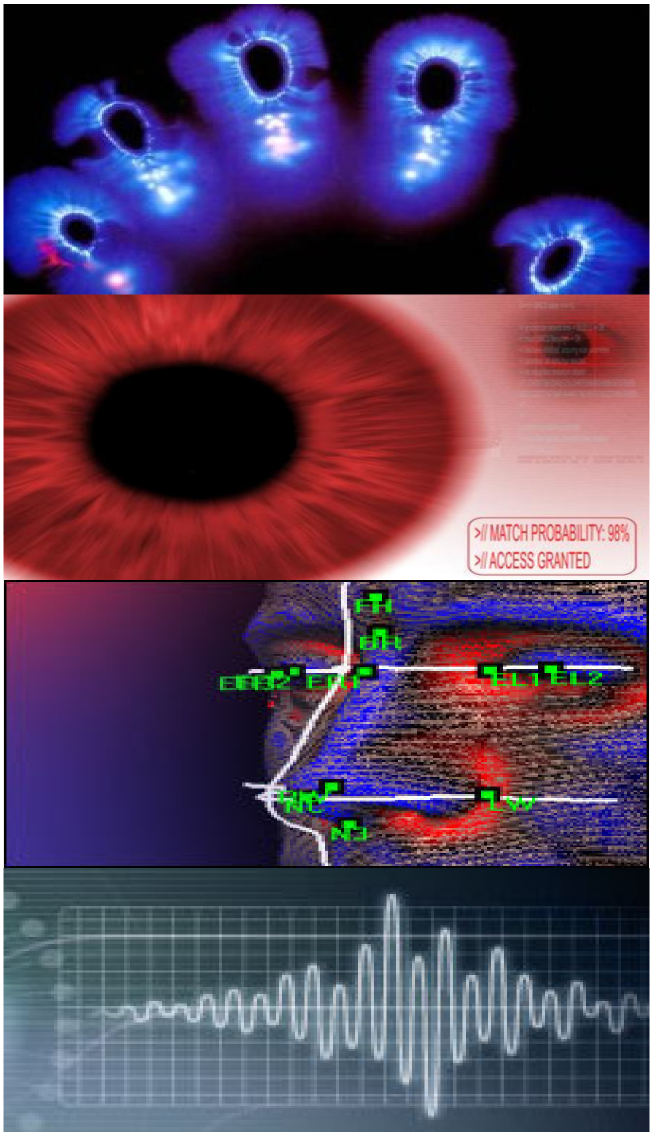
European Biometrics Portal



Biometrics in Europe

Trend Report

June 2006

UNISYS

Brussels, June 2006

Disclaimer

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 2006

Patrice-Emmanuel SCHMITZ	*Project Director*

With contributions from :

Roberto TAVANO	*VP Justice & Public safety programmes*
Pr. Juliet Lodge	*University of Leeds (Jean Monet Centre)*
Ronald Huijgens	*Chief biometric solution architect*
Kamini Aisola	*Business Consultant*
Marc Flammang	*Business consultant*

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

Contents

1 Management Summary

This first 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 8 months of portal operation, the main trends are highlighted here. A second report will complement this first one by the end of 2006.

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.

After positioning the context of biometrics adoption in the EU, (section 2) we discuss the technological trends, regarding fingerprint, face recognition, voice, iris and other new technologies such as vein pattern (section 3).
In section 4, we explore the legal aspects and main applications of biometrics in Europe. This section illustrates one of the most difficult aspects of the question that is "progressing" on various "fronts" at the same time: law, technology and standards, societal acceptance and concerns.

Ethical trends are highlighted in section 5, taking as an example the use cases developed during the eJustice project: to what extent could technological innovation be applied without taking the time of supporting a democratic debate?
For not doing so, or for providing inappropriate justifications (e.g. the fight against terrorism) many large e-Government projects have been re-worked, re-processed, re-scheduled or re-sized causing delays (2, 3 years and more) and industry deceptions regarding the market size and timing (budget slipping, as explained in section 6).

Last, we updated in section 7 our 25 Member States survey, mainly regarding the adoption of biometric passports, ID cards or other biometric documents in the area of transportation, payments, health, sport events etc.

2 Biometrics adoption in EU

Credentialing, Identity Management and Widespread Adoption of Biometric Systems in the EU

Roberto TAVANO
VP European Programmes, Global Public Sector
Unisys Corporation
Brussels, Belgium

2.1 Context

Globalisation – with all its political, economic, financial and technological dimensions – is multiplying and strengthening Europe’s links with the rest of the world, and fostering its integration into an emerging global society. These developments create new opportunities as well as new risks.

On the one hand, the increased flow of people, goods, services, and capital across borders boosts economic activity and enhances prosperity. The spread of ideas and information, across the Internet and via other worldwide media, broadens cultural horizons and becomes a powerful tool to advance the cause of human rights and democracy. Technological innovation is faster, and the spread of know-how is wider than ever before, offering new chances for greater wealth and prosperity.

On the other hand, globalisation also brings new dangers. In an interdependent world, conflicts in remote regions can destabilise the international order and directly affect European security and interests. The growing dependence on interconnected infrastructures in transport, energy, information and other fields increases the vulnerability of modern societies. At the same time, the natural diffusion of technological know-how resulting from scientific and industrial development makes it easier for technological advancements to be used malevolently. Increasing mobility allows diseases to spread easily and rapidly across borders and continents. Humanitarian crisis situations can spring up on our borders and demand instant responses.

In the recent years, credentialing, positive identification and biometrics have become increasingly important. The biometric passport is now live in Australia. The Australian Federal Government is proposing an integrated welfare service card.

Malaysia has the MyKad multi-purpose national identity card. Europe is currently busy building the largest biometric application ever conceived, the BMS, intended to offer co-ordinated support to EU Member States visa systems de facto securing and facilitating the safe mobility of people throughout Europe.

At the 15th World Congress on Information Technology Congress in the United States in May 2006, industry leaders called for an expanded definition of "security" to encompass these new worldwide realities of colliding economic, political and consumer forces that demand more accountability from businesses and governments.

Taking this perspective on the issue culminates in the representation of a single problem: how to ensure positive identification of human beings (and tracking of goods) throughout an open, free ecosystem that encompasses the collective political, physical, social, and economic environments, stretching well beyond the borders of the EU.

By focusing on electronic identity, the role of e-government and the importance of safeguarding privacy, it becomes clear that governments play a primary role and responsibility in securing themselves and their people against those who seek to do harm, to immigrate illegally, or commit fraud.

European government leaders are on the front lines of the debate, and have much to share with their colleagues around the world. However, despite recent advances in biometrics, it is critical not to loose sight of the fact that these technologies are merely tools. Because of their relatively new role in government, they have the potential to introduce new problems that a society hasn't yet anticipated, including technical challenges and privacy debates. Already, trust in government is on the wane, and the handling of personal data promises to be a hot issue in the foreseeable future. Whether the discussion is focused on credentialing, or privacy and legal issues, it all comes down to one critical factor: people. Engaging citizens and government officials in a dialogue can shed light on the issues, hear opinions that express core truths, and earn the trust that is imperative to the success of initiatives that put us all at the edge of a new frontier: the convergence of identity, technology, security and privacy.

2.2 A Digital Self

"Identity is one of the most difficult issues to be resolved during Europe's shift to a knowledge-based economy" – said famously a

Head of Unit for Trust and Security at the European Commission[1] - "accomplishing this shift will require collaborative research and new legal frameworks".

The more complex the social network, the more roles people play, so that everyone has many different identities and pseudonyms, whether a password or user name. Thus, identity management includes all the functionality that takes into account multiple identities of the identity owners and of those parties with whom the owners interact. Each entity that a person might engage with in cyberspace - whether a government site, an online merchant, a friend, or an entertainment site - could potentially involve a different identity, which raises several questions:

- How can a person be assured that his or her private information is shared only to the extent that he or she wants?
- How can security be managed for a person engaged in multiple roles in a variety of online relationships?
- How can fluid, spontaneous cooperation be managed without imposed or fixed roles and rules?
- Can a trusted access capability be built into security-protected environments, to allow emergency help - such as the police or the fire department - to intervene if needed?
- What measures and standards are needed for dependability, trust and privacy?
- What security policies can't be implemented top-down?

These questions are important because in real- or cyber-space, one's own security policy will collide with other participants' security policies, necessitating the negotiation of a joint security policy. As a result, the top-down policy is over as security must be defined for each subject and object in each region of cyberspace by a security policy that takes into account its location in space and in time.

2.2.1 Hype & Facts

Credentialing and positive identification solutions using biometrics, such as giving frequent fliers a quick pass through airport checkpoints, make headlines. Also making the news are "futuristic" front-end technologies like facial or iris scanning. But the bigger part of the story, in fact, lies behind the scenes. Whether it's a smart card, access token or biometric technique employed on the front

[1] Santucci, G.: Presentation given at the seminar "Safe Mobility of People and Goods in a Greater Europe", Saint-Paul de Vence, 2004

end, the secret to positive identification is a robust technological infrastructure on the back end. After all, the workhorse technology is what translates, transports and processes a captured image, and then compares it to those previously captured and stored in vast databases. So, while positive identification based on biometrics has a James Bond-ish allure in the headlines, it is driven by high-performance technological capabilities that may not make the news, but that make sure a person is who he or she claims to be.

In considering the possibility of a new identity card, any country should think of electronic identity as infrastructure, like a railway, electricity or transportation system. And this concept should be considered across the EU, although this will require legislation and cooperation between Member States.

2.2.2 Digital Privacy vs. Digital Piracy

Several countries in the developed world are discussing the issue of balancing personal privacy and security with respect to national multipurpose identity systems. The privacy concern is a huge issue and has recently reignited in the UK when discussing the new national ID card scheme. Defining privacy can also be a difficult process, leading to some sobering reflections on the potential for public disquiet.

Oftentimes, governments attach the concept of identity to the function of administration and the services that go along with it, like good policing, strong borders and strong national security. Rather, governments should produce the evidence to back up these claims.

When an identity card is proposed, the programme might appear logical. Among countries currently considering identity systems, police have often said that a biometric is good for law enforcement without articulating why, and that's simply not good enough.

One should wonder whether an ID card actually increases the potential for criminality and criminal false identity, and wonder also what new areas of crime people are exposed to that they'd never anticipated. The big issue with ID cards is function creep. That is, once a national biometrics system is established, it could open the door to a range of future applications and utilities and no government can provide assurances otherwise, unless a technological solution is applied to limit the application of the technology.

The benefits are still unclear, and there is an interesting disparity between government claims and public expectations.

2.2.3 Security

Biometric systems are more secure than traditional identification systems. But they only represent a secure identification process in as much as they provide a strong link between physical persons with their identity data. This means that the integrity of the linking process must be high. This will depend on the secure operation of each one of the four stages of a biometric identification process (enrolment, storage, acquisition, matching). In addition it cannot rely on secrecy, since most biometric features are either self-evident or easily obtainable. On the other hand, since biometrics is only a part of the system, it is not enough to secure the biometric system if the rest of the process remains open to circumvention. In the end, the notion of a biometric identifier being absolute proof of identity has to be discarded. Biometric identification systems are subject to errors and circumvention and thus are not perfect. It is important for whoever uses biometric identification systems to understand this principle.

2.2.4 The Business Opportunity

All the above remains true when considering an ID card scheme per se, as an identifier issued by a government to serve its purposes. If, however, we take a different, wider angle to look at the problem, we see a great deal of opportunity there.

In fact, a national ID card scheme could represent the foundation of a digital infrastructure that de facto constitutes a trusted domain. All actors allowed to enter, and thrive, within are certified and can play the role of either a services provider or a services user.

In such a scenario, citizens, businesses and government agencies can interact based on the reciprocal certified ID, thus validating entertained relationships and binding informative and economical transactions.

Interacting in such a trusted domain will foster the development of new business models and innovative services that today are simply inconceivable or non-realistic or, simply, too risky. A whole new economy based on “trusted transactions” will be encouraged, accelerating the adoption of a personal ID card as a means to access these new opportunities and services. These new services would affect our daily life in positive ways, including eventually simplifying it.

In this perspective, recent findings from two world-wide independent survey show an encouraging disposition of the general public to evaluate and offset a risk of diminished privacy with acceptable and valuable services. Interestingly, this mindset is not limited to one specific geography or culture, thus signalling how vast the business opportunity is.

Those countries that favour the adoption of multi-purpose ID cards, opening the doors to a mixed public-private use of the latter, will be able to accelerate the transition towards a truly pervasive digital economy.

2.2.5 What do Citizens Think

During the last months, we proceeded to a Global Study on the Public's Perceptions about Identity Management[2], addressing individuals' attitudes about the importance and value of different identity verification methods. The study also attempts to determine possible differences in the privacy or data sharing preferences of people residing in four different regions of the world. While identity management is essential to achieving the security goals of business and government, it is unclear how the public would react to identity verification or authentication methods. It is also unclear how the public might perceive different enabling technologies.

Understanding the public's opinions about identity verification methods is important for two reasons. First, identity management only works if the public cooperates fully and accepts the identity management technology in use. If the public considers a particular method or technology as encroaching on their rights to privacy, they will be resistant to adoption. Second, because many organizations operate in the global economy, identity management systems need to function across national borders. Hence, it is important for businesses and governments to construct identity methods that do not violate the cultural, social or ethical sensibilities of a nation or region of the world.

The following findings are the most informative about respondents' perceptions.

- Respondents appear to be willing to share a significant amount of their personal information with organizations to prove or verify their identity. However, findings suggest that individuals' propensity to share sensitive personal information with businesses and governments varies across geographic regions. Specifically, our survey findings show:
- Individuals in North America and Asia-Pacific are willing to share more personal data with both a trusted business organization and government than respondents in Europe and Latin America.

[2] "Global Study on the Public's Perceptions about Identity Management", Unisys funded research independently conducted by the Ponemon Institute LLC, 2006. – Published on the European Biometrics Portal

- Individuals in North America, Europe and Asia-Pacific are willing to share more sensitive personal information with government than a business organization. In contrast, respondents in Latin America are willing to share more personal data with business than government.
- Individuals in all four regions are willing to share substantially more sensitive personal information to receive enhanced verification capabilities (such as having one multi-purpose identity credential that can be used for various functions).
- The data elements that respondents are most willing to share with business and government includes, name, address and telephone number. The data elements respondents are least willing to share include race, religion, and credit card number.
- The data element “mother’s maiden name” is accepted by North Americans for identity verification purposes, but is not well accepted in other parts of the world (especially Latin America).

Respondents in all geographic regions prefer having one identity credential that can be used for multiple purposes or functions. Specifically, our survey findings show:

- According to respondents, the most important functions for a multi-purpose identity credential are to prove identity in order to access transportation channels (such as airplanes, trains, and buses), enter public locations (stadiums, airports and others), cross borders (customs) and access Internet accounts.
- The least important functions for a multi-purpose identity credential are to use cellular telephones, enter workplace locations (office), drive automobiles (replace key), use PDAs or enter homes.
- While many individuals prefer the multi-purpose identity credential to reside on an ID card, a large number of respondents like the idea of having it contained in a biometric, within a cellular phone, or in an article of clothing or jewellery.
- While most respondents do not like the idea of an identity credential as a chip implanted in their body, over 10% of individuals in the Asia-Pacific region prefer the implanted chip.
- On average, respondents in all regions believe that banking institutions would be the most trusted to issue and manage the multi-purpose identity credential. In contrast, law enforcement (police) and tax authorities are the least trusted to issue identity credentials.
- Interoperability across national borders is critical to the success of the multi-purpose identity credential. That is, over 68% of individuals believe it is important or very important that the credential is able to operate across national borders.

A majority of respondents in all geographic regions accept the use of biometrics for identity verification purposes. Specifically, our survey findings show:

- Individuals in North America hold the most positive view of biometrics (71% say yes), while respondents in Latin America hold the least positive view (58% say yes).
- The most preferred biometric methods are voice recognition and fingerprints, and the least preferred method is a scan of the iris or eye.
- The top reasons why respondents consider biometrics a good idea is convenience (not having to remember passwords) and efficiency (or speed) to prove identity. For those who don't want to use biometrics, the top reason is fear or suspicion about how these technologies work. Another concern by some respondents is the loss of privacy.

A majority of individuals believe certain types of business and governmental organizations need to have more rigorous identity verification methods than others. Our survey findings show:

- Banks, law enforcement (police), credit card companies and health care providers are viewed as having the strongest (or most effective) forms of identity verification.
- Food (grocery) stores, utilities and education are viewed as having the weakest (or least effective) identity verification methods.

We anticipate that the results of our study will assist global organizations in the private and public sectors determine the most appropriate identity management methods. Each will have to decide on the following:

- Who should administer the identity credential?
- How should it be administered?
- What features should be contained in the credential?
- What education and outreach efforts need to be implemented to ensure acceptance?

Based on the results of our study, banking institutions are most trusted to issue and manage identity credentials. The least trusted organizations of credential issuance are police or law enforcement. Tax authorities are also not viewed favourably as an issuing entity. In consideration of the administrative issues, many respondents in our study appear to be worried that having too much information about themselves in one place will make them more vulnerable to criminal attacks and identity theft.

Respondents to our study are receptive to a variety of methods to prove and manage their identity. However, there are cultural differences that need to be considered. It seems that smart cards, biometrics and chips imbedded in cell phones or articles of clothing are accepted by people in most countries. While respondents in Asian countries are more accepting of chip implants, the rest of the world does not hold a favourable view of this identity method. With respect to biometrics, people are most receptive to voice recognition and fingerprints. They are uncertain about facial scans, hand geometry and iris (eye) scans.

People are supportive of a multi-purpose identity credential that operates across national borders. Most important to people is the ability to use this credential to travel safely, cross national borders and enter public places that require security safeguards. There is no agreement, however, to use such a credential for more mundane tasks such as having access to your home or starting your car. Another universal finding is that people in all regions of the world are willing to share three key facts about themselves. These are: name, address and telephone number. And, they do not want to share information about their race or religion.

Identity management and technologies are new concepts for most people to understand and feel confident about. Therefore, organizations need to take steps to educate and inform people about how the possible use of identity management methods will make them more secure and provide greater convenience in their daily lives. Without such awareness, universal adoption will be much harder to achieve and may be met with resistance.

2.2.6 Collaboration and Co-operation.

One of the key challenges is the need to foster cooperation between government and business. If business needs to implement new systems, they will need to see a return on investment. Too often from a government point of view, business is viewed with suspicion, rather than as a potential collaborator whose co-operation will be essential. With drug smugglers, there are patterns to their actions, but terrorist acts are more likely to be one-off situations, and so it's critical to work with legitimate trade because they know the flow of traffic even better than governments do.

A significant issue can be the differing attitudes among states: some have an interest in security and want to participate; others are more focused on increasing revenue for the state and directing resources into that. The most significant issues for the future remain worldwide solutions and coordinated efforts. Some countries are pressing ahead, and worldwide action will require even more time.

Coordinating actions with other agencies is also critical.

On data exchange, a single regional system would be ideal, but the reality is that the level of computerization varies among different nations. While sharing data is a possibility, a regional approach is unlikely for a number of years. A common portal with data exchanged between systems would be a less costly option.

2.3 Tracks

Securing the safe credentialing of people into and from the EU demands the integration of legislations, practices and technologies. As the overall progress in the region is a mosaic of different national approaches – some advanced, some virtually nonexistent – achieving an acceptable level of integration is still a goal. There's variation in technology, too. What is more, concerns and debate on privacy won't go away, and will only grow. More importantly, the other half of the privacy equation is accountability.

One could compare the current state of privacy with the early days of the Internet and the World Wide Web, noting that although there is a great deal of coverage about privacy in the press because of the emotion surrounding it and the issue of political accountability, privacy is rapidly approaching the tipping point where there will suddenly be colossal interest among private citizens. Collectively, everyone will have to deal with public awareness and debate about these issues, keeping in mind that such debate won't always be favourable.

After 9/11, the United States was an early mover in adopting biometrics and other border-control techniques. Today, the EU faces similar problems. As technologies can be adapted to suit the needs and sensibilities of different countries, a common and coherent approach needs yet to be defined, paving the way towards a truly integrated region.

3 Technology trends - 2006

Ronald HUIJGENS
Chief Biometric Solution Architect
Unisys Europe

3.1 Context

With the wide introduction of biometrics in everyday life in Europe, caused by the EU decision to implement biometric features (face and in the near future also fingerprints) in EU passports and to require biometric enrolment from visa applicants and refugees, it is worth taking a look at the state of the art in biometric technology and the development and evolution of new and existing technologies.

Below is a brief impression, which is not complete, but it contains the highlights of what the author considers to be relevant at this point in time (May 2006).

3.2 Fingerprint technology

3.2.1 Capturing resolution

Capturing fingerprints is becoming a necessary step in more and more processes, as this technology is getting popular in civil applications.
The availability of good quality live scanners at a reasonable price enables this. At the same time more products are reaching the market, and offer the users a wide variety of products to create the solution that best fits their needs.

The fact that fingerprinting will be used in EU visa projects soon, and in EU e-Passports in the foreseeable future, implies that there is also the need to be able to capture fingerprints from everybody, including juveniles and people with very fine prints.

The commonly used live scan devices with a resolution of 500 pixels per inch (ppi) offer insufficient resolution to be able to capture prints of sufficient quality. A resolution of 1000 ppi is required to be able to capture good prints also from kids, and to be able to do proper feature extraction for matching purposes. In the forensic practices, there is a tendency to start implanting scanners of this resolution. Crossmatch is the undisputed market leader at this time.

The EU Commission (DG JLS) has recommended to use live scanners at 1000 ppi resolution for visa applications, the US JAUG (Joint Agency User Group) has recently published the requirements for live scanners for capturing prints. The industry has picked up on this, and new 1000 ppi live scanners have been announced.

3.2.2 IAFIS systems

Using this technology, it becomes possible to effectively capture good prints of almost all people.

Simultaneously, the AFIS vendors have adapted their systems to support both the currently used 500 ppi fingerprints and the new 1000 ppi fingerprints.

The drawback is the fact that the 1000 ppi prints require more storage capacity, the size of the files will typically be 4 times the current files, assuming the same compression technology (WSQ) and compression rate (15). The MITRE institute in the US has recommended compressing the 1000 ppi prints using JPEG2000 rather that WSQ and has defined the profile for this, which effectively means that the increase in file size will be less than a factor 4.

3.2.3 Liveness detection

The risk with all biometrics is the fact that fingerprints can be forged. This is relatively easy to do, and at low cost. With a small kit consisting commonly available products, ranging from just glue(!) to more sophisticated photographic technology, it is simple to duplicate a fingerprint and apply it to one’s own finger. This threat is currently combated by having dedicated and trained personnel to supervise and control the capturing process. This is good practice, though it is costly, as this requires well trained and specialized staff. In some cases, it would be desirable to allow self-service, to increase process efficiency. An effective liveness detection would facilitate this is some applications. And, in fact, the US based company Lumidigm is the world’s first company with optical single fingerprint capturing device with liveness detection that really works. They have the J100 operational at Disneyworld, doing 200;000 (!) non-supervised authentications per day.

The key selling point is that this technology is based on multi-spectral optical technology, and that it can capture prints even from worn, wet, very dry, dirty fingers, which make it very appropriate for self-service applications.

Now, we are waiting for this technology to be implemented in slap scanners at 1000 ppi, and there will be the possibility to select applications where supervision may no longer be required.

3.2.4 Minutia standardization

With the increasing use of fingerprint technology and the increasing resolution of the fingerprint images, the amount of data to be shared is increasing at very high speeds.

There are good reasons for defining standardized minutiae template for fingerprints, such that the proprietary algorithms of the various vendors of fingerprint matchers become interoperable.

This would make it possible to not send the images (a single image ranges in size from 8 – 20 kbyte) but just to send the minutiae template (of less than 1 kbyte).

It would also take away the necessity of extracting the minutiae over and over again, which is a computing-intensive procedure. The EU Commission has started the MIT project to study the interoperability of the standardized template, which comes in a small and large variant.

Though a similar project in the US revealed that proprietary templates often lead to better performance, under certain conditions it would be possible to apply this standard template. If this is successful, it could save a lot of space on the chips in the EU e-passports in the future.

3.2.5 Capturing prints from ‘difficult’ fingers

Typical problems when capturing fingerprints are too dry or too wet fingers. In prints from dry fingers, the ridges are difficult to locate. The intensity and contrast are low, and it is difficult, if possible at all, to find minutiae. Prints taken from sweaty fingers often show ridges that touch each other and larger dark areas. This also makes minutiae detection difficult. With wet fingers, the valleys between the fingerprint ridges are filled with water, with as a result the whole area is black.

Other problems are worn prints, just think about a mason or painter, whose prints will ware out because of the daily work.

New technology is emerging that address these issues. The scanner from Lumidigm, as mentioned above is able to capture these difficult prints, the same goes for the NEC H scanner. These are optical devices using spectral analysis. Authentec has an active silicon fingerprint scanner that uses ultrasonic technology. What these products have in common is that they analyse the fingerprint pattern that is already available just underneath the surface of the fingerprints.

3.3 Face recognition technology

3.3.1 2 or 3D face

We are used to 2D face recognition technology, which is now being implemented in e-Passports around the globe, based on ICAO recommendations and EU directives.

The issues with 2D face are plenty, they have to do with pose, lighting and expression. ICAO has defined guidelines to address these issues, when applying these guidelines the performance of 2D face recognition is considered sufficient.

However, by implementing 3D face recognition technology, the issues can be solved to a certain extent. Moreover, 3D models contain more information which makes distinction between various individuals larger.

A4Vision is the undisputed leader in 3D face recognition at this time, and they have an interesting portfolio of products. Various tests and pilot projects have demonstrated the ease of use of the technology and its performance, which is much better than 2D face recognition. Currently, standards are being developed to include 3D face in e-Passports.

There is also technology available to integrate 2D and 3D technologies such that current investments can be protected and the benefits of the new technology can be fully used.

Other companies who are working on 3D face technology are NEC and Viisage Technologies AG.

3.3.2 Skin texture

A lot of 2D face recognition is based on global geometric analysis of the face. This is based on defining positions of features, such as tip of the nose, corners of mouth, etc., relative to each other.

With the availability of high resolution (megapixel) cameras, it is now possible to also use the skin texture technology. This is based on analysis of the skin and is based on various characteristics of the skin, such as imperfections, light absorption etc. This requires high resolution images, but when these are available, this technology can contribute to better performance. Identix is one of the companies who include this technology in their products.

3.4 Voice recognition

Maybe not the right name, more precise would be the term voice authentication or voice pattern recognition.

This technology is very well usable, as it is widely accepted by the public. That is natural, as everybody is used to using telephones. There are several good products on the market today, which are very well capable of being used in resetting password in corporate networks. Knowing that about 80% of all helpdesk work is related to resetting passwords, applying this technology would help reduce cost dramatically. Product vendors are, amongst others, Voice Vault, Daiphonics, Trade Harbor, and University of Canberra.

There are more possibilities of applying this technology, where combining voice authentication with speech recognition and positioning technology (e.g. GPS or GSM network positioning) can improve legal processes, such as duty reporting in case of stadium bans.

3.5 Iris

The fact is that the Iridian patent on identification of people based on their iris has expired last year (2005). As a result, new iris recognition algorithms are now being published.

This is interesting, as iris recognition is very reliable, and has proved itself in many projects (e.g. Privium at Schiphol Airport, United Arab Emirates immigration, IRIS at London Heathrow). So, finally, there will be more choices in iris algorithms (e.g. University of Bath). Though the patented Iris Code® is widely used, the ICAO has recommended an interoperable format for iris images. This would make the way for more iris implementations in the future.

3.6 New technologies

3.6.1 Vein pattern technology.

Blood Vessel Authentication is a more secure authentication method and is difficult to counterfeit. A blood Vessel pattern is captured by a high resolution infrared CCD camera module. A computer algorithm registers pattern characteristics of blood vessel in the finger, and stores it into a database for future authentication. Key advantage over fingerprints – Blood Vessel patterns do not change or wear with age, and capturing does not require touching a device
This technology is promoted by companies like Bionics, Hitachi and Fujitsu and applied in fingerprint and palm scanners. There are several pilot applications ranging from physical access control to ATM cash dispensers, all mainly in Japan.

3.6.2 Other technologies

New technologies continue to emerge. To mention a number of them which are being developed (no particular order):

- 3D Ear Recognition,
- DNA,
- themographic Facial Recognition,
- retina,
- lip.

These technologies are mostly being used in forensic applications.

Others like:

- odor,
- gait,
- signature/hand writing,
- keyboard strokes,
- skin chemical composition

may become more important over time, if there is an application that can benefit.

Typically, it would be possible to create a DNA profile for everybody. In fact, there have been initiatives to actually setup a

DNA database for entire countries. At the moment is would be helpful in forensic investigations. In future, we can expect dedicated kits that will be able to create a DNA pattern within minutes.

Then it will become possible to use DNA for ID verification purposes. But, I expect that this will be far away in the future. Note that DNA has its drawbacks; just consider identical twins, it will not be possible to distinguish between them using DNA….

4 Legal aspects and Applications

4.1 EU Background

4.1.1 Legal basis

In general, the common provisions of the Treaty on the European Union, (Title I, Article 6) provides that:

- The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.
- The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950

This European Convention for the Protection of Human Rights and Fundamental Freedoms provides in particular (Article 8) that:

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Based on the above provisions, the Data Protection Directive **95/46/EC**3 constitutes the legal background of biometric technologies in Europe. It is also in line with the Convention 108 for the protection of individuals with regards to the automatic processing of personal data adopted by the Council of Europe in 1981. The Directive aims to remove obstacles to the flow of personal data by requiring a high level of protection of fundamental

[3] Available on line at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

rights (in particular, privacy) in the Member States. In particular art.8 (par 1, 3 and 4) of the Directive establishes the legal framework in which the implications of biometric identification technologies should be collocated:

> *Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. […]*
>
> *3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.*
>
> *4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.*

The Directive's core values are therefore the reduction of the processing of personal data to the unavoidable and necessary extent, maintaining the highest transparency possible, and the institutional and individual control of processing this personal data as efficiently as possible.

In particular, the Working Party Data Protection article 29 composed by Member States national representatives of control authorities have warned of the danger of storing biometric information in databases[4].

The Data Protection Directive 95/46/EC is complemented by:

- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector;
- Regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;

[4] http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

4.1.2 Biometrics are personal data

Biometric information must be considered as personal data within EU and Member states legislation, at least if the template is associated to other personal data such as the name, birth date etc., or if the collected biometric data provides a direct or indirect link to the data subject, which is most likely to be the case in concrete applications. This results from Art 2 of the Directive 95/46/EC. The sensitive character of such personal data could be reinforced if the collected data (like facial images) may provide additional information related to race or to religion. On the contrary we could estimate that raw biometric data collected only for testing purpose without any link to other personal information (e.g. a collection of 100,000 anonymous fingerprints) are not personal data , but the interest of such a collection is therefore strictly limited to performance evaluation or benchmarking (e.g. comparing the speed, the match and non-match rates of two systems).

4.2 Community and national applications

At the European level, the EURODAC system, based on the Dublin Convention, is the first large biometrics data base, installed in order to reduce fraud and “asylum shopping” with regards to benefits for asylum seekers. Fingerprints are taken from persons applying for the status of an asylum seeker, and these biometric features are used to detect if the person tries to re-apply in another country or at a later time. From its first months of activity, the system has proven efficiency by detecting a significant percentage of multiple hits and by preventing further multiple demands.

After the successful development Eurodac, the European Commission investigated the potential use of biometrics in parallel with the development of the new generation of the Schengen Information System (SIS-II) and of the development of a new Visa Information System (VIS), where biometric identifiers are seen as the tool to fight the phenomenon of visa shopping (multiple application of visa by the same person, in various EU member States consulates, possibly under various claimed identities). In this approach the Commission proposed[5] the mandatory storage of the facial image as a primary biometric identifier in order to ensure interoperability. When a secondary biometric identifier should be added, it should be the fingerprint, as it provides the best solution for so-called "background checks", e.g. the identification (one-to-many searches) in databases.

It is considered that existing security standards could be improved by the integration of two biometric identifiers, combating not only document fraud, but also fraudulent use by establishing a more reliable link between the holder and the visa or the residence permit format.

The European Union data protection supervisor monitors the use of personal data in information systems managed by or for the European Institutions.

4.3 Member States

Member states have implemented Directive 95/46 in national laws.

Even before the Directive, France had the first national authority especially in charge of personal data protection, the CNIL. As there is no legal definition of biometrics, the CNIL decides on whether to allow the use of biometric information or not, according to the French Data Protection Act. Guidelines were proposed by the CNIL, such as using preferably a decentralised database or "on-chip" biometric smart cards and the respect of proportionality and decisiveness rules (use of biometrics for accessing school restaurants, limitation of the use of fingerprint as this could be left without consent of the persons etc. The CNIL role will be especially important in evaluating the future National biometric ID Card (the INES - project of CNIE - "Carte Nationale d'Identité Electronique »).

Similarly, Germany, has set up BSI (the German Federal Office for Information Security) supporting a Federal data Protection Commissioner, to ensure that its Federal data Protection Act is effectively implemented.

All Member States' data protection supervisors coordinate and exchange experience within the Working Party data protection art. 29. A more complete overview of the situation in every European country is provided in section 7.

[5] COM 2003 (558) - Proposal for a COUNCIL REGULATION amending Regulation (EC) 1683/95 laying down a uniform format for visas

4.4 Various Applications

4.4.1 The transfer of Passenger Name Records to USA

A famous application (or - rather – a non-application) of Directive 95/46 was recently judged by the European Court of Justice [6] in its 30 May 2006 decision to annul the agreement between the European community and the United States of America on the processing and transfer of personal data[7]. The Court decided that neither the Commission decision finding that the data are adequately protected by the United States nor the Council decision approving the conclusion of an agreement on their transfer to that country are founded on an appropriate legal basis.

Following 9/11 events, the United States passed legislation providing that air carriers operating flights to, from or across United States territory have to provide the United States authorities with electronic access to the data contained in their reservation and departure control systems, called ‘Passenger Name Records’ (PNR). To prevent data protection issues, the Commission negotiated with US until reaching a conclusion on 14 May 2004[8] that the US bureau of Customs and Border Protection (CBP) was ensuring an adequate level of protection for these transferred PNR. This was approved by the Council on 17 May 2004[9] and an agreement with the US was signed.

On application to the European Parliament, supported by the European Data Protection Supervisor, the Court has annulled both the Commission and the Council decisions. However, the judgment is not based on data protection or privacy, but is based on a pure question of competence: even if originally collected by private operators for commercial purposes, the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law, for law-enforcement purposes. Such uses are excluded from the directive’s scope, as defined in its article 3 (activities outside the scope of Community law). Sending the negotiation with USA back to Member States is probably not the most efficient way (we assume, at least from the

[6] Case C-317/04 see: http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-317/04

[7] See also previous decisions of 20 May 2003 in Joint Affairs C-465-00, C-138/01 and C-139/01, and the Case C-101/01 - Bodil Lindqvist

[8] Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection (OJ 2004 L 235, p. 11).

[9] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183, p. 83, and corrigendum at OJ 2005 L 255, p. 168).

EP and Data protection Supervisor’s point of view) to reinforce both privacy protection, the consistency of the European legal order and the authority of European institutions in the field.

4.4.2 Member States Passports

Council Regulation 2252/2004/EC (that entered into force on 18/01/2005) has laid down standards for security features and biometrics in passports and travel documents issued by the Member States.

The definition of minimum security standards for passports was introduced by a Resolution of the representatives of the Governments of the Member States, meeting within the Council, on 17 October 2000. The Council regulation upgraded this Resolution by a Community measure in order to achieve enhanced harmonised security standards for passports and travel documents to protect against falsification. At the same time biometric identifiers will be integrated in the passport or travel document in order to establish a reliable link between the genuine holder and the document.

The Council Regulation is limited to the harmonisation of the security features including biometric identifiers for the passports and travel documents of the Member States. The designation of the authorities and bodies authorised to have access to the data contained in the storage medium of documents is still a matter of national legislation, subject to any relevant provisions of Community law, European Union law or international agreements.

Regulation 2252/2004 only lays down such specifications that are not secret. These specifications need to be supplemented by specifications which may remain secret in order to prevent the risk of counterfeiting and falsifications. Such additional technical specifications will be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission.

In order to ensure that the information referred to is not made available to more persons than necessary, each Member State has to designate no more than one body having responsibility for producing passports and travel documents, with Member States remaining free to change the body, if need be. Member States communicate the name of the competent body to the Commission and the other Member States.
Passports and travel documents must include a storage medium which shall contain a facial image. Member States shall also include fingerprints in interoperable formats. The data shall be secured and

the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.

This Regulation applies to passports and travel documents issued by Member States. It does not apply to identity cards issued by Member States to their nationals or to temporary passports and travel documents having a validity of 12 months or less. Additional technical specifications for passports and travel documents are established in accordance with the procedure referred to in Article 5(2) of the Council Regulation:

- additional security features and requirements including enhanced anti-forgery, counterfeiting and falsification standards;
- technical specifications for the storage medium of the biometric features and their security, including prevention of unauthorised access;
- requirements for quality and common standards for the facial image and the fingerprints.

The practical implementation of biometrics has followed various paces depending on the pressure to be compliant with the US visa waiver program and the stringency of privacy laws and supervision bodies. The various initiatives taken by Member States at governmental level are detailed in section 7 (e.g. Germany leadership in the deployment of e-passports and UK efforts to create a national ID card and a national ID register).

Based on 2252/2004, the European Commission supported a project on digital passports involving organisations from six countries, to explore the way to harmonise European Homeland security.

4.4.3 Various cases: Airports (Registered Travellers), Stadiums etc.

At a more fragmented level, various programs have been implemented, e.g. in airports: the Frankfurt/Main airport (Germany) has deployed a registered traveller system that is reported to be especially useful for frequent flyers. The system allows trusted individuals, who are now authenticated with iris recognition, to save precious time and avoid queuing when crossing airport checks. Such deployments however illustrate fragmentation, as it is not interoperable with other deployments in other airports.
Several studies and best practice benchmarks will be launched in the very near future by the European Commission to assess the benefits, opportunities and threats related to such “pre-selection”.

Another relevant area of biometric experimentation is the fight against hooliganism. In the UK a voice verification system is tested to ensure that hooligans do not attend the games to which they are not allowed. In Switzerland, the club of Bern is experimenting with a wide facial recognition program for positive identification of hooligans.

In Justice and law-enforcement, the current attempt to implement interoperability between the various Criminal Records files has illustrated the opportunity to consider biometrics as key identifier. Between four first countries (BE, FR, SP, GE) a pilot project has been implemented in April 2006 for a systematic notification of convictions (to the European State of nationality of a convicted person), and a rapid processing of information request (based on a common exchange format). One of the key issue for the extension of the pilot to other Member States is the definition of a standard to identify uniquely a person (e.g. in some countries like UK and Ireland, biometrics is the key, while it is not considered in other states).
In justice too, the authentication and traceability of documents exchanged between local law enforcement and justice authorities from various states (via the Europol and via the Eurojust networks and points of contacts) could be based eventually on a common biometric smart card (eJustice FP6 project).

4.4.4 Domestic applications

Biometrics is increasingly used in business and domestic applications (transportation, accesses to offices, worker time registration and even access to schools and scholar restaurants). As Biometric IDs are considered as personal data, the national authorities in charge of data protection are playing a prominent role in authorising (or not) the use of biometrics, if adapted to the situation and proportional to the need.

The French CNIL role is especially remarkable. The CNIL has restricted in particular the use of fingerprint databases, if no fundamental security imperatives exist.

This is based on the fact that fingerprints are tangible traces, left in various places and occasions, that could be used for person identification and linked with personal data if accessible in data bases. OnS the contrary, if the fingerprint or other biometrics would be stored only on a personal document (smart card) allowing “on chip” matching, the system would be most probably accepted. For the data protection authority (CNIL), other technologies leaving no persistent traces (like iris recognition or palm recognition) are less questionable.

4.4.5 Health sector

The 95/46 directive provisions may be compared with Chapter III Art.10 (Private life and right to information) of the European Convention on Human Rights and Biomedicine:

- Everyone has the right to respect for private life in relation to information about his or her health.
- Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed.
- In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient.

As reported by Professor E. Mordini, "The medical implications of Biometrics are becoming important[10] and we see the emergence of critical issues related to confidentiality, reliability and effectiveness, in particular where physical or mental characteristics or conditions might be deducible from biometric measurements". Biometrics may affect biomedicine in several senses:

- For security purposes and to restrain access to sensitive data: to restrain dual use technologies (i.e., technologies that can be used to produce both drugs and bioweapons), to improve secure communication and information exchange between healthcare service providers and networks (e.g., in clinical trials, in transborder networks such as organ exchange organisations, etc.), to limit physical access to buildings and hospital wards, to authenticate medical and social support personnel, and to restrain access to sensitive data (medical databanks, genetic, etc.)

- In becoming the pivot of ICT architectures, with a tendency to centralise in the same bank (or in interconnected banks) biometric, medical, economic, legal data, where data matching (the process of linking systems, by a biometric or another one identifier) and "interoperability" of information systems may provoke legal and ethical concerns

- In Applications to avoid illicit use of social welfare and/or medical support, for detecting and preventing duplicate benefits (financial losses) potentially resulting in billions of savings on public spending, or abuses in assistance programmes (e.g., heroin addicts who participate in methadone maintenance plans): in the Netherlands, fingerprint is used in the health sector for controlling the distribution

[10] See the elements reported by the BITE project directed by prof E. Mordini, the final report the SIBIS project – funded in the "Information Society Programme" of the European Commission (SIBIS, 2003) – and the European Commission funded study "BIOVISION, 2003"

of methadone, in order to make sure that members of the drug substitution program get the correct methadone dose rate.

- To identify people who are not able to identify themselves (e.g., infants, elderly suffering from dementia, incapacitated patients) or other vulnerable groups (e.g., disabled persons, drug abusers, migrants and mobile populations), which may be critical from an ethical point view when these populations have no or reduced capacity to give an informed consent.

- As a potential source of biomedical or comportment information about an individual – because some biometric characteristics (let alone DNA which could disclose a wide medical information including potential illness) can reveal if a person is drinking, is taking drugs, is pregnant, is aged or not, is subject to emotions etc., increasing the risks of discrimination and the multiplication of compulsory testing procedures.

4.5 A new liability and risk mitigation area

A strict application of EU and Member States data protection rules is not only necessary for law enforcement reasons (respecting imperative provisions of the EC and national rules), it also represents now an economic value and becomes an essential component of ICT risk mitigation for both governments and enterprises.

The costs of not having efficient security policies and processes and strong authentication for devices and data are illustrated well by the recent (3 May 2006) theft of personal data concerning United States army veterans. This personal information was stored without specific protection on an external hard drive and a laptop computer stolen from the house of a Veterans Affairs (VA) department employee. About 17.5 million veterans and military personnel were affected by the data breach - which included their names, birth dates and Social Security numbers (the fundamentals for personal identity in the US – no biometrics in this case).

The VA department is now under pressure to grant a one-year credit monitoring for the 17.5 million veterans (at a cost estimated to $1500 per person and per year: total cost $26 Billion) In addition the department, is facing a law suit based on privacy violation, asking for $1000 per veteran ($17.5 Billion), is spending an emergency $25 Million for sending a mailing to all veterans and had to set up specific call centers to respond to questions at a cost of

$200,000 per day (or another $6 Million in a month)[11]. The data privacy violation has also forced the government agency to undertake several structural measures to prevent another data breach, including hiring a special adviser on information security, accelerating security and privacy training, and reviewing procedures for accessing and storing sensitive data. Every VA facility had to observe a "security awareness week" and the department had to hire a specialised investigation company to determine whether the stolen information was, is, or could be misused.

The above example demonstrates that having an efficient privacy policy is of economic value for governments and enterprises, and that not implementing it is a major risk.

[11] Source: Zachary A. Goldfarb - The Washington Post, Thursday, June 22, 2006; A27

5 Ethics

Juliet Lodge
Professor
Jean Monnet Centre
University of Leeds

5.1 Foreword

The EU is committed to creating sustainable freedom, security and justice. In order to attain this ambitious goal, the EU envisages numerous programmes, measures and framework decisions to facilitate e-government, mobility and migration, and judicial cooperation. In this framework, a workflow or process secured by biometric authentication (we take here as example the system proposed by the eJustice FP6 project) has two elements. One focuses on ICTs as a means to expedite and facilitate the relevant process (in the example, justice cooperation). The other concerns the ethical issues raised by implementing core principles – such as proportionality, fitness for purpose, and availability – in the absence of sufficient democratic political accountability for e-governance.

Based on the most recent use case (eJustice, concluded in April 2006 and paving the way for a more ambitious FP6 "Research for eGovernment (R4eGov)" project developed by 20 public and private partners from 2006 to 2010) we identify the area covered by eJustice (freedom, security and justice) as an area of EU policy where the application of ICTs poses acutely difficult problems for policymakers. It highlights the need for an ethical debate about the adoption of ICT-based instruments in this area. It stresses the implausibility of simply adopting codes of ethical practice from the health sector to close the public trust deficit. It argues that the relevant professionals (health, justice, migration organisations etc.) need to cooperate with others in order to create a code of ethical e-governance fit for an e-governance age.

5.2 The eJustice example

Under an FP6 project called eJustice, work has proceeded to pilot and model cross frontier judicial cooperation facilitated by ICTs in

four core areas: rogatory letters, the European Arrest Warrant and euro-payments. This report is not concerned with the content of the policies. Rather, it focuses on the ethical and democratic dilemmas raised by applying ICTs to the process of prosecuting crime across different jurisdictions within the EU.
*e*Justice provides a demonstration project of judicial cooperation in the areas where it should be possible to:

- identify technical feasibilities of authentication and access
- make a preliminary identification of a capabilities audit of law enforcement authorities in using state of the art technologies and next generation technologies
- identify costs of non-comparability in capacity of different Member States (financial, political, technical and training implications)
- identify appropriate level of access and authentication rights eg is it possible to consider ab initio ways of regulating authentication and access in order to prevent the selling of data by either public authorities or private agencies that may have accessed data about individuals (e.g. as in the US). Does this require examination of property rights?
- Types of data needed to make judicial cooperation effective (as part of the effectiveness audit) e.g. needs of the European Arrest Warrant; rogatory letters, etc).

eJustice seeks to identify how e-judicial cooperation across frontiers is evolving with a view to identifying and accessing the nature and level of democratic accountability mechanisms and codes of procedure and regulation that could form the basis of a common ‘gold’ standard for ethical use of ICTs and biometrics across e-governance policy sectors. Its starting point is cross-frontier judicial cooperation in respect of organised crime because this is the most sensitive area to which governments and the EU Commission routinely allude in order to justify the introduction of biometric, digitised identity documents. The objectives are to help identify and formulate consistent, coherent ethical parameters for e-governance and responsibilities.

5.3 The Judicial cooperation case: a typical challenge

Judicial cooperation is seen as essential to combat international organised crime and terrorism, and to enable the EU to develop a common effective, fair and just asylum and immigration policy. The territorial scope of the EU and its Member States provide the starting point for this but the justice, freedom and security goals of pillar III are predicated on assumptions about the *e-governance* advantages of capitalising on technological innovation in non-territorial space. The European Council’s over-arching goal of facilitating information and data exchange among judicial, security and law enforcement authorities rests on the explicit assertion of a borderless area of *e*judicial data exchange. The Brussels European Council of 22 October 2004 stated: 'The mere fact that information crosses borders should no longer be relevant'[1]. This translates into the principle of availability whereby if information exists in one Member State, it should be made available to corresponding agencies in other Member States.

Realising a more secure and safer society within the borders of the EU is a common goal of the EU's member governments. The instruments chosen to facilitate this increasingly rely on the application of ever more controversial information and communication technologies (ICTs), including 'biometric identifiers'. The problem for EU and member government decision-makers is that the public neither trusts them nor those who employ them to safeguard the privacy and integrity of the individual. Thus, while these technologies potentially bring the EU – at least symbolically – ever closer to the citizen, they give rise to a paradox of proximity : the greater closeness they imply is defied by increasing public distancing from those issuing them : public distrust of governments increases as government agencies reach ever deeper into the personal space of the individual. As a result, a communication deficit arises that exacerbates the trust deficit in the EU at the very time when ICTs are deployed with a view to convincing the public that their security and safety is paramount and being better protected by the ICTs.

Suspicions remain that: *e*judicial cooperation instruments and agencies will escape appropriate democratic controls; the principle of 'availability' will enable agencies to elude appropriate oversight; and that as a result 'unethical' procedures and practices will arise that will erode and compromise individual privacy. Democratic controls are not believed to keep pace with technological advances which citizens see as unnecessarily intrusive, expensive, and open to fraud and subject to inadequate ethical oversight procedures.

The collection, storage, automatic transmission, ownership and particularly the use and application of biometric information is accelerating in the absence of proportionate, consistent, ethical or democratically legitimated legal regulations or appropriate codes or procedures regarding virtual identity, privacy transfer and related rights. This situation poses risks to civil society, democratic governance, the integrity of law and legal procedures, competitiveness and security, and compromises public trust in the EU. It endangers some of the core objectives of the EU (such as solidarity) and the core legal principles underlying the EU (including those that can be loosely grouped under the headings of equality and non-discrimination; a level-playing field for the Single Market in all its dimensions; *e*judicial cooperation, security, law and order.

5.4 Information exchange versus freedom, democracy and justice

The EU implicit assumption is that ejudicial cooperation has minimal costs over and above the hardware requirements. However, it will be difficult to reconcile the requirements of liberty, freedom, democracy and justice with the operational needs and priorities of security. By taking just one aspect of ejudicial cooperation – information exchange - the tensions between the security imperative and the implications associated with the collation and exchange of personal and sometimes sensitive information across and within jurisdictions shows how problematic it is to balance security with ethical, democratic e-governance. From the point of view of the EU, its goal of an ever closer union is brought nearer by the one policy area that evokes the greatest public suspicion : internal security.

The use of ICTs deploying biometric identifiers gives rise to fears about ‘Big Brother’ and potentially exacerbates the public trust deficit in government broadly conceived. The reasons offered by government to justify the collection and storage of biometric data in inter-operable databases create suspicion as to the proportionality of the measures proposed to the goals to be attained. Government agencies are seen to have ‘unethical’ goals and practices; policies and instruments are poorly explained, and the trust deficit widens. At EU level, the proposed use of egovernment ICTs based on the principle of availability to realise judicial cooperation raises particular concerns. The transfer of responsibility for data protection, moreover, from the Internal Market DG to that concerned with pillar three issues potentially threatens to create a conflict of interest within the Commission since the former is geared to openness (with all the attendant parliamentary controls) and the latter to different decisionmaking rules not subject to effective parliamentary input with or without the Constitution in place. The situation has been likened to putting a wolf in charge of sheep by Tony Bunyan of Statewatch in April 2005. If it is possible to identify appropriate and adequate ethical procedures to ensure accountability in this area, then lessons may be transferable to the interlocking and increasingly securitised areas of e-governance in general.

5.5 Ethical Considerations

The ethical problems raised by applying information and communication technologies to a range of policy sectors involving the transfer of sensitive personal data about individuals has so far been largely considered within the realm of civic and civil policy areas. These primarily concern matters relating to the swifter access to routine local services and routine administration of local government matters (such as applying for and processing online driving licences, local taxes, birth certificates etc.). These are issues where the individual citizen remains in the position of demandeur. Citizens rarely think much more about the data they make available to the relevant authorities for such purposes.

More sensitive issues are raised in respect of the processing and sharing of individual health and social service records. Data privacy questions as well as the ethical questions of transparency, openness and accessibility of data to unknown people and unknown agencies have been articulated. In these cases, not only does the individual citizen very rapidly cease to be the demandeur and the subject voluntarily disclosing information, instead the citizen becomes a data subject whose information is manipulated by unknown agencies and people. High standards of ethical practice concerning data disclosure and data management are expected within organisations but these are not necessarily mandatory. Nor are they known to or approved by the individual citizen or their elected representatives in parliament. The problems this raises for all citizens in general and for the socially excluded, educationally disadvantaged, handicapped and marginalised ICT under-class are recognised but as yet insufficiently robustly addressed. They have been identified as problematic in terms of a human rights agenda. This is but part of the problem. Much remains to be done.

An inter-disciplinary exploration of how different policy sectors have addressed ethical issues – such as those that arise, for instance, in respect of stem cell research – may help us to identify common issues and build a common platform for ensuring that high ethical standards are obligatory and universally applied, maintained and enforced by agencies of e-governance in both the private and public sector.

5.6 ICTs and crime : rationale

The application of information and communication technologies to cross-frontier judicial cooperation is considered to be an asset in tracking down and prosecuting crime. It is seen as adding value to efficient, effective administration in civil and criminal law, across frontiers and jurisdictions as well as within the territory of a given state in much the same, often non-critical way, that eadministration and e-governance are believed to have done. E-governance is believed to provide efficiency and effectiveness gains in the general administration of government. E-governance services are widely deployed : online payment of council taxes, registration of births and marriages, driving licence applications, social security and tax matters etc are common. The computer storage of health records is also becoming more wide-spread. The EU's eHealth card scheme for the 2004 Greek Olympics was designed to facilitate swift checks on visiting individuals' entitlement to receive health care if necessary. However, ehealth possibilities already outstrip the idea of an eHealth card being used purely as a means of verifying individuals' entitlement to treatment. The creation of the verichip (inserted in an individual's body) as a means of authenticating and verifying an individual raises serious concerns about the technical incorruptibility of the data on the chip, as well as about the economic gains, and global commercial ambitions (sometimes dubbed biocolonialist inclinations) of the chip providers and data storers. More seriously, it raises concerns about the individual's right to privacy and ability to keep the implanted chip secure 'for life'. While it is argued that verichips would help accelerate the identification of corpses or body parts, the underlying ethical issues have been neglected. More importantly, the implications for the conduct of society and the presumed traditional relationship between the governed and the government have hardly been considered. Moreover, whereas these areas are usually seen to lie within the realm of civil life, fraud and criminal activities associated with the theft of identities (of all kinds, including biopiracy) evoke quite another scenario.

It is too readily assumed that e-governance is separate from 'normal' political processes; that it is essentially no more than a matter of presenting information on the web for apolitical purposes. As such, not only does it elude democratic accountability and controls as well as tests of ethical appropriateness and safeguards but the latter are often not seen to be necessary. This fallacious assumption is especially challenged by the *implications and applications* of ejudicial cooperation.

eJudicial cooperation, as an arm and instrument of e-governance, when portrayed in terms of efficiency gains, occasions little concern. For example, online dispute resolution has its advocates and, although it is in its infancy, attention seems to focus on the quality of mediation online compared to face-to-face, much like in the case of eLearning. However, the instruments and practices, procedures and mechanisms for giving effect to ejudicial cooperation across frontiers – notably in criminal issues outside the asylum and immigration spheres under SIS and Eurodac, as well as in the difficult civil areas of family law - challenge our understanding of and trust in the robustness of our democratic accountability and openness mechanisms.

5.7 Technology without democracy? The ethics challenge

The introduction of mandatory biometric identifiers in passports has been opposed on the grounds of Big Brother. But this misses the point. Biometrics per se are not the problem. The central question has to be control over their use : who's controlling 'Big Brother'?.

If traditional territorial political controls in cyberspace are both inadequate and impossible to achieve, there is a vacuum in political accountability. This vacuum has not (yet) been filled by new cyber political accountability arrangements that are transparent, open tamper proof and subject to public surveillance, reform and overthrow. In cyberspace, the 'masters' are the programmers and those transferring and accessing data on altogether nebulous, unclear, unexplained bases. The response to the publicly articulated concerns to this has been to examine management procedures internal to organisations. Ethics (loosely conceived) has become a vague argument deployed by those using or advocating the use of the technology to justify their adoption in the absence of genuine, traditional controls. Loosely defined and often voluntary ethical codes of practice not only vary across and within jurisdictions, private and public sectors, but they are insufficient and no substitute for democratic political controls.

Are ethical requirements regarding the verification, authentication and robustness of procedures for accessing and holding, and the processes for transferring and exchanging edata become a sufficient alternative? What do they mean? In the case of ejudicial cooperation, the 'ethical issue' is presented as a test of proportionality and fitness-for-purpose. But proportionality and fitness for purpose are not necessarily adequate tests to ensure ethical practice. The internal security arena proves an illustration.

When the EU Commission and Council fell foul of the European Parliament over the exchange of passenger name data (PNR), their failure to respect EU democratic procedural requirements was highlighted. The question of the proportionality and fitness of the PNR measures themselves, though central to the EP's objections, were somewhat obscured by this. However, it is entirely proper that these procedures that flow from the constitution's structures are honoured : structures in the constitution provide and protect the collectivity – all citizens together, while individual rights protect the individual citizen. They are complementary and inseparable, mutually reinforcing and mutually dependant.

The 'ethical' issues and tests – proportionality and fitness-for-purpose - are embedded in political constitutionally and territorially bounded concepts of democratic rights and responsibilities. This example highlights that. The problem is, however, that a further principle has been tied to these in the arena of ejudicial cooperation and the realisation of freedom, security and justice. That principle is the principle of availability. Its application is designed to (a) expedite data exchange; (b) heighten efficient identification and prosecution of suspects; (c) create consistency within and especially across jurisdictions by removing the need to first go through the procedures applicable within a particular jurisdiction which may result in significant delays and so undermine successful apprehension and prosecution of suspects and even compromise collective security.

The principle of availability means that if data is available in one state that is potentially useful to another, it must be made freely available to the latter. At a technical level, this seems feasible. At a political level, it offends and compromises the requirements and sustainability of democratic practice and ideals of openness and public accountability. It also potentially erodes individual fundamental rights and freedoms. This is nothing new. What is new, however, is the linkage between *e*data transfer for judicial purposes and the overarching role of the state and its overriding responsibility to maintain collective security. Without clearly addressing this and the ethical implications of e-governance, there is a danger that the profound shift in the relationship between the agents of the state and the citizen will be overlooked. There is more at state than the erosion of civil liberties. This is real but the focus on one aspect arising from opposition to the collection, storage and transfer of biometric *e*data detracts from this.

The EU's Hague programme (2004) stressed expediting the means and adoption of the requisite technologies to facilitate cross-border cooperation and information exchange by law enforcement agencies in order to realise the overarching goal of sustainable freedom, security and justice. A stepped approach to this focuses on combating international organised crime and terrorism using instruments to track the movement of people across borders, including the collation of biometric data in inter-operable systems potentially linked to a central database. Central data storage raises numerous issues of trust and confidence in government and the practice of democracy. They relate to but go beyond: robust identity management systems to prevent system abuse and identity theft, ambient intelligence systems, function creep, cost, accountability mechanisms and personal privacy. The Hague programme prioritises the enhancement of mutual trust, adoption of minimum substantive and procedural rules and methods of implementation. The European Parliament calls for a quality charter. The underlying assumptions, not yet probed, relate to the ethical underpinnings of the rules, principles and methods of implementation.

5.8 Issue for the EU?

The EU has a three dimensional horizontal and vertical challenge. The issues concerns:

- nature of political control (institutional horizontal and vertical)
- nature of technical/political processes (gold standards applied horizontally and vertically)
- nature of differential regulatory frameworks at national, supranational and international levels

There is a need to first create a shared vision for a cooperative approach, and create consensus on implementing effective instruments and mechanisms. This would lay the groundwork for creating a supranational structure complete with clear political accountability and control mechanisms. This shared vision cannot compensate for the lack of such political accountability at present. The risks are too great of doing nothing and allowing ahaphazard ambiguous, contradictory, partial and fragmented systems to develop. That is not a sensible option for an organisation like the EU seeking to be a competitive international player, and it is certainly not one to be recommended to those wishing to develop an European solution or model to a universal problem which will otherwise be defined by other larger players who may not share the EU's commitment to democratic e-governance and protection of human rights. While stakeholder forums might help to better identify players' concerns and ambitions, the time lag between deliberation and action could be too long to allow the EU to develop an appropriate model. This needs to be complemented by independent, external interdisciplinary analysis of stakeholder goals and 'solutions' to rendering function creep democratically accountable.

Ethical practice in e-governance, and especially in the sensitive domaine of ejudicial cooperation must pave the way for bolder, integrated political steps if the EU is to remain on the playing board of e-governance in all its dimensions.

5.9 Challenging search for ethical e-governance

The UK has some of the most comprehensive legislation on terrorism and data retention of all the Member States. The UK, Ireland, Sweden and France put forward a Draft Framework Decision on Data Retention which not only lacks the safeguards of the SIS mechanisms but is symptomatic of (a) function creep; (b) ambiguity and imprecision in respect of the who, what, why and when of the proposed measures. The eJustice Committee convened in the UK has been examining a series of questions relating to the need to ensure proportionality and consistency in any EU *and crucially national* legislation giving effect to ejudicial cooperation, including data retention. This requires discussion of the nature and purpose of accessing and retaining data on individuals. The starting point for the initial discussion was the JAI DG Consultation Document on Traffic Data Retention published on July 30 2004. It was produced by DG Information Society (Dir B – Communication services : policy and regulation framework) and DG JHA Dir D (Internal Security and Criminal Justice).

Actual workflows within judicial processes have been modelled by eJustice and an ICT-based deployment system has been developed that is as secure as any, and allows documents to be readily tracked and identified (but accessed only under strict verification and authentication) within and across jurisdictions. If eJustice can show that the technology works and is secure, the problem that remains concerns the public trust deficit.

In general, publics across the EU do not trust the idea of interoperable data bases, central data storage and automatic information transmission because it implies a loss of ownership by the individual of the self and also because too much is unknown (and in criminal matters has to be unknowable – judicial and police authorities would argue, for operational reasons). Success depends on secrecy. The facelessness and advantages of eAdministration where the individual as demandeur can opt out of the process at will becomes a distinct disadvantage in the context of ejudicial cooperation in both civil and criminal matters. Somewhat paradoxically therefore there is a need for a visible, human interface to be re-established in e-governance that is more than a cosmetic 'voice' or façade. e-governance, no matter how sophisticated and universalised, cannot forever evade the democratic needs and requirements of modern society. The problem is that these are poorly articulated outside human rights discourse and ICT advances outstrip knowledge readily available to be voiced by politicians and publics alike.

Accordingly, there is a need for eJustice ethics work to consider:-

- Existing practices (who has access, how is it authorised, how (eg judicial orders?)
- Actual needs (why and when)
- Capabilities (technical feasibility eg what systems are used; identification of absence of comparability and inter-operability; training needs of personnel; codes of practice)
- Effectiveness Audit (analysis of safeguards)
- Elaboration of common rules, training and standards to facilitate a level playing field, guard against discrimination, arbitrary application, non-comparability, and risks of corruption

Member states' laws on data retention, for example, are not comparable. There is evidence of disproportionality, function creep and a lack of clarity about what is technically feasible, as opposed to what is on the wish list of certain governments. The dual problems of authentication and access highlight a critical obstacle to the realisation of a common playing field in ejudicial cooperation, and across other *e-governance* arenas. National rules remain paramount. If harmonisation and commonality are not yet possible, then a step towards that is offered by eJustice in its models of tracking systems and making cross-country comparison simple to see, understand, track and operate.

This does not dispense with the need to identify the EU baseline legal framework on biometrics, and biometry in *e-governance*; provide an overview of ethical and legal issues related to biometrics (robust identity management, automatic authentication, data storage, transfer and inter-operability, and function creep); and describe legal and regulatory frameworks (where they exist) for different biometric technologies.

Different tasks and goals may have different security requirements especially in different Member States. Existing institutional frameworks need to be modified in order to secure civil society confidence in the proportionality and legitimacy of policy relating to the one issue that affects each individual and which potentially brings the EU closest than ever before to the citizen : biometrics; and seek to identify a *parameter of sufficiency* and issues needing further regulation to create a balance between security and privacy and sustain proportionality and consistency across the Member States. Identify the ethical, legal and institutional challenges and risks to the EU arising from inadequate common rules on *e-governance* in general is vital because the technological feasibilities of collating, selling and automatically exchanging biometric data exceed what is necessary, may be disproportionate to the goal and escape democratic oversight, thereby posing significant legal risks. We must assess whether there is a need for EU level regulation and changes to the legal framework to complement existing practice in the Member States, and if so what changes are needed and how they can be given effect. eJustice begins this by providing a tool, and building block.

5.10 Ethical tools

The Commission's commitment[2] to enhancing ethical and social debate and to integrating discussion platforms as a strategic element of research highlights the need for the ethical questions concerning the application of biotechnology to new fields of science. The implementation and application of such technologies, for example, by governments at all levels raises specific issues of ownership, intellectual and property rights which have been addressed in the relevant Directives awaiting complete implementation across the 25. While life sciences have addressed the ethical issues (eg in respect of GMOs and human embryo cloning), newer applications of science based biotechnology to other fields of governance of central importance to the EU, have not. In particular, the EU's commitment to the realisation of freedom, security and justice, and to sustainable and dependable security raises, in its operationalisation through the introduction of biometric identity cards, passports and databases (beyond those in Schengen, SIS-VIS and Eurodac) a number of ethical issues that are only beginning to be discussed.

Discussions within forums concerned with the promotion of judicial cooperation to help attain FSJ, suggest wide variation among the Member States in legislation, practice and attitudes to private-public partnerships, the storage and exchange among different administrative jurisdictions within national governments as well as across Member States and further afield with private and public sectors. This presents the EU with a new range of problems concerning and going beyond intellectual and property law, legal practices, cyber law, human rights, privacy and data protection. The issue of digitised biometric smart cards and passports along with multiple virtual identities raises ethical issues about the ownership, authentication, possession, transfer, sale and accountability for any fraud or misuse of biometric data. There is a need to establish good practice and a gold standard in a new area of EU policymaking that applies science to the service of society, and notably to each individual's security.
Under-developed and inadequately exploited networking and information exchange potential among the various levels of governance within the EU in respect of judicial cooperation and sustainable security must be addressed. However, egovernment and technology raise ethical issues which are central to understanding the potential for convincing the public of the necessity, desirability and appropriateness of ejudicial cooperation. Given that citizens will not have any choice but to accept e-governance, biometric identifiers etc, it is imperative that ethical and transparency concerns are seen to be addressed through appropriate institutional and instrumental means. Trust has still to be established and sustained.

There is an urgent need to discover what and whether there are proportionate measures that may be derived from a comparative assessment of the values, standards and ethical concerns that individual Member States may have in respect of the application of biometrics to an ever widening sphere of e-governance. Mutual recognition of existing standards has already been ruled out in view of the wide discrepancies in respect for and trust in the law enforcement bodies in different Member States. It is important therefore to identify where there are convergent or common standards, values, and ethical concerns that could be used to try and discern a distinctive European standard.

Without a European standard, ad hocism will prevail that will compromise other EU goals – equal treatment, citizenship, non-discrimination and the charter of human rights – and will compromise the EU's ability to deliver its promises under the draft Constitution and remain an independent international player. If Europe is to deliver a European standard to the international community in an era of globalisation, it must accelerate its current work in this field.

6 Market Aspects

6.1 Environment

Biometrics are (still) a young and promising technology field. This sentence is repeated across several reports for years now, since the technology was – too early perhaps - triggered by strong public security concerns, in particular on account of terror threats following 9/11 events.

The common belief, despite common claims from media and government, that biometrics ID cards and passports would do anything to contain terrorism is now vanishing. The real benefits from new technologies regarding the standardisation of travel and migration control processes and the range of new business or government services (part of the Lisbon 2010 knowledge society targets) that could be obtained with reduced risks of fraud have still to be clarified and explained to all citizens, as the exact level of privacy that these citizens could give up to benefit from these services.

This relative lack of clarity regarding the fundamental motivations to adopt secure documents (including biometrics) is to be combined with the fact that the various technologies are still evolving fast and have made impressive progress during the last three years. In parallel, experiences with first generations of biometric systems have shown up flaws and warned policy responsible on the risk in blindly trusting technologies. The combination of these factors has caused several delays regarding some of the largest national and EU projects.

Technological progress is going together with the emergence of new innovative companies, merging and acquisitions, diversity of non-interoperable initiatives and pilots. The paradox of such progresses, innovations and fragmentation regarding both enterprises and technologies is the impression of a lack of maturity. Can you reasonably invest massively (or more than in supporting pilots projects) in a market where the most recent applications could be so quickly out-dated?

Governments and authorities have placed great hopes in biometrics however, for enhanced security solutions to protect borders, issue secure identification documents and monitor public places.
At the same time, the private sector demand could even exceed the demand for sovereign applications.

6.2 Analyst forecasting

Optimistic scale estimations of the market were produced in 2002, based on a world market volume of biometrics increasing from $98.3 million in 1999 to $260.1 million in 2002 (average annual growth rate of 39%)[12].

A quarter of this revenue was generate in Europe (against 53% in North America) with the United Kingdom dominating. UK domination is a result of historical factors and the lack of personal ID card and national registration number, biometrics becoming therefore the primary identification key in a number of domains.

Two years later (in 2004) the forecasts were reviewed and 40% lowered[13], however the growth rate was boosted to much higher levels with a top of 109.5% in 2004.

Year	2002 forecast ($ millions)	2004 forecast ($ millions)
1999	*98.3*	
2000	*120.0*	*64.8*
2001	*160.4*	*96.4*
2002	*260.1*	*158.1*
2003		*303.3*
2004		*635.3*
2005		*1257.2*
2006		*2075.0*
2007		*2740.0*
2008		*3197.0*
2009		*3548.0*

World biometrics market (2002 and 2004 estimations)

In 2006, market expectations are, if not lowered again, at least delayed in time due to various reasons:

[12] SCHULZ, S. KÖLTZSCH, G. & AMBROSIO, L. "The German Biometric Strategy Platform" – BITKOM study – May 2005 version 1.1 (p. 52)

[13] FROST & SULLIVAN "World Biometrics Markets" 2004, 3-36

- lack of citizen awareness, education and consensus on expected benefits due to the lack of clarity of government policies as explained above;
- complexity of the legal framework;
- necessity to evaluate impact regarding privacy and proportionality (data protection supervisor, CNIL);
- multiplicity of technologies;
- multiplicity of uses (not only technology but also the way it is used: if technology is generally neutral, the way it is applied is not, e.g. biometrics can be centralised in a central database (being transmitted through networks at every checks, representing potentialities of theft or lack of privacy) or being stored and matched locally on smart cards (with more potential of counterfeiting);
- fast evolution of technologies (unequal maturity).

Despite these delay producing factors, 2006 sees the deployment of numerous initiatives and plans: driven by pressures from a number of external incentives including the US government, the development of the Schengen space, the requirements and standards agreed through the International Civil Aviation Organisation – IACO, most European countries have announced imminent efforts to deploy contact less passports containing a significant amount of biometric information, biometrics add-on to ID cards or completely new ID cards systems, registered passengers pilots etc.

The global European market size may be estimated as follows, the strong growth rate observed since 2004 producing most effects between 2006 and 2008:

Year	*€ million*
2000	7.3
2001	9.0
2002	14.2
2003	23.8
2004	46.3
2005	101.6
2006	212.0
2007	360.0
2008	483.5
2009	558.1
2010	614.9

European biometrics market (2006 estimation)

Fingerprint and Facial recognition hold a dominant market share in Europe, although other technologies, in particular Iris Scan since the expiration of locking patents, are now in progress.

The usability, maturity and accuracy of finger-scan products has improved over the last years, as a result of high R&D spending by different manufacturers.
Large scale implementation in different vertical market segments such as airports, healthcare and financial institutions are still dependant upon the success of pilot projects.

In general, large enterprises – especially financial, and later on healthcare - are expected to be the next biggest customer for finger-scan and other biometrics in Europe, but they are waiting for governments to take the first initiatives and to establish standards prior to entering into this market, because in addition to the technological and human risks (acceptance by employees) they have to address political risks (what if the government or the data supervision authority cancels the whole project).

6.3 *e*-Passports, Visas and ID cards as driving case

Compared with the traditional passport delivery, the new personal documents including the digital photo and the optional inclusion of other biometrics data have requested a modification of the delivery processes and infrastructure, with trends to outsource parts of this processes to private sector (at national level) and other trends to develop common infrastructures for reducing costs and harmonising the processes of biometric visas enrolment (this trend is illustrated by the recent 31 May 2006 proposal of the European Commission for a Regulation of the European Parliament and of the Council in order to create "Common Application Centres" (CAC) to reinforce local consular cooperation, streamlining and cost-saving for Member States as resources can be pooled and shared.

Concerning passports, the IOCA provided technical specifications and recommendations that facilitated a technical standardisation and international interoperability, which is a major issue in order to protect the large investments to be made over the coming years by European governments and citizens.

The technical production of the passport booklet has changed with the integration of new materials: RFID antenna integration, holder page, cover page and electronic chip. New concerns appeared concerning the durability of the passport, the protection against falsification over its life cycle, the mechanical stability of the support integrating the various heterogeneous components, the security measures to protect the chip and its operating system. New and existing industry players have started to develop corresponding new activities.

The following table illustrates players for Passport and ID cards

	Passport	***Partners***	***ID card***	***Partners***
Austria	RFID-chip based (Summer 2006) Flex cover	OeSD (State's printing institution)	Burgerkarte (2002)	n/c
Belgium	RFID-chip based (Summer 2006) Flex cover	Oberthur	First ID card distributed to 11million citizens (from 2003)	Zetes, Steria Ubizen
Cyprus	n/c	n/c		
Czech Republic	Polycarbonate cover	Cz National Printing Agency STC Trüb (CH) Axalto tech		
Germany	RFID-chip based (Summer 2006) Flex cover	Bundesdruckerei		
Denmark	Polycarbonate RFID-chip based.	Setec (Gemplus)		
Estonia	n/c	n/c	Fully functional e-ID cards (2003)	
Spain	Flex cover	FNMT	National ID cards with Biometrics (2006-2008)	IDRA, Telefonica, Software AG
Finland	Polycarbonate RFID-chip based.	Setec (Gemplus)	e-ID card including social security)	
France	Flex cover	Imprimerie nationale	CNIE "INES" (2007 ?)	Tbd
Greece	Flex cover	Toppan (JP) ASK	n/c	
Hungary	Flex cover	Multipolaris		
Ireland	Polycarbonate	Bearingpoint		
Italy	Flex cover	Polygraphico	The largest implementation in Europe	NSC
Lithuania	Polycarbonate RFID-chip based.	Setec (Gemplus)		
Luxembourg	n/c	n/c		
Latvia	n/c	n/c		
Malta	n/c	n/c		
The Netherlands	Polycarbonate	SDU Datecard group Collis		
Poland	n/c	n/c		
Portugal	Flex cover	INCM	eID card (2006)	
Sweden	Polycarbonate RFID-chip based.	Crane / Setec (Gemplus)	Nat eID Card (2005, not compulsory)	
Slovenia	Flex cover	Mirage / Cetis		
Slovakia	Planned (2006-2008)	n/c	Combined with driving licences	SBS
United Kingdom	Flex cover	SPSL	In discussion	

Activities in Passports / ID cards and players

7 Member States survey

Marc Flammang
business analyst

Unisys Europe

7.1 Austria

1 e-Government

a. Historical information

Austria is active in this field: the Austrian government recently set itself the target of bringing Austria in the top five of the European e-government league table. On 19 September 2002, a report presented the Austrian approach to e-government and its view as to what facilitates the use and the participation in it.

b. Developments

With the Citizen's card or *Bürgerkarte (2002),* Austria was second only to Finland in introducing fully operational electronic ID cards in Europe. Other initiatives were launched, such as an e-Government Platform (2003), an e-voting system (2003), electronic health insurance card (2004), an official and secure e-mail system (2004), the *Elektronischen Akt*, or ELAK (2004), which enable paperless internal government communications.

2. Biometrics

a. Staring Point

Austria is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other

features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.
The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Development

In this respect, Austria started to develop biometric passports even if a press release on the 15 December 2005 revealed that the new biometric passports which had to be issued starting during the summer 2006 were causing some concern. Privacy rights advocates were claiming that the system was leaving itself open to misuse and were worried about increased chances of identity theft as the system is based on radio waves (RFID chip).

7.2 Belgium

1. e-Government

a. Historical information

In 2003, Belgium was the first country to announce it would supply with electronic ID cards in Europe its entire population (around 11 million people). The Belgian Personal Identity Card (BeIPIC), which is the size of a credit card, should give Belgians simpler, faster and more secure access to administrative procedures. It allows citizens to access various e-government services, such as e-voting, tax returns and civil records.

However, despite its major progresses in the field of electronic ID cards, it is a fact that it is one of the latest EU countries to convert to e-Tax with Tax-on-web.

b. Developments

Other initiatives were launched, such as e-Notaries (2000) aiming to digitise all proceedings and communications between notaries public and public administrations, Irisbox (2002) providing online services for the public in the Brussel's 19 administrative districts, e-voting (2003), e-ID technology into MSN Messenger for online identification (2005),

2. Biometrics

a. Starting point

Belgium is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.
The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image

and fingerprints in future passports and travel documents issued by EU Member States.

b. Debate

Belgium's new electronic identity cards will cost up to four times the price of their low-tech counterparts (€10 to €15 every five years against €5 to €7 every ten years). Every Belgian citizen will be required to own an electronic ID card by the end of 2009.

c. Developments

The future Belgian passports, presented on 17 May 2004 by Foreign Affairs Minister, will feature a contactless microchip that will store personal identification data including a biometric identifier. Face recognition is likely to be chosen as the biometric technology to be used, but the passport could also include the holder's fingerprints as a second biometric identifier.

The Belgian e-ID card currently being distributed is only the first card generation. Second generation cards will be issued until the end of 2007 and a third generation of cards will be issued after that date. Knowing this, the ADAPID project (ADvanced APplications for electronic IDentity cards in Flanders) has been launched in 2003 by a consortium of researchers and industry representatives in Flanders. Its aims are to make the next generations of Belgian e-ID cards more compatible with the privacy rights of citizens

7.3 Cyprus

1. e-Government

a. Historical information

An ad-hoc Ministerial Committee for the development of the Information Society has been established, comprising representatives of several Ministries as well as of the Planning Bureau, the Telecommunication Authority and the Department of Computer Science at the University of Cyprus. Several pieces of legislation were in the pipeline in 2003, in particular regarding Personal Data Protection and Digital Signatures, which should facilitate and encourage the development of the information society and e-government.

b. Developments

At that time, the government was building up an ICT infrastructure and it was actively engaged in building a Government Data Network (GDN) interconnecting all government information systems. A government portal had also been built.

2. Biometrics

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

7.4 Czech Republic

1. e-Government

a. Historical information

An Act on Information Systems in Public Administrations was passed in September 2000 and a Ministry of Informatics has been established in January 2003. The framework is complemented by legislation passed in the field of Freedom of Information (May 1999), Data Protection (April 2000), and Digital Signature (June 2000).

b. Developments

A "Public Administration Intranet" has been built to ensure secure and cost-efficient data and voice communications, as well as access to central information resources for all public administration bodies, including schools and libraries. The development and provision of authorisation and authentication services (including smart cards), data standards, interoperability and security were due to be conducted during 2003 and 2004.

The Czech Republic has launched a new e-government portal for citizens and businesses in October 2003. Data from local government are obtained from the ePUSA project. Information concerning the support of commerce and export are derived from the BusinessInfo Portal.

Systems for m-ticketing (transport passengers, 2004) and e-tolling (lorries, 2005) have been put into place.

2. Biometrics

a. Starting point

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image

and fingerprints in future passports and travel documents issued by EU Member States.

b. Development

The Czech government declared it was intending to deliver its first electronic passports to citizens by early April of 2006. The Czech national printing agency STC (Statni Tiskarna Cenin) has selected Swiss secure printing company Trüb to supply the document's polycarbonate data page, which, in turn, will embed Axalto technology.[14]

STC expects to ramp up production to 200,000 e-passports by end 2006. The STC currently produces between 500,000 and 600,000 passports each year. The contract includes the supply of three million documents by 2010.

[14] The Swiss company will supply the electronic data page made from polycarbonate for both contracts, as well as the system solution for personalisation. Trüb says it uses a hinge flap system to securely embed the plastic page into a paper passport book. Because this process uses laminated plastic tissue, the company says the data page cannot be damaged during filament binding.

7.5 Germany

1. e-Government

a. Historical information

As early as 2002, Germany launched a consultation on e-Voting and adopted the BundOnline 2005 initiative, which aimed to have "all feasible federal administration services available online by 2005" (that concerns almost 400 services).

Since 2003, Germany organised EU-wide conferences in on e-Government (CeBIT, eGO, etc.) and it stepped into a new phase of the standardisation of federal e-government applications with SAGA (Standards and Architectures for e-Government Applications). An e-Government manual was also published.

b. Developments

In June 2003, the Federation, Länder and municipalities agreed on a common e-government strategy entitled “DeutschlandOnline” and identifying five priorities in order to bring faster, more consistent and more efficient services by working together.

In January 2004, the Federal Administrative Court adopted the central e-payment platform developed within the BundOnline 2005 framework.

Germany is also studying the feasibility of introducing an electronic health insurance card (for January 2006) and an e-Tax system (with a change course in July 2004).

An e-Toll system for lorries is running since 1st January 2005, and several m-Parking (Berlin) and m-Ticketing (Berlin, Frankfurt) systems are running.

The Franco-German e-government cooperation aims define common specifications and standards (applicable for instance to e-ID or e-health insurance cards) which the two countries believe may also be shared with other EU Member States and thus, at a later stage, evolve into a common European standard.

2. Biometrics

a. Starting point

Germany is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Debate

In 2003, a debate took place regarding the topic of e-Government: federations of industries and workers wanted more development of e-Government. On another hand, studies shown that SMEs were not enough informed and the e-services were not enough available for them.

c. Developments

i. 2003

In September 2003, The Minister of the Interior saw urgent need for the introduction of biometric identification documents in Germany and in Europe. He said, it was necessary to create without delay "the legal bases for inserting biometric characteristics in passports, identity papers and visas". He also said that it was 'nonsense' to consider the use of biometrics as being detrimental to citizens' rights.

The Federal Information Security Agency (BSI) released a study in 2003, which raised doubts about the possibility to deploy face recognition technology for large-scale identification and border control systems (BioFace project).

ii. 2004

On 13 February 2004, the Minister of the Interior kicked off a new biometric border control system based on iris scanning at the Frankfurt airport, where a six months (extended for twelve) pilot project was run.

In April 2004, the Office of Technology Assessment (OTA), an independent scientific institution that advises the German

Parliament, published a first report analysing the technical, political and legal issues of introducing biometric identifiers in ID cards and passports. It identifies a number of challenges that should be addressed before such an introduction can be considered.

In October 2004, in a second report, the OTA evaluated the costs of switching to biometric passports and ID cards. Depending on different scenarios and document features, the report says, the price tag could range from €22 million to €700 million for implementation and from €4.5 million to €600 million for annual maintenance.

iii. 2005

Called “ePass”, the new German passport, which is expected to be launched on 1 November 2005, will include an embedded radio frequency identification (RFID) chip that will initially store personal information such as name and date of birth, as well as a digital facial image of the holder.

In a second phase – starting in March 2007 – the chip will also store a scan of the holder’s left and right index fingerprints. According to Mr Schily, a third biometric identifier – iris scans – could be added at a later stage.

With this decision of the German Cabinet on 22 June 2005, Germany will become one of the first countries in the world to issue its citizens with biometric travel documents.

In August, the decision to collect biometric identifiers (digital photographs and fingerprints) of visa applicants in the Philippines and compare them with records stored in German government databases was taken further to the conclusion of trials undertaken by the German embassy in Nigeria from April 2004 to March 2005. According to press reports, the Nigerian trials revealed that 40% of a total of 600 individuals applying for a long-term visa had already tried to enter Germany under a different name, had a police record in Germany, or had had an application previously rejected by the German authorities. The implementation of biometric checks at the German embassy in the Philippines is likely to signal a wider shift to biometrics in German diplomatic missions. In this respect, the federal Ministry of the Interior recently stated that in future biometrics will help identify visa applicants at the visa application stage.

iv. 2006

In February 2006, an expert private company -Riscure – told the press that German passports, among others, could also be vulnerable to the attack. This company had previously made revelations that the Dutch electronic passport could theoretically be forced to reveal all its content after a couple of hours of number crunching leads quickly to the question – which other countries could be vulnerable. The issue was that these critics were much more significant than the Dutch example because Germany had already rolled out in excess of 400,000 ePassports, whereas the Dutch electronic passport had yet to be launched.

During the same month, the press was referring that an ID card-based biometric accreditation system was used as a system protecting the Germany's "Haus" at the Winter Olympics in Turin which is a meeting point for Germany's athletes, officials, politicians, journalists and business partners.

In November, Germany started to introduce Biometrics passports, being one of the first European countries to do so. Among other things, the authorities hope it will help to shorten the queues at the borders and simplify the procedures. Since February 2004 the automatic passport check at the Frankfurt airport had been tested as a pilot project. The Police concluded in 2006 that the attempt was a great success. Moreover, the project had been closely been monitored by the federal data protection agency which completely supported the project. Nevertheless, the authorities said that some bias were still possible in this system and that the Police was working on it.

7.6 Denmark

1. e-Government

a. Historical information

The Danish government has published as soon as on February 2003 a white paper on enterprise architecture that includes recommendations on e-government architecture development in the Danish public sector.

b. Developments

Digital signature, data standards website, celebration of e-Days, adoption of the OASIS Universal Business Language as a standard, e-Invoicing, virtual police station… these are Danish developments in the field of e-Government.

2. Biometrics

a. Starting point

Denmark is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Developments

On February 2004, company Setec announced that it had won an order from the Danish Government to provide almost 3 million biometric passports over the next 5 years. The passports, which will be produced in Finland and personalised by Setec Denmark, will feature a biometric identifier (a facial image of the holder) stored in a microchip.

Since 2006, a number of Danish companies and institutions plan to establish a biometric research consortium to strengthen the interplay between public and private sector research in biometric products and solutions. It plans to form part of the establishment of a new Danish security industry with international potential.

7.7 Estonia

1. e-Government

a. Historical information

An important development took place in June 2002 regarding the online availability of public sector information, when the electronic version of the official gazette went live on the Internet, In order to provide electronic and public access to all legislation.

b. Developments

On 12/03/2003 a new and ambitious e-government portal was unveiled. Branded 'the Citizen's IT Center", the site is meant to provide a single, one-stop umbrella for the many government services already online, and for all new services being developed.

The Government published on 12/03/2003 a white paper on its electronic machine-readable format ID card initiative. Estonia was, together with Belgium, Finland, Italy and Austria, one of the first European countries to issue fully functional electronic ID cards to its citizens.

The developments in Estonia are: a harmonisation of digital signature practices with Finland, e-Tax, creation of an e-Governance academy, e-Voting in Tallinn (and soon in the whole country, in spite of a recent controversy after a veto of the President).

2. Biometrics

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

7.8 Spain

1. e-Government

a. Historical information

Spain doesn’t seem to be one of the most advanced country in the field of e-Government. Thus, in April 2003, Emergia edited a study showing that most Spanish public sector websites were insufficiently accessible to users with disabilities.

However, the government has launched a €84 million e-government plan for the next three years. And on the other hand, in the field of e-Taxing, Spain is the European champion with more than 14.5% of the declarations submitted electronically in 2004 (11.5% in the UK and less than 4% in France).

b. Developments

As far as the available information is concerned, it seems that Spain is not one of the most advanced countries in the field of e-Government: in April 2003, Emergia edited a study showing that most Spanish public sector websites were insufficiently accessible to users with disabilities.

Moreover, the City of Barcelona has received the ‘eCitizenship for All’ award for its ‘Citizen’s Folder’ service, which has been evaluated as a model for the re-engineering of local public administration.

Digitised archives, digitised property and company registries, e-Voting (e-Referendum in June 2004), e-ID card announced in May 2003, e-Signature approved in December 2003, etc… these are developments in the field of e-Government in Spain.
Despite of those, e-government services offered by the Spanish central administration are still insufficiently accessible, according to a recent survey commissioned by the Infoaccessibility Observatory of the organisation Disc@pnet.

2. Biometrics

a. Starting point

Spain is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Developments

The Spanish Council of Ministers approved on 13/02/2004 the creation and distribution to Spanish citizens of new electronic national ID cards containing a biometric identifier. Among other things, the new card should allow citizens to access sophisticated e-government services. The electronic ID cards, which will be identical to the current card in terms of size (similar to a credit card), will contain the following information stored in an embedded microchip: an electronic certificate to authenticate the identity of the cardholder; a certified digital signature, allowing the holder to sign electronically; keys for its use; a biometric identifier (fingerprint); a digitised photography of the holder; a digitised image of the holder's handwritten signature; all the data that is also printed on the card (date of birth, place of residence, etc.)

In July 2005, the Spanish government awarded the 12 million euros contract in the framework of a public call for tenders that covered the design and development of the new ID document in Spain as well as its distribution and the management of the scheme to a consortium made up of Indra, Telefónica and Software AG. This first e-ID contract covered the pilot phase of the project.

Meanwhile, on 7 July 2005 the Ministry of the Interior and the Ministry of Justice signed a cooperation agreement aimed at fostering the development of electronic ID. The agreement assigned 23.1 million euros to fund common activities for the successful delivery of the project, including software, hardware and organisational aspects. According to the Spanish government, the e-ID card was going to be “interoperable and technically compatible” with the electronic cards being developed in Germany, France, Italy and the United Kingdom.

In March 2006, more than a year later than originally expected, the new electronic identity card has been officially launched in Spain with a high-profile media campaign, a new eID website and a Freephone helpline for citizens. The Spanish Police Department, which is the institutional body in charge of issuing ID cards in Spain, has allocated €50 million to this campaign from now until 2008. The consortium had to implement a pilot centre for the issuing and personalisation of e-ID cards.

7.9 Finland

1. e-Government

Finland has developed its e-government activities through e-Signature (January 2003), e-Notifications for crimes (2002), e-ID card (including social security card), harmonisation of e-signature practices with Estonia, establishment of a one-stop shop for e-Government services (September 2003)…

Finnish citizens might be able to vote electronically through the Internet or via mobile phone in 2007. This is the goal of a new project to develop a smart card-based solution for e-enabled elections.

2. Biometrics

a. Starting point

Finland is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Developments

It had been announced on 10 January 2005 that a new passport information system and biometric passports should be introduced in May 2005 at the earliest, at a rhythm of approximately 400,000 documents per year over a 4-year period. These e-passports have high-tech security features, including a polycarbonate data page containing a ‘contactless’ crypto processor chip storing the holder’s personal details and biometric identifiers.

In addition to the facial image of the holder, a second biometric identifier – fingerprint scans – will be introduced in 2006-2007. And in addition to complying with the standards set by the ICAO, the passport will include the following optional security features: a personal identity code; prevention of unauthorised reading, copying or substitution of the chip; encryption of data communication between chips and chip readers.

In April 2006, a press release mentioned that Finnish police were to take delivery of a new-generation AFIS (Automated Fingerprint Identification System), which would not only allow standard AFIS police services (i.e. identifying criminals with latents, palmprints and fingerprints), but would also be used when issuing visas, passports and asylum ID. As part of the new contract, Sagem will supply and deploy high-resolution fingerprint and palmprint capture stations and latest-generation laboratory stations.

7.10 France

1. e-Government

a. Historical information

As early as January 2003, the government announced the creation of an e-government agency, which should act as an information technology consultancy to public administrations and should employ around 50 people.

b. Developments

In March 2003, a call for projects for the development of the 'Daily Life Card' has been launched. This card was intended to be a locally delivered and administered smart card providing citizen identification and/or authentication for accessing a series of public services delivered locally.

Followings are the developments of e-Government in France: e-Voting (which firstly was allowed for French citizens living abroad and only for the elections to the 'Superior Council of the French leaving abroad', then it was tested for the 2004 regional elections, finally an Internet voting system was tested for the professional election of October 2004), e-Taxing (as early as 2000), Public-Private solution for public e-Procurement (July 2003), e-Signature, e-ID (announced in September 2003 for 2006), e-enacting for legal acts and regulations (February 2004), e-Parking Fines (in Cannes).

France cooperates with Germany in the field of e-Government: the Franco-German initiatives aim at fostering the mobility of citizens by developing a common electronic authentication structure and a number of cross-border e-services. Currently, they are focused on the use of smart cards. In this respect, the two governments are working on the development of common technical specifications for e-ID cards.

2. Biometrics

a. Starting point

France is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU

Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Debate

On 26 May 2005 organisations representing a wide-range of civil society and professional sectors launched a campaign against the biometric ID card and a petition demanding the “immediate withdrawal” of the project.

"The project aims to build a nation-wide centralised police file containing the biometric data and the address of each citizen”, the petition says, adding that because information would also be stored in each ID card’s ‘contactless’ chip, personal data could be read without the consent of the cardholder. "The government recognises that the ultimate goal of the project is to set up a universal card which integrates the identity, the benefit of social rights and the ability to access services and pay transactions. The idea is to make the individual totally transparent to both public authorities and commercial actors", explained the six organisations.

In addition to warning against potential breaches of privacy and human rights, the campaign also questions the strategic motivations of the French government, particularly with regard to the fight against identity fraud and terrorism. Indeed, the six organisations point out that the authorities were unable to provide reliable figures on identity fraud, and believe that organised criminals would be able to produce fake biometric IDs.

The INES project will among other things merge, secure and simplify the procedures for requesting ID cards and passports, improve the management of ID documents, and provide citizens with an electronic signature that is expected to foster the take-up of e-government and e-commerce services. Personal information contained in the future ID cards and passports will be stored in a new, common database, while biometric data – facial image and fingerprints – is expected to be anonymously stored in separate files.

A report published on 16 June 2005 by the Internet Rights Forum – an advisory body bringing together 70 organisations from the public, private, and not-for profit sectors – has raised concerns regarding the French e-ID card project and called for a review of the proposed scheme (known as 'INES').

Position of the government

On 1 February 2005 the Ministry of the Interior launched an online debate over the proposed national electronic ID card. In particular, citizens are invited to make their opinions heard on a number of key issues such as:

- Replacing the current national ID card with an e-ID card containing biometric identifiers – digital picture and fingerprint scans – stored in a microchip.
- Defining the measures required for privacy protection.
- Accessing e-government and e-commerce services via the electronic ID card.
- Delivering the card, including logistics and cost aspects.

Due to strong opposition to the project (six associations + CGT + report of 20 June), in late June 2005 French Interior Minister Nicolas Sarkozy said he wanted to "think more" about the project in order to "assess were we want to go, and at what cost". Mr Sarkozy also said that "while European rules force us to implement biometric passports rapidly, the e-ID card is a different matter".

c. Developments

In April 2003, in order to deal with illegal immigration and the threats of terrorism and organised crime, the government was looking at using biometrics to improve border control. According to plans prepared by the Ministry of the Interior all applicants for tourist visas should be fingerprinted and a central database designed to track and identify illegal immigrants should be put into place.
In September 2004, the Government declared that the e-ID card announced a year before would include a second biometric identifier – probably scanned fingerprints – in addition to the facial image of the holder.

The French e-ID project, baptised "INES" ('*Identité Nationale Electronique Sécurisée*', or 'Secured Electronic National Identity'), has been accepted originally (first draft) in April 2005. Procurement for the project was originally expected to begin before the end of 2004, with a view to develop and test the card during 2005 and start distribution in 2006. According to press reports, distribution of the e-ID cards (modernisation of the CNI "Carte Nationale d'Identité") is now expected to begin in 2007, while the government still hopes to start issuing biometric passports during 2006. The INES project is expected to cost about €205 million per year, including the initial investments.

The card, containing a chip carrying all identity information of the holder person, will provide each citizen with an electronic signature allowing secure access to both e-government and e-commerce services and transactions.

The French CNI-INES case illustrates both the difficulties and challenges of such project, producing successive re-scheduling and delays when the political context and the involvement of all stakeholders are not optimal. A reorganised project team has revised all processes and includes now in the loop the 2000 municipal authorities (via the "Association des maires de France" (AMF)), préfectures, Ministries (Affaires étrangères, outre-mer, Défense (gendarmerie), Finances, Justice, SGDN).

New timing includes:

Project of bill: in discussion at the CNIL, then will be revised by the Conseil d'Etat to be discussed in the council of ministers in September 2006 and adopted at the end of 2006

The project has been clarified :

- The current FNG file, used for the CNI will be used, and complemented separately (with specific data protection measures) by digital photography and fingerprint.
- The new CNI (smart card) will be optional in a first stage
- The smart chip will be bi-modal : with contact (for authentication purpose) and contact-less (for identity information)
- A 24x7 helpdesk will be implemented, responding to the care to inform and fight against fraud
- Ad-hoc Competent Civil servant only will be entitled to access the data (with reinforced protection and sanction in case of privacy violation). Other civil servant in charge of managing the cards will not access the content of the files (only a hit/no hit checking system will be enough in most processes).

A Study on fingerprint, iris, and facial-recognition data collected since October 2004, has been carried out by the French civil aviation authority in January 2005 (for 6 months).

The pilot programme Pegase, a voluntary biometric identification programme for travellers, which is available to EU and Swiss citizens, was launched on 1 June 2005 by Air France and the border police at the Charles de Gaulle Airport. It is designed to allow for quicker and easier border control for registered passengers while increasing border control security.

Created by Air France, the programme is based on a fingerprint identification application developed by SAGEM and could raise a number of privacy issues because it implies the creation of a centralised database storing personal details, including scans of the left and right index fingerprints of the enrolled passengers. As enrolment in the scheme is voluntary, the creation of the trial database was approved.

In October 2005, the Data Protection commissioners adopted during their 27th international conference the resolution on biometrics use in the identity documents. In conclusion, it was stated that biometry could be used in "passports, identity cards and travel documents". Moreover, there couldn't be only one identifier.

In December 2005, a press release announced that the issuing of the e-ID card would be delayed. Previously forecasted for 2007, the CNIL (Commission nationale informatique et libertés) said that the future biometric card should be valid in 2008 and could not be compulsory.

The 12th January 2006, the CNIL authorized two access controls for school restaurants through biometric means while rejecting four access controls and time management tools for companies as these were not used for security purposes.

In February 2006, as France hadn't hit the previous year's visa waiver deadline next to the US-imposition deadline that all passports issued on or after October 26 2005 had to include either a digital photo or a chip containing biometric information. The deadline was apparently missed because labour unions wanted the passports to be produced at France's state-owned printing company rather than a private one. As a result, French citizens with new passports had to apply for a US visa either to visit or transit the country. Due to the situation, applicants have been facing a delay of more than five weeks before securing interviews with consular staff. The embassy's consul general, Don Wells, said that 23 consular employees were handling about 500 applicants a day - roughly four times the section's normal workload.

7.11 Greece

1. e-Government

a. Historical information

As early as during its Presidency of the EU, Greece launched an e-Vote initiative on its website.

b. Developments

On 19 October 2004, the Minister of the Interior reaffirmed that reforming the state through e-government is a key goal and a priority for Greece. Combining structural state reforms with the adoption of new technologies should allow the Greek Government to make the country’s public administration more transparent and citizen-focused.

Announced in late 2004, the first Greek Digital City is being developed and should be completed by mid-2006. The e-Trikala initiative aims to improve everyday life by simplifying public transactions, reducing telecommunication costs, delivering new electronic services, and offering new methods to enable citizens to participate in policy-making. The Digital City model consists in four layers:

- Infrastructure: hardware and software necessary to make the Digital City operational (such as broadband networks, public terminals, etc.).
- Applications: e-government services.
- Back-office: all public authorities and organisations that produce and deliver information and electronic public services to end-users.
- End-users: citizens, groups of citizens, and businesses.

2. Biometrics

a. Starting point

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Development

The Hellenic Data Protection Authority announced on 10/11/2003 that advanced identity checks using biometrics keys such as fingerprint and iris scans would breach the Greek data privacy laws. The authority thus banned Athens International Airport from checking and recording passengers' fingerprints and irises as part of a pilot security program that was scheduled to start before end November and to last five months.

According to our sources, Greece is today the latest in a line of European countries to make ePassports a reality.
Still, in May 2006, Japanese company Toppan, the current provider of passport personalisation solutions to the Greek authorities, has selected ASK’s Smart Paper ID technology for the scheme. ASK will be delivering ePassports from June 2006.

7.12 Hungary

1. e-Government

a. Historical information

The formulation and the coordination of the implementation of Hungary's e-government strategy, presented in 2002, is the responsibility of the Electronic Government Centre within the Prime Minister's Office. It is based on the vision of a service-providing State. By contributing to making public services customer-focused, e-government indeed acts as an important catalyst for the modernisation of public administrations. At the same time, it gives citizens an opportunity to voice their opinions and to interact with public authorities in a direct way, thereby opening new doors for democracy.

b. Developments

In January 2003, Hungary already wanted to improve local and national e-Government services by the second half of 2004. Thus, as early as in November 2004, the government has developed m-Government services. In addition to this, a report presented in March 2005 showed that the Hungarian e-Parliament programme, launched in 2002 to support the modernisation of parliamentary work, is achieving increasingly tangible results: constant improvements have been observed regarding both the effectiveness and the transparency of law-making processes, while the paper consumption of Parliament has been significantly reduced.

In spite of that, a recent survey has revealed that Hungarian local authorities are still a long way from realising the e-Government vision, and a new law aimed at removing obstacles was recently passed by Parliament and will enter into force on 1 November 2005.

2. Biometrics

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.
The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image

and fingerprints in future passports and travel documents issued by EU Member States.

7.13 Ireland

1. e-Government

Despite the e-Government strategy was suffering of a "lack of strategic direction" – according to professionals in 2002 – developments are numerous: mobile e-Services for nurses (2002), passport applications online (€22mln contract awarded to KPMG Consulting), e-Enable Civil Registration, e-Voting, e-Procurement, e-Motor Tax (2003).

But there were also the establishment of a unique Personal Public Service Number for public services and e-government, a proposition to creating a Public Service Card, the launch of e-Cabinet that allows the entire Cabinet decision-making process to be online, m-Parking services in Dublin (2004), a tax administration's SMS service, a single smart card for all public transport, etc. (2005)

2. Biometrics

a. Starting point

Ireland is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Developments

Given the numbers of Irish travellers to the US, the Irish Foreign Affairs minister said in February 2004: “it is highly desirable that Ireland should remain a participant in the visa waiver programme and I am recommending to the government, therefore, that Ireland should introduce passports containing biometric information, subject to the conduct of a feasibility study of the detailed arrangements for implementing this”.

In May 2006, the Dáil's Public Accounts Committee has been told that The Department of Foreign Affairs makes a substantial profit each year from issuing passports. The Secretary General of the Department said the passport division cost about €10 million a year to run, not counting office rents. But last year 670,000 passports were sold, bringing in about €39 million, while in the previous year the 600,000 passports sold brought in about €30 million. The Department plans to issue passports with biometric data on them but there will be no price increase for these, he said.

7.14 Italy

1. e-Government

a. Historical information

Italy is one of the most active countries in this field. The government adopted policy and common vision for e-Government as early as in 2002. In 2003, it announced the distribution of 1.5 million of e-ID Card by the end of the year. For its EU Presidency, Italy announced a ambitious e-Government plan.

b. Developments

In May 2003, the government has taken a new initiative that confirms the innovative use it makes of e-government as an instrument of foreign policy: it announced that it was creating a preferential policy to assist Balkan countries in the process of implementing e-government.

Developments in the field of e-Governments are numerous: e-Procurement, e-Social Security Card, e-Voting, legal status to registered e-mails, t-government (which will promote the delivery of e-government services through digital television), e-Government Services Cards (including an e-payment function), e-ticketing in Rome.

2. Biometrics

a. Starting point

Italy is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Developments

On 11 December 2003, the government presented a prototype of its future passport, including three biometric identifiers (the holder's facial image and two fingerprints) stored in a microchip. Italy was therefore on track to become the first country in the world to introduce a biometric passport.

On 31 March 2004, the government created a new working group that will establish guidelines for the use of biometric technologies in the public sector. A competence centre was also established to assist public administrations in the biometric area.

On 28 October 2004, the government has published the first version of its biometric guidelines, aimed at providing public sector bodies with useful information regarding the integration of biometric technologies in e-government projects.

In October 2005, according to a comparative analysis of smart card use in Europe published by Card Technology magazine, the Italian government seems to have issued more smart cards than all other EU Member States combined. Over 13.1 million smart cards providing access to a range of e-government services have been issued in Italy to date, according to the magazine. At 9.3 million, with a further 3 million about to be issued, the National Services Card (NSC) makes up the lion's share of these smart cards for government-related use. Following two sets of trials, over 2 million Electronic Identity Cards have now been issued in Italy. Starting in January 2006 e-ID cards will completely replace paper ID cards and it is expected that all citizens will hold one within 5 years. Another Italian smart card is the digital signature card, of which over 1.8 million have already been issued. Leaving aside the 3 million NSC s awaiting issue and the over 10 million e-health cards issued – which allow access to e-health services but do not feature a microchip – there are over 13,1 million smart cards aimed at providing secure access to public services in circulation in Italy.

7.15 Lithunia

1. e-Government

   a. Historical information

In June 2003, the “state of e-government in the accession countries (Part 2)” IDA document said that a relatively well-developed legal framework was in place to support the development of e-Government, including the Law on Legal Protection of Personal Data (1996) and the Law on Electronic Signature (2000). In April 2002, the Ministry of Economy also approved regulations regarding some information society services, in particular electronic commerce.

   b. Developments

On another hand, the infrastructure was still under development, but the government has given priority to infrastructure and back-office projects, with specific efforts dedicated to creating an integrated system of state registers. In particular, the integration of the tax inspection and social security registers was due to be finalised soon. An e-Tax system has also been implemented.

2. Biometrics

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

7.16 Luxembourg

1. e-Government

In February 2005, the government has decided to adopt Hermes, the ICT project management methodology used by the Swiss federal administration. The latest version of Hermes – 'Hermes 2003' – is a global project management solution composed of three elements:

- A guide providing project managers and other staff with the necessary know-how to deliver projects successfully.
- Additional tools (electronic and/or paper-based) to implement the methodology.
- Knowledge dissemination, including information on the methodology and on previous cases.

On 13 June 2005, the new e-Government strategy has been presented, including an action plan for the further implementation of public e-services in Luxembourg: "e-Governance means much more than creating websites", commented Minister for the Civil Service and State Reform. In this respect, the new strategy and action plan make a distinction between three main categories of projects:

- Short term Internet projects, such as for example the creation of an online service for VAT returns or the development of an e-procurement project.
- Short term administrative management projects, such as the setting up of an integrated system for the management of housing grants.
- Medium and long term strategic projects, such as infrastructure, interoperability, and service integration projects, as well as initiatives for the organisational reform of public bodies.

2. Biometrics

Luxembourg is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other

features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

7.17 Latvia

1. e-Government

a. Historical information

Only little information is available on Latvia in the field of e-Government. Latvia's information society strategy is coordinated by a Department at the Ministry of Transport and Communication, which is notably in charge of driving forward the implementation of the Latvian e-government "concept" (strategy) adopted in September 2002. Nevertheless, at an operational level, part of the e-government drive is conducted by the State Information Network Agency (VITA).

b. Developments

In the last few years, the country has adopted a package of legislation which has paved the way for the creation of an e-government infrastructure called State Significance Data Transmission Network.

In September 2001, the Latvian Government approved a “Concept on Identity Cards”, and in 2002, it adopted an “e-Government Functional Model”.

In October 2004 the previous Latvian government decided to put on hold its electronic identity card project until precise EU requirements for travel and identification documents are known.

On 19 April 2005 the new government started consultations with telecommunications about the implementation of secure electronic signatures in the country. The Prime Minister considers that its implementation has to be hastened and should start already in the autumn of this year.

The government also has to make further decisions concerning funding for the creation of the e-Signature infrastructure and for the implementation of the secure e-Services using it.

2. Biometrics

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other

features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

7.18 Malta

1. e-Government

a. Historical information

The Government published a White Paper describing its e-Government vision and strategy in October 2000. The Central Information Management Unit (CIMU) is in charge of ensuring the coordination of the initiative.

b. Developments

On 7 April 2003, the government officially launched the first set of m-Government services. Malta has indeed decided to integrate multi-channels delivery in its e-government strategy in order to adapt to the wider diffusion of mobile phones than of computers in the island. The services available to mobile users include:

- Notification of acknowledgements and status change of customer complaints
- Notifications of court deferrals
- Notifications for license-renewal to the holders of licences issued by the Trade Department, Malta Tourism Authority, Malta Maritime Authority and Public Transport Authority
- Notification of exams results for students.

Other developments are: online vehicle licensing, e-ID service, e-ID card, e-Procurement, migration to voice over IP, e-Application for passports.

2. Biometrics

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.
The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

7.19 The Netherlands

1. e-Government

In the Netherlands, the development of the e-government has started as early as in 2002. It already includes: e-Signature, e-Reporting for crime, launch of an e-Government knowledge centre, e-Taxing, e-Voting in 2003, the creation of a unique identification number in 2004. And, in spite of previous studies saying that Dutch e-Government suffers of a lack of transparency and interactivity, a new study has shown in May 2005 that it is getting better. In addition, the Netherlands has organised the world's largest e-Voting experiment in 2005 also (with more than 2.2 million of voters).

2. Biometrics

a. Starting point

The Netherlands is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Debate

According to Government Reform Minister the new Dutch biometric passports will be phased in after mid-2006 in order to meet the 28 August 2006 EU deadline.

c. Developments

In January 2004, the government was about to jump on the biometric bandwagon as it prepares to launch pilot tests of high-tech passports and ID cards in early 2004.

The pilots, to be carried out over a 6-month period in a number of local communities, should test the adequacy of the prototype documents. Both the new passport and the new ID card should feature facial and fingerprint digital scans as biometric indicators. In early June 2004, two Canadian companies were chosen by the Dutch Government to provide technology for the passport and ID card pilots. Bioscrypt should provide the fingerprint technology, while BioDentity should be supplying the face recognition system as well as the necessary border clearance technology to deliver fully operational kiosks and counter inspection systems.

In September 2005, a study commissioned by the Dutch Ministry of the Interior and Kingdom Relations has raised fresh concerns over a number of technical issues related to the issuance of biometric passports. It showed that the quality of fingerprint information used in the tests was sometimes poor and that the biometric documents were less robust than the traditional passports.

In November 2005, Datecard Group has been chosen to provide inline passport issuance systems for the Netherlands' biometric passport. This Passport issuance system should offer enhanced quality.
In May 2006, Dutch firm Collis has introduced a set of ePassport testing tools to determine whether or not a given passport meets ICAO standards.

7.20 Poland

1. e-Government

a. Historical information

In March 2003, the legal framework for the development of e-Government was formed by a series of laws passed in the previous few years and covering access to information, personal data protection, electronic provision of services, electronic payments, and electronic signature.

b. Developments

An e-Government portal providing centralised access to public administration information and services for both citizens and businesses should be created, as well as a nationwide network linking government departments, offices and agencies, and local government, which was due to be completed by the end of 2005. The development of a 'Multifunctional Personal Document' (MPD) that will act as an intelligent, PKI-ready smart card to replace the current plastic ID card was also in the pipeline.

Since that time, an e-Customs system has been created, as well as a wireless network in Slupsk, a new e-Government plan has been adopted for 2005-2006

2. Biometrics

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.
The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

7.21 Portugal

1. e-Government

In 2003, Portugal launched an e-Declaration for VAT, an e-Procurement plan. In 2004, Portugal launched its new e-Government portal and tested e-Voting. In 2005, it introduced e-Medical Prescriptions and launched its e-Procurement portal. In addition, its e-Tax service has become popular.

2. Biometrics

a. Starting point

Portugal is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.
The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Developments

Presented in January 2005, similar to a credit card in appearance, the future Portuguese ID card will feature a chip and a magnetic stripe storing personal information and biometric data. The government's goal is to create a more secure ID document, after the Brazilians experience.

In addition to fingerprints, the future electronic ID card might also include iris scans and/or other biometric identifiers. The current Portuguese national ID document already includes a fingerprint;

however, it is not digitally stored but directly transferred to the card with black ink.

On 8 March 2006, the new Portuguese ID card (Cartão do Cidadão) has been presented. The Cartão will include an electronic chip containing all data visible on the ID document, as well as the digital signature necessary for the electronic identification and authentication of the card-holder. No biometrics is currently integrated. The new card can be used as an eID card and will provide access to a great number of administrative services available on-line. It will also aggregate and replace five of the other existing ID cards: the social security card, the public health service card, the tax-payer's card, the elector's card and, of course, the current ID card or Bilhete de Identidade.

7.22 Sweden

1. e-Government

In 2002, Sweden has put into place 24/7 agencies and has launched an e-Procurement service. In 2003, a study said Sweden was the information society world leader. In 2004, Swedish government launched an e-ID Card program, a biometric passport program, a new e-Government portal.

In March 2005, the use of e-Prescriptions has reached a level of more than a million (45% of prescriptions were sent electronically, up from 32% in September 2004 and 9% in November 2001). Over 2.1 million Swedish citizens used the e-Service offered by the National Tax Board to file their income tax returns this year, a two-fold increase over 2004.

2. Biometrics

a. Starting point

Sweden is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Developments

In September 2004, Sweden announced it should start issuing its citizens with biometric passports in 2005. The new document should be consistent with the facial recognition standard of the ICAO and should fulfil the US VWP's requirements.

Finnish smart card and security printing company Setec – which currently supplies passports to Finland, Sweden, Norway and Lithuania – announced on 31/08/2004 that it had won an order from the Swedish Government to provide 5 million biometric passports over the next 5 years (a €100 million contract). In addition to the biometric passports, the Swedish authorities will start issuing electronic ID cards in October 2005 under a similar 5-year contract with Setec.

The passports, should feature a biometric identifier (facial image) stored in a microchip. The Swedish authorities will first issue the new passports without the microchip, and start issuing the biometric passports in October 2005.

On October 2005, a press release stated that Sweden had become the second European country to start issuing biometric passports compliant with the standard recommended by the International Civil Aviation Organization (ICAO). In addition, Sweden has also introduced biometric ID cards valid as travel documents across the Schengen area. The new Swedish passport introduced on 1 October 2005 has an RFID (Radio Frequency Identification) microchip embedded in its polycarbonate data page. The chip contains a digital photo and personal information of the holder. The main reason for the speedy introduction of biometric passports in Sweden is that the previous contract for the supply of Swedish passports came up for renewal in 2005. Another reason was the Swedish Government's will to comply with the US Visa Waiver Programme (VWP) requirements.
In addition to starting issuing biometric passports, Sweden has also introduced on 1 October 2005 a national ID card containing biometric data. The new 'national identity card' (*nationellt identitetskort*) is not compulsory and does not replace previous paper ID cards. It also complies with ICAO standards.

7.23 Slovenia

1. e-Government

a. Historical information

As early as in February 2001, Slovenia adopted a "Strategy of e-Commerce in Public Administration for the period from 2001 until 2004”, and in January 2003, a new action plan in the field of e-Government.

b. Developments

In September 2003, Slovenia was considered very advanced in the use of IT. The Ministry of Information Society holds the political responsibility for the information society, including e-Government. However, at an operational level, the Government Centre for Informatics (GCI) is the body in charge of developing the country's e-Government infrastructure, and to support, control and coordinate government departments' ICT projects.

With this infrastructure in place, the Slovenian government has implemented a number of e-Government applications for internal use. In particular, cabinet sessions are now held electronically (e-Sessions). Henceforth, the priority of the Slovenian e-Government action plan consists in developing e-Services for citizens and businesses.

2. Biometrics

a. Starting point

Slovenia is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Development

In January 2004, the Slovenian Government announced it wanted to do everything in its power to start issuing biometric passports before the 26 October 2004 deadline set by the US authorities. A specific task force created in September 2003 was analysing technological aspects and developing implementation strategies for the new high-tech passport.

“The main question in the production of biometric passports is the availability of contact less chips with enough memory, while interoperability issues also need to be sorted out”.

7.24 Slovakia

1. e-Government

a. Historical information

Concerning e-Government in Slovakia, the main actor is the Office of the Government, which oversees the eSlovakia initiative – a scheme launched in May 2002 to boost Internet access and use in the country. However, most e-Government developments are instigated on an ad-hoc basis by various government departments. The two main actors in public sector IT projects are the Ministry of Education, and the Ministry of Transport, Post and Telecommunications.

b. Developments

At the local level, a project to enable Slovakia's towns to deliver information and services online has been developed by the not-for-profit organisation eSlovensko. These information services are delivered through a central website (www.mesto.sk) providing structured access to 138 local authorities throughout the country. In addition, a national public information portal Obcan.sk (Citizen.sk) was launched in April 2003. It was created with the support of private suppliers, including Microsoft, Siemens Business Services, and HP.

By the end of 2004, more than 300,000 drivers in Slovakia should carry forge-proof driving licenses, complying with the security requirements laid down by the European Union.

2. Biometrics

a. Starting point

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Developments

The €6 million project of new driving licenses was a first step towards the delivery of a new generation of ID and travel documents. Indeed, the IT infrastructure used for its production should also be used to create high-tech ID cards and passports, which will most likely feature one or more biometric identifiers.

A similar solution was implemented by SBS in Bosnia-Herzegovina, where plastic driving licenses and ID cards – the latter including the holder's fingerprint stored in the form of a barcode – are already in use.

New passports by September 2006

In April 2005, the Slovak government has announced plans to start issuing biometric passports by 1 September 2006 and has already launched new passports having greater security features and being "biometric-ready".

According to Interior Minister, a digital facial image of the holder will be included starting in September 2006, while a fingerprint scan will also be added from March 2008.

The biometric passports will provide Slovakia with further arguments to negotiate visa-free travel to the United States for its citizens. Despite an official request by the European Commission in 2004, the US Administration has so far refused to extend its Visa-Waiver Program (VWP) to the new EU Member States. US policy is to assess VWP eligibility on a country-by-country basis, based on their rate of visa denials and their record of dealing with stolen passports. In March 2005, the US Department of State invited Ambassadors from Latvia, Lithuania, the Czech Republic, Hungary, Poland and Slovakia to discuss the initiatives that should be undertaken to allow for the introduction of "visa freedoms". Such visa freedoms could be granted by 2007 in return for a number of measures, including the adoption of more sophisticated and secure passports.

7.25 United Kingdom

1. e-Government

a. Historical information

According to new research presented on 31 May 2005 the UK, with €21bn, represents almost a quarter of the total ICT spending by European governments.

b. Developments

The developments of e-Government in the UK are the followings: e-Procurement of non-medical supplies within the National Health Service, e-Voting, organisation of a G7 e-Summit and e-Signature in 2002; secure e-mail system for the public, launch of an "Online Nation" campaign by the Office of the e-Envoy, Online CAP payments system for farmers, multiplication by 5 of e-Voting use, e-Payment of social benefits in 2003, creation of e-Marketplaces to sell online services, etc.

2. Biometrics

a. Starting point

The UK is one of the 27 countries currently in the American Visa Waiver Programme included in the US-VISIT programme. Thus, it is required to hold computer-readable passports containing biometric identifiers that comply with the International Civil Aviation Organization standards.

In order to ensure EU-wide consistency, the European Commission presented on 18 February 2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports. According to this proposal, future passports issued by EU Member States should contain only one mandatory biometric identifier, the holder's facial image. However, fingerprints or other features could be added at the discretion of individual Member States.

Moreover, on June 2004 the G5 Ministers called for ever closer co-operation on policing, data sharing and border security in order to tackle international terrorism and organised crime. This includes the introduction of biometric passports for all EU citizens.

The General Affairs Council meeting in Brussels on 13/12/2004 adopted a regulation mandating the inclusion of both facial image and fingerprints in future passports and travel documents issued by EU Member States.

b. Debate

In favour of developing

On 20 December 2004, a bill calling for the first ID cards to be issued in 2008 with biometric passports passed its first reading in the House of Commons with 385 votes in favour and 93 against.

On 28 June 2005 the House of Commons voted in favour of the ID Cards Bill by 314 to 283, with 20 Labour MPs rebelling against the government and joining the Conservatives and Liberal Democrats in opposing the ID scheme. The proposed legislation will now go to the House of Lords, where intense debate is expected.

Against developing

Before talking about including biometrics in its ID card, the UK had a debate on the introduction of such card. In December 2002, a first public meeting on the UK Government's proposed national identity card scheme resulted in a unanimous vote of no-confidence. The Government was criticised for not having engaged citizens in a national dialogue on the card. The Home Office said that the 1,500 responses received so far were split "two-to-one" in favour of the scheme.

Position of the government

The UK Home Secretary announced on 11/11/2003 that an ID card scheme would be phased in over several years. ID cards, however, will not be made compulsory before 2013 and only after a decision by the Cabinet and a vote in Parliament. This announcement followed the compromise reached by the cabinet on 06/11/2003, which delayed any decision on compulsion for years.

The detailed plans are not yet finalised but it is likely that:

- The card will contain basic personal details, including a unique number, which will appear on the face of the card.
- The card will feature a secure encrypted chip containing the holder's personal details in electronic format and a personal biometric identifier, which may consist in facial recognition, iris scans or fingerprints.
- ID cards will be linked to a new and secure national identity database that 'will not have details of religion, political beliefs, marital status or health records'.

On 22 July 2005, the Home Office responded to the alternative blueprint for e-ID cards proposed by the London School of Economics and Political Science (LSE). It said it would be less secure and more risky than the government plans.

c. Developments

2003

On 29 April 2003, the UK Home Office announced that passports of airline passengers travelling to the UK will be screened upon departure with new hi-tech scanners able to instantly identify passengers posing a security risk. This new scheme should include the increased use of biometric technology.

According to the UK Passport Service's (UKPS) corporate business plan 2003-2008 published the same week, biometric chips could be included in all UK passports by 2005.

On 03/12/2003 the launch of a trial of biometric technology was announced. It was run by the UKPS and should test facial, iris and fingerprint recording and recognition. This trial was delayed to the beginning of May.

2004

The UK Home Office announced on 15/06/2004 its intention to improve immigration control by rolling out a biometric identification system in a number of key airports across the country. Dubbed IRIS (for Iris Recognition Immigration System), the system is based on iris recognition technology and is aimed at increasing security while speeding up immigration control procedures.

The first major output of the UK Government's e-Borders programme, IRIS will store and verify the iris patterns of specially selected groups of travellers. The scheme will build on the successful trial held at Heathrow Airport in 2002.

2005

In April 2005, the government has plans to begin issuing biometric passports – including a microchip storing a digitised facial image of the holder – before the end of the year. Fingerprint scans could then be added to the chip in 2006, echoing a EU decision to include fingerprints as a second biometric identifier in passports that the UK is not bound to follow as it retains its "opt-out" over such arrangements.

Because UK passports are issued by Royal Prerogative, changes to passport formats and features do not require the passing of new legislation. And because no-one is forced to have a passport, the government is considering the possibility of going ahead with fingerprinting regardless of what may happen with current ID card plans.

On 25 July 2005, the UK Foreign & Commonwealth Office (FCO) announced that starting from January 2006, British passports issued outside the UK will include facial recognition and individual demographic data – such as name, age and birthplace – stored in a microchip.

In October, a biometric information campaign was launched in mid-September at Manchester Airport. Its aims were to raise awareness amongst current and future passport holders about the introduction of biometrics. Visiting seven locations around the country, the mobile facility wanted to enable members of the public to have their irises and fingerprints recorded and to see how the biometric passports will be read.

On the 10th October, The UK Presidency of the EU issued a paper supporting a number of policy priorities entitled 'Liberty and security, striking the right balance', which outlines its plans to push forward EU-level action on issues such as data retention, biometric passports and ID cards, passenger name records (PNR), and closed circuit television (CCTV).

On October 18th, Members of the House of Commons adopted the ID Cards Bill by 309 votes to 284 after a rebellion of Labour MPs narrowly failed to block the legislation. Nevertheless, the Bill still had to face a difficult vote at the House of Lords, the Parliament's upper chamber. Conservatives, Liberal Democrats, and a growing number of Labour MPs oppose the ID Card Bill. Although the UK government claims biometric ID cards will help tackle terrorism, organised crime and identity fraud, opponents remain highly sceptical.

Speaking at the Biometrics 2005 conference in London on 20 October 2005, the director of ID Projects with the UK Passport Service, said the current technology needs to be improved to carry out more efficient biometric scanning. The (UKPS) claims that iris recognition is still not an accurate enough method of biometric identification for mainstream deployment, following extensive trials of the technology. It was also revealed that E-passports with facial biometrics along with ID cards are set to hit the UK early next year and the Government also plans to include fingerprints in both by 2009.

On 21st October 2005, experts from the International Biometric Convention called for global biometrics standards agency as the increasing use of biometrics at national borders has prompted calls for an agency to guarantee a common experience for travelers. The agency could then monitor usage of the technology to ensure that it is deployed as efficiently as possible across multiple countries. During the same day, the director of identification for Police IT Organisation (PITO) said during the Biometrics 2005 conference that combined fingerprint and facial recognition could help UK police improve the identification of suspects and management of

prisoners. Therefore, he outlined plans to greatly increase its use of biometrics (mainly facial biometrics) over the next five years to help it identify suspects more easily and accurately.
In December 2005, the United Kingdom Driver and Vehicle Licensing Agency Awards Face Recognition Technology Test has been contracted to Viisage. The purpose of the UK trial is to determine if DVLA's extensive database of facial images from driver license applications can be used for machine-assisted face recognition.

On December 27th, Tory and Liberal Democrat peers watered down the Government's plans by making it voluntary rather than effectively compulsory to register on a new national database, which will include biometric data such as iris scans, facial images and fingerprints. Peers are expected to back an amendment to the Identity Cards Bill that would allow people to apply for a passport without having to submit their details for the ID cards database. Labour's majority was halved when a similar move was made in the Commons in October

2006

On the 25th January 2006, The PITO has been given the go ahead by ACPO to develop a business case for the deployment of face recognition technology on a national basis for the police service.

In the beginning of 2006, a great interest has been given by the media for the political debate started in the end of 2005 between UK government and opposition on the question of biometrics. Different issues were raised as the cost and price of ID cards as well as the safety of the use of Biometrics.

On the 10th February 2005, UK government gave concessions on ID cards after following defeat in the House of Lords one month before. The government will have to introduce a separate bill before ID cards can be made compulsory. The government is also addressing the controversy surrounding the potential costs of the scheme by stating it will provide progress reports every six months with the latest pricing information.

Five days later, the UK’s identity cards scheme was then put back on track following a string of close votes in the UK’s House of Commons last night, which overturned a series of amendments made by the Lords. From 2008, anyone applying for a passport (currently amounting approximately seven million per year) will not only be given a full biometric passport, but they will also receive an ID card and their details will automatically be entered onto the national identity database. This is something that has been called "creeping compulsion" by critics of the system.

In the same time, a press release said the Home Office Minister Andy Burham put the costs of identity fraud in UK at a staggering £1.7 billion. Following the government's acceptance of the Lords' opposition to plans to make ID cards compulsory, a step closer was done to ID cards incorporating biometrics as these were designed to prevent forgery, but British ID specialists TSSI caste doubts on the 20th February.

In March, the focus was put on the Biometrics in Airports. As a result of this massive increase of passengers in travel, coupled with the fear of international terrorism, the government said it was wanting to tighten and automate security at borders. The government talked to suppliers about the £400m e-Borders project, which will use biometrics and databases to check the identity of passengers even before they travel to the UK. On the 2àth march, a press release stated that the Iris Recognition Immigration System (IRIS) would now enable registered passengers to enter the UK without queuing to see an immigration officer at passport control. Instead individuals signed up to the scheme will be able to walk up to an automated barrier, simply look into a camera and if the system recognises them enter the UK, leaving immigration officers to concentrate on other priorities.

On the 29th of March, the home Office revealed that 25 prisons already had introduced biometric systems which recorded facial images and fingerprints that are used to confirm visitors' identities each time they enter or leave the prison. She also said that 20 more prisons would introduce the technology.

Finally, on April 21th, according to the new “Identity and Passport Service” business plan, it spent £25m on the ID card "set-up" in 2005/06 and has a budget of £56m in 2006/07 as the project takes shape.

8 Conclusions

The way European States have started to implement electronic documents based on biometrics standards is still highly dependant on the culture of each country.
In places where groups of citizens reject the very idea of having a personal ID card, because they think that simple fact would imply that somebody is permanently watching them, the same groups have accepted the mobile phone, for instance, forgetting that such technology is much more invasive (regarding not only the identity, but also the movements of each person).

We are still under the influence of the Big Brother myth, and this has an impact on the market and has delayed many European projects for several years! Should we eventually burn Orwell? Of course not, we have to read it again. But we cannot give up any objective analysis concerning multi-functional electronic identity advantages and see European industry and projects lagging behind with the most innovative developments that would be performed elsewhere in the world just because of this novel written in the middle of the late century.

It is clear that governments have to do a great deal more to implement and publicise these advantages if it could lead Europe to a safer, efficient and less energy consuming “knowledge society” where more business and administrative tasks and services could be obtained on line, from anywhere, at lower cost and at any time without physical transportation, reducing also the risk of fraud, abuses or identity theft. Governments have also to debate in full transparency and in democratic assemblies on the exact “level” of privacy it would be reasonable, necessary and acceptable to give up to trusted organisations (and to which ones) in order to benefit of these advantages or services, possibly on a voluntary basis.

Could biometrics be potentially dangerous? Well yes, as all technology could be - for that matter as anything could be, if used with ill intents. What is really dangerous is not biometrics, but its dictatorship. Otherwise we should fix priorities: automobiles should be forbidden first as potentially dangerous (it is quite easy to demonstrate that you incur more risks to suffer in a car accident than in a biometrics accident). Then it could be appropriate to forbid dogs, football, kitchen-knifes etc.

The current fragmentation of European industry is resulting for a part of the relative lack of maturity of the technology (still knowing rapid improvements, controversial benchmarks), and for a part of the lack of clear government policies, causing delays and cancellations regarding many projects. The emergence of international standards (mostly available from the ICAO web site) has facilitated the task by reducing the specification effort and size: rather than producing nearly 1000 pages specs in some cases, government producing national ID cards will be able to concentrate their efforts on national specific services (10% to 20% of the work, related to security, card management, lifetime management etc.). Some countries (especially Nordic countries) have adopted similar solutions from the same provider and a merging movement was initiated, both within Europe and with enterprises based in North America. On the other hand, fragmentation is encouraged by the fact some governments still develop this national part together with their own national industry: France works with six industry members to specify the new CNIE, in Germany the minister of interior established a programme for the German industry to work out the German ID cards specification. We may therefore see the emergence of locally protected champions prior to see some more consolidation in a second phase.

While implementing these national or European specific services, governments should also be more open and proactive in facilitating the use of their cards in other sector of economy: health, social security and finance for example, and re-evaluate the real risks of merging or not services and information. They have to create better public awareness about real short term, medium term and long term multi-functional services or benefits that could be obtained by any citizen rather than still presenting safer biometrics documents as just a new method of controlling phenomenon like terrorism – which appears definitely not the case.

Industry needs such a framework, where at the same time privacy rules (and risks) are well defined and potentialities of imagining new multifunctional services not limited by irrational fears: in fact, a national ID card scheme interoperable at European level could represent the foundation of a digital infrastructure that de facto constitutes a trusted domain. All actors allowed to enter, and thrive, within are certified and can play the role of either a services provider or a services user.

In such a scenario, citizens, businesses and government agencies can interact based on the reciprocal certified ID, thus validating entertained relationships and binding informative and economical transactions.

Interacting in such a trusted domain will foster naturally the development of new business models and innovative services that today are simply inconceivable or non-realistic or, simply, too risky. What is the most important in the production of safer, if possible biometrics, documents is not the immediate investment (and market) for the biometrics producers: it is to facilitate the development of such new industry field in Europe because it will generate growth and employment in a new branch of economy based on "trusted transactions".