issues, which are much more related to policy than technology:

- ▶ How to determine that a person could be registered as a passenger presenting a lower risk? Is the lack of past criminal behaviour or the lack of any negative intelligence information enough (checking criminal records, SIS, Europol)? How far to collaborate with non-EU intelligence services? Is lifelong citizenship (v/s recent citizenship) a valid criterion? Is a prior rejected application a motivation for denials?
- ▶ How to avoid discrimination by sex, race or ethnic origin, religion or belief disability, age or sexual orientation?
- ▶ Who will act as "competent authority" to award the registered Passenger" status, in particular to immigrants or non-national? Is any kind of liability attached to such award (e.g. in the trusted passenger endanger security)?
- ▶ Who will store the collected data (and where, centrally or distributed, will it be stored)?
- ▶ How will the data be made accessible and who will have access?
- ▶ What kinds of security and privacy measures to implement, how far processing and transfer of Passenger Name Records' (PNR) personal data will be allowed when foreign counter-parts are involved?
- ▶ How to ensure mutual recognition, based on the trust that a person who has been granted the "Registered Passenger" status

in one country will be trusted in all the other Member States?

- ▶ Will the trusted status need to be verified on a regular basis? How often will this be necessary to safeguard against changes in passengers risk level (new intelligence information etc.)? How can this be automated?
- ▶ How to ensure that the checked passenger is the same person that was previously certified as registered traveller?
- ▶ How can the risk assessment criteria take into account the possibility of individuals with no previous records committing terrorist acts (such as in the London bombings? Would limiting the access to RP schemes to, say, frequent travellers with a certain established history with a frequent flyer programme help to reduce the risk?
- ▶ From which security checks could “Registered Passengers” be exempted without compromising security? What is the scope for lightening or accelerating certain checks without going as far as exemption?

The most appropriate technology

Regarding applied technology, the approach has to consider the use of dedicated lanes as test beds for emerging technologies to enable security checks to take place in an expedited fashion without interrupting the flow of traffic.

- ▶ “Corridors” of checks performed sequentially;
- ▶ Biometrics such as iris or face that would speed throughput (iris/face on the move) and alleviate health concerns about other technologies (i.e. fingerprints and transmission of bacteria).

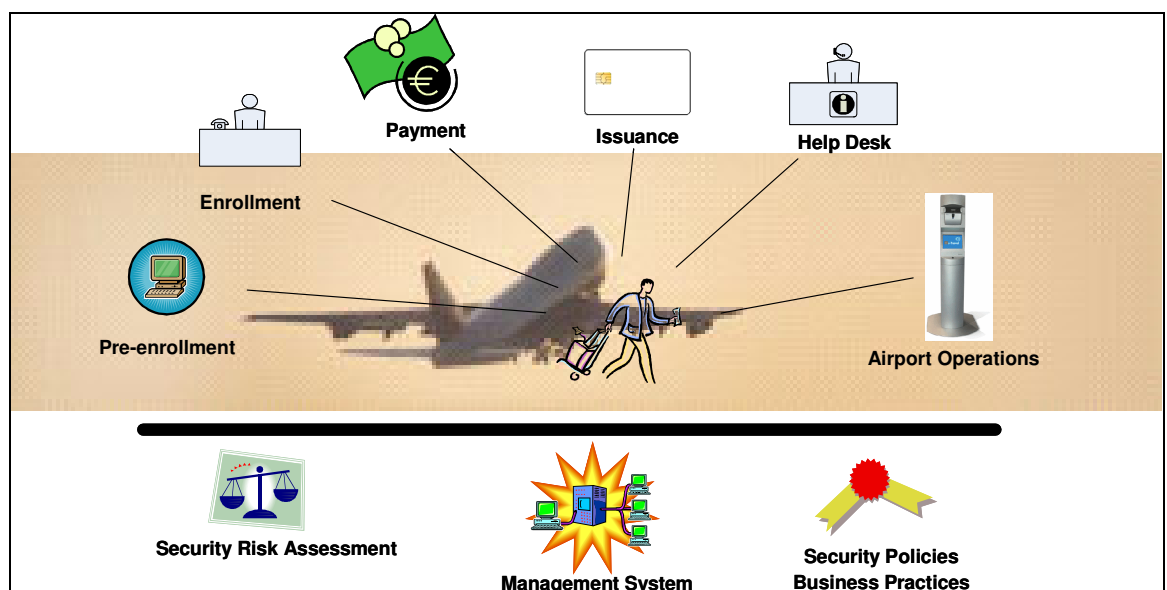


Figure: from pre-enrolment to airport operation, a whole set of operations to assess regarding risks, management, policies.

The creation of “Registered Passengers clear lanes” is complex because it requests also non-biometrics technologies, in particular concerning the detection of explosives and dangerous material. For passengers who could undergo a (EU valid ?) background check and pay an annual fee to receive biometrically encoded cards and access to a special lane for expedited passage through the security checkpoint, a major concern is predictability. For example, not having to remove laptops from cases, or not having to remove shoes in public are considered as the biggest benefits sought by potential members. Unfortunately, each advantage is related to the implementation of a specific technology: “shoe scanning” for example, is being tested in the US (Orlando airport¹) The Clear shoe-scanning technology, developed by [General Electric Security](#), is intended to detect traces of explosives and suspicious metal, and to allow most travelers to pass through clear lanes without having to remove their shoes. As all detection technologies are not equally mature, security specialists and integrators have the difficult task to carefully propose options that are really “reasonable” regarding the risks and provide more benefits².

¹ By Verified Identity Pass, which already operates a Registered Traveler program called Clear at Orlando and four other US airports.

² As reported by Larry Zmuda (Unisys) “the scanner rejected an unexpectedly high number of travelers’ shoes in Orlando, requiring members to remove their shoes just as they would at regular checkpoints”
http://www.nytimes.com/2007/01/30/business/30memo.html?_r=1&oref=slogin

2.2 Reducing welfare and identity fraud: saving €20 billion yearly?

For many stakeholders involved in the fight against welfare fraud, the use of biometrics looks as one of the most promising way to dramatically reduce recipient identification fraud. In UK only, identity fraud has been considered as one of the fastest growing crimes. When first studies done on 2002 estimated the costs at £1.3 billion a year, opponent to the reinforcement of controls questioned the seriousness of such numbers, reporting that it was based on unscientific estimations, combining multiple frauds in customs (VAT and money laundering), health, credit cards, driving documents. However, the most recent Home office updates (2006 numbers) reinforced early estimation, rising this cost at `£1.7 billion yearly³. The situation is not different in other Member States where even the Nordic States “welfare paradises” are now evaluating the need for global system reengineering. Extrapolated at the size of the European Union (492 million population in EU-27 – 60 million in UK) fraud could be estimated between 18 and 22 billion Euro yearly.

The most important issues that must be addressed in proceeding from a system concept to a successful operational solution could be defined as follows⁴:

- ▶ **Multiple registrations.**
Identification Matching is required for detection and elimination of multiple registration fraud, also known as "double-dippers". Implementation will consider system topology (numbers of terminals, hosts, nodes, interfaces, etc.), system capacity (number of current records, growth, archiving requirements, etc.), system performance (identification speed and accuracy requirements, query response timing, etc.), and other operational considerations (initial enrolment processes, records management, update procedures, etc.). This requires the development of a detailed set of specifications.
- ▶ **Fraud at Benefits Access Points.**
Identification verification at benefit delivery points could also eliminate many of the forms of recipient fraud. Decentralized verification could be the preferred approach, using a counterfeit-resistant ID card with encoded biometric information. In such field, smart cards storing biometrics data or two-dimensional bar codes representing biometrics are both low-cost and promising.
- ▶ **Lack of interoperability** with other Public welfare management systems. An efficient identification system must be interconnected with existing public welfare data bases, at least at European level. Interoperability of the systems will

³ <http://press.homeoffice.gov.uk/press-releases/identity-fraud-puts-1.7bn-hole?version=1>

⁴ See the similar approach developed by the State of California - http://www.sfis.ca.gov/id_req.htm

require not only interfaces between the new and existing systems for data interchange, but also an integration of biometric identification functions into the overall operations of the existing systems infrastructure. At European level, where person identification fields are by tradition extremely diverse, the adoption of common biometrics appears as a possible way to realise such interoperability. Such preoccupation should be considered in developing any new welfare database systems.

▶ **Needs of Interfaces to External Systems.**

In addition to integration with other public assistance management systems, interfaces with other systems could be necessary, if appropriate or legitimate to reduce frauds, i.e. with the various Member States national population registers, with the EURODAC data base concerning asylum applications, or with the Visa Information System concerning immigrants visiting Europe.

Some basic system requirements are fundamental to the use of any biometric technology in a welfare application:

- ▶ Biometrics must be based on unique human characteristic that is actually capable of automated matching.
- ▶ This matching must generate very low error rate regarding False Rejection and False Acceptance.
- ▶ Automatic one-to-many identification matching, with a high positive identification accuracy (near 100%) must be possible in searching database containing i.e. 50 to 100 millions of individual records
- ▶ Technology must be mature enough, providing a stable base for development of a large scale application where all “youth problems” will be already identified and resolved.
- ▶ Technology must be accepted in court as a legal proof of identity.

The most appropriate technology

Due to the five basic requirements above, fingerprints seems still today the most mature technology for welfare applications. Other technologies based on physiological characteristics (i.e. facial, eye retina and iris patterns, hand geometry, hand blood vessel patterns and bone structure, DNA, etc.) and behavioural (e.g.: voice, signature patterns and dynamics, and keystroke dynamics) had some successes in identity verification but were not experienced enough in very large applications. In some countries, fingerprint may have negative connotations related to criminal use. However, several studies demonstrate a growing acceptance from citizens (welfare applicants) if abuses impacting the whole welfare finances could be eliminated or strongly reduced: in UK, seven out of ten people

favoured compulsory ID cards as a way to fight fraud⁵.

2.3 Biometrics in Banking and Finance

Most security conscious financial institutions are investigating for implementing new authentication technologies. They are demanding multi-factor authentication: a password with something else, a token such as a device generating code numbers, a smart card, and a USB device. As such devices may be stolen or copied, sometimes together with the password and other personal data (who has not his password list written somewhere or on his PC?) Enterprises are evaluating biometrics for more security, portability and ease of use. The financial sector has been cautious in its adoption of biometric technologies to combat identity theft for many reasons:

- ▶ Reluctance to be early adopters of technology that continues to mature in technical capability and reliability;
- ▶ Concern about negative customer reaction;
- ▶ Few customer implementations demonstrating quantifiable cost savings;
- ▶ Higher internal system development priorities;
- ▶ Preferable expenditures on alternative technologies and consumer education about identity theft;
- ▶ Lack of clear structure and business model for cross industry/multi-company implementations;
- ▶ Difficulty of presenting and implementing new biometric solutions to a complex payment system;
- ▶ Operational issues such as data security;
- ▶ Cost and complexity of deployments given legacy system integration, interoperability concerns, and absence of standards.

Therefore, the choice of which biometric to use, or the 'best' biometric to use is less a function of the core technology than it is a function of how, where, and why, based on a detailed cost-benefit analysis; and on customers' comfort level.

After an initial enrolment, subsequent activities are usually transactional in nature. A number of banks and financial institutions have developed prototypes of biometrics to use for employee access control and other limited internal functions, as well as for access to specific products and services used by customers. The results of the trials often have been positive in terms of functionality and customer acceptance.

⁵ See: [BBC http://news.bbc.co.uk/1/hi/business/4311693.stm](http://news.bbc.co.uk/1/hi/business/4311693.stm) , The Independent: <http://news.independent.co.uk/uk/crime/story.jsp?story=616326> or The Times: http://www.thisislondon.co.uk/news/articles/PA_NEWMONEYIDth01idfraud?source=&ct=5

Various systems are currently experienced:

- ▶ Hand geometry to permit customer access to safe deposit boxes;
- ▶ Smart token containing fingerprint biometrics housed in a key fingerprint reader at the teller window to match the customer fingerprint against the biometric fingerprint data stored on a smart device (a match causes the device to transmit account information stored in the device to the teller, thus authorizing a transaction);
- ▶ Laptop computers with keystroke biometrics;
- ▶ Two-factor authentication systems where a traditional password is combined with biometric;
- ▶ Signature recognition could eliminate the need to manually compare signatures (dynamic signatures could be captured without adding burden by using electronic signing pads when a customer opens a new account and be used subsequently in future transactions);
- ▶ Iris and facial recognition
- ▶ Palm or digit vein patterns recognition

The most appropriate technology

Despite some successes, a documented US study⁶ led to the conclusion that biometric technology was not yet a “silver bullet” for reducing identity theft generally or identifying the party to a financial transaction specifically. Issues can be grouped in three areas: technological and operational issues, cost and consumer acceptance.

A commonality with all these technologies is the difficulty to process easily with on-line transactions that are now becoming the preferred way of banking for a new customer generation: they are more adapted for authentication “in the bank premises” or possibly in shops or restaurants (“pay by touch” systems at the time of paying with a credit card). At the contrary, on-line transactions requires large scale hardware rollout in customer’s homes. Issues are not so much related to the cost of such devices (less than € 50 for a facial recognition camera or a fingerprint reader) than to implementation (support by the various hardware and operating systems) maintenance, help desk and interoperability, and than to the danger of specific related fraud: without very elaborated “life test” detection, could it encourage some new forms of home jacking?)

⁶ The Use of Technology to Combat Identity Theft - February 2005 Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act. http://www.treas.gov/offices/domestic-finance/financial-institution/cip/biometrics_study.pdf

For home banking, new developments in voice authentication seem the most promising as it requires no or minimal hardware: most personal computers already contain a microphone. The new generation mobile devices (internet connected GSMs, the new Apple iPhone etc) already combines voice and internet transactions. At the end of 2006, **Agnitio** (a spin off of the University of Madrid) presented a new biometric voice verification product as the most convenient solution for online banking, finance and corporation sectors. The system can be used from any fixed or mobile phone. It prevent pre-recording frauds by randomly generating numbers which callers need to speak (these numbers are then matched to the enrolled voice pattern). The main advantage of such system is that it cannot be used without an active participation of the customer and that it provides a growing interoperability and a good privacy (no specific hardware at customer side, it may be used for multiple purpose and combined with classical password or pin code). Occasional disadvantages are related to poor quality and ambient noise, however this is less critical at home or by choosing any silent place than in open public space.

3. Trends in biometrics technology

By Ronald Huijgens, Director
Biometric Technologies, Unisys

Many existing products have evolved and have reached maturity, and there are many new products that have been or are about to be launched since the previous report was issued. We have seen the market develop, partly driving this technological evolution based on new or changing requirements and changes in legislation. The new technology also enables new business applications. So, there are both a market-pull and a technology-push that continuously bring biometric technology to a higher level. It is interesting to observe that this is in line with the trends in the smart card industry, where the next generation Global Platform and JavaCards take that industry to the next level of maturity. This will further enable the introduction of highly secure, flexible and personalized services. The combination of smart card technology and biometrics will be the foundation for this. In this chapter, some of the new technologies and product evolutions will be described. It is impossible to mention all new developments, but the most eye catching developments are described below.

3.1 Evolving Markets

Society is getting ready for deployment of biometric technology. This is reflected in both the public and private sectors.

Public Sector

In the public sector, we a trend towards introduction of biometrically enabled (national) ID cards, health and social security cards and drivers license cards that allow provision of services to citizens who are entitled to receive it.

Biometrics, often fingerprints, enable service providers to positively identify their clients and deliver the appropriate services to that individual only. All over the world there are large projects for issuing these cards, and biometrics is being introduced as prominent means of user authentication.

A side effect of this is that some services, like health services, are no longer available to people who do not have such a card. This became clear in the Netherlands after the introduction of a new health care system.

The planned introduction of the Visa Information System in the EU creates a new demand for high volume, high quality fingerprint capturing all over the world. This also initiated the development of the largest biometric identification system.

From August 28, 2006, EU countries have started issuing ePassports, which support automated facial recognition now, and which will support automated fingerprint recognition as of 2009. This requires EU Member States to expand their travel document systems with fingerprint capturing capabilities. This creates the potential of being able to detect individuals having multiple identities. National legislation obviously needs to allow this. It can be expected that there will be discussions on this related to the protection of citizen data, which is one of the fundamental rights in the Union.

Events, such as the MP3-murder in the station at Brussels in 2006, the recent car bombings in Madrid and the well-known other terrorist attacks in the past years, have increased the need of intelligent video surveillance and well trained staff whose effectiveness can increase dramatically with this technology. It would be great to be able to predict if and when an individual will throw a street tile from a fly-over on a car driving on the highway, by just analysing his behaviour from live video footage. This can really save lives. In many countries, there are initiatives to test technology for this purpose.

Private sector

In the private sector, the financial institutions are very active at this moment exploring possibilities for developing new services, which can be personalized, are very secure and are attractive to their clients, while reducing operational costs and improving the client experience. A good example of this is the ABN AMRO bank in The Netherlands, who have launched a telephone service with user authentication using voice verification, which enables their clients to do telephone transactions in a very secure way.

The same trend is visible in the transportation sector, where airlines and air- and seaports can distinguish themselves by providing outstanding, personal services. Biometrics enables this, providing reliable positive identification or ID verification of travellers. One good example here is the move in the US to implement Registered Traveller programs in the airports. In this case, applicants with approved background checks pay a small fee for a smartcard containing their ID and biometrics to move through security checkpoints more easily.

Also in other areas the interest in developing solutions for customer convenience and loyalty is growing. There is legislation that is mandating companies to implement these schemes, but the idea that biometrics can actually be used to improve competitiveness is gaining momentum.

Next to supporting their front-office process with biometrics, the industry is exploring the benefits of deploying biometrics in the back-office. Many applications are developed, such as physical and logical biometric access control systems. Other examples are location based access control systems that use knowledge about the location where the user resides to control access to resources. And, this is true for both fixed and mobile workstations.

3.2 New and emerging products

We see an interesting trend towards low-cost and easy to use devices, applications, less complex infrastructure, high reliability, integration with existing infrastructure components and the introduction of mobile devices and applications.

3.2.1 True Single Sign-On

For years it has been possible to implement Single Sign On solutions that allow users to log on to their PC, and get access to all the network resources automatically. User authentication can be based on a secret (username/password or PIN), a token (smart card) or a biometric feature or combinations of each. Many vendors have solutions for this.

Mobile users may require hard-disk encryption to protect their data. Again, there are quite a few vendors of those products, including some that use the biometric tie as a part of the encryption. However, for the users of mobile PCs with disk encryption, this is not very nice. After power-up, they need to authenticate to the boot software, then after a while they must log on to the operating system.

In 2006, Precise Biometrics and WinMagic created a solution for laptops and desktops, including hard-disk-encryption and Single Sign On. The solution makes use of the Precise Match-on-Card(TM) technology that increases the security of the system, and also preserves the user integrity by storing and matching the fingerprint information on the card itself. Just switch on the PC, plug in your card that holds your fingerprint information, put your finger on the scanner when prompted, the system boots and off you go. Now, that is convenience **and** security at the same time.

3.2.2 Biometric Security Card

One Time Passwords have also been around for many years. The issue was always, that once your OTP device was lost or stolen, security could be compromised.

[Quard Technology](#) from Denmark has patented its 'Biometric Security Card' solution that integrates fingerprint recognition and smart card technology. The result is an OTP device that will generate an OTP after the user has been authenticated to the device. Nobody else can use the device. Since the fingerprint is stored only on the QuardCard itself and NOT on any server system or database, it fully complies with regulations about privacy and data protection. Authentication in the network is based on Radius Technology in combination with the OTP server. This is a very useful solution for on-line transactions, very secure with very little investment required in the network.

It may be possible that this technology can be integrated in the smart cards of the future, sticking to the physical requirements of the card. Another company in the US, Identitia has several smartcard-based solutions that generate a random key the user enters or a series of tones that can be used to sign on.

3.2.3 Electro-physiological Signal recognition

Everybody knows that the human body uses electric signals. We can use that to detect how organs perform, just think about the electrocardiogram (ECG) to monitor the heart or the Electro Encephalogram (EEG) to monitor the brain's activity.

[IDesia's](#) BioDynamic Signature™ (BDS) is the first and only personal biometric authentication technology that captures electro physiological signals unique to each individual. These signals are naturally emitted by different systems of the human body (such as the heart and the nervous system) and share numerous common characteristic features.

This is very interesting technology, it is very easy to use, and you do not need to leave any physical features, like fingerprints or photos, just touch two contacts with your fingers. Placement of the fingers (orientation, position) and their condition (dry, normal, wet) of the fingers is not critical. This also implies spoof detection, as it is really difficult to imitate the signal.

The technology is still young, but this year it will be available on the market. The specifications of the performance characteristics are promising, but when the first independent tests have been conducted we will know what the value of this technology really is. Currently, independent tests are being conducted by the National Physics Laboratory in the UK. Keywords are ease of use, low cost, high accuracy and durability, security, small footprint, high durability and reliability.

3.2.4 Laser Surface Authentication™

[Ingenia Technology](#) has developed a new, patented Laser Surface Authentication technology to analyse the surface of any item and to translate the unique structure of the item into a digital code. This code can be regarded as a fingerprint that uniquely identifies the item. In this way it is possible to authenticate documents, cartons, cards etc.

The application is not limited to authenticating documents, it would also be possible to detect false brands on, for instance, jeans.

Although this is not a biometric technology, it has the same goal, and it can help secure documents in various sensitive processes, such as in court cases.

3.2.5 Voice Verification and Analysis

Voice recognition is a technology that is well accepted by the public. The telephone has helped this, for sure. With voice technology, using speech recognition and voice authentication, it is possible to create interactions with the user, increasing the accuracy and reliability of positively identifying the user while enabling them to navigate help desk and other activities without human intervention..

The technology is being used at banks and with insurance companies to verify identity when making telephone transactions and performing account maintenance.. It is also being used extensively in many markets to reset passwords in corporate networks, reducing costs.

The technology is also used to reduce fraud in welfare programmes, such that only people who are entitled will get the benefits.

In forensic science, voice analysis technology is becoming available to determine the truthfulness of responses a witness gives as part of an investigation.. The technology is becoming mature enough to be combined with other technology, such as video surveillance, and to be used in solutions that prevent unwanted behaviour in public areas.

3.2.6 Embedded biometrics

Biometric sensors are getting smaller and smaller, the algorithms improve all the time, processing capabilities of mobile devices increase continuously. This is Moore's law in practice.

New products are being announced, bringing biometric user authentication to commodity products such as cell phones. [OKI](#) and [JIRIS](#) have announced iris recognition for cell phones. This would make the cell phone a real personal device. [LG](#), [Motorola](#) have equipped models with face- and fingerprint authentication.

The user can then authenticate to (the SIM card in the) phone, making the device personal, but also allowing the user to perform secured transactions.

The same goes for PDAs, the border between cell phones and PDAs is vanishing. Nowadays you can make phone calls with your PDA or write e-mails with cell-phone. So, embedded biometrics enable the development of personal, multi functional, mobile devices.

PC's are being equipped with Trusted Platform Modules (TPM), sometimes integrated with a fingerprint sensor, which means that the PC will become a personal device. The security features of the TPM can be useful when biometrics are required for user authentication, as that enables secure storage of the data. However, it can be questioned if the TPM is necessary for creating secure solutions.

Biometrics are also being integrated into rapid access portals to verify the identity of persons attempting to enter. Coupled with the new Gen2 RFID card, verification of ID is very quick since the card can be read from a range of 5-7 meters and access privilege checked as they approach the doorway, face recognition confirms the person's claim of identity.

3.2.7 Fingerprint technology

With the market asking for more, more reliable, accurate, affordable and easy to use fingerprint capturing devices, the industry is introducing new products at a high speed.

Traditional, criminal and forensic applications were all supervised by well-trained staff. With fingerprint technology becoming more accepted by the public, self-service applications and semi self-service applications will be developed and deployed more often.

This means that user-friendliness, accuracy and spoof detection capabilities are important. We have seen [Lumidigm](#) introduce their single print J1x0 scanners at Disney World that have all those features. [L1-Identix](#) have released the TP 4100 scanner can capture dry and even soaking wet ten prints of high quality, and [NEC](#) with it's H-Scanner can capture very good prints. [Crossmatch](#) is using excellent optics with heated platens in their newest products. All vendors continue to improve their products.

3.2.8 Vascular Pattern recognition

Vascular pattern recognition, from [Hitachi](#), [Bionics](#), [Fujitsu](#) and others, is taking off, and is being installed in many places. While access to residences, particularly in Japan has been the main applications, banks are beginning to use it to verify identify instead of using fingerprints. The technology is very accurate, as it uses the random pattern of blood vessels underneath the skin. It is also the most private biometric in as much as it does not leave a latent image like fingerprints or material like DNA. Not can it be read from a distance like face, iris, and voice. It is also easy to use, and it is contactless, though some sensors feature support brackets to help position the hand or finger properly.

3.2.9 Iris recognition

In the previous (2006) report, we mentioned developments from the University of Bath (UK). Throug [Smart Sensors Ltd](#), it has resulted in a new, independent suite of iris image pre-processing, recognition and matching algorithms with an SDK available since mid-2006.

This project has also collected a significant iris image database (400 people, 16000 reference quality images) with a subset of 50 people, 1000 "bad" test images. This database has been collected specifically to offer a test resource that can set aside many issues caused by collection of images using commercial cameras (e.g. focus blur, motion blur, illumination differences, reduced resolution, image sub-sampling and compression). Tests where done with [Sarnoff](#) Corporation to demonstrate successful use of algorithms within their Iris On the Move terminal, conducted by Deloitte/NPL in the UK which reported at the UK Biometrics Conference in October 2006.

[Jiris Co., Ltd.](#), a company based in Korea, has presented a new iris recognition algorithm, which differs from the algorithm patented by L1 Identity Solutions.

They offer a range of cameras and an SDK that allow the creation of iris based solutions. Using a modified low cost web cam with a two way mirror, covering the lens, individuals can quickly centre there eye and capture is nearly instantaneous from several inches away. This is the first iris recognition solution that works outdoors using the natural IR present in sunlight.

While L-1 Iridian, Panasonic, and LG have iris cameras that can capture two irises at a time, the camera head must be in the correct position before the iris can be captured (enrolled). The iris camera from Oki automatically locates the eyes, zooms in to capture the iris, and captures the images automatically, significantly enhancing the customers' experience.;

3.2.10 Face recognition

Over the past few years, the performance of face recognition solutions has increased significantly. With the advent of 3D face recognition from companies like A-4 Vision and AC Technology, lighting issues have been largely overcome. Smaller high resolution lenses and higher density sensors have enabled 2D face recognition solution providers to embed their solutions in a variety of new applications. Cognitec recently announced the release of surveillance solution that can locate the faces of and identify up to 20 individuals in a single frame. 3VR, a video surveillance solution company has integrated the Cognitec engine into their video recorder solution that enables alerts to be sent when a particular face is recognized, and searches can be made through a database containing feeds from thousands of cameras to identify other instances where that face has been seen.

4. Recent developments in EU and Member States

By Marc Flammang, Consultant,
EU management consulting team,
Unisys

4.1 EU

Recent developments of Biometrics in European affairs come in line with the continuation of efforts regarding the implementation of the new SIS-II and VIS systems and of new policies applied for the fight against terrorism and the border control.

In Member States (MS) two main debates occurred in parallel: the difficulty for the MS to comply with the US-Visa wave Program deadlines and the security risks in Biometrics technologies. This section firstly describes the different events that took place at a wide EU level and then gives the most relevant facts country by country.

Background:

Likely in response to (non-binding) standards set by the International Civil Aviation Organization (ICAO), an agency of the United Nations, and requirements put in place by the U.S. government for its US-VISIT Program, Member States of the European Union (EU) have begun including biometric identifiers in passports. Under the US-VISIT program, as of 26 October 2006, the 27 countries that are participating in the U.S. visa waiver program⁷ must issue machine-readable “e-passports.” These passports must contain an integrated computer chip capable of storing biographic information from the data page, a digitized photograph, and other biometric information.⁸

Member States strive to be in line with the US-Visa waiver Program

In 2004, the EC issued a regulation that stipulates that passports and travel documents shall include a storage medium which shall

⁷ http://www.travel.state.gov/visa/temp/without/without_1990.html#1

⁸ <http://www.parl.gc.ca/information/library/PRBpubs/prb0630-e.htm#bunited>

contain a facial image, and that the documents shall also include two fingerprints in interoperable (across the EU) formats⁹. All Member States had until 28 August 2006 to implement the facial image requirement, and have until 28 June 2009 to implement the fingerprint requirement.

EU news since June 2006:

In August 2006, short time after bombing attempts were reported to be discovered in London-Heathrow, European ministers pledged on August 16 to increase their cooperation against terrorism. Ministers from Finland, Germany, Portugal, Slovenia and France met in London with British Home Secretary John Reid to map out new anti-terrorism measures. Afterward, they announced the allocation of nearly 200.000 Euro to research the best ways to detect liquid-based explosives. Franco Frattini, vice president of the European Commission, said passengers on flights to or from European nations may be subject to biometric screening, which could include fingerprint and iris scans.

In the same month, according to an EU document presented by Statewatch (in July 2006), The Visa Working Party on 13-14 June 2006 proposed another approach on the issue of the biometrics to be introduced on national ID cards. The issue had met resistance back in February when several members of the European Council have expressed doubts especially as Belgium and the Czech Republic opposed to the measures proposed by EU, without a public debate. In December 2005, the two governments had given a statement by which expressed their view that the introduction of biometrics into the ID national cards involved discussions of private life protection, financial and organizational issues, besides the technical aspect.

In September 2006, while the 30 September deadline imposed by the European Court of Justice for the EU to end passenger data transfers to the US was rapidly approaching, the European Parliament has adopted a report calling on the US to ensure that it offers adequate protection of European passenger data and that sufficient safeguards are in place¹⁰.

During the same month, European ministers agreed to Spanish and Italian requests that they share some of the burden of illegal immigrants arriving on their shores, even as Spain came under criticism for regularizing many illegal aliens. European Union interior and justice ministers meeting in Tampere, Finland agreed that the EU as a whole should negotiate agreements with African countries where the migrants are from, rather than leave it up to the receiving countries alone.

⁹ This regulation is binding for all Member States except the United Kingdom and Ireland that sets out minimum security standards for passports and travel documents

¹⁰ European Parliament Press Release

In October 2006, only seven out of 25 MS had respected the deadline of the 28 August where they had to be able to deliver the biometric passports. Therefore, the European Commission had to postpone by 20 days the transition period. For different reasons, Europeans take a lot of time to put this decision into practice: so far only Austria, The Netherlands, Denmark, Belgium, France, Germany, Sweden and the Czech Republic were able to deliver this type of passports¹¹.

With some fears of an eventual chaos between the Atlantic allies, officials from both sides of the US and European Union have confirmed that a new anti-terrorism agreement was almost certain to be signed on two days before the current regime expires for sharing airline passenger information. The US had been pushing for revisions of an existing accord that was ruled illegal by the EU's top court and expires on September 30. However, because time is short it has accepted the EU's offer of a similar deal under a different legal basis that would satisfy the judges. In return the EU has pledged to start almost immediately negotiations on a new framework that could incorporate additional US demands, with the aim of implementing it well before November 2007, when the new deal will expire¹².

Regarding SIS-II and VIS, the next generation large systems currently developed at DG Justice, liberty & Security, the SIS/VIS Biometric Matching System (BMS) was awarded on 26 October 2006 to a consortium formed by Accenture and Sagem Défense Sécurité¹³. This will cover both the supply of hardware and software for a large-scale BMS for fingerprints and the provision of related services. The BMS implementation in the new Schengen Information System II (SIS) is complemented by the development, installation, maintenance and support of a BMS for the future Visa Information System (VIS). At a later stage, it may be necessary to extend and connect the BMS to other large-scale IT systems in the field of justice, freedom and security.

In November 2006, following the US requirement that EU passports must be biometric enabled by 26 October, the EU Council has published a document which provides a record of member's states who have reached this requirement and others who are working towards it.

In parallel, critics of the EU's planned biometric passports scheme note that the inclusion of a digitized photograph in passports meets the standards set by the ICAO, but that the EU has gone further by requiring the inclusion of fingerprints. They also point out that

¹¹ <http://www.fenetreeurope.com/php/page.php?section=actu&id=6401>

¹² www.ft.com/cms/s/f3fac4c0-4cc6-11db-b03c-0000779e2340.html

¹³ Official Journal 29 December 2006 (2006/S 247-265231)

since only two fingerprints will be taken, the error rate for an EU-wide database will be relatively high if it is to be used for identification (rather than just verification) purposes.

In November 2006, the EU-funded FIDIS (Future of Identity in the Information Society) Network of Excellence (NoE) has issued a stark warning that implementation of the current generation of biometric travel ID will dramatically decrease security and privacy, and increase the risk of identity theft. Indeed it stated that “the current implementation of the European passport utilises technologies and standards that are poorly conceived for its purpose”, and recommends that corrective measures should be adopted by stakeholders in governments and industry to address outstanding issues. Failure to do so will exclude EU passengers from participating in the US Visa waiver Programme.

In December 2006, The European Data Protection Supervisor, Peter Hustinx has issued a follow-up opinion to the proposal for a framework decision for data protection in the third pillar. Worried about indications that current negotiations in the European Council are leading to a fragmented and lowered level of protection for the citizens, the European Data Protection Supervisor (EDPS) has strongly urged EU member states to reconsider their current positions. The EDPS has said that he is concerned that legislation aiming at facilitating police and judicial cooperation might be adopted while the legal data protection framework is delayed and diluted.¹⁴

In January 2007, The European parliament has given final approval to the creation of a European driving licence, which will replace the many national licences used in the EU. The credit card-style licence, with photograph and possibly a microchip, will start to be introduced in 2013.

By the end of 2007, the interior ministers will make the final decision, whether all necessary conditions are met, in the Council under the Portuguese presidency. Poland, Hungary and eight other ‘new’ European Union member states should join the Union’s border-free area from the end of this year under a deal reached in Brussels last month. EU Home Affairs Ministers agreed that the countries could enter the Schengen zone on December 31 2007 on condition that they met security and technical criteria.

4.2 Relevant news in brief, by Member State

¹⁴ <http://www.eubiometricforum.com/index.php?option=content&task=view&id=594&Itemid=2>

AUSTRIA

In November 2006, 3M ePassport Verification Systems have been chosen and installed at passport issuance locations throughout Austria. The 3M ePassport Verification System gives Austrian passport holders a means to personally check the electronic data stored on the new high-security passports the country began issuing in June.

BELGIUM

In November 2006, a press release¹⁵ stated that already 4 millions of citizens had an electronic ID. It seems so far to be a real success. By 2009, 8.2 millions electronic ID cards should replace the former ones. Non-Europeans living in Belgium could also receive one. The current e-ID card however does not include biometrics. This could be the case with a new release, for which Belgium could look for collaboration and standardisation with a pool of other Member States.

CZECH REPUBLIC

Early September, the Interior Minister declared the launching of Biometric securised passports. In October, Mrs. Radka Kovarova, the spokesperson of the Minister, stated that the delivery of the Biometric passports was a success in the whole country.¹⁶

DENMARK

In September 2006, Danish Biometrics entered into an agreement with Copenhagen Hospital Corporation about testing, research and development on biometric recognition. The objective of the agreement is to result in solutions for secure log-on procedures when doctors and nurses for instance are entering the Electronic Patient Records (EPR) as part of their daily routines.

The 6th of October, the Integration Ministry of Denmark and Sagem Defence Security signed a contract for providing a system capable to register biometric data of Visa applicants. This project should take 4 years to be implemented and the information could be used in the VIS (Visa Information System).

Four days before, Gemalto announced that the Danish National Police had started issuing electronic passports that integrate the most advanced secure technology.¹⁷

¹⁵ <http://www.zdnet.fr/actualites/informatique/0.39040745.39364280.00.htm>

¹⁶ http://www.menara.ma/Infos/includes/detail.asp?article_id=11766&lmodule=Technologie

¹⁷ <http://www.tmcnet.com/submit/2006/10/02/1945261.htm>

ESTONIA

In October 2006, Gemalto has been named by the Citizenship and Migration Board of Estonian Republic as the provider for future Estonian electronic passports¹⁸.

During a visit of President Bush in December 2006, the US President called for an expansion of the Visa-Waiver program to additional countries, such as Estonia. The President's proposal ran into criticism from those who called it an expansion of a dangerous loophole in the nation's effort to secure its borders¹⁹.

In January 2007, Cognitec Systems has announced a deal with IBM Estonia to provide facial recognition technology for the Estonian Ministry of Internal Affairs, Citizenship and Migration Board. The technology will be used as part of a large ID management system, including the country's ePassport project, which will see documents rolling out from March this year.

FINLAND

In July 2006, Finland's Ministry of the Interior assured in a statement that there were no security problems with the new biometric passports to be introduced in August. "Finland's new passports meet all the requirements set for biometric passports."²⁰

FRANCE

Since October 2006, the debate in France has been quite strong against the entry into force of an electronic DNI (called "Ines") as different voices rise against the project : political parties, forums or Human Rights NGO's. Therefore, a law on electronic ID cards shouldn't be expected before the Presidential elections.²¹

Moreover, the Commission Nationale Informatique et libertés (CNIL) refused to give its approval, blocking completely every project involving biometrics.

¹⁸ <http://ipcommunications.tmcnet.com/hot-topics/security/articles/3198-estonia-adopts-next-gen-immigration-solution.htm>

¹⁹ <http://portsecuritynews.com/news/templates/registered.asp?articleid=1323&zoneid=1>

²⁰ http://www.bioxs.nl/go_web.php?id=622&link=1982

²¹ <http://www.zdnet.fr/actualites/informatique/0,39040745,39363810,00.htm>

GERMANY

In Germany, different initiatives have taken place in which biometrics were included: casinos, train stations²², schools, etc. These projects have been carried out in parallel with some reinforcements of the use of biometrics in the border control.²³

In October 2006²⁴, a press release declared that an electronic “foreigners’ card”, similar to the planned eID card for German citizens, may soon replace residence permits in Germany. In this view, electronic ID cards would be then a further contribution to the development of biometrics on Germany, providing digital signatures and making positive identification possible on the internet, thus eliminating security problems such as phishing.

IRELAND

In October 2006, The Irish government has begun issuing RFID passports with biometric data that can be read at a distance to comply with US regulations for its visa waiver programme. But unlike the RFID passports the USA is now issuing, the Irish ones lack a security feature preventing them from being skimmed, or read surreptitiously.²⁵ Ireland has launched its e-passport, just days ahead of a US deadline to bring in biometric passports or risk being booted from the visa waiver scheme. Ireland is one of the top 10 visiting nations to the US, and some 500,000 people visited the country last year. The cost of introducing the e-passport was estimated at €8.8m at the outset and it has been completed for €6.1m.²⁶

In December 2006, two Irish law enforcement agencies, the Irish Naturalisation and Immigration Service and Ireland’s National Police Service (An Garda Siochana), have signed an €18 million deal to support the introduction of new digital fingerprinting technology. An international consortium, including Accenture, Motorola and Daon Biometric Systems, have been commissioned to design and implement a new integrated electronic fingerprint system, or automated fingerprint identification system (AFIS), for use by police and immigration services.

ITALY

²² http://www.cio.com/blog_view.html?CID=26000

²³ http://www.bioxs.nl/go_web.php?id=622&link=2275

²⁴ <http://de.internet.com/index.php?id=2045782&ion=Marketing-News>

²⁵ http://www.theregister.co.uk/2006/10/23/smart_chips_for_smart_crooks/

²⁶ http://www.theregister.co.uk/2006/10/17/ireland_epassport_launched/

During the month of September and October 2006, related news on Italy dealt with the insertion of biometrics in schools²⁷. The march of technology now means school children here can pay for their cafeteria with their fingers. For instance, Rome City Schools is switching to a scanning system that lets students use their fingerprints to access their accounts.²⁸

LATVIA

In January 2007, the Latvian government has awarded German technology group Giesecke & Devrient (G&D) a contract to produce 1.1 million ePassports over the next five years.²⁹

LITHUANIA

In December 2006, the Ministry of the Interior of Lithuania, BIS Bundesdruckerei International Services GmbH has developed an e-sticker for biometric passports. Bundesdruckerei GmbH is to supply the corresponding electronic personalisation system which will allow an upgrade of the Lithuanian passport system.

LUXEMBOURG

End of August 2006 was the time for External Affairs Minister, Nicolas Schmit, and the Minister of the Public Function, Claude Wiseler, to announce the entry into force of the Biometric passport. Some changes with the past are linked to this new passport, namely: criteria for the picture are stricter, children must have their own passport, and validity of the passport will be of 5 years³⁰.

MALTA

In November 2006, the British High Commission issued its first biometric visa to a non-EU citizen wishing to travel to the United Kingdom on Wednesday. The British High Commission has been the first foreign representative office in Malta to issue visas using biometric technology. This state-of-the-art system has for purpose to recognize applicants' fingerprints using an electronic scanner, before sending them to a central database for cross-checking against previous applications.

²⁷ http://www.silicon.de/enid/client_server_host/23410

²⁸ http://www.bioxs.nl/go_web.php?id=622&link=2107

²⁹ <http://www.securitydocumentworld.com>

³⁰ <http://www.mae.lu/mae.taf?IdNav=2652>

THE NETHERLANDS

A new Dutch passport with a chip containing biometric data of the holder has been introduced on August 26. Starting on that date, all new passports had personal data chips that contained facial features of the holder. The data in the chip can be read worldwide. The Census Office has required the new type of picture in passports for quite some time.

NORWAY

In December 2006, Motorola announced a contract with Norway's Ministry of Foreign Affairs and the National Police Computing and Material Service to provide for the collection and verification of biometric data for Norwegian passports, visas and other travel documents.³¹

POLAND

In October, Poland launched officially the introduction of its biometric passports. At a first stage, the biometric passports will only numerise the faces of people. Passports delivery should take 15 days and cost 35 Euros (which is more expensive than the former one)³².

PORTUGAL

On the 28th August 2006, Portugal joined Belgium, Sweden, Norway, Germany, UK and few other countries and started issuing new electronic biometric passports fully compliant with the standard recommended by the International Civil Aviation Organization. Nevertheless, the previously issued normal passports remain valid until expiry.

One of the main goals of the new electronic biometric passport is to combat fraud and forgery through the use of facial image recognition technology and of high-capacity, contactless integrated circuit chips.

³¹ www.kauppalehti.fi/.../releases/press_release.jsp?selected=other&oid=20061201/11653112164690&lang=EN

³² http://www.menara.ma/Infos/includes/detail.asp?article_id=11766&lmodule=Technologie

ROMANIA

In September 2006, according to a release from the Romanian Interior Affairs Ministry, the Biometric passports would be introduced at the beginning of 2007. These passports will take 20 days to be issued, both at central and local level.

The release also stated that in order to make the transition from the old passports to the electronic ones easier, temporary passports valid only for one year, will also be issued in 2007. Passports which are now being used are going to be valid until the expiry date written on them.³³

SLOVENIA

At the end of August 2006, Slovenia started issuing its new biometric passports, featuring a biometric facial scan, and in accordance with EU Regulations requiring all Member States to include facial scans on their passports as of August this year. It is also in response to requirements set by the USA for countries with a visa-free entry regime (Visa Waiver Programme – [VWP](#)).

A few days before this declaration, ID Development had announced that it would provide data capturing software technology for electronic passports for Slovenia³⁴.

SPAIN

In July 2006, Spain's national printing office has contracted Sagem Défense Sécurité to provide its biometric software licences for use in its new national electronic ID card, DNI-e. The software matches the DNI-e holder's fingerprints with those securely stored in the chip. According to the company, "this allows the identity of the DNI-e holder to be checked while ensuring the confidentiality of the biometric data".³⁵

SWEDEN

In October 2006, Scandinavian Airlines declared it had become one of the world's first airlines to introduce biometric security check-ins. It is now using biometric security at baggage check-in and boarding gates on domestic services across Sweden, following a

³³ http://www.daily-news.ro/article_detail.php?idarticle=29713

³⁴ <http://openpr.com/news/10718>

³⁵ <http://www.securitydocumentworld.com>

successful trial period in northern Sweden. This is part of Scandinavian Airlines' vision of "simple travel" to maintain an efficient self-service flow as security requirements are intensifying at the airports³⁶.

In November 2006, the result of tests of the biometric technology implemented by SAS showed an improvement in passenger flow beyond expectations, and a warm welcome to the introduction of biometrics by passengers.³⁷

SWITZERLAND

Since 4 September 2006, the Swiss can apply for biometric passports. This type of passport not only involves "engraving" personal data into the document, but also storing it on microchip. Within the framework of a six-year contract, Siemens has developed the solution for capturing and verifying the biometric data of Swiss citizens and checking Swiss biometric ID documents. This system is based on ID document readers and fingerprint scanners from CrossMatch Technologies, a photo capture station and camera from Digital Card Systems (DCS), and the Homeland Security Suite from Siemens, developed by the Biometrics Center of Siemens PSE (Program and System Engineering) in Austria³⁸.

In the same time, some biometric applications have started to be used by Private Banks³⁹.

UNITED KINGDOM

At the contrary to France, where initiatives are blocked both by the CNIL and by the proximity of presidential elections, UK is currently the main area for debate around biometrics and identity management.

Background information⁴⁰

In 2006, and as explained in the former trend report, the British Parliament passed legislation to introduce biometric-based national identity (or ID) cards⁴¹. Under a timetable set out when the legislation was passed, from 2008 onwards, everyone renewing a

³⁶ www.etravelblackboard.com/index.asp?id=56240&nav=2

³⁷ [http://www.travelbite.co.uk/newsbrief/flights/scandinavian-airline-first-use-fingerprint-scans-\\$452572.htm](http://www.travelbite.co.uk/newsbrief/flights/scandinavian-airline-first-use-fingerprint-scans-$452572.htm)

³⁸ 28 June 2009 is the deadline by which the Schengen countries will have to include fingerprints into their passports as well.

³⁹ <http://www.ws-huethig.de/news/5/d7424e4fb87.html>

⁴⁰ <http://www.parl.gc.ca/information/library/PRBpubs/prb0630-e.htm#bunited>

⁴¹ http://www.identitycards.gov.uk/downloads/ukpga_20060015_en.pdf

passport will be issued an ID card and have his or her personal information (including biometric data) placed in an associated database – the National Identity Register. The biometric portion of the system will likely use face recognition, fingerprints and iris scans. Until 2010, people can choose not to be issued a card, though they will still have to pay for one, and will still be placed in the database. Possessing an identity card will eventually become compulsory.

Vulnerability and Cost⁴²

Concerns related to the accuracy and vulnerability of biometric systems have been raised with respect to the national identity cards scheme. A report⁴³ released by researchers at the London School of Economics and Political Science (LSE) prior to the passage of the legislation suggested that the technology at the core of the scheme has been untested on the scale proposed by the United Kingdom's Home Office, and that the database with the details of every ID card holder is likely to become a major target for security attacks. Another report⁴⁴, by a House of Commons committee, noted that there was a lack of transparency surrounding the incorporation of scientific advice, and that "choices regarding biometric technology have preceded trials". Although there are privacy concerns related to the identity cards proposal, much of the criticism of the scheme has centered on its cost.

Recent news reports and statements from the Home Office suggest that the identity cards scheme, at least in its present form, may be in trouble. According to these reports, the timetable for introduction of the cards is under review as part of an examination of all Home Office operations. The British Prime Minister has stressed, however, that the initiative will go ahead, and that it is a major plank of the Labour Party's manifesto for the next U.K. general election.⁴⁵

Relevant facts in the UK in brief:

July 2006:

The price of a 10-year British passport will go up from £51 to £66 on October 5. Following a £9 rise last December the new increase constitutes a rise of 57 per cent in less than a year. The cost of a standard child's passport will also be raised from £34 to £45. This follows a 36 per cent increase in December, bringing the total rise to £20. The increases are intended to pay for new passport microchips that will store digital photographs and enhanced background checks

⁴² <http://www.parl.gc.ca/information/library/PRBpubs/prb0630-e.htm#bunited>

⁴³ LSE Identity Project 2005, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications (PDF)*, London School of Economics and Political Science, June 2005.

⁴⁴ House of Commons Science and Technology Committee, *Identity Card Technologies: Scientific Advice, Risk and Evidence (PDF)*, Sixth Report of Session 2005-2006, August 2006.

⁴⁵ <http://www.pm.gov.uk/output/Page9960.asp>

on applicants.⁴⁶

British children, possibly as young as six, will be subjected to compulsory fingerprinting under European Union rules being drawn up in secret. The prints will be stored on a database which could be shared with countries around the world.⁴⁷

August 2006:

Parliamentary Science and Technology Committee has published its report on the Government's treatment of scientific advice, risk and evidence associated with ID card technologies. The report found areas where the Home Office's treatment of scientific advice and evidence had followed good practice, such as through the use of advisory committees, the use of Office of Government Commerce (OGC) Gateway Reviews and the development of risk management strategies. The report also highlighted the benefits of the Home Office's approach of implementing the scheme gradually rather than using a 'big bang' approach.⁴⁸

September 2006:

The government is taking the first steps to creating the national identity card project from existing systems, confirming a shift away from earlier plans to build the scheme from scratch.⁴⁹

The UK government has won an award from the Liberty Alliance for its efforts in developing and rolling out federated identity management solutions.⁵⁰

The costs of the identity cards scheme could be cut "quite substantially" by making more use of existing government databases, the Home Office Minister Liam Byrne said in a Labour conference.⁵¹

October 2006:

The U.K.'s identity card project will cost 5.4 billion pounds (\$10.2 billion) to set up and run over the next 10 years, according to the British government.⁵²

A senior Home Office advisor has warned that biometrics has a massive usability hurdle to overcome before systems can be rolled out.⁵³

The government is funding the roll out of fingerprint security at the doors of pubs and clubs in major English cities.⁵⁴

⁴⁶ http://www.biox.nl/go_web.php?id=622&link=1995

⁴⁷ http://www.biox.nl/go_web.php?id=622&link=1988

⁴⁸ <http://www.securitydocumentworld.com>

⁴⁹ <http://www.itweek.co.uk/computing/news/2164137/id-card-scheme-changes-tack>

⁵⁰ <http://www.computerweekly.com/Home/Default.aspx>

⁵¹ [BBC News](#)

⁵² http://news.zdnet.com/2110-1009_22-6123997.html

⁵³ <http://news.zdnet.co.uk/0.39020330.39284242.00.htm>

⁵⁴ http://www.theregister.co.uk/2006/10/20/pub_fingerprints/

The town council of Yeovil (Scotland) has now made the fingerprint systems mandatory for reducing liability; those pubs that refuse to implement the system are in danger of losing their licenses.

A survey suggested positive response to new security measures if they can speed up check-in. The majority of UK airline passengers would welcome the use of biometric security if it could speed up check-in procedures while guaranteeing safety, according to new research.⁵⁵

November 2006:

The Guardian stated it had managed to pirate the new Biometric Passport⁵⁶

U.K. Prime Minister Tony Blair, seeking to promote the nation's 5.4 billion (\$10 billion) pound program to introduce identity cards, said new biometric data collected for the cards will help fight terrorism. Blair used his monthly news conference to explain say ID cards will help counter the cost of identity fraud, which the government estimates costs 1.7 billion pounds a year.

Although opposition to biometrics - the authentication of the individual based on factors such as iris or fingerprint recognition - remains strong, support appears to be growing as long as there is a tangible benefit for the average man and woman on the street.⁵⁷

December 2006:

- ▶ The British government is having second thoughts about plans to create a national database that would hold personal information and biometric data for British citizens⁵⁸.
- ▶ In a major speech, UK Minister, Liam Byrne, announced the use of biometric technology as a key part of his newly published Strategic Action Plan for the national identity scheme and for Border, Immigration and Identity management.⁵⁹
- ▶ Passengers at Heathrow airport have been invited to sign up for a trial of the most advanced passenger screening equipment in the world.⁶⁰

⁵⁵ <http://www.vnunet.com/computing/news/2165996/air-passengers-welcome>

⁵⁶ <http://www.techovore.com/actu/internet/000989.html>

⁵⁷ <http://www.silicon.com/publicsector/0,3800010403,39163308,00.htm>

⁵⁸ <http://government.zdnet.com/?p=2783>

⁵⁹ <http://www.eubiometricforum.com/>

⁶⁰ <http://www.popgadget.net/2006/10/biometric.php>