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 D4.2

Exploring the business case for biometrics in remote electronic services

Final version

Classification: PU

Dissemination level: All

Date of submission: 29th April 2011

Table of Contents

Preface

This is the second 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 further progression of the key discussions held between the Working Group and other WG members, since the last deliverable, on whether a viable business case exists for the use of biometry in electronic identity, specifically in the context of remote services.

Input for this deliverable came from the following sources:

- Online discussions and numerous telephone conference calls between the WG members between December 2010 and March 2011.
- An online LinkedIn discussion on 'Why Biometrics Fail'.
- A WG conference call held on 27th January 2011.
- Input from representatives from other WGs, namely WG 2 (Emerging applications) and WG 7 (Ethical, legal and social dimensions)
- A Workshop hosted by RAND Europe in Brussels on 7th March 2011 where members of the Working Group and associated WGs 2 and 7 were invited. The purpose of this workshop was to explore three main questions:
    - Why is there currently no clear business case for use of biometry in remote applications? What barriers; gaps or challenges exist to the determination of this business case?
    - Should the discussion be more re-orientated toward a consideration of the positive aspects of biometrics and an understanding from the deployment perspective about how biometrics can add value rather than merely as a way to minimise or mitigate risk?
    - What are the disruptive implications of biometrics in remote eID? How would we determine what signals would indicate the emergent disruptive implications of these technologies?
- Subsequent input submitted via email from the members of Working Group 4 of the BEST Network between 01 March 2011 and 15 April 2011.
- Summary desk research carried out by RAND Europe and the Graz University of Technology between January and April 2011.

The purpose of this document is to build upon the work of D4.1 of this Working Group and the activities of Working Group 2, Emerging Applications, by illustrating possible business cases for biometrics in eID. To this end, representatives from WG 4 attended a meeting of WG 2 on 28th January 2011. In addition, other representatives of WG 4 were present at a workshop hosted by the Chair of WG 7 on 23rd March 2011.

The rest of the document is structured in the following way. First an introduction is given. This sets the scene and links to the predecessor deliverable D4.1 "State of Art: Biometrics in eID

systems". A section on models for remote biometric use follows. Following the notion that has been introduced in D4.1, we distinguish between who controls the biometric data and the biometric sensor – the service provider or the user. Positive and negative aspects of introducing biometrics are developed from both a user's perspective and a service provider's perspective. This assists in understanding the business cases biometrics can bring.

We continue with a section on "*Why do biometrics fail?*" – this meant to partly summarise provocative discussions launched by the Working Group in the light of roughly a decade after biometrics getting a significant attention in border control or travel documents, its use in eServices is relatively rare. At these discussions, the following contributing factors were identified: security and privacy concerns, perceptions of biometrics, unclear business rationale, convergence between public and private uses, standardisation, communication & registration and operational considerations.

Finally, we describe a few selected use cases out of the rare examples where biometrics actually has been employed in remote eServices before concluding with a short summation and illustrative ideas for discussion as to possible routes to overcome these challenges.

Annexes document the networking that has been carried out including:

- A Record of the LinkedIn online discussion following the question: "Why do biometrics fail?"
- Minutes of the two main WG meetings held on 27th January and 7th March 2011.

Introduction

This second Deliverable D4.2: *The Business Case for Biometrics in remote electronic services* is a review of the business case for biometrics, with a focus on different types of remote electronic services. Discussions between the members of the BEST Network and respective Working Groups (WG) have indicated that so far, outside very narrow application areas already covered in other working groups (such as access control and travel documents), there is a limited business case for the use of biometrics in remote services.

The conclusion of this WG, reported in this Deliverable are that there are a range of types of reason leading to the widespread practical failure of biometrics: which could be more or less prevalent depending on the specific case and deployment. These include security and privacy concerns, the question of perception and the also un(clear) business case as to what problem biometrics should be solving, as well as standardisation and operational issues.

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) to support eID[1] 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 infra-structure)
- Uptake and social acceptability
- Cost benefit analysis (linked to the issue over thresholds; see below).

As services move from provision of just information to one-way transactional to two-way trans-actions 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. This is where biometrics, as a way to highly accurately and robustly authenticate and identify individuals, becomes important.

However, there are other related 'non-identity' uses of biometrics.[2] These include the use of soft biometrics in sensor and monitoring applications. These include tele-health, military and hazardous applications and other areas where it is useful to monitor different types of biometric parameters without them necessarily being used for identification.

[1] 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.

[2] e.g. see Deliverable D2.1 of Working Group 2 of the BEST Network: Survey of existing (non-governmental applications) and emerging biometric applications (1st September 2010)

There are also many potential uses that either bypass the Internet or develop in Internet and non-Internet phases. Non-Internet uses of course include Automatic Teller Machines (ATM), but also reasonably include other 'private network' uses within enterprises, between collaborating institutions, via non-Internet fixed or mobile connections (with or without end-to-end assignment of responsibility), etc. Other examples include vehicle borne measurement systems that keep track of 50-some aspects of the drivers' physical and cognitive state. Given the external stakeholders interested in who drives a given car for example, law enforcement, of course, but also insurance, working time directive monitors, employers, manufacturers and the legitimate owners of possibly stolen vehicles, it is not hard to envisage car-based biometric uses. The 'remote' aspect comes via the need to contact/interact with those third party stakeholders (e.g. via unlicensed very high frequency spectrum, as used at present to report on the car's condition and to signal emergency services when airbags deploy).

There are a number of issues that must be considered prior to the deployment of biometrics as a support for remote electronic services. 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,
- 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 market for biometrics

Market research firms suggest growth for biometrics. Gartner Group indicated that biometrics was relatively high on the list of priorities for those responsible for company decision-makers.[3] According to recent data, the market is expected to grow from $4.2 billion in 2010 to $11.2

[3] Fenn, J.; Gartner Group: *Prepare for Emerging Disruptive Technologies through 2020* (visited April 20, 2011) available at:
http://www.gartner.com/it/content/1282200/1282214/february_24_prepare_for_disruptive_emerging_tech_jfenn.pdf

billion in 2015.[4] Automated Fingerprint Identification Systems (AFIS) is by far and away the largest component of this, growing from $1.4 billion in 2010 to $3.3 billion in 2015. Technologies taking advantage of other biometrics (iris, vein and facial recognition) are expected to witness marginally larger Compound Annual Growth Rates (CAGR) of 27.5% for iris, 25.4% for vein and 24.2% for facial vis-à-vis 19% CAGR for fingerprinting technologies. Of course this market data covers biometrics for identification only, and the somewhat more nascent market for 'softer' biometrics is more difficult to determine (being bound up in estimations for tele-health or remote monitoring applications.

[4] Markets and Markets *Biometric Technologies Market*
http://www.marketsandmarkets.com/PressReleases/biometric-technologies-market.asp (visited April 6, 2011)

Models of remote usage

It is possible to determine four models in distinguishing ownership/control of biometric data and sensors in a matrix for classification.[5] The purpose is to try to see if there is use in defining what could be inside and outside the remit of understanding potential business cases for the use of biometrics in eID. Our working assumption (given the scope of other WGs) is that Example 1 is within scope and all the others are either being covered by other WGs or are untenable.

Electronic Identity (eIDs) - use of remote services over the Internet (e.g. Internet banking; replenishing travel smart card; management of medical records etc)

e-Services - biometrics enabled ATMs, Points of Sale but also remote tele-monitoring (e.g. for healthcare applications)

The difference is in the physical presence and the extent of control or assurance that the service provider can exercise over the biometric sensor. Architectural or security characteristics common and pertinent for one scenario may not be the case in the other. Furthermore, it may be that e-services have more in common with the other WG (e.g. WG1: RT programme). Indeed the difference is in respect of what the authentication opens up: money instead of access.

The use of physical presence when considering how to lay out the business case for biometrics is in and of itself a complex characteristic to understand: whilst in the case of an ATM transaction the end user has to interact physically with the infrastructure, there might not be any supervision (except for a CCTV camera used to detect shoulder surfing) but this might not be sufficient to address fraudulent fingerprints. This brings the discussion back to the question of how trust is built up between the service provider and the user; which is via remote authentication (like a PIN code or smartcard). Here it may be possible to consider the concept of 'mutual biometrics' since more and more valuable interactions requiring a high degree of trust cannot be decomposed into binary and asymmetric user provider pairs, where the data subject provides a biometric to a system or faceless infrastructure. Therefore from the perspective of trust, the ATM (or even the mobile with emergent micropayments and the increasingly popular 'app' market) could be considered a 'remote' application.

A different approach is to consider the physical presence necessary at time of enrolment. Are there applications or scenarios we might imagine where an individual could remotely enrol in biometric infrastructure over the internet, then using it in a physical / remote manner? For example, if a biometric is based on facial recognition, then an individual could submit a digital photograph (assuming to certain standards) online (through an appropriately secured communication channel validated by a digital signature). Does there have to always be some kind of physical presence with biometrics?[6]

---

[5] E.g. see the INCITS "Study Report on Biometrics in E-Authentication" http://standards.incits.org/apps/group_public/download.php/24528/m1070185rev.pdf (visited 30 May 2011)

[6] For example, the validation of physical existence (as opposed to presence) is currently handled 'remotely' via notaries; this provides a clear example of "biometrics to secure biometrics."

Further examples of architecture alternatives relating to '"Store on Server/Match on Server" and "Store on Token/Match on Token" are described in the INCTIS Study Report on Biometrics in e-Authentication.

If the ATM example is within scope then there are plenty of other examples we might use in similar scenarios (e.g. citizen registration at the local town hall).

Example 1 - The case of eID as proposed in Deliverable D4.1 Fig. 1.

eID	**Biometric**	
Ownership	data	sensor
Service Provider		
User	X	X

Example 2 – the use of biometrics to perform transactions at an Automatic Teller Machine ("ATM" – 'cashpoint'). In the example below this may not be considered a remote business case as the user has to physically touch/interact with the equipment of the service equipment. This also applies to the remote tele-monitoring application. It may therefore mean that it is possible / necessary to develop a finer definition of 'remote' in order to avoid such distinctions?

Example 2 – ATM usage

ATM	**Biometric**	
Ownership	data	sensor
Service Provider	X	X
User		

In Example 3, if the user has (government) certified biometrics on an Electronic Passport (ePP) and the airport owns the sensors for a registered traveller service then the matrix would look like Table 3.

Example 3 – electronic Passport

ePPs	**Biometric**	
Ownership	data	sensor
Service Provider		X
User	X	

Finally, Example 4, may prove to be a untenable or unsustainable model for authentication or identity due to security concerns. If the user controls the sensor the service provider has little

assurance that the user has not defrauded the system or presented a counterfeit input to the sensor.

Example 4 – security model

	Biometric	
Ownership	data	sensor
Service Provider	X	
User		X

Understanding the business case for biometrics

In this short section we present an economic overview of why the firm, when interacting with its customer, would wish to use biometrics. This summary is meant to spur debate whether we are looking at the utility ('business case') of eID from the wrong way around – namely from the perspective of whether biometrics in support of eID is used to control costs/reduce liabilities (or to create positive externalities). These tables illustrating the business case are relevant only for the discussion on the private sector uses of biometrics and additionally, only in the context of biometrics as supporting identity and authentication functions.

With biometrics

		User	**Provider**
Positives	**Externalities**	• Reduced chances of identity being stolen • Reduced chance of error (false positives and false negatives) • Increased accountability (esp. if 2-way) • Greater ability to place trust appropriately (because more is not always better) • Greater levels of service (made accessible by providers' reduced IA costs) • Ease of access to secure information, transactions possibilities, contacts, etc. • SSO economies of effort • Enhanced usefulness of users' electronic identities • Access to safer 'biometrically secured' interactive and immersive environments	• Less fraud • Greater confidence • Reduced regulatory impact • Less costs in dealing with security breaches • Reduction / avoidance of regulatory liabilities (fines) • Increased revenues (existing customers do more business for those that view security as important) • Enhanced reputation • Ability to 'fit the identification/authenticatio n level to the use (and thus to user Willingness To Pay).

	Costs	• Reduced costs and hassle of claiming identity or access	• Reduced maintenance and support costs (e.g. frequent password resets)
Negatives	**Externalities**	• Loss of trust caused by perception of surveillance and intrusion into privacy • Increased digital divide (enrolment easiest for certain age bracket)	• Decreased revenue (existing customers not participating in market) • Stagnant or decreasing market share (potential new customers deterred due to use of biometrics)
	Costs	• Cost of visiting enrolment facility • Time of enrolling • Difficulty • Fear / impact on civil liberties	• Deployment costs • Costs of enrolment facilities • Costs of dealing with false positives (counterfeit being let through as legit) • Cost of dealing with false negatives (legitimate being denied)

Without biometrics

		User	**Provider**
Positives	**Externalities**	• Convenience (mobility / device independence) • Many tools	• Increased market share (potential new customers not put off by onerous authentication mechanisms) • Increased revenues (existing customers do more business)
	Costs	• No investment in sensors	• Lower Capex/Opex for authentication
Negatives	**Externalities**	• Increased risk of identity theft	• Increasing identity theft and cyber-attacks on less secure authentication • Loss of customer trust with incidents
	Costs	• Remembering multiple password & PINs and authentication tokens	• Costs of security measures (distributing two factor systems, PIN, smartcard)

Why *do* biometrics fail?

In this section we present the results of expert discussion into answering the question: "why biometrics fail?", focusing on the aspects of their function as a more secure form of authentication and identification, as evidence that the use of biometrics to perform such functions ought to be considered as part of a clearer cost benefit analysis (appreciating all the different types of biometric deployment for remote services) and secondly that value may lie in broadening public understanding of the business case of biometrics from these narrow identity related functions, to encompass roles better suited for softer biometrics.

Any discussion concerning attempting to arrive at an understanding of why biometrics fail, should necessarily begin from a general characterisation of the characteristics and possible architectures as well as their security considerations: since one of the primary functions of biometrics is to act as a more secure form of authentication and identification.

The core elements of these architectures can be split up into:

- Server: the database holding the biometric information (in the case of *1 to n* matching) and performing other important applications (e.g. enrolment). The server may also run a credential manager service. The server would contain the biometric engine. In verification mode, the server stores the biometric template, upon which the presented biometric is tested against when someone wishes to claim an identity.
- Client: the software that interacts with the server to take inputs from different types of biometric token
- Device: the hardware used to acquire the biometric – for example, a fingerprint scanner, retinal reader or CCD camera.
- Token: the device which may be used to store the biometric template – examples include smart-cards and USB tokens.

Each of these core elements may be arranged according to different architectures, depending on whether large or small biometrics are envisaged in the resulting system. There may also be centralised or decentralised approaches depending on where the verification or identification tasks are intended to be performed.

The storage of biometrics (and the computation of authentication or identification) is undertaken at the server. At this level (and in a large scale *1 to n* application) the database of biometric templates represents a major attractive target for possible hackers. Therefore, confidentiality is of prime concern. Furthermore further standard information security requirements exist: for example integrity of the platform upon which the server is being run. As it will be outlined in the following, in the recent years, several approaches have been proposed to protect the biometric template both from a procedural and a technological point of view.

Matching is undertaken at the client level. Interoperability concerns along with compromise of software integrity (e.g. through poor coding or software bugs that may compromise the ability of the client to perform its function) may be considered as the main security issues associated at this level.

At the device level, matching is undertaken. Issues relevant at the device level include failure to capture (FTC) and failure to enrol (FTE). FTC rate only is relevant if the device incorporates automatic capture functionality. FTC is the percentage of times the device fails to capture a sample: when the quality of the biometric (for example, a faint fingerprint) is below a set threshold. FTE concerns the percentage of times the user cannot enrol in the recognition system which typically occur when poor quality templates are rejected during enrolment (because the database contains only high quality templates). Since a degree of human interaction occurs at this point, the associated human factors issues may also present security concerns.

At the token level, storage of biometric data may be performed. On the token, confidentiality again becomes a concern, particularly in respect to smart cards which may include RFID technology and be subject to eavesdropping. There are other concerns too, which reflect the fact that such tokens may become attractive targets for physical theft. Measures to provide for confidentiality must therefore also be deployed at the token layer.

Although these aspects are particularly pertinent to the consideration of biometrics for identity, some of these issues (e.g. security concerns at the server and client) level may also apply to non-identity related uses of biometrics.

Following the discussion above on some of the security aspects of each element going to make up the overall system architecture, let us now briefly consider some of the larger concerns regarding the geometry of biometric infrastructures.

From the end user perspective, decentralised biometrics appear to have more public favour, since the implications of surveillance appear to be less (as the biometric information is stored 'closer' to the individual). However, the applications are narrower than large $1 > n$ architectures and have attendant security issues (e.g. in respect of achieving a more favourable cost/benefit security trade-off). On the other hand, with centralised biometrics it may be possible to obtain a clearer cost benefit as they have larger domains of application and the security investment required may be easier to understand (since it revolves more around confidentiality provisions on the centralised data store).

Furthermore, there may be other relevant architectural types of centralised and decentralisation: for example, administratively (at the national level) a decentralised system may be set up within different communes or municipalities, or there may be decentralised systems operating between schools, healthcare and social security systems, that pass data on the result of biometric checking (effectively a binary yes/no answer to a request for authentication) without the need to collect massive single databases with all the attendant other security risks. This is in contrast to a centralised national system of a large public registry based identity system where biometric templates are kept centrally.

We now turn our attention to a derived list of considerations of why biometrics fail: security and privacy concerns, perceptions of biometrics, unclear business rationale, convergence between public and private uses, standardisation, communication & registration and operational considerations.

Security and privacy concerns

Regardless of the architecture of the employed biometric system, in order to enable "biometrics not to fail", that is, in other words, to have a successful deployment of a biometric system in real life, security and privacy issues are critical issue for user acceptance. This applies whether we are considering biometric data used for identity and authentication or softer biometrics used for other purposes.

Within the biometric framework, the term “security” refers to making the data available for authorised users and protected from non-authorised users, whereas the term “privacy” is used to limit the use of shared biometrics, to the original purpose determined for collecting the data. As is well known, most biometric characteristics (face images, voice, iris images, fingerprints, ECG, gait, etc.) are exposed and therefore not secret, and technology is available to covertly capture with different degrees of difficulty. This could lead to identity theft. Moreover, raw biometrics cannot be revoked, cancelled, or reissued if compromised, since they are user's intrinsic characteristics and they are in limited number. On the other hand privacy means something more than keeping biometric data secret.

Privacy and security have been treated in the recent past, as requirements hindering or in direct opposition to each other, which imply that when more emphasis is given to security, less emphasis is accorded to privacy.[7] However a different perspective is beginning to be taken by redesigning security technologies in such a way that both enhances system security and minimises the invasion of privacy. This is achieved both using technological and procedural solutions.

The very fundamental question we need to answer is whether biometrics is privacy-invasive or privacy-protective. Within this respect, both the perception by the user of the potential threats to privacy and the real risks to privacy must be carefully considered when designing a biometric system.[8]

Specifically in the following, the main characteristics of biometrics which must be addressed in order to avoid "their failure" are described below:

- Biometrics may be collected or shared without the specific user's permission, adequate knowledge, or without specific purpose.
- Biometrics, which has been collected for some specific purposes, can be later used for another unintended or unauthorised purpose sometimes based on emergent innovation and functionality identified by the service provider. This is known as ``function creep", and it can have dramatic consequence since it can lead to the loss of public trust in a given system.
- Biometrics can be used for purposes other than the officially declared purpose or biometrics can be misused to generate extra information.
- Biometrics can be copied or removed from the user and used for secondary purposes.

[7] This is sometimes referred to using the language of balance of two competing interests being weighed against each other: that is to say more of one must mean less of the other

[8] Prabhakar, S. et al. *Biometric Recognition: Security and Privacy Concerns* IEEE Security and Privacy (2003)

- Biometrics use can violate the "principle of proportionality'', which states that biometric data may only be used if adequate, relevant and not excessive with respect to the system's goal. If this principle is violated, the users may feel that the benefit coming from revealing their biometrics is much less than what they get in exchange. As an example, it is very likely that a retinal scan authentication system used at a Point-of-Sale makes the user uncomfortable, whereas the use of dynamic signature biometrics is more accepted by users.
- Biometrics can be used to reveal gender and ethnicity. Medical conditions can be deduced by comparing biometrics acquired at the time of the enrolment and biometrics acquired later for authentication. Moreover, biometrics can give directly information on health conditions. As a consequence, biometrics can be used to profile people according to their health status. Whilst this may be beneficial in some respects, due care should also be placed on the use of this data in associated applications (e.g. as indicated by the specific requirements placed on Special Categories of Data in the European legal framework governing privacy and personal data protection or the US Health Insurance Portability and Accountability Act.
- Biometrics can be used to pinpoint or track individuals. Since biometric data are considered unique, they have the potential to locate and track people physically as they try to access facilities or their biometric traits are recorded by some surveillance system. Associating in an un-authorised way people's biometrics to their identifiers, such as name, address, passport number, may result in other attendant risks, since it is then possible to access, gather and compare a wide range of information starting from a single biometric trait. Moreover the use of biometrics as a universal identifier could facilitate and make easier the tracking of users across different databases. This could lead to the perception of covert surveillance, profiling, and social control.
- Biometric use can be associated by individuals just to forensic purposes. Therefore the use of biometric traits, such as fingerprints, which are associated, for historical reasons, to criminal investigations and forensic activities, can have a low acceptability rate in respect of other applications (since society or the individual may consciously or unconsciously link fingerprints with criminalisation leading to the connation of biometrics with cultures of suspicion)
- Biometrics can be improperly stored and/or transmitted. Such poor management would expose biometrics as being more vulnerable. Moreover biometrics may also be exposed to administrator or operator abuses, since they could misuse their privileges for accessing a biometric database (much as in the same way now, insider attacks may compromise stores of personally held data).

A deeper exploration of the legal, social and ethical implications of these issues may be found in Deliverable 7.1 of the BEST Network.[9]

To answer the need to deploy privacy protective systems, guidelines have to be followed. The International Biometric Group in the framework of the IBG BioPrivacy Initiative [10] has suggested

[9] BEST Network Working Group 7: Legal, Social and Ethical Implications of biometric Technologies, Deliverable D7.1 (April 2010)
[10] IBG BioPrivacy Initiative (IBG BioPrivacy LLC) available at: http://www.bioprivacy.org (visited 20th April 2011)

some best practices for privacy aware deployment in line with the OECD Fair Information Principles.[11] Specifically, four categories of best practices have been defined, namely:

- Scope and capabilities,
- Data protection,
- User control of personal data,
- Disclosure, auditing, accountability, oversight.

These best practices have been designed in order to answer the needs relating to a broad range of biometric based applications. We summarise these below:

Scope and Capabilities

The scope of the system should not be expanded to implement more functionalities than the original envisaged. If some scope modifications occur, full documentation should be provided as well as the possibility for the user to revoke enrolment, if applicable. Biometric data should not be used as a universal unique identifier since it would facilitate cross matching among databases, thus introducing serious threats to privacy. Biometric information should be stored for the stated purposes and for the necessary amount of time. When the system is no longer in use or the user is not enrolled anymore in the system, the data should be destroyed or rendered useless. The potential system attributes that threaten privacy should be carefully analysed, since very few systems clearly appear to be privacy invasive, whereas they may have hidden capabilities which could impact on privacy. Biometrics which can be easily recognized by human inspection, such as face, fingerprint images, or voice signals, should be cancelled after having generated the biometric template. Moreover, the storage of non-biometric information such as the subject's name, social security number and similar should be limited to the minimum possible and a direct link among these data and biometric data should not exist.

Data Protection

Biometric data must be protected throughout the different stages of a biometric based authentication system (sensors, liveness detection, quality checker, feature-generator, matcher, and decision modules). It is worth pointing out that post-match decisions should also be protected since, if the channel is not secured, the final decision could be overridden. Data management, such as access to the biometric database, should be limited to a restricted and well defined number of operators in such a way as to limit potential misuse of the stored data. Furthermore other controls should be performed. Information such as user name, address, etc. should be stored separately either physically or logically accordingly to the application, from the biometric data.

User Control of Personal Data

If applicable the user should have the possibility to revoke enrolment, to make their data inaccessible, to destroy their biometric data, or to correct, update and view the information stored together with the biometric data. Some extent of anonymity could be guaranteed if compliant with the application.

[11] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data available at: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (visited 20th April 2011)

Disclosure, Auditing, Accountability, Oversight

Whenever possible, the enrolment should be overt. In fact, informed consent is a basic requirement for privacy preserving applications. Disclosure should be provided whenever biometric data are used without explicit user consent like in camera based surveillance applications. The purpose of a biometric based authentication system should be fully disclosed. If the system use changes from its original extent, users must be informed and they must have the possibility to withdraw their enrolment if they do not agree to a broader use of their biometric information. A full disclosure should be given to indicate whether enrolment is mandatory or optional. The operators of biometric systems have to be considered as responsible for the system's use and it should be clear who is responsible for system operation and the processing and control of the biometric data. Moreover, since internal misuse can occur, third party auditing should be implemented, and users should have access to the data resulting from the auditing. Individuals should be informed about the different stages involved in the whole process, about the biometrics used in the system, the non biometric information they are asked to provide, and the matching results. Users should be informed about the protection used to secure biometric information. Whenever applicable, alternative procedures should be put in place to involve people when they are unable or unwilling to participate in the biometric based system.

Of course different biometric applications can have a different impact on privacy. The applications associated with authentication and identification processes which link biometric data to rights, or access or other dependent functions performed by other organisations are particularly worthy of note. Overt biometric applications are less privacy-invasive than covert ones. Mandatory biometric based authentication systems bear more privacy risks than those which are optional. Privacy is considered to be more at risk when physiological data are used since they are more stable in time and allow a higher accuracy than behavioural biometrics. If the biometric based authentication system is used in the verification mode, less privacy concerns are implied than those involved in a system operating in the identification mode. This is due to the fact that in the identification mode, $1 > n$ comparisons are performed through a database search. This action of searching introduces more privacy threats than the same actions performed when $1 > 1$ comparison is undertaken as in the verification mode. Privacy risks increase when biometric data are stored for an unlimited amount of time. In fact, if the system deployment is indefinite in time, threats such as function creep may become all the more pressing. If the database is violated, biometric traits related to several users are compromised. Biometric systems where identifiable biometrics, such as faces, voice patterns, and so on, are retained, are more prone to privacy risks than those which store templates. Moreover, if the biometric data are stored in a centralised database, serious privacy concerns arise since data are stored out of user's control, whereas if the user can maintain a greater degree of ownership of his or her biometric data, the privacy risk may be reduced since the user can exercise greater control over the collection, usage, etc. of such information. The use of biometrics can have secondary purposes when both governmental institutions and private companies are involved. In different societies, one or the other can be perceived more threatening to privacy. Also the role of the individual in the biometric system, employee, citizen or individual, customer, impacts on the privacy assessment.

Approaches to secure biometric templates

Together with procedural approaches, in recent years, technological solutions, known as privacy enhancing techniques (PETs), have been proposed to secure biometric templates.[12] In fact among the possible threats regarding users' privacy and security which have to be considered when designing a biometrics-based recognition system, the unauthorised acquisition of the stored biometric data is probably the most dangerous one. Specifically, a properly defined PET system should satisfy the following requirements:

- Security: it should be impossible or computationally unfeasible to obtain the original biometric template from the transformed one;
- Revocability: it should be possible to revoke a compromised template and issue a new one based on the same biometric data;
- Diversity: each template generated from a biometrics should not match others previously generated from the same data;
- Performance: the recognition performance of the protected system, in terms of False Rejection Rate (FRR) or False Acceptance Rate (FAR), should not degrade significantly with respect to an unprotected system.

A possible classification of the possible approaches able to create secure and renewable biometrics has been recently proposed. [13] Specifically, two macro-categories, referred to as biometric cryptosystem and feature transformation approaches, have been introduced. Hybrid approaches, which exploit the advantages of both biometric cryptosystems and feature transformation approaches, have also been proposed.

Biometric cryptosystems typically use binary keys to secure the biometric templates, and during the process some public information, usually referred to as helper data, is created. The approaches belonging to this category are extremely important to integrate biometrics into existing cryptographic protocols, which require a secret binary key to perform user recognition. Biometric cryptosystems can be further divided into key generation and key binding systems.

In key generation approaches both the helper data and the cryptographic key are directly generated from the biometric template. In this way, the security of the key can be guaranteed by means of hash functions, which can also be employed to provide the requested non-invertibility[14] property to protect the original biometrics. The main issues of this approach regard the stability of the cryptographic key, which affect the recognition performances, and the possibility of generating multiple keys from the same data.

In key binding systems random binary keys are employed in conjunction with the biometrics to generate the helper data. Typically, these approaches are able to manage the intra-user variations in biometric characteristics through the use of error correcting codes. However, it is generally not possible to use matchers specifically designed for the considered biometrics, thus

[12] London Economics *Study on the economic benefits of privacy - enhancing technologies (PETs)* Final Report July 2010

[13] A.K. Jain, K. Nandakumar, A. Nagar, *Biometric template security*, EURASIP Journal on Advances in Signal Processing, 2008.

[14] That is to say, the property that by reversing the steps used to create the template, an attacker could compromise the transformed data

reducing the system matching accuracy. Feature transformation approaches modify the original templates according to a key-dependent transform. It is possible to distinguish two sub-categories: salting and non-invertible transform approaches. A salting method employs invertible transforms: the security of the templates thus relies in the secure storage of the transformation keys.

On the other hand, when non-invertible transforms are considered, it is computationally hard to recover the original data from the transformed templates, even if the transformation keys are known to the attacker. Feature transformation approaches typically produce transformed templates which remain in the same feature space of the original ones: it is therefore possible to employ, in the recognition stage, the matchers originally designed for the considered biometrics. Following this approach, recognition performances close to those of an unprotected approach can be therefore achieved.

Perceptions of biometrics

Aside from security and privacy concerns, perception of these technologies is often at the core of this debate. Some of these concerns are not unique to biometrics but are inherent to technology more generally. However, as described below, concerns regarding the perception of biometrics appear to be most acute regarding their use in support of identity systems: as has been shown, this is a narrow and focused use of biometrics, but not the only application.

The discussion very often is about "here is the technology; what shall we do with it?", rather than "this is the problem and this is how the technology should solve it". That implies that we are often driven by solution-thinking (“bottom up”) rather than moving to higher ground in order to understand the real problem first and than analysing your way down to the appropriate solution (a top down approach).

Especially with complex large scale identity systems, where different users have different problems to solve, this easily leads to unclear and even contradictary requirements. If this is combined with a lack of knowledge about the technology and the practical challenges which go along with their deployment, different stakeholders will each have their own expectations of what the technology should bring to solve their particular problem. With biometrics, the step towards central storage is easily taken, because there is an easy suggestion that that would serve a broad range of needs. However, the larger impact of central biometric databases is not always understood and in many cases creates more problems than it aims to solve.

Technology discussions are always very interesting and are often characterised by a high degree of vigour by stimulating the imagination of what the technology could do from a potential business perspective. Nonetheless, there are other strategic issues which need to be taken into consideration to avoid failure in the deployment.

(Un)clear business need

The business need must clearly and honestly answer the question: “What is the reason of applying biometrics: adding security or making the process more convenient?” For defining the

business case it can not be both: one needs to serve the other. In general, there may be three different types of business need:

- Security – to reduce fraud or the illegitimate access to services
- Convenience – for the end user (to speed up a certain process or reduce their costs: e.g. in having to remember numerous password combinations or to always carry around a two factor authentication system to login to their e-banking application)
- Efficiency – for the provider or agent deploying the technology, to make certain processes more efficient

There are a host of other ancilllary factors relating to establishing clarity of the business need, namely:

- Security: risks (e.g. spoofing, misue) and liabilities
- Society: the proliferation of all biometric modalities for intelligence services and subsequent spillover of adoption into the commercial world
- Technology: lack of standardisation/interoperability/independent testing
- Requirements for security are significantly different than for convenience. This affects the business case all the way down. In practice these can be confused, even within a single case.
- The intrinsic failure rates of biometrics depend on many factors. It is difficult to manage these in such a way that liabilities can be valued and ensured.

Convergence between public and private uses

Within the public security and law enforcement domain there is a movement towards the use of all kind of biometric data, particularly for intelligence services. Whilst the requirements of security services can drive industrial innovation in this area there is less of a case for commercial services. The industrial implications are that providers offering types of biometric technology deployed for public security and law enforcement uses may turn to the commercial services as new markets. However, this will lead to greater risk, since cracking those systems will become more rewarding. Biometric Encryption (BE) may have potential to solve this conundrum between the usefulness of biometrics for intelligence and commercial (private) services and to what extent this might reduce the instances of spoofing and misuse. Furthermore, the important cultural differences between interpretations of privacy and data protection and the respective roles, responsibility and behaviour of the public and private sector in different European countries is an important consdieration. That means that some type of cultural assessment is required when looking at the success or failure of certain biometric applications. That implies that a succesful implementation in country A might fail in country B. Multi modality could be helpful in solving these issues at least partly, but not completely. Finally, this question of convergence (and the second order effects of innovation and take-up in the public sector, for the private sector) has implications on questions regarding how fixed some paramters are (and how comfortable people and operators are with them). Parameters or criteria for success that might apply and be robustly tested and validated in one sphere might not be relevant in another. How much spoofing and FRR do we accept? How are we measuring the True Accept and True Reject Rates as part of a risk assessment and what do we consider to be acceptable?

Standardisation

Vein pattern technology and BE remain protected by patents and trade secrets, making it difficult to discern how these technologies work perhaps leading to a perception of them as black boxes. For large scale (payment) schemes with a national or international scope this might not be the most desirable situation. We know what happened with iris recognition in the early 2000s. Greater transparency on the performances of these technologies as well as interoperability between different providers will be required. All this needs to be tested and certified by independent laboratories.[15]

Is the problem about communication or registration?

Another mistake which is very often causing failures of biometric deployments is the ability to see if a problem should be solved by improving communication or registration. When we speak about communication we mean people and organizations who exchange information in order to meet business or organisational objectives. Intervening in this domain is always difficult. It can be hard (possibly even 'policy suicide') to announce better co-operation and communication because that implies that people have failed in working together. So it is easier to introduce a technical solution, e.g. another register of data. However, this does not solve the problem of bad communication. A lack of communication and co-operation will lead to central systems which are not up to date and therefore unreliable. If communication between or within organisations trying to acheive some economic or social objective does not take place, the data will stay in the system, not being able to reach the requested party on time and in the right place. Perhaps a different way to overcome is via focusing on decentralised systems, using reliable data from existing sources, where data accuracy is crucial for their operation. Such biometric infrastructures can be more efficient and effective, as the starting point of such systems is co-operation and exchange. The easy technical orientated solution that a centralised system can solve all problems might lead to less co-operation between partners and to unreliable data arriving too late and in the wrong place.

Operational considerations relating to biometrics in practice

There are several reasons why even the most technically robust state-of-the art biometric systems may result in less than optimal service delivery. These include:

- Legacy system problems (incorporation of new technology to existing infrastructures)
- Training of personnel problems
- Insufficient manpower to enrol biometrics properly and to process the document in which the biometric is to be embedded
- Biometric entropy (degradation of biometrics over time)
- Local administrative practices (nuances of local administration)
- Legal issues (e.g. administrative burden of compliance with different legal frameworks regarding personal data, sensitive personal data or personally identifiable information)
- Cost to the administration or organisation acquiring them (high capital costs)
- Cost to the individual required to enrol a biometric as a condition of being able to access a service (eg passport); and the ancillary secondary costs of getting to an enrolment

[15] see http://www.biotestingeurope.eu

point, including travel, time-off-work, actual cost of document, cost of picking up document after processing

- Secondary social and economic impact on aggravating the social and digital divide (biometrics are most easily enrolled from able-bodied 18-45 year olds)

Use cases for biometrics in remote electronic services

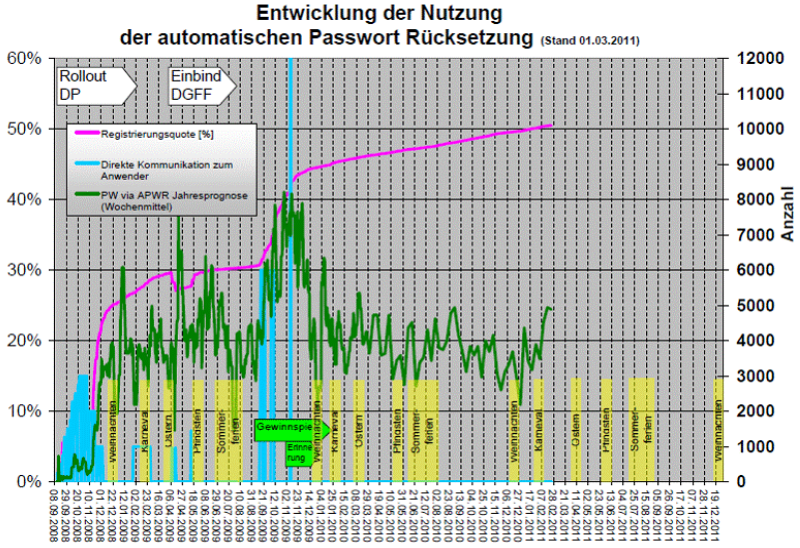
Although we argue that using biometrics remotely is rare which might be caused by limited business cases, there still are a few. In this section we present a few examples where introducing of biometrics lead to measurable gains. This has been done to give a few examples where use cases may be transposed to eServices.

We also focus our case studies on illustrative examples of the some of the benefits of biometrics described in the section 'why biometrics fail', namely: organisational efficiency, clear rationale, user convenience and security (and a clearly defined trade-off between the two.

Case study #1 – Password reset (Deutsche Post)

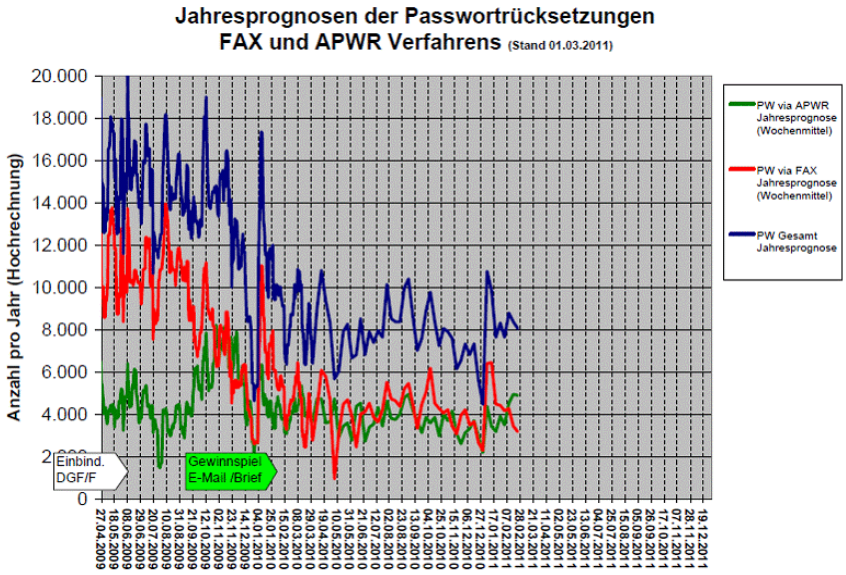
This first example concerns biometrics in a real remote use environment with Deutsche Post's IT service desk. Deutsche Post has about 40,500 PC users. The service desk handles about 1,500 password resets a month with peak rates around 4,000. As one can imagine, in a distributed environment of that size, some means of authentication is needed. This used to be a fax process where the average password reset duration was 4.5 hours – a period where Deutsche Post staff could not access their PC.

At the end of 2008 the fax system was complemented by a automated password reset "APWR" system using voice recognition that employees could enroll onto. The following figure[16] shows how the enrolment developed over time in percent (in pink, steadily growing line and the number of password resets using the biometric system as a green line). Note some password reset peaks after holiday periods (indicated by yellow rectangles). Significant increases in enrolments at the end of 2009 originate from a raffle to increase take-up.



[16] The information has kindly been provided by Waldemar Kammerloch, Deutsche Post from his presentation: "*Sprachbasierte Services mittels Stimmerkennung Deutsche Post DHL*" at the 32nd meeting of TeleTrusT AG Biometrie, Darmstadt, September 8th, 2010

Meanwhile the number of password resets using the biometric APWR system roughly equals the password resets using the fax system (which one might also guess from the 50 % enrolment indicated in the figure above). The figure below gives the prospects of password resets over time: the green line indicates the voice recognition system APWR; the red line indicates fax password resets and finally the blue line is the total. Note, that the green line (APWR) gradually draws nearer the red line (fax) and reaches it about end of 2009 – where the APWR usage crossed 40 % according to the figure above (a green arrow indicates the raffle that lead to a significant enrolment increase).



The interesting aspect in terms of a biometrics business case however is not restricted to the take up by users alone. It is the raw productivity gain for employees and service desk cost reductions. With the introduction of the voice recognition APWR system:

- the average password reset duration went down from 4.5 hours to 20 minutes
- service desks costs were reduced by 16 percent

Case study #2 –Throwaway biometric – boarding card (SAS Airlines)

The second use case that has been chosen is using fingerprints. In 2008 Scandinavian Airlines (SAS) launched a biometric system (PreciseBioFlight) for unattended self-service kiosks i.e., within the airport facilities thus providing some control over the environment. This was driven by the new requirements imposed by EU initiatives requiring that airline companies verify that a domestic passenger checking in baggage also boards the aircraft. At the time of the introduction of these regulatory requirements, SAS was establishing an efficient self-service system and assessed that the benefits would have been undermined by the imposition of these new requirements. Therefore, the airline was confronted with how to fulfil their obligations without impeding the speed and efficiency benefits already predicated on the self-service system being developed.

The purpose of the system is to ensure that the person checking in luggage is the person that actually boards the plane. The passenger checks-in as usual at the self-service kiosk. When handing in the luggage, the passenger can register his finger and thus logically link themselves to the luggage. When boarding the passenger presents the same finger to a sensor at the gate. This provides evidence that the passenger and their luggage is on board the plane. The system replaces manual ID card checks at the gate.

Security procedures require a degree of verification at the gate before boarding the aircraft, to verify that: every passenger has a picture ID that compares to the person and the name on the picture ID is the same as that on the boarding card.

In this way, indirectly, the person is matched against the boarding card. When the passengers receive their boarding pass upon check-in, they can optionally enrol their fingerprint biometric and the system stores the biometric template only for the time period between check-in and boarding. The traditional fall back option is also present if the passenger doesn't want to enrol their biometrics.

The automatic gate consists of a boarding card reader (a bar code) and a fingerprint sensor which compares the fingerprint to that of the enrolment and if there is a match opens the gate.

According to the airline, the success of the system seems to be determined by:

- It is simple and perhaps more importantly simple to understand for passengers
- Enrolment is very fast
- Convenience is evident in "just walking through the gate" as opposed to "standing in line"
- there is also a savings/convenience benefit for the airline operators
- The privacy issues are minimised since the biometric is stored only for a single purpose and very short time period

The system seems to have good take up. Helena Tranaeus Bonnedal, Manager, Airport Self Service for SAS noted that: "the fact that 98 percent of the passengers choose to verify themselves with fingerprints on our domestic flights in Sweden proves that the system works and that the passengers are willing to use it." [17]

Case study #3 Voice authentication for pension plan (Philippine Government Service Insurance System)

[17] PreciseBiometrics *PreciseBiometrics, SAS' Passengers Travel Smart with Fingerprints*, http://www.precisebiometrics.com/filearchive/3/3032/SAS_eng_casestudy_lr.pdf (visited 20th April 2011)

This case concerns the deployment of a voice authentication technology to serve 1.5million people in the Philippines.[18] In 2008 the Philippine government undertook a massive programme to use voice biometrics for authentication of user identities. This was deployed within GSIS, which is the primary pension programme for about 1.5million government retirees in the Philippines. GSIS was moving ahead with the deployment of systems extending the reach of its services (given the unique geography of the Philippines with its many islands) across a network of ATMs, wireless kiosks, in order to simplify and control the process of applying for loans and distributing benefits.

GSIS originally deployed e-Cards to offer new financial services in addition to the transfer of pensions in 2004: this was then supplemented with the deployment of e-Cards Plus: using a smart card and near field contactless based technology. The cards supported access to services through wireless kiosks called GWAP which included fingerprint based biometric authentication. The GSIS managers recognised that biometrics permitted them to derive a high degree of confidence when identifying members and authenticating their identity in respect of specific front line transactions (loan applications or the transfer of insurance payments).

Voice technology (using PerSay's Vocal Password) was deployed to allow remote authentication: thereby removing the need for pensioners holding the e-card plus to even visit a GWAPS kiosk. Such a requirement was particularly noteworthy given the aforementioned geography of the Philippines (an archipelago of some 7,0000 islands). Although travel to a GWAP site would thus require a great deal of inconvenience, the fact that wireless carriers in the region have deployed a relatively mature network across many of the islands, means that it made sense to find some way that GSIS members would be less inconvenienced.

Users are still required to have an e-Card in their possession – so at some time they must have physically appeared in a bank branch or GSIS office to enrol in a face to face setting. Enrolment involves the member saying the digits 0 through to 9 three times. GSIS is also exploring the possibilities of remote enrolment via Skype – perhaps more concerning from a security standpoint as the member is required to show the GSIS employee undertaking enrolment two permitted forms of identification (and it seems that confirming documents via Skype might be open to presenting forged identity documents). Once enrolment is complete (however it is accomplished) the member can then call the GSIS toll-free number and are prompted to enter a eleven digit GSIS membership number. After this they are asked to say the nine digits three times to authenticate their transaction and a randomly selected further four digits to 'sign' the transaction.

[18] Miller, D.; Voice Biometrics Case Study: Government Service Insurance System http://www.opusresearch.net/wordpress/pdfreports/adv_gsis_112508.pdf 2008 - (OPUS Research) visited 30th May 2011

Case study #4 – Remote tele-monitoring for healthcare (Clalit Health Services)

In this case study we consider the remote use of 'soft biometrics' such as heart rate patterns or Vital Sign Parameters (VSPs). The use of biometric data that is less 'identifiable' than other forms (e.g. fingerprints) may constitute a promising avenue for illustrating the positive aspects of biometrics and helping to inform the public debate and counter the prevailing arguments regarding the negativity of biometrics and its connotations with privacy invasions by the public and private sectors.[19] Having said that, there are also opportunities to consider such 'soft' biometrics as being equally as pertinent for the purposes of identification and authentication: S.A. Israel et al show that electrocardiograph (ECG) readings of individuals when in low or high stress environments may be sufficiently distinct to permit identification.[20]

To illustrate these possibilities, we present the final case regarding the use of telemedicine in Israel, where the Gertner Institute and Clalit Health Services operated a large telemonitoring project for sufferers of Chronic Obstructive Pulmonary Disease (COPD). COPD is a lung disease that robs the sufferers of breath and according to the World Health Organisation is the fourth largest leading cause of death worldwide.

A telemedicine solution from Medic4all was deployed by Clalit Health Services, the largest Health Maintenance Organisation (HMO) in Israel, to help COPD sufferers to maintain their personal routine, whilst being medically monitored by Clalit's healthcare personnel from a remote location. The technology and service is aimed at treatment and supervision of the patients health condition in their own homes, using a dedicated national monitoring centre.

Source: Medic4all[21]

The devices automatically and wirelessly transmit measurements to two medical monitoring centres, where the data is automatically received into the patients Electronic Medical Record (EMR). An operator is alerted if the measurements are outside the patients personally predetermined range.

[19] E.g. see workshop on Security and Privacy in Implantable Medical Devices, EPFL Lausanne Switzerland 01 April 2011 http://si.epfl.ch/SPIMD

[20] S. A. Israel, et al. *ECG to identify individuals* Pattern Recognition, 38(1):133{142, May 2004.

[21] Medic4all Telemedicine 2008 available at http://en.medic4all.it/medic4all-telemedicine/ (accessed 21 April 2010)

The drivers for the deployment of this example of biometric technology are increase in quality of life, reduction of healthcare costs and increase of quantity of services provided.

Conclusions

As we have seen, establishing and identifying business models for biometrics, particularly in the online environment where establishing identity is an increasingly essential pre-requisite, is fraught with uncertainty and questions. Furthermore, there are a number of factors that have been identified as to why biometrics fail, including issues around security and privacy (the extent to which deployment of biometrics meets legal and regulatory norms regarding privacy and personal data protection and whether security procedures are sufficient to cope with the highly accurate identity information represented by biometrics).

With these factors in mind, one might consider whether biometrics are an example of a disruptive innovation – that is to say, an innovation which initially is outperformed by its competitors but 'out of the blue' suddenly becomes incredibly popular.

Characteristics of disruptive innovation (according to Clayton Christensen) are, as described in the Innovators Dilemma:

1. It initially costs more than the item it is initially seen as replacing, for example, the initial 5 inch hard disk drives cost more on a per megabyte basis than the 8 inch drives they were seen as replacing.
2. It doesn't perform as well as similar previous devices; doing the same task, the new innovation is not quite as good as the existing innovation.
3. Customers and market research did not show a great desire for the new innovation or device, e.g. 8 inch disk drive customers had little desire for a smaller form factor device with a higher price.
4. There was confusion about exactly what one would do with it, or how it fits into the existing market.
5. The initial market was small.

In matching these questions from the perspective of biometrics, the overall answer may be a considered: '*possibly*'. Biometrics are currently more expensive than other security mechanisms which are regarded as a better cost/benefit trade off (for example, user name and passwords or two factor authentication). Although the discussion on error rates varies for each biometric[22] biometrics are seen as relatively costly to deploy compared to other validation techniques. Clearly, as has been shown, the initial market for biometrics remains relatively small, being mostly concerned with public sector deployments of identity and authentication solutions. Furthermore, there is a great deal of confusion of what can be done with biometrics, since it appears to be a more complex and (from a user perspective) uncomfortable form of measure for providing for security. There is also little demand for this technology at the present – as it is a security orientated technology demand is not yet driven by innovative uses but rather as a cost avoidance mechanism. All these factors combine to indicate that generally biometrics may be regarded as a form of disruptive innovation. In the context of any discussion about business drivers, this leads to the obvious question, what are the indicators which may suggest an

[22] it is generally accepted that fingerprint or iris recognition are two of the most reliable types of biometric

approaching tipping point where this form of innovation will start to behave in a disruptive fashion? If the initial use-case or deployment involves:

- Low start-up investment
- Good performance for the demands of the initial application
- Transparent balance of the interests of all parties
- Appropriate requirements for skill, co-investment, etc.
- Short payback periods (speedy Return On Investment)
- Good provision for subsequent (and even user-led) innovation, etc.

Then a business case can be expected to develop based on e.g.

- New and higher-value uses (the increased potential for assurance offered by biometrics permits providers to offer higher value transactions)
- User-led innovation
- Altered business models e.g. in relation to who looks after data, what degree of liability attaches to breaches, whether biometrics is used for privacy-enhancing or –invasive purposes, whether it is expected to be used as PET or Privacy Invasive Technology (PITs), whether it is used to enhance or replace trust, etc.
- Proliferation of new, high-value service models based on the availability, acceptance and understanding of biometrics (e.g. 'protected spaces' for Massively Multi-player Online Games or collaborative production, enhanced partnership platforms, personal tunnels to the cloud, etc.).

Moving the debate forward

At a broader level, in order to try to overcome these challenges, it may be possible to identify a number of potentially interesting high level considerations:

- Firstly, softer or 'weaker' biometrics may prove an interesting way forward to re-shape the debate about this kind of technology away from a focus on narrow identity orientated uses of this technology. The debate about biometrics should be articulated outside the scope of such identity and authentication applications. Will the business case be proven by applications (such as have been indicated) using softer or weaker biometrics? These are certainly clearer and as we have seen with the case study on remote tele-monitoring, have clearer rationales.[23]
- The positive convenience aspects of this technology should be promoted more clearly, specifically in respect of the user side.
- Understanding the business case more clearly is not a problem of the technology, but rather the fact that there remains little public robust actuarial data on security cost benefits which would inform better decision-making. For example, the cyber-insurance market has not approached the consideration of linking the use of this kind of technology to premiums, which may serve to stimulate take-up.
- Focusing upon better co-ordination and admitting the failures of inter and intra-organisational communication and co-ordination (particularly in biometric applications

[23] e.g. see Ailisto H. et. al. *Soft biometrics—combining body weight and fat measurements with fingerprint biometrics* Pattern Recognition Letters 27 (2006) 325–334

in the public sphere such as citizen registration systems) may help to stave off the desire for commissioning yet another large technology project involving a centralised database with all its attendant vulnerabilities and risks, not to mention the potential for it to undermine trust between individuals and governments.

- It may be worth exploring the value of mutual biometrics as a way to help build trust between the data subject and the entity or agency requesting such data. This might help to provide a perception of a human face on these exchanges. In turn this could help to overcome the fear of technology and feelings of powerlessness when confronted by faceless systems and establish a mutual platform of trusted interaction between the data subject's personal space and technology enabled infrastructure.

Annexes

Annex A: Agenda and Terms of reference for workshop 7th March 2011

WG 4: Workshop on Barriers and Incentives on the business case for eID in remote services

RAND Europe – 7th March 2011 – 14.00 -17.00h - 37, Square de Meeus Brussels Belgium
WG 4 of the BEST Network in its Deliverable 4.1 developed the argument that a clear business case for eID in remote services is difficult to articulate. Given the lack of deployed applications outside border control, physical access control and travel documents, the second deliverable from this Working Group will seek to gather the views of experts from across the BEST Network to deliberate on the rationale for the use of biometrics in eID and explore the reasons why there is this absence of a business case.
The central purpose of the day will be to answer the following questions:

- Why is there currently no clear business case for use of biometry in remote applications? What barriers; gaps or challenges exist to the determination of this business case?
- Should the discussion be more re-orientated toward a consideration of the positive aspects of biometrics and an understanding from the deployment perspective about how biometrics can add value rather than merely as a way to minimise or mitigate risk?
- What are the disruptive implications of biometrics in remote eID? How would we determine what signals would indicate the emergent disruptive implications of these technologies?

Format
The Afternoon will be an open moderated discussion and brainstorming/whiteboarding session.
Networking
The afternoon workshop is expected to principally involve members of WG4 and WG2 (Emergent Applications). Other BEST WG Members are also very welcome.

1. Summary

The purpose of the workshop is to prepare the second WP4 deliverable D4.2 "The Business case for biometrics in eID and electronic services", **due date March 31st**. As of the Description of Work (DoW), this deliverable shall be:

- *defining scenario's where biometrics are a key enabling technology to increase security, convenience and/or efficiency*
- *turn the added value of using biometric for e-services into a business scenario*

The scene has been set by a preparatory conference call[24], using linked-in discussions[25], and a background paper[26]. Special gratitude is to be given to Ancitel – Bud P. Bruegger and John Forrester contributed definitions and discussion on eID[27]. Based on these, the workshop shall further elaborate on the eID business cases.

Agenda

14:00 – 14:30	Welcome and initial thoughts on deliverable structure
14:30 – 14:40	Opening Conf-Call, - Roll-Call - Agreement on Workshop Objectives
14:40 – 15:00	Short position statements by each participant - Purpose of D4.2 - What shall be in / left out?
15:00 – 15:15	Relation to D2.2 "*Inventory of factors for failure and success*" - Synergies, overlaps, and where is D4.2 complementary
15:15 – 15:30	Re-Cap of input material - see Annex 1 – Annex 3
15:30 – 16:00	Detailled discussion on D4.2 content - Development of an annotated ToC
16:00 – 16:15	Distribution of work - who, what, by when - closing of conf-call
16:30 – 17:00	Preparation a minutes and to-do list; Wrap Up

WG 4 – Teleconference meeting 27/01/2011 – Minutes of teleconference

Present were:

- Max Snijder (EBF) – BEST Network Co-ordinator
- Cathy Donnelly (EBF) – Best Network Co-ordinator
- Herbert Leitold (TU Graz) – Chair WG 4

[24] 27 January 2011, see minutes in Annex 1
[25] „*Why do biometrics fail*" at http://www.linkedin.com/groups?gid=3429037 ; see Annex 2
[26] See Annex 3
[27] Paper „eID -- The Concepts" by Bud P. Bruegger and John Forrester

- Neil Robinson (RAND Europe) – Co-Chair WG 4
- Bruno Benato (SAGEM)
- Jon Forrester (Ancitel)
- Bud P. Bruegger (Consultant for Anictel)

Points raised:

The Co-Chair thanked Bud P. Bruegger and John Forrester of Ancitel for stepping in to present the WG on the 8th Dec 2010 review meeting at the COM and also for preparing a paper following this meeting outlining some basic concepts of eID which may prove useful material for further WG deliberations.

It was agreed that some flexibility in respect of the scope of the activities of this WG exists (the message coming out of the review meeting 8th Dec). A clear outcome from the first deliverable D4.1 was that there was no clear business case and outside of travel and physical access control (covered by other working groups) for the use of biometrics in remote services. There is little specific / concrete examples of clearly deployed services. The formal objective of the next deliverable was 'the Business Case for biometrics in eID' but what is becoming clear is that outside of the specific remit of cases covered by other working groups, there is limited business case. Therefore perhaps the objective of this group should be to summarise what we view as business cases; whether they do exist; and if not (compared to other WGs e.g. MRTD why not? What is missing or absent that prevents this business case from being developed and brought to maturity).

Furthermore, in order to stimulate debate and get expert input in the next deliverable (due absolute latest 31/03/2011) it was proposed to use two mechanisms:

- A workshop which RAND Europe could host at its offices in Brussels in mid-late February – proposed date w/c 14 or 21 February) at which members of this WG, WG 2 and WG 7 would be invited.
- The stimulation of moderated discussion on the LinkedIn Community via a poll or Delphi type research exercise covering a number of questions designed to spark controversy and debate. The key other WG's with which this would interact are WG 2 (Emergent Applications) and WG 7 (Ethical and Legal Aspects). To this end it was agreed that we post a poll / question on LinkedIn consisting of three questions:
    - Why are there no business cases? What is preventing broader take up of biometrics in eID?
    - Are we looking in the right direction? Is it appropriate that we should only consider the benefits and costs of biometry in eID as a way to reduce costs and companies avoid liability of ID theft rather than positive benefits?
    - What disruptive innovations / challenges might be perceived by experts as to the landscape in the near-medium term (e.g. how technology might not be used for the purposes in which it was originally envisaged – for example growth in popularity of SMS).

Actions:

- WG Chair/co-chair to attend meeting of WG 2 on 28/01/2011 and discuss possibility of attendance at workshop in Feb (already discharged TU Graz 27/01)
- WG Chair/co-chair to post message on LinkedIn Board to explore three questions
- RAND Europe to prepare draft flyer and circulate to audience for attendance at workshop 21st Feb at Sq de Meeus Brussels.
- RAND Europe to prepare notes from meeting (discharged 31/01)
- Bud P. Bruegger to forward on some emails that had gone missing to Chair and Co-chair along with matrix of user/vs service provider ownership of token/infrastructure to help illustrate conceptualisation between remote and physical distinction(already discharged 27/01)

Best Network WG 4 – LinkedIn Discussions – "Why do biometrics fail?"

The following question has been raised at the LinkedIn WP4 Group

Why do biometrics fail?

We investigated business cases for using biometrics for remote access via the Internet. Empty sheets is where we started with – and basically ended up! We would like to hear your opinions on why this might be the case. WG 4 will also hold a workshop in Brussels on the 7th March 2011 14.00-17.00 hosted by RAND Europe to discuss the above.

Three comments have been received

Bud P. Bruegger

I would think that the main reason is security: If the verifier is not in control of the sensor, then the link to the person is lost. The biometric data may not be a biometric characteristics of a person measured by some sensor, but just some replayed digital message, or otherwise created data. Instead of a "something you are" it would become a "something you know"--and biometrics are not actual secrets...

Herbert Leitold

Assuming that security in the remote access scenario isn't increased by introducing biometrics, can there be other benefits for a service provider? Can convenience for the user (not typing in passwords) be a reason to invest? I guess not, given that sensors in COTS products (e.g., fingerprint sensors in PCs) usually come with password safe software hat already give the user experience. To the contrary the user might feel it privacy invasive if biometrics are asked by the SP.

Reinhard Posch

Biometrics fail? Rather we fail understanding biometrics. Biometrics like eID and the identity management area are assumed and accepted to be a major step forward. Indeed they are but not for everything - by overloaded expectations everything fails. It needs to build a broad and clear understanding of the fields where these technologies are applicable and contribute - the

tools their capabilities and their limits and impacts. Unless we yield this understanding biometrics will be overloaded with fears and expectations technically and commercially that can never be met. It would be time for the "green book of biometrics" but it has to be done by the right institution giving the broad acceptance it deserves. As long as we stay in a wild mix of research development and application biometrics has to fail.

BEST-NW Conference call WG 4 (Biometrics and eID); Brussels; 7th March 2011

Participants:

- Alex Bazin (Fujitsu)
- Bruno Benteo (Morpho)
- Bud Bruegger (Consultant for Anictel)
- Cathy Donelly (EBF)
- John Forrester (Ancitel)
- Juliet Lodge, University of Leeds
- Max Snijder (EBF)
- Herbert Leitold (TU Graz & WG 4 Co-chair)
- Jonathan Cave (RAND Europe)
- Neil Robinson (RAND Europe WG 4 Co-chair)

Objectives of the meeting

The objectives of the meeting were to gather input on a set question: why is it difficult to find a suitable business case for the use of biometrics in electronic identification systems? Participants were asked to explore what they saw as the barriers and challenges preventing further interest in the use of biometrics in online remote services.

Drivers for use of biometrics generally (in a private sector setting)

- Repudiation
- Digital identity protection
- Liability control
- Content (e.g. age restricted content)
- Match on card solution
- As a way to determine where information is coming from – that it is not lost, stolen
- DRM – cost realisation
- Fraud reduction

Scope of WG 4

What do we mean with use of the term 'eID'? are we restricting ourselves to eID across a number of public and private applications? The scope of our WG is markedly different from that of others (e.g. WG2 and other WGs on passports and MRTDs). Given WG 2.2 Deliverable has covered private sector drivers comprehensively, should we focus on public sector? For example, there are deployed examples of biometry being used in ATM applications in Brazil and also in Japan. In the context of service delivery, there are applications of voice recognition in call centres (and other 'soft ID' where there is a 'looser' requirement to identify someone. However, in understanding this concept of boundaries and scope, we need to be clear that in some respects this could get blurred.

The fuzziness of some public and private sector boundaries regarding service delivery raises into question interesting issues of legal liability. Are the private sector agents of the government; are they simply 'delivering a service?' or are they actually doing something entirely different (in the

case of Japanese norms for private sector involvement which goes beyond the simple 'delivery' of public services.

- Specific modes of usage (or use cases) might include those from the mobile domain
- Specific sectoral applications of interest might include health services. For instance, VoiceVault was used for the signing of e-Prescriptions and Palm Secure was being used for Patient Registration and EHR in a HIPAA environment. Telemedicine would also come under the 'healthcare' domain.

Government backed identity

In the area of the delivery of public services there is interest in postal services; tax submission; movement and helping to reduce bureaucratic burdens on individuals (e.g. filing in the same form over and over again to the public authorities). The public service use case is important because there is a character of the variable of the extent of choice in the system that the biometric will support, plus whether the biometric is used as a platform or facilitator of a highly accurate identifier (could be referred to as a 'Gold Standard'). In this case, the discussion perhaps is whether it is necessary for a biometric to be a constituent part of such a 'Gold Standard' source of identity. The question falling out of this is whether a single biometric is enough given it would be used to open up access to a whole lot of other services. However the barrier to this is that there is not even a single way to assign ID numbers (nationally or between Member States) which would be a necessary precondition for a business case to reduce the cost of e-services by making a single eID available to a wide range of services.

Another alternative is for government to be a provider of identity directly and try and leverage a private market. For this to happen it would be necessary to connect biometrics to a national identification system (with all the attendant weaknesses indicated above).

Expectations are having simplified to an application level.

Expectations are currently that biometrics are needed for big national projects. What about 'throw-away' biometrics e.g. SAS checkin ticket, used to validate duty free purchases after passing through checkin. This sort of application could provide a baseline for other uses 1>1 matching. Keep it small with a principle of being scalable. Another aspect would be that there would be the creation of localised databases which could be viewed as both a privacy/IT strength and weakness.

1>1 Matching allows for the automation of processes – replacing manual tasks with an automated system

1>n service allows the provider to ensure that any one person only gets one document – able to spot a document in another identity.

Identifying and characterising the benefits

Need to ask the question to whom are biometrics and services of benefit? Biometrics are a way to build trust and derive and apply a certain set of behaviours on the basis that everyone around you in that specific context has been authenticated to the same level. Its a mechanism to build trust and a discussion of this should not be omitted. Furthermore, co-operation of the biometric subjects is necessary and the rationale for the deployment has to be convincing.

How do the benefits characterise themselves? Profit? Is the profit always passed onto the citizen?

The business drivers are normally characterised in three ways:

- Citizen: convenience
- Organisational benefits – automating transactions
- Security benefit – lower cost of fraud or helping to defray the cost of regulatory compliance

Expectations of biometrics

Have to disconnect biometrics on a national level from application and change expectations about why this technology is needed? What about govt offering ID uniqueness validation services – role of biometrics in the chain? Biometrics just used for de-duplication and the biometric stays uncompromised and is only used to see whether the ID is unique. To what extent would this compete with existing ID providers such as Tivoli, U-Secure and SSO/Facebook?

There is a total misperception about the use of biometrics. It may represent an ability to derive a ground truth of someone's identity but is often seen as a panacea which weakens ability of policy-makers to address real root cause of problems.

Practical case study given of Disneyland where the biometric is just used to see if the ticket was valid.

Perhaps what is required is a list of questions that organisations must ask themselves before deploying biometrics? A set of non-binding guidelines or a checklist (not imposed by governments, however) which help them answer the questions whether biometrics are really a suitable solution for a proposed identification/authentication problem.

Biometrics: a solution in search of a problem?

There are a number of multifactor questions regarding why an organisation would choose to deploy biometrics in order to fashion a security operational space. Also the CBA is extremely difficult for security since you have to undertake predictive risk assessment on the efficacy of different security measures. ICAO have done this though (confirm) and developed a theoretical business case for which types of ID theft biometrics can help address.

Voice biometrics

The use of voice authentication is perhaps one growth area. Voice has applicability for a host of reasons including helping to manage passwords (the business case is reducing or eliminating time spent by frontline support staff in helping users to restore passwords).

How to determine what or how a business case should be developed?

Going forward for D4.2

- Need to focus on exact use cases
- Provide a clear logical argument
- Recognise benefits of 1>n in national and local systems – and not create overly strict guidance
- How would we use this (question of guidance or checklists for org to follow) – maybe best to consider whether we ought to have it in?
- Is there a relationship between Anonymity and biometry the exploration of which would add value here?

- Use cases on physical remoteness and consider the viability (or otherwise) of business cases
- Max and JC to follow up on possible involvement in further research via biometrics special interest group.