



COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

ICT-PSP-2-Theme-3 - Consensus building, experience sharing
on internet evolution and security

ICT PSP call identifier: ICT PSP 2nd call for proposals 2008
ICT PSP Theme/objective identifier: 3.2 Trusted information infrastructures and
biometric technologies

Project acronym: BEST Network
Project full title: Biometrics European Stakeholder Network
Grant agreement no.: 238955

Deliverable D4.1

State of Art: Biometrics in eID systems

Final version

Classification: PU

Dissemination level: All

Date of submission: 15th April 2010

Table of Contents

Introduction	4
The relationship between biometrics and eID	8
PESTLE Assessment.....	13
Political	13
Economic.....	14
Social	16
Technological	17
Legal	18
Environmental	19
Current state of the art in usage.....	20
Public Sector applications	21
E-govt	21
National identity schemes	22
Other.....	23
Private Sector applications.....	24
Access control	24
Transportation	25
Finance & banking.....	25
Telecommunications.....	26
Bibliography.....	27

Preface

This is the first formal deliverable for WG 4 “Biometrics in eID and electronic transactions” of the BEST Network. WG 4 deals with one of the application areas for biometrics, namely in the context of eID. The deliverable represents a rapid scan of the most applicable uses of biometrics in electronic services (e-services) across governmental and non-governmental applications. When discussing e-services we mean services delivered electronically – that is to say, Internet banking, receipt of social security benefits and so on.

Input for this deliverable came from the following sources:

- A Workshop hosted by the Austrian Federal Government in Vienna in March 2010 where members of the BEST Network and other interested stakeholders were asked to comment and submit practices or examples of the use of biometrics in electronic services in order to create a typology.
- Subsequent input submitted via email from the members of Working Group 4 of the BEST Network
- Summary desk research carried out by RAND Europe and the Graz University of Technology

The purpose of this first state of the art is to understand (in an overall context) trends, gaps and challenges that further research in the WG and elsewhere might address. Examples of these research challenges include:

- Template protection techniques,
- Security evaluation of biometric methods,
- Remote biometric authentication methods (via the Internet).

To better understand the challenges in the different environments biometrics can be applied to in the public and private sector, a structure is given that settles the main focus of the working group. An assessment of the Political, Economic, Societal, Technological, Legal, and Environmental (PESTLE) aspects is made. This is complemented by a risk assessment. The state of the art is sketched by giving a few use cases where biometrics have been employed in public and private sector applications.

Introduction

eID is the representation of identity in electronic form. Although a number of different approaches and definitions exist which aim to conceptualise identity, many understand this as a highly contextual idea which is dependent upon the purpose and market in which sets of personal data may be transacted in exchange for goods and services. For example, an individual may be at the same time a resident of one country, a citizen of another, a customer of a bank, a member of a club and a family member. In each context, different identifiers are used to identify and in certain circumstances authenticate the individual against eligibility for certain services or transactions.

Electronic Identity (eID) is the representation of these attributes in digital form that can be similarly used in a variety of contexts and situations. This has become more prevalent due to the widespread take up of information systems by the public and private sector. Although the public sector necessarily lags behind the private sector in rolling out widespread information systems, nonetheless an increasing number of public and private sector applications are emerging taking advantage of the digitisation of identifiers.

The importance of electronic identity (eID) has been identified by the Manchester Ministerial Declaration which explained how interoperability and electronic identity were key enablers for eGovernment in general whilst European legal instruments aimed at the Internal Market such as the Services Directive (2006/123/EC) highlight the relevance of eID to achieving the freedoms of people, goods, services and capital. A number of other initiatives describe targets and signposts that will support the achievement of these objectives including the eIDM roadmap and eIDM Signpost paper. Indeed, interoperable eIDs are seen as important in supporting the realisation and facilitation of an internal market having knock-on effects on the competitive position of the EU-zone.

The increasing deployment of national eID solutions underlines the importance of eIDM. The IDABC study on eID interoperability for PEGS (2009) reports for Europe that 13 out of 32 surveyed countries already deploy government issued eID cards. Five countries were reported to plan to issue eIDs. While 5 out of the 32 surveyed countries actually have biometrics on the eID cards, the report also states that “... *the use of biometric data has not been reported as an authentication method for specific eGovernment applications in any country.*” This deliverable is mainly concerned with biometrics in e-services. We give rationales on where opportunities and challenges for biometrics in e-services are.

Although the underlying technology may be the same there may be different purposes for electronic services containing biometric functionalities: a passport (which is essentially the front end of a border control system and used to permit access entry and exit across international borders) is different entirely from an access control card used by a private organisation to gain entry to a secure facility.

The three components of an eID system are IAS – Identification, Authentication and Signature.

- Identification – the process of using physical or digital identity related data
- Authentication – the process of associating and permitting a specific identity or set of identity related credentials to access specific services
- Signature – a verifiable credential in an agreement from a specific identity that cannot be revoked.

The inclusion and use of biometric data may be seen as an additional form of card security mechanism present on a credential used in an identity management system (IMS). Such an IMS may be public (e.g. a national Identity card system) or private (e.g. a financial or access control system).

This is embedded in the context of extending existing ID card systems to make them more secure. This means that it is harder to forge (supposedly), and additional services (facilitated by the presence of a highly accurate form of identifier in the form of biometric data) may be possible.

The operation of any infrastructure which uses biometrics in conjunction with electronic services (achieved chiefly but not exclusively through the use of some form of credential containing a biometric identifier such as a smart card or token) is subject to many of the constraints, challenges and opportunities present in more general eID systems, namely:

- Systems and processes surrounding their usage (enrolment, usage, loss and re-issuance, application context, organisational aspects, supporting physical and logical infrastructure)
- Uptake and social acceptability
- Cost benefit analysis (linked to the issue over thresholds; see below).

Currently, in the most part the deployment of biometric functions in eID is being driven by the public sector.

As services move from provision of just information to one-way transactional to two-way transactions and subsequently wholly electronic, there is a need (for those services which impinge particularly on identity) to properly authenticate and identify the user of the service.

Drivers for use of biometrics in electronic services:

- National security (e.g. identification of terrorist suspects)
- Law enforcement (e.g. anti-fraud measures or compliance with pan-European police co-operation efforts)
- Legislative compliance (e.g. complying with electronic Signatures directive; e.g. Austrian and German signature laws state biometrics as option for qualified signature authorisation, though no broad usage is known)
- Broadening public interaction (e.g. e-Government)
- Efficiency (e.g. use of biometrics to automate processes, make operation of something cheaper driven by ability to control costs, reduce shrinkage due to reduced fraud / misuse)

- Effectiveness (deliver new services e.g. personal biotech that can determine from biological characteristics e.g. use of DNA information to determine efficacy for specific treatment).

Differing thresholds of identity requirement across the public and private sector may dictate which biometrics are used and how rigorous the error rates need to be. For example, the private sector may only require a lower level of identification (merely that the person is able to pay for example or that the identity is sufficiently accurate for contractual purposes) than the public sector, where there is more knowledge about the person to reach a degree of absolute 'truth' about his or her identity.

Biometrics help the eID card achieve its role as being a tangible representation of eID in the context of an eID system as defined by CEN/ISSS:

“Electronic identity solutions have the aim to guarantee the identity of a person (or a legal entity, e.g. a company) during the access to e-services and in order to provide the trust to the parties involved in the electronic transaction.”

One of the key questions is whether in the context of e-services, biometrics is necessary beyond what can be achieved with current technology. Although biometrics provides a high degree of trust and assurance, its use may be ultimately down to a process of risk assessment. For some applications there may be requirements for a high degree of identification and authentication (which biometric data can provide).

The introduction of a more robust form of Identity in various applications is seen as an essential solution to a variety of policy problems. This is made possible by a number of empirically observed trends as suggested by Lips et al:

- Increasing use of digital forms of identification and authentication of personal data instead of physical forms
- Increase in ability to discover and track personal info in real-time across physical barriers, locations and over time
- Increasing integration of life activities with the generation of personal information (e.g. use of credit cards or mobile phones)
- Increased blurring of the lines between public and private places makes personal information more publicly available
- Increased merging of previously compartmentalised personal data
- Expansion of ways of measuring and classifying citizens with greater precision compared to traditional measures such as paper based methods

The potential application areas for biometric technologies in e-services are being driven by the need to assure identity and prevent or manage the risk of identity related fraud. Due to ever increasing quantity of social security and welfare disbursement fraud, credit card transactions, cellular phone calls, ATM withdrawals, and visa applications, a number of organisations are evaluating the use of biometrics to enhance security, reduce fraud and improve customer

satisfaction. The ability of biometrics to establish identity with a high degree of authenticity represents an opportunity not to be missed.

As is known a number of biometric technologies are already deployed, primarily in access control environments, law enforcement (e.g. automated fingerprint identification system - AFIS) and border control/registered traveller applications. However there are a number of further possible application areas particularly in respect of financial services and network access (e.g. computer security). In respect of e-Commerce and Internet security, biometrics are being proposed as a solution to ensure that only authorised individuals can access sensitive data or execute transactions. However, for those that are deploying such solutions, achieving successful deployment is more than just simple replacement of existing security and authentication mechanisms with a biometric interface.

There are a number of issues that must be considered prior to the deployment of biometrics as a support for identification technologies. This includes such issues as:

- providing for maximum compatibility across the range of registration and enrolment technologies deployed across different form factor devices (e.g. desktop computers, mobile phones, PDAs etc);
- accommodating the widest range of individuals who have trouble successfully enrolling or verifying,
- integrating biometric match decisions into payment and clearance systems,
- defining applicable accuracy requirements (which may differ between public and private spheres), establishing the most appropriate location of data storage (smart-card or other device) to fulfil security and privacy requirements (e.g. availability and compliance with privacy principles such as end-user control) and associated measures for accountability
- the integration of biometric acquisition processes into existing interfaces
- management of the account process (revocation, user problems, management by exception etc)
- establishing appropriate protocols for secure data transmission to permit biometric information to be used in remote transactions over different types of infrastructure (e.g. the public Internet or 'walled garden' mobile networks).
- Technological compatibility (e.g. with the latest trends toward cloud computing)
- Selection of most appropriate biometric identifiers to use (e.g. different biometrics may have different levels of trust and 'authenticity' associated with them due to differing false acceptance and false rejection rates)

The relationship between biometrics and eID

Biometric technologies have been source of controversial discussions for a while. Opinions as diverse as claiming a silver bullet in law enforcement to highlighting the privacy threats have been raised. One source of the controversy may be that experience where a technology is proven and mature in one domain, such as with AFIS or border control, may not be mixed up with or cannot necessarily be transposed to other domains, such as unattended environments with remote access to services.

In an attempt to structure the scope of our work, we distinguish e-services in various dimensions: First we distinguish between the public sector and the private sector where the users' perception on duties and safeguarding their information may be different. The second dimension specifically directed to biometric technologies is whether biometric data is stored under the users' control or whether third parties or databases are involved. The final dimension is whether the technology is applied in a remote access environment, i.e. to e-services, or whether an attended face-to-face environment is given.

In remote-access environments it is not possible to simply replace passwords stored on a server with biometric templates stored on the server since biometric data, in contrast to passwords, are in general no secrets. It is necessary to prevent bypass attacks where unobserved attackers would simply feed in public biometric data of enrolled users. Furthermore, template protection is a challenge in particular in case of centralized storage of biometric data on a server. The storage of the reference data and the comparison of the biometric data may take place on the client side, possibly in a tamper-proof smartcard. Then, cryptographic methods could be used for authentication against the server.

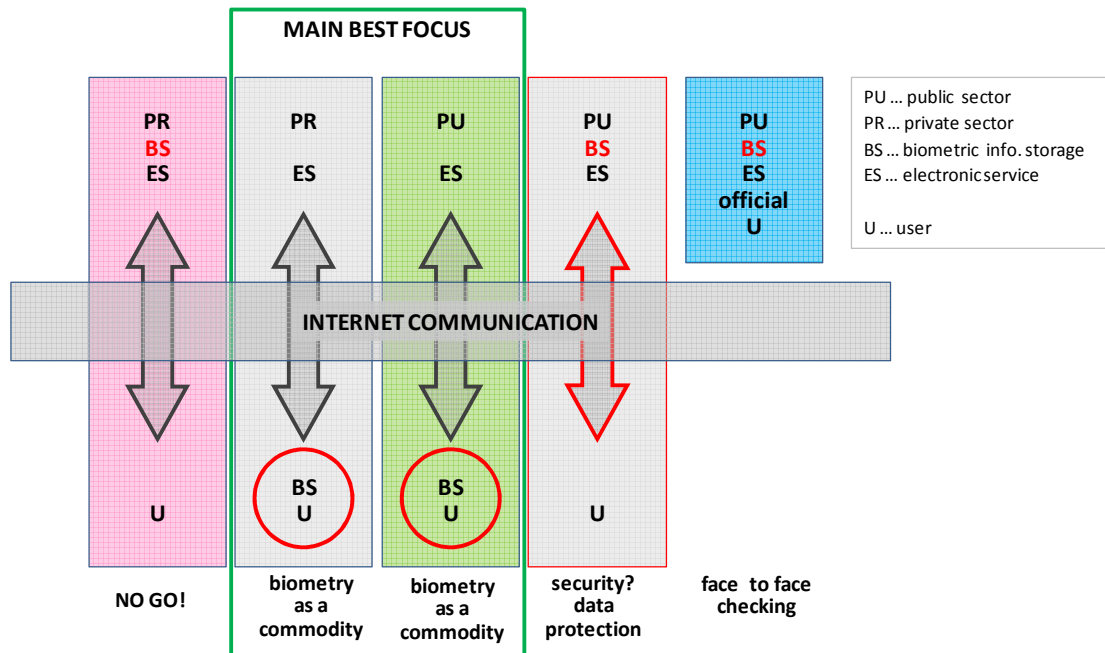


Figure 1. Explanation of focus of this WG (source: TU Graz)

In Fig. 1 above the key focus of this working group is presented. As can be seen, Internet communication (defining e-Services) is the key underlying platform enabling transactions between the public or private sector (PU/PR) and the User (U). Biometric Information Storage (BS) is the commodity which enables these transactions. In our preferred scenarios, biometrics may be interpreted as a commodity to be traded in both public and private sector applications. Both our 'preferred' architectures above include the use of biometrics at and under control of the user, which can be accessed by the public or private sector. Even though face-to-face pilot schemes with biometric data storage by the private sector already exist (e.g. digiProof system www.it-werke.com) for fingerprint-based customer identification, which is used in some Edeka markets), the capture and storage of biometric data by the private sector may be regarded as a no-go application area as it would represent a socially and politically unacceptable private sector intrusion. However, even though there is also reasonable mistrust towards the state due to bitter historical experiences, the same cannot be said for the public sector due to the complex philosophical, legal and socio-cultural interactions of the relationship of a state to its citizen. Nowhere is this more manifest than in the responsibility of the state to provide for security of its citizens, which in the context of the use of biometrics may require storage and manipulation of biometric data by the government. Perhaps one of the most compelling examples of this currently is the UK's National DNA Database, seen as effective by some in supporting criminal justice and security objectives, unnecessary and illegal under European Data Protection Law by others (e.g. the recent ruling by the European Court of Human Rights) and ultimately destructive to society (e.g. privacy advocates have argued that the collection of the DNA profiles of those arrested rather than convicted represents a structural assault on society itself).

Risk assessment

The use of biometrics carries risks. It may be possible to separate out three type of risk¹ affecting the use of biometric systems for identification in e-Services. Firstly, accidental risks or hazards might occur as a result of acts of nature e.g. disruption of infrastructures upon which biometric identification systems rely or emergent risks from the sheer complexity of the infrastructure. Secondly, directed or motivated risks which are specific attempts to undermine or compromise the integrity or authenticity of the biometric identifiers. Finally, there are 'risks of trust' which may occur as a result of the 'downstream' compromise of the trusted third party. These may be policy or contractual in nature (for example deliberate forwarding of biometric data by a third party in order to defraud the identity subject).

The deployment of biometric methods also adds the users' limbs to the assets requiring protection and puts them at risk. It has already happened that attackers chopped off a victim's finger to get round a fingerprint recognition system used for disarming a car's immobilizer.

It should be stressed that the objective of risk assessment is efficient allocation of risk. This depends on three things: i) the ability of different parties to bear the risk (e.g. the degree to which failures could trigger bankruptcy or irreversible loss of business vs. the extent to which risks can be diversified or insured or hedged); ii) potential risk holders' risk aversion (which is a consequence of other characteristics, such as knowledge, expectations, demographic factors and the consequences of failure); and iii) the ability to take steps to reduce the likelihood or consequences of harm.

The complexity of risks demands specific attention. Biometric identification systems in themselves consist of different subsystems linked together through electronic, physical, legal and even intangible (e.g. interchange standard) connections. Moreover, the biometric identification system is connected to other identification and record systems, and ultimately to a wide range of 'application systems' and societal structures that rely on them. Linked systems are complex, and risks arise at the interstices/interfaces between the systems (which may lie in the 'blind spots' of those responsible for each subsystem) or at the whole system level. These may be particularly hard to foresee; the underlying mechanisms are highly non-linear and hard to observe. In fact, information about the performance even of subsystems - let alone the system as a whole - is likely to be endogenous (e.g. driven by events or design decisions about what data get recorded, how they may or may not be combined, etc.). It is also subject to biases of selection and incentives. The selection incentives refer to the choices people make to engage with biometric systems. For instance, if financial institutions do not use biometrics (or use a particular form of biometric) in delivering specific services, then they do not collect risk information relating to those uses. This may distort subsequent decisions – for example, false accept/reject rates for a given biometric based on, say, deployment at borders may not give an accurate picture of the rates for, say, ATM deployment, where the population, the purposes and the stakes on both sides are vastly different. In much the same way, the use of a biometric for authentication not only weights false acceptances and false rejections differently than use of the

¹ An alternative classification separates false positives, false negatives and a precise solution to the wrong problem (Type I, Type II and Type III risk).

same biometric for identification, but produces a systematically different evidence base; a different population, different levels of compliance and understanding, and even different probabilities that mistakes (in either direction) will be detected or recorded. On the population side, the deployment of biometrics, the availability and familiarity of alternatives and popular expectations about risks and benefits all influence the degree of 'opt-out' or (deliberate or accidental) non-compliance. Again, it may not be possible to identify those opting out, let alone to assess their characteristics, to say nothing of ascertaining whether those characteristics are correlated with performance metrics. This means that: a) the success of one biometric depends on the success of others; and b) risk assessments based on single applications of single (combinations of) biometrics are likely to be misleading. This, in turn, complicates the degree to which markets (from application markets to investment markets, can aggregate and price such risks.

These elements are particularly important for gathering and aggregating information about risks, assessing their likely magnitude and consequences, and allocating the impacts (or responsibility) appropriately. To conclude this discussion, we highlight two likely complications. The first concerns the aggregation of micro-level or specific risk to produce assessments of overall risk and uncertainty². The second concerns the importance of structure and the dangers of nonlinearity and path dependence. With regard to the first, the above discussion points up the importance of overall attributes such as trust. This can have the effect of transforming idiosyncratic or localised risk into systemic risk. For example, if a well-publicised incident with one biometric or one application erode confidence or distort patterns of application with others (e.g. reducing secure transactions, encouraging use of inappropriate alternatives, etc.) the risks spread – this means that the risks in one part of the system are not independent of those elsewhere and thus that they cannot simply be added. Indeed, it is generally not possible to hedge against such systemic risks or diversify them away. A direct practical consequence is that it may not be appropriate to manage such risks at the application or enterprise level; rather, they must be managed jointly, even to the extent of creating a *prime facie* case for government involvement³. With regard to the second, if biometrics are adopted in order to provide assured and trustable identity services to service providers or their clients, the returns depend directly on the patterns of trade and interaction. The more clients a firm has who demand (implicitly) strong identity, the greater the rewards to providing it and managing the attendant risks. On the other hand, the expected return also depends on the likelihood of attracting opportunistic or careless parties who might be deterred by biometrics or whose mistakes could be limited in extent by appropriate identity technologies. Thus, the hopes of suitable returns motivate technology adoption, enterprise reengineering and performance monitoring. But this is limited by the cascade effects of expectation formation; if a well-publicised loss of private data, for example, causes a loss of business, the firm may find itself unable to attract privacy-sensitive customers, and may therefore have little incentive to correct errors or improve its practices – in the event, a poor reputation becomes self-fulfilling, especially if weakened identity practices attract less honest or careful clients. There are two practical implications. The first is that firms

² We take as read the well-known distinction between quantifiable risks of known outcomes and unquantifiable uncertainty of possibly unknown or even unknowable consequences.

³ This may not be efficient if the reputation risk is removed, and may give rise to undesirable free riding and underprovision of risk management by individual organisations.

may hesitate to adopt unproven (especially innovative) technologies if the perceived risk of such a reversal of reputation is too high. The second is that the normal realisation of random failures may produce a form of 'identity divide' between firms able to successfully implement strong identity and those no longer able to do so⁴.

⁴ The threat of 'crossing the divide' may make firms excessively risk averse or open to opportunistic threats.

PESTLE Assessment

Political

The broad political acceptability of the use of biometrics for e-services is as yet hard to determine. Whilst some countries have been able to invest in biometrics in very narrow contexts (mainly air travel and borders) for specific applications, the broader objectives which may be met by biometrics have yet to be identified.

The increasing focus of European politicians toward the ‘rights of the individual’ as a key theme in the new Commission is also of high relevance in this respect. This presents both an opportunity and a challenge for the broader use of biometrics in e-services. It is an opportunity since biometrics permits end-users to have a greater degree of control over the uses of their personal data.

A crucial issue that has been alluded to in current deployments of eID based systems (in national contexts for example) is the impact of the broader use of biometrics in administrative organisation. For example, as the UK Identity Card has approached full roll out, the agency charged to be accountable for its deployment has evolved in its remit, from the Passport Service to the Identity and Passport Service. For example, the IPS has also had to embed a further culture change regarding the stewardship of personal data – the different culture has been a notable comment in the recent report of the Identity Commissioner (The Register).

This fundamental question may be articulated as whether the increased opportunity for identification to a high ‘quality’ standard made possible by biometric data mean that governments and public administrations will have to radically change or re-orientate themselves in order to facilitate the use of such identifiers and maximise the opportunities for administrative efficiencies made possible by these type of identifiers?

At the EU level the Stockholm programme for an area of crime, justice and security has identified a number of requirements for intervention at the EU level that may provide further public sector application areas for biometric technology. For example two policy developments of interest include a policy initiative to establish pan-European rules on the attachments of bank accounts (to enable debtors to pursue debt confiscation across EU borders) and similar pan-European rules on asset confiscation. Both measures may include the governmental use of biometric data stored and used in government data warehouses.

The ongoing developments regarding pan-European criminal justice systems such as the Visa Information System (VIS) and the second generation Schengen Information System (SIS II) and its associated BMS (Biometric Management System) provide a bellwether for discerning the future political acceptability of these technologies, not to mention whether they are useful in contributing to desired social outcomes.

Finally other national or pan-European level applications which may demonstrate political acceptability of the more widespread use of biometrics in e-services include those in the health-

care sector (e.g. current efforts to establish a pan-European system for traceability of tissues and cells procured as donations) and for crisis management to authoritatively identify and authenticate victims, rescuers, refugees and asylum seekers in a crisis management situation.

Economic

There are various ways to frame the economic factors affecting biometrics development, adoption and use. Some arise at the micro level and follow the biometrics value chain (or value mesh). In this perspective, biometrics provide inputs to many other types of economic activity (notably in the service sectors).

Demand for them is a derived demand, and affected by the demand for the services thus produced and by the availability and cost of other inputs that substitute for (e.g. non-biometric identity technologies) or complement them. Businesses able to offer biometric enhancements may gain access to more, and more profitable (higher value, etc.) custom. On the other hand, offering biometrics involves a degree of set-up and operational costs, exposes businesses to associated risks (see above) and may change the underlying business model. Indeed, small businesses may find biometric adoption by rivals constitutes an entry barrier, necessitates the acquisition of costly human and ICT capital or may even be forced on them by competitive necessity, with few or even negative net benefits. On the other hand, biometric capabilities can improve customer-facing, supplier/partner-facing and internal business processes; these benefits may be realised over time, regardless of the initial business case. In this regard, it is worth recording that the development of biometrics and their inclusion on the broader sweep of economic activity is thus strongly affected by cyclical and exceptional changes in business conditions (e.g. the current ‘crunch’).

On the supply side of the biometrics sector are the factors affecting the biometric industry itself, running from the underlying R&D to the manufacture and supply of biometric equipment (e.g. sensors, cameras, associated ICT equipment) and software to the supply of biometric services by dedicated suppliers, system integrators, etc.⁵ Because this set of markets is interconnected and varies with technology and ‘downstream’ socioeconomic development, it is perhaps more appropriate to think of it as a dynamic ‘value mesh’ than a linear and well-defined value chain. This dynamism is emphasised by downstream developments, notably globalisation (which increases the range and variability of parties making transactions and potentially⁶ the need for strong identity), convergence (in which services in sectors with very different needs for and histories of identification become linked or provided over common infrastructures into which

⁵ An analysis of this structure can be found in Cave (2005) and IPTS (2005)

⁶ On the other hand, it has been argued that identity-based biometrics (those tied to named individuals’ official records) is most appropriate in small-scale applications in relatively closed systems, and that for large-scale applications, especially those spanning very diverse groups and/or multiple jurisdictions, ‘weaker’ applications (e.g. pseudonymised applications providing biometrically-secured temporary or local identification – as with the fingerprint verification of anonymously-purchased admissions tickets to Disney theme parks – non-biometric identity or even anonymised transactions. As an example of the latter, credit transactions (on the Internet or elsewhere) can generally be traced back to legal – if not always physical – persons, while cash transactions cannot. In some cases, the lower costs and reduced accountability of cash is efficient; there is in general no presumption that stronger identification is always better, or that it benefits both sides of a transaction (and other interested parties) to the same degree.

biometrics can be integrated, virtualisation (which increases the potential risks of accident, attack or emergent failure while weakening the appropriateness of connection to a physical person), etc.

The prospects for biometrics are also strongly affected by market structure considerations. For example, the vigorously-enforced patent on iris identification algorithms both concentrated the markets for hardware, systems and applications and (it is widely believed) slowed overall development and uptake of this biometric. The resulting distortion of deployment and additional R&D has locked-in choices of substitute (typically weaker) biometrics and thus limited the extent to which an initial demand driven by the potential of biometrics more effectively or efficiently to provide legacy identity services can give way to innovative applications exploiting the potential of these technologies to deliver enhanced or novel services and to support additional business models⁷. Thus monopoly power – especially that derived from IPR – becomes an important consideration in both the current use and dynamics of biometrics.

Beyond the direct economics of the industry, the economic factors affecting private- and public-sector economic value associated with biometrics come from the contribution made by identity to the overall efficiency and effectiveness of the economy and public service delivery. Provided the deployed biometric recognition methods are sufficiently accurate, resistant to fraud and easy to use, this ranges from obvious contributions in the form of reduced levels of fraud and abuse and reduced costs of monitoring to more subtle effects such as a shift in the costs and entry barriers facing firms less able to adopt or manage biometrics, loss of revenues in sectors providing alternative identity services, reduced level of cost and loss associated with failures of these alternatives (e.g. loss or theft of passwords, etc.), enhanced levels of trust throughout the economy, or the separation of an ‘identified’ and a ‘shadow’ version of the economy, with consequent potential advantages of specialisation or disadvantages from lost gains from trade between the two parts.

This part of the economics is primarily concerned with aggregate effects. Equally important may be the distributional effects. The costs and benefits of biometrics are not equally spread – as in the above discussion of risk allocation, distribution matters. One area of particular importance concerns the possibility that biometrically-linked data may make activity profiles even more valuable than they are already. When biometrics are used in commercial and retail transactions, they tend to be applied asymmetrically – the customer or service user must identify themselves but (in most current applications) the seller or service provider need not. The seller/service provider thus has an incentive to insist on biometric identification and the transmission of other personal data that are not strictly needed to deliver the service and protect the immediate interests of those involved. This incentive (already present in almost all online transactions) could be exacerbated by biometrics, since the possibility of repudiation is reduced. This makes it harder for those asked to supply such information to reverse ‘mission creep’ individually or collectively. But this ‘externality’ of the inclusion of biometrics in a widening range of economic activity is not essential. It is equally possible to develop ways in which access to or reuse of

⁷ An example might be the use of strong identity to support more differentiated and ‘flat’ models of cloud computing and shared innovation.

profiles is itself biometrically secured, giving far greater effect to current privacy and personal data protections.

A further consideration arises when biometrics are used in non-anonymised ways; the acquired biometric must be compared to a template. This creates three sources of risk; stored template data, template or acquired data transmission and the processing necessary for comparison. Briefly, it is necessary to consider the implications of these externalities for associated business models (e.g. the cloud, as noted above) and the potential emergence of 'biometric intermediaries' to manage these risks. Note as well, that the risks and consequences are in part endogenous – for instance, the concentration within a data centre of large amounts of biometric data is likely to increase their attractiveness to criminals and other malign actors and to correlate the occurrence or consequence of risks associated with accident or systemic failure.⁸

Social

Social acceptability of biometrics in e-Services may focus around fear of the unknown, (specifically fear of use) and what the use of such data represents. Research into the acceptability of biometrics have shown that once initial fear of use is overcome (mainly through exposure to the technology) and provided that efficiencies are demonstrated (and achievable) then acceptability increases.

These concerns may stem from different social expectations of identity between those offering an e-service (either the public or private sector) using biometric identifiers and those 'data subjects' who may regard such information not as simply another form of personal data but rather as representative of a different contextual interpretation of their identity as being more physical and related to their humanity. Different cultural attitudes may illustrate this – witness the different interpretation of privacy as a quality related to personal space or the physical attributes of humanity in India vs. a view of privacy more focused upon informational self-determination popular in Western Europe and North America. Successfully bridging this gap in respect of the more widespread deployment of biometrics in the context of eID will require knowledge of and understanding of the different social constructs that may be affected and may influence its use and further uptake.

One of the key social issues yet to be decided is whether within the context of demand side applications, a service offering which advertises itself as being highly private (by dint of relying upon biometric data) will actually be commercially viable. Some work has shown that individuals do not explicitly consider privacy as a determining factor in how they express preferences between one service provider or another (otherwise the personal data market would be more dynamic as companies would have to alter their offerings to address this customer factor and privacy policies would need to be more user-friendly) and so the promotion and introduction of a technology that is based on providing more and more privacy may be seen as unnecessary.

⁸ To give a mundane example, if retail systems become wholly dependent on biometrics using centrally-stored templates and/or central match processing, any system or network failure prevents transactions. On the other hand, locally-stored templates and local processing can proceed

On the other hand, a study carried out for the financial industry on e-Banking shows that as soon as an incident or security compromise occurs, a great portion would just leave the bank no matter what the reason of the incident was. Similarly, a study on e-Government take-up by the Oxford Internet Institute et al. (2007) for the European Commission showed lack of trust and inadequate security and privacy safeguards among the seven key barriers to e-Government.

There are other social concerns of interest too; namely whether further use and collection of personal data by public and private sector organisations will be viewed as further evidence of the existence of a surveillance society, despite the greater opportunities for choice that biometric technology may represent.

Finally, there may be significant social implications if the technology and deployment fails to meet inclusivity requirements for large portions of the population that fall at the margins or as outlying data points in biometric systems. The implementation must be matched to social expectations regarding inclusion and the governments' (and some companies') role in maximising inclusion.

Technological

The technological application of biometrics is closely linked to the science and mathematics of statistics and this informs technological possibilities. Matching an individual's fingerprint to a given fingerprint (1-to-1 matching) is fairly reliable and this is seen as the more common technological pathway for eID in e-services. However, technological solutions to address the more complex problems posed by so called 1-to-n matching (where an individual's fingerprint is checked against a fingerprint database) are more complex, even if there is a high degree of certainty that the record is present in the database.

Some of the technological considerations will revolve around what is the 'best' technology to be used. Current state of the art is based on use cases and applications in either Registered Traveler or MRTD (Machine Readable Travel Document) purposes; namely fingerprint, facial or retinal scans.

Fingerprint technology may involve either one, two or, as has been seen in the United States, even all ten fingers. With facial recognition, data points (of different granularity depending upon the system) may be parsed out of a photograph of the individuals face, and then used to form an identifier for matching purposes. Similar technology is used for retinal scans.

However, a discussion on the most appropriate technology to use will be necessary; whether this is due to technology that is delivered by a commercial entity in order to facilitate customer access. Technological aspects will need to consider form factor as well as delivery means; the capture and storage of a biometric on a smart card versus other form factors (e.g. a mobile phone) will ultimately be a commercial decision given the infrastructure costs associated with the deployment of ubiquitous fingerprint scanning technology or other end user / consumer orientated biometric scanning devices.

Other examples specifically directed to privacy preserving biometric technologies are match-on-card approaches or biometric encryption dating back to Tomko et. al. (1994).

The technological capability is determined by other existing technological dependencies – e.g. biometrics for secure remote access is limited (e.g. for telecommunications) since the hardware is the limiting factor – not every computer built has a fingerprint reader or scanner. Despite the popularity of laptops with fingerprint scanners (which are seen as a novel means to execute access control upon a local machine), there is still no popular examples of this hardware facet being used for purposes other than local access logon.

Finally, there are backend technological developments that may affect the utility of biometrics as part of an eID to support identification and authentication for services. Examples include cloud computing where data is stored in a ‘cloud’ whose provenance and exact location is opaque to the organisation relying upon the cloud service provider. Another example is the holy grail of encryption; so called homomorphic encryption where some (arithmetic) operation on plaintext can be executed by an agent possessing the encryption key and the cipher-text, without decrypting the latter.

Legal

There are a number of significant pan-European legal instruments which may influence the use of biometrics to support identification for e-services. These include Directive 1999/93/EC on a Community Framework for Electronic Signatures (establishing the electronic signature as having comparable legal standing as the physical signature), the 1998 Data Protection Directive 95/46/EC (governing the use of personal data) and the Services Directive 2006/123/EC which establishes and facilitates the framework for a consistent market for electronic service delivery across Europe.

In the European context, the surrounding legislative is governing the use of personal data by European Institutions (such as EUROPOL or Frontex) (so called former second pillar) and the former ‘third pillar’ instruments governing the use of personal data for the purposes of police and judicial co-operation is also highly relevant. This covers the use of personal data to address European level cross border issues (e.g. collection of data for terrorist watch lists) or where national competence may be supported by facilitation at the European level (e.g. in regard to the exchange of personal data concerning suspects in the Schengen Information System).

In particular the Data Protection Directive via its national transpositions sets out several overall principles that must be adhered to when using personal data (which biometric data will fall directly into); several of these will be relevant in respect of the delivery of biometric enabled e-services. Although many large organisations in the public and private sector will no doubt be already used to the intricacies of compliance with 95/46/EC (and its national instantiations), the aspects of compliance relating to data quality will perhaps be brought most acutely into focus in respect of the techno-legal system to permit individuals to update their (personal) biometric data.

Further depth on relevant legal issues are highlighted in Deliverable 2.2 Report on legal interoperability of the eID Large Scale Pilot STORK (Secure Identity Across Borders Linked). While bio-

metrics is beyond the scope of STORK, the analysis on data protection aspects in relation to eID, identifiers and attributes can equally be applied to biometrics.

A further legal framework specifically relevant to e-services is the Services Directive. Article 8 Clause 1 of 2006/123/EC highlights the purpose of electronic access to services by:

1. Member States shall ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities.

As well as these overall legal frameworks, the current state of flux of the entire legal framework relating to data protection and privacy in Europe presents a serious uncertainty in respect of understanding how the legal environment will affect the use of biometrics in e-services. This has come about because of the structural consequences of the successful passing into force of the Lisbon Reform Treaty which, by dint of changing the voting procedure for agreement, effectively removes the former pillar structure of European policy-making and gives the European Commission greater mandate to act in national areas of police law enforcement and judicial co-operation matters.

Knowledge of these issues at a pan-European level, however, must also be tempered by consideration of the differing legal contexts and interpretations in each Member State which have transposed European law. Despite the existence of the Directives listed above, national transpositions may differ considerably. Another issue heavily coloured by national cultural and philosophical constructs is how the judicial and criminal justice system would react to the use of biometrics and what the forensic or judicial implications of the broader use of biometrics as a form of supporting eID enabled e-services.

There are other specific issues which understanding this context from a private law perspective brings into focus, namely questions of accountability and liability. Accountability will be important to determine in who is responsible for maintaining chains of assurance once biometric identifiers have been provided. This can be compared to the eID environment. The STORK Project report on legal interoperability identified liability as a major obstacle in the cross border context, if it is not provided by mutual recognition regimes (such as for “Qualified Certificates” under 1999/93). The same may hold for biometric use in eID for cross border use.

Environmental

The increased technological infrastructure required for the deployment of biometric technology whether that delivered by the supply side (e.g. by banks rolling out fingerprint scanning technologies or demand side (e.g. the presence of fingerprint scanners in laptops and other end-user devices) may have some implications for the environment in terms of the added production and manufacture of electronic components.

Current state of the art in usage

In this chapter we present indicative examples of current uses and limited adoption for the use of biometric technology in e-services. As can be seen there are limited deployments of biometrics in the context of the different sorts of applications. This is due to a current focus of biometrics on physical applications (i.e. where the subject or item to be transacted) is present. An example is border control or registered traveller programs (covered in another of the working groups) where the individual and the device are both present in order to gain access to the border.

There may be horizontal or vertical markets and applications where biometry might have a role to play. In the horizontal applications, Point of Sale/ATM and e-Commerce are the most relevant. The vertical markets and applications may be split according to the following classification:

Law enforcement

- AFIS
- Surveillance
- Mug Shots
- Corrections
- Home Arrest

Government

- National ID
- Voter registration
- Driver license
- Benefits distribution
- Employee authentication

Financial

- Account access
- ATM
- Online banking
- Telephone transactions

Healthcare

- Access to personal information
- Patient and health professional identification
- Disease information access

Travel and Immigration

- Air Travel
- Passports
- Border crossing
- Mass Transportation

Other

- Education
- Entertainment

Public Sector applications

E-govt

E-Government is on using ICT to provide better services to citizens or businesses. Biometrics can play a role in identification and authentication of the natural person. Using the structure we introduced in figure 1 above, one needs to distinguish between e-Government carried out remotely via the Internet or using ICT in face-to-face contacts.

Examples to apply biometrics to the latter, i.e. in traditional face-to-face contacts, are biometrics in voter's registration such as introduced in Mexico and Nigeria or planned for Bangladesh and Gambia. A number of applications of biometric exist for reducing fraud such as reclaiming benefits (sometimes referring to "double dipping"). An example is the introduction of iris scan to food ration cards in Andhra Pradesh, India, in 2005. Similarly, the recognition of asylum seekers in Europe by using fingerprints is meant to avoid double applications. Fingerprints are used in South Africa where e.g. pensioners can claim pension cheques using this biometric.

The most prominent examples of biometrics in government application are however forensics with DNA databases and AFIS systems, and amendment of ID cards and passports with biometrics, respectively. Both are discussed later in this section.

On using biometrics remotely in online e-Government services, however, no case studies are known.

Crime, justice and Security

Below we present some indicative examples of the use of biometrics in crime, justice and security applications.

e-Verify: US senators have begun to explore the inclusion of biometrics in the US e-Verify system. Introduced in 2004, e-Verify is a system to replace paper based processes to correctly determine the status of employees. In late Nov 2009, the system became mandatory for federal organisations and was being rolled out to private companies holding federal work contracts. The drive to include biometrics will take the system from a current internet based employment eligibility system to a potential database of some 160m American workers. The system is now mandatory to some degree in 12 states and has faced opposition from US businesses, in particular the US Chamber of Commerce who argue that it represents additional costs to business in an economic climate when they can ill afford more governmental requirements.

The pan-European Biometric Matching System (BMS) is a planned additional system that will run alongside the second generation of the Schengen Information System and the Visa Information System (VIS).

Other notable examples include the UK's National DNA Database (NDNAD). The NDNAD has been run by the Forensic Science Service on contract to the Home Office since 2005. In 2006, there were more than 4 million records on the database. It has proven its usefulness in tracking down serious offenders in a number of occasions – however, it is not without controversy (Cragg and Mahy, 2009). In 2006, Genewatch reported that the large number of unconvicted individuals on the database (in 2006 there were 124,347 people who were arrested but not subsequently charged or cautioned with an offence) were not beneficial in terms of its effectiveness (Genewatch UK, 2006). Recently, the Forensic Science Service has begun to use familial searching, which uses DNA found at crime scenes to see if there is a 'close match' on the database, raising further civil liberties concerns. Between April 1995 and March 2004, the database cost £182 million. It has come under some criticism for the storage of information for individuals who have not been convicted of any offence, leading to assertions that, given enough time, it will end up storing the DNA of the entirety of various ethnic groups. The capture of the DNA data of arrested suspects (rather than those convicted) in the NDNAD was recently ruled as being unlawful and contrary to Article 8 of the European Charter of Human Rights.

Finally, other examples include the use of biometrics for overt and covert surveillance as a possible application area. This may become more and more urgent given recent US government policy shifts regarding the extension of the use of behavioural profile and 'non compliant' matching of travellers to watch lists or no fly lists based on large scale surveillance of crowded places.

National identity schemes

There are a significant number of countries deploying national ID cards to support citizen access to electronic services (e.g. e-Government) at both the local and national levels. Deployment models range from a simple plastic or printed card that acts as little more than a personal identifier when accessing basic government services to more complex smart cards which include some form of automated biometric technology so that the card can always be linked to the cardholder. The examples of the Octopus card in Hong Kong (which is not a national identity scheme) show that, as awareness and the market for the use of such a smart card increases, more and more applications can be added to the system.

A number of countries have been implementing identity schemes either by digitising existing identity and national registry systems or creating new systems based around electronic functions (e.g. the UK). When putting these initiatives into relation to biometrics, one in most cases needs to distinguish between the access to e-services such as e-government, and the use of the document as a conventional ID card or travel document. The physical ID card function when enhanced by a chip often follows MRTD standards and adds a biometric feature. On the other hand, the e-services function of eID cards rarely uses the biometrics. While both functions, travel document and e-services access, may reside on one token, the usage of biometrics is often limited to the MRTD. Well known examples include:

- Austria's Bürgerkarte which has an eID scheme based on technologically neutral qualified certificates which can be used in a wide variety of devices (no biometrics)

- Belgium's BELPIC is based on normalised and qualified certificates and chip cards. Its use is restricted to certain categories of authorities and instances where permission is gained from the Rijksregister (photo stored electronically; not used for e-services)
- Estonia has a smart card system with qualified certificates. (no biometrics)
- Germany will introduce new electronic ID cards in 2010. They will offer the functionality of e-passports with biometric data usable for verifying the identity of the cardholder and, optionally, functionality for the secure remote identification via the internet (called eID function) and the creation of qualified electronic signatures. The biometric data (face image and optionally two fingerprints) are only allowed to be used for government applications.
- The Malaysian MyKad card is a multi-purpose smart card which includes biometrics and can be used as an identification card, driver's license, medical card and can be used for the transfer of electronic funds. It contains fingerprint template data.
- The UK's Identity Card/NIR will cover a wide range of citizens and includes two forms of biometric; facial recognition and fingerprint data. Full roll out is expected to take place in 2017.

Finally, certain eID cards contain no biometric functionality such as the Swedish and Finnish cards.

Other

Healthcare

Case studies for biometrics in healthcare exist for amending staff identification documents by biometrics, patent identification systems, or biometrics for dispensation of drugs for special categories of patients.

Staff identification with biometrics is used by several health care providers in the US. Biometrics are (aside passwords, PINs, phone call-backs, or tokens) among the technical security services for entity authentication to comply with the Health Insurance Portability and Accountability Act (HIPAA). Similarly, in Denmark the Copenhagen Hospital Corporation entered into a research and testing exercise in 2009 on using biometrics to access electronic health records. Fingerprints (with match on card and on-card scanners), iris scan, and voice recognition are investigated.

If sufficiently secure, biometric on-card comparison could be used on health professional cards (HPCs) being introduced for instance in Germany. For more comfortable cardholder authentication prior to the creation of electronic signatures, biometric methods could be used in addition to the PIN authentication, which would be carried out once before creating multiple electronic signatures. However, given the lack of sufficient security certificates for biometric products, as yet there are no plans to deploy biometric methods on the German HPCs.

Patient identification systems using biometrics are introduced both for reducing fraud or for increasing patient safety. An early example of biometrics in healthcare is the Texas Medicaid ID card to inter alia avoid phantom billing and card sharing. Pilots with smartcards and fingerprints

started in 2004. For patient identification in hospitals, one of the several examples is palmprint scanning used at El Camino Hospital, California, during patient admission since end of 2009.

If sufficiently secure, biometric on-card comparison could also be used instead of PIN authentication on electronic health cards (eHCs) that are being introduced for instance in Germany. If PINs, such as the PINs on eHCs, are used only infrequently, there is a high risk that they get forgotten or stored at insecure places. However, as yet, there are no plans to deploy biometric methods on the eHCs.

An example for using biometrics in drug dispensation is the Australasian MethaDose programme that has been launched in 2002. Iris scan is used at automated dosing systems at dispensing point to identify heroin addicts in a methadone programme.

Private Sector applications

The current established and accepted view is that transportation market will be the second largest sector of users of electronic IDs next to telecommunications. However, biometric recognition is often not needed in mass transportation. As the financial sector continues to suffer from the rise of phishing and identity related attacks, it may be expected that they may increasingly turn to biometric data as a route to help manage the risks from such types of attack.

Access control

The use of biometric smart cards for access control is possibly the nearest broadly adopted application.

Access control to computers using biometrics is becoming commodity; think of laptops increasingly being equipped with fingerprint sensors or additional software that uses the laptop camera for or a mobile phone camera for face recognition. We therefore give case studies for physical access control in public areas.

Physical access control involves the use of biometrics to control access to specific physical locations and may encompass such technologies as facial, fingerprint or palm based biometrics in a variety of applications, in combination with other security technologies (such as keys or PIN codes). Such technologies may be deployed in certain high risk areas, for example, control centres, military installations or areas where sensitive information or assets are located (e.g. data centres). For example the US Personal Identity Verification system permits access to US federal government systems and facilities via the use of biometric data. Biometrics are also deployed for access control in critical infrastructures (e.g. the nuclear industry) and high availability data centres which may contain or transact large volumes of sensitive personal data including financial transaction data, healthcare information and so on.

Pilots of biometric access control at big sports events using smart cards and fingerprints have been carried out by German Bundesdruckerei at the world football championship 2006 (about 2000 users to access a public viewing place in Berlin) and at the Torino Winter Olympics 2006

(5000 authorised persons at the “German House”). An anonymous access control project of not granting access has been launched at the Bad Homburg gambling casino in 2006. Pathological gamblers can enrol themselves to a voluntary ban and face recognition assists in alert supervisory staff in case the client enters the gambling rooms. Similar projects exist in nine further casinos in Germany.

Another sensitive application is in respect of access control for some schools in the UK. Fingerprint biometry has been deployed in around 100 schools to replace swipe cards for access to library services, cashless catering and registration.

Transportation

There are a number of smart card implementations in intelligent transportation systems (e.g. France, the United Kingdom, the United States, Asia and Australia).

Finance & banking

A variety of biometric technologies are being considered for use in the finance and banking sector, including hand geometry, voice, fingerprint, signatures and vein pattern.

Current usage models in the finance and banking sector include transaction security (securing client transactions remotely or onsite), network security (security of infrastructure), access control and applicant checks (background checks to protect against internal fraud and illegal transactions).

The use of biometric technology in ATM installations was demonstrated already in 1996 in South Africa. In that installation a Diebold ATM has used fingerprints. Meanwhile, several banks have ATM or other similar installations that use biometrics. Examples include Western Bank in Puerto Rico (which uses fingerprint biometrics) Harrah’s Casino Las Vegas and First Financial which uses it for Kiosk - credit union application. In the UK, NCR Self Service Strategic Solutions reported on various research conducted regarding biometric systems at ATM interfaces in 2003 which indicated that although a number of barriers were identified (e.g. the fact that such technology was unnecessary, difficulty believing that the technology will work, privacy and health concerns), these were overcome the more users interacted with the technology and identified its utility (Coventry 2003).

If sufficiently secure, biometric on-card comparison could be used in electronic-cash payment procedures without on-line connection instead of, or in addition to, PIN authentication on credit and debit cards. In Japan for instance vein-pattern on-card comparison is used in addition to PIN authentication on bank cards to allow unlimited disposition (in case of biometric non-matches, the credit is limited).



An example of an e-purse application is the Malaysian MyKad. It is national ID and multi-application card (driver's licence, health information, toll payment, etc.) The Malaysian Electronic Payment System (MEPS) e-purse application can be used.

Telecommunications

Current state of the art for the use of biometrics in telecommunications applications is focused around the use of voice to authenticate users. However, the Polish telecommunications operator NASK has teamed with Telefonica to develop a suite of biometric enabled technologies for network access (such as BiomVPN). This is a complete solution for biometric authentication for Virtual Private Networks (VPNs) and has been tested between Poland and Spain.

Bibliography

Ailisto, H., Lindholm, M Mäkelä. S-M, Vildjiounaite, E. (2004) Unobtrusive User Identification with Light Biometrics NordiCHI '04,

Beynon-Davies, P; (2009) The UK National Identity Card International Conference on Information Systems (ICIS)

Bhargav-Spantzel, A.; Squicciarini, A. and Bertino E. (2006) Privacy Preserving Multi-Factor Authentication with Biometrics DIM'06

Bundesministerium des Innern; Press Release; (2009) The electronic ID card

Bekkers, V. J. J. M &. Duivenboden, Hein van and Thaens, M. (eds) (2006) Information and communication technology and public innovation: assessing the ICT-driven modernization of public administration

Cave, J. (2005) Economic Aspects of Biometrics; prepared for the Institute of Prospective Technological Studies, DG JRC

Coventry, L, Antonella De Angeli A. and Johnson G. (2003) Usability and Biometric Verification at the ATM Interface Usability of Large Scale Public Systems CHI 03 Vol 5 No. 1

Elliott J.; (2005) Biometrics Roadmap for Police Applications; BT Technology Journal Vol. 23 No. 4 October

European Commission Staff Working Document (2009) *Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large scale IT systems in the area of freedom, security and justice* SEC(2009) 837

European Commission (2009) Study on eID Interoperability for PEGS, Analysis & assessment report; ENTR/05/58-SECURITY, SC N°13.

Hartmann D. and Körting, S. (2009) Risk Assessment Report Security Issues in Cross-border Electronic Authentication; European Network Information Security Agency

Hendry, M.; (2001) Smart card security and applications (2nd ed) Artech House, Inc

IPTS (2005) Biometrics at the frontiers; prepared for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE)

Lips, M. Taylor, J. And Organ, J (2006) Identity Management as Public Innovation; Looking beyond ID cards and authentication systems;. IOS Press

Jafar M. H. and Hassanien, A.A.E.; (2003) An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory Advanced Modelling and Optimization, Vol. 5, No. 2

Jones, A. L., Antón, A. I, Earp, J. B., (2006) Towards Understanding User Perceptions of Authentication Technologies WPES'07

Khan, M. B. M.; Khan M.K. Zhang; Dian Ye, Z. (2005) Implementing Biometric Security in Intelligent Transportation Systems

Lyon, D.; (2002) Surveillance as social sorting: privacy, risk and automated discrimination; Routledge;

Michaud C. and Krawczyk S.; (2005) Biometrics in the banking industry; CSE 891

Naumann I. (ed); (2009) Privacy and Security Risks when Authenticating on the Internet with European eID Cards; European Network Information Security Agency (ENISA)

Naumann, I. And Hogben, G.; (2009) Privacy Features of European eID Card Specifications; European Network Information Security Agency (ENISA)

Oxford Internet Institute et.al. 2007) Breaking Barriers to eGovernment, MODINIS contract 29172, Deliverable 2, prepared for European Commission Directorate General for Information Society and Media

Oostveen, A-M & van den Besselaar, P.; (2004) From Small Scale to Large Scale User Participation: A Case Study of Participatory Design in E-government Systems Proceedings Participatory Design Conference

Ranga G., Flowerday G. (2007) Identity and Access Management for the Distribution of Social Grants in South Africa SAICSIT 2007

Ronald Leenes, R., Priem, B. van de Wiel, C. and Owczynik, K.; (2009) Report on Legal interoperability; Towards pan-European recognition of electronic IDs (eIDs) STORK Deliverable D 2.2

Scott, M., Acton, T. and Hughes, M. (2005) An assessment of biometric identities as a standard for e-government services International Journal of Services and Standards ; Vol 1, No. 3

Tomko, G.J., Soutar, C. and Schmidt, G.J. (1996) Fingerprint controlled public key cryptographic system. U.S. Patent 5541994

Zhang, D. (2002) Biometric solutions for authentication in an e-world (The Springer International Series in Engineering and Computer Science) Springer