



## **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 2<sup>nd</sup> 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 D2.2**

### **Inventory of factors for failure and success**

Final Version  
Dissemination level: PU  
Date of submission: 24 February 2011

## Table of contents

1. Summary.....	3
2. Introduction.....	4
2.1 Scope.....	4
2.2 Structure of the document.....	4
3. Methodology.....	5
3.1 General Methodology.....	5
3.2 Limits of the deliverable.....	5
4. Theoretical framework.....	6
5. Technological dimension.....	8
5.1 Supplier reliability versus compatibility.....	8
5.2 Technology Adoption and Standardization.....	9
5.3 Compatibility between technological components.....	10
5.4 Usability of the biometric components and ergonomic design.....	10
5.5 Use procedure.....	11
5.6 Technology adaptation.....	11
5.7 Technology Safety and Privacy assurance.....	12
6. Business consumer dimension.....	13
7. User interaction dimension.....	14
8. The importance of negotiation and clear business drivers.....	15
9. Main teachings.....	20
10. Conclusions.....	21
11. References.....	24

## 1. Summary

The present deliverable provides a further analysis on the success or failure of the biometric commercial applications explored in the previous deliverable D2.1 'Survey of existing (non-governmental applications) and emerging ones'. The analysis establishes a framework for the success and failure around specific factors determined from the information available. The factors found relevant to each commercial application, are then grouped into three main dimensions, which help provide a structured and comprehensive view of the result of the analysis of each factor, its influence and relationship with other factors. The analysis confirms that success or failure of each biometric application does not solely depend on one factor, but a combination of them.

For the complete analysis of success or failure of each application, not only those related to the application itself (i.e. characteristics, application, technical specifications, etc.) have been explored, but also those related to the parties involved in their supply, implementation, and use. The final sections of the present deliverable aim to provide an understanding of the results of the analysis and the relevance of each dimension here defined.

## **2. Introduction**

The research goal is to provide a state-of-the-art analysis of biometric commercial applications in Europe and explain the main drivers for the success or the failure of such applications. In other words, the motivation lies in the need of understanding the interests and opportunities for main stakeholders to adopt and use biometrics solutions in retail. The objective remains to be explanatory, for instance, validate the opportunities for such biometrics solutions in retail (viewed globally, banking and retail) and the focus of interest in them. It is mainly based on qualitative research and theoretical analysis since there is no real opportunity to test adoption potential on a large scale, i.e. near end users.

### **2.1 *Scope***

In this deliverable, we analyse the data collected in the previous deliverable (D2.1), survey the existing and emerging commercial biometric applications (banking and commercial services/retail). The technical specifications of the applications will not be explained in order to increase readability.

### **2.2 *Structure of the document***

The document structure is divided in two main parts. First, we the methodology is defined, and second the main results of the analysis are presented.

## 3. Methodology

The aim of this work is to define and validate a list of factors that will help outline the success or failure frame of a biometric commercial application. The methodology used is relevant to the on-going explanatory research here followed.

### 3.1 *General Methodology*

Based on the data collected in the D2.1 deliverable and the BIOSIG Conference held in Darmstadt<sup>1</sup> in September 2010, a content analysis is conducted. Then, to explain the success and failure of biometric commercial applications outlined in D2.1 deliverable, a set of factors is listed.

### 3.2 *Limits of the deliverable*

There are several limits to this deliverable. The census performed on biometric commercial applications relies on a rather small sample which reduces the capacity to generalize the results here shown. Added to the size of the sample, the high confidentiality level of current projects increases the difficulty to obtain detailed information.

The complementary information gathered at the BIOSIG Conference sessions in September 2010 helps complete the analysis of the different projects. Nevertheless, more information is still required; information difficult to obtain because of changes in the organizations that have left key contacts out of reach, the sensitivity of such information that is not disclosed to the public, or simply because there is no information available related to the implementation.

---

<sup>1</sup> BROMME Arslan, BUSCH Christopher (Eds), BIOSIG 2010: Biometrics and Electronic Signatures, Proceeding of the Special Interest Group on Biometrics and Electronics Signatures, Lectures Notes in Informatics, Vol P-164, 09-10 September 2010, Darmstadt, Germany, 161 pages, ISBN 97-3-88579-258-1, GI, Bonn.

## 4. Theoretical framework

The success or failure of a technology may be explained in different ways, being one of them the adoption rate, which in the end fuels its diffusion speed.

Technology is knowledge, the development of such leads to an increased utility and also may conduct to commercial applications. If we take a look at the technology developments up until 2010, it seems that the technology developing pace is increasing quite rapidly, with ever increasing utility. As for commercial applications, they are still in the first stage of development, with on one hand many suppliers providing solutions and on the other hand few consumers buying and using them. There is no question regarding the interest in the technology but rather when to use it.

To better understand the success or failure of such commercial applications, a model is defined. The model is based on three dimensions, which are related to each other, and therefore converge:

### 1. Technological dimension:

Technology matters in itself to explain success or failure. Competition between technologies, Technology Life Cycle, norms and standards, compatibility, and network effects may explain the perception of the utility by the users.

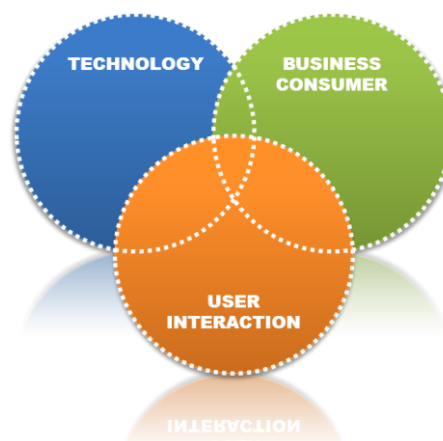
### 2. Business consumer dimension:

The success or failure in the adoption process may be based on the organisation, decision-making, top-level involvement, project management, the scope of the project, etc. of an organization.

### 3. User interaction dimension:

End users are the individuals that make a product or a solution either a success or a failure, in particular when dealing with commercial applications, since they are not obliged to buy or use the product.

The model is depicted in Figure 1.



*Figure 1. The three dimensions*

In the description of the diffusion paradigm, Rogers explained that there are two characteristics to describe the adoption decision process.

**1.** The decision to adopt may be either imposed to or optional for the user; i.e. when a government decides to use biometrics for passport, there is no choice for citizens but to adopt it. On the contrary, access control to a building is a decision proper to the building owner. Others will not have to use it. In the former case, the obligation will force the adoption then the diffusion; for the latter, the diffusion should be slower because of the option left to individual initiative.

**2.** The decision may be individual or collective. Buying a laptop with access control depends on the buyer itself whereas the decision to equip sales team with such a solution will depend on a buying group decision. The decision should be made faster in the former case than in the latter; there should be less time required to make an individual decision than a collective one.

	Decision to adopt is Optional	Decision to adopt is Compulsory
Individual Decision	Commercial applications such as Laptop ID	E-governments applications such as Biometrics for immigration policy
Collective Decision	The banking industry agreed on biometrics for banking cards ID	A given set of governments agreed on biometrics for passports

*Table 1. Type of decision*

## 5. Technological dimension

Technology diffusion is a dynamic process, wherein the adoption fuels the process. It is a “self-reinforcing” mechanism, based on positive network effects. There are several sources of network effects:

- User experiment
- Network externalities
- Economies of scale
- Technical interrelations

A technology might be made of different components working together. Components may be more or less standardized and standards more or less open. But standard and norms do not apply only to technology, they also apply to behaviours. Therefore, compatibility deals with both technical interface and behaviour. And it becomes a key issue whenever:

- a. Different components are provided by a group of suppliers, technical compatibility and interoperability is required between the different components.
- b. The use of new technology should be compatible with the current portfolio of technologies used by the user, skills of employees, current business process, etc.

The more standardised the technology, the more reinsuring for the user about the future of the new technology. For there will be enough suppliers involvement to secure sourcing for a given standard, resulting in less perceived uncertainty regarding the future benefits.

In fact, compatibility may be built *ex ante* (built-in as the technology is developed) or *ex post* (built by adding technological components).

Based on the information gathered in the deliverable 2.1, we can list a set of technological factors explaining the success or failure of projects.

### 5.1 *Supplier reliability versus compatibility*

Given that the technology is still in development, there is a high risk that the supplier will not be able to provide the finished solution in time. If there is no other supplier available developing the same technology or if there is another but with limited capacity to insure compatibility, the user will not adopt the solution for there is too high a risk. Also, the user will need to possess (or be capable to prioritize the acquisition within the organization) sufficient resources to ensure the success of the projects by either generating its own solution or rely on several suppliers.

For a continuous adoption, the application should be simple to adapt and not require a high level of technology development.

## 5.2 Technology Adoption and Standardization

One of key factors for a successful story of a biometric system from its initial design to the actual market placement, is the adoption of existing biometric standards in all architectural levels; such as the devices and sensor specifications, biometric modalities implementation standards and the standardized way of creating the database of signatures (either in smart cards or in a centralized way according to the target application scenario).

Thus, the direct and indirect integration and development costs for vendors and end users are important in the adoption process.

While the design and implementation of the internal components of a biometric system making use of non-standardized Software Development Kits (SDKs) may seem reasonable, special attention shall be paid by the biometric technology makers since the later testing, evaluation, compatibility issues and maintenance of their proprietary SDKs could lead to high costs, thus making them non-applicable in different public and/or private sector deployments. To cope with this, the technology developed must specify and follow uniform quality requirements according to existing published standards<sup>2</sup> (including technical guidelines<sup>3</sup>) in order to ensure their interoperability with other hardware or software following the same standards, as well as to be able to utilize the same biometric technology (as a whole or components) in various application domains. For instance, the BIODEV II<sup>4</sup> project has shown that quality assurance and standardization is very important and has a huge positive or negative effect on the overall process of incorporating a biometric system (adoption) as an additional security system.

Regarding standardization, the biometric market includes a significant number of separate hardware and software vendors, each with their own Software Development Kits for data acquisition, feature extraction and data storage/retrieval and algorithms for signature matching. Thus, a critical factor for their successful placement in biometric projects is the utilization of biometric standards (e.g. BioAPI<sup>5 6</sup> for overall design and development of a biometric management system, standards for template file format and storage<sup>7</sup>), that will allow on one hand the development of interoperable biometric components (e.g. allow sharing of biometric modalities templates among different biometric matching vendors) and on the other hand an effective comparison and evaluation with different biometric technologies.

---

<sup>2</sup> Published Standards Relevant to Biometrics,  
<http://www.nationalbiometric.org/downloads/published-biometric-standards-update-september-2010.pdf>

<sup>3</sup> Federal Office for Information Security (BSI): Technical Guideline TR-03121, Biometrics for Public Sector Applications (TR Biometrics), Version 2.1, 2010.

<sup>4</sup> BIODEV II was a pilot scheme conducted in 2007. The aim was to develop customised biometric enrolment solutions for each of the participating EU member states, and to integrate them with their existing national visa processing systems to test interoperability.

<sup>5</sup> BioAPI Consortium website: <http://www.bioapi.org>

<sup>6</sup> ISO/IEC 19784-1: Information technology – Biometric application programming Interface – Part 1: BioAPI specification, Ver. 2.0, 1 May 2005

<sup>7</sup> Common Biometric Exchange Formats Framework (CBEFF), INCITS 398-2008 and ISO/IEC 19785-1:2006

### **5.3 Compatibility between technological components**

If all the components of the solution are compatible enough or if the level of compatibility is simple, the project will be more secure and thus more successful. Otherwise, users will perceive a risk of not having the “future” successful solution and therefore will not adopt the solution. See for instance the BIODIV II Project<sup>8</sup>. As stated by F Rahmun and S. Hick, “*all elements, i.e. general mechanisms (e.g., training, acquisition guides, auxiliary utilities), hardware components (e.g. silicon pads, feedback monitor, sensor positioning) and software/workflow improvements (e.g. iterations, feedbacks, algorithms) are necessary to achieve suitable quality*”.

### **5.4 Usability of the biometric components and ergonomic design**

As of today, the design, implementation and assessment of commercial biometric systems has been focused on technical related issues such as system performance, functionality, robustness and efficiency in terms of speed, accuracy and error rates. In the initial stages of development of a commercial product, this is essential in order to provide the market a reliable and high performance product. However, as these new types of technologies reach full maturity from the performance point of view, it is obvious the need to evaluate other factors, such as, the usability<sup>9,10</sup> and/or the ergonomic design<sup>11</sup> of these systems for their successful incorporation into the growing market of biometrics. By developing biometric components such as biometric sensors, devices, interfaces and finally end user biometric systems that fully exploit the human interaction with them will not improve only the future acceptance of such technologies by the users but will implicitly lead to the improvement of the overall design and performance of a biometric management system. The ergonomic design of sensors and their effective interaction with humans is not only related to the deployment of successful and future proof biometric systems but it also concerns the design and development by the biometric vendors of usable devices and systems, with the ultimate goal of achieving the maximum performance (e.g. lower enrol failure rates, higher verification rates due to lower acquisition failures from the devices, etc.).

---

<sup>8</sup> RAHMUN Fahes, HICK Sibylle, « Towards Best Practices for Biometrics Enrolment », pp 121-126 in BROMME Arslan, BUSCH Christopher (Eds), BIOSIG 2010: Biometrics and Electronic Signatures, Proceeding of the Special Interest Group on Biometrics and Electronics Signatures, Lectures Notes in Informatics, Vol P-164, 09-10 September 2010, Darmstadt, Germany, 161 pages, ISBN 97-3-88579-258-1, GI, Bonn.

<sup>9</sup> Eric P. Kukula, M. J. Sutton, Stephen J. Elliott: The Human-Biometric-Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements. IEEE T. Instrumentation and measurement 59(4): 784-791 (2010)

<sup>10</sup> International organization for standardization, ISO 9241: Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability. p. 28. (1998)

<sup>11</sup> Eric P. Kukula, Stephen J. Elliott: Ergonomic Design for Biometric Systems. Encyclopaedia of Biometrics 2009: 274-280

## 5.5 Use procedure

Biometric technology does need to be properly implemented, due to existing limits of the current solutions. We may see for instance that enrolment might show high rejection rate. See for instance the BIODEV II Project<sup>12</sup> or the BanCafe project<sup>13</sup>.

Technology is most likely to become a success when it is deployed in a large variety of applications. And it also needs certain coherence and synergy with the users for them to adapt their current behaviour to the one required by the use of a new technology.

In the BIODEV II Project, the technology applications had to be coherent with user's behavioural norms and standards, as a result, a set of guidelines were proposed to ensure correct usage and behaviours. The rejection rate decreased significantly as a result.

## 5.6 Technology adaptation

Most applications we observed still required complementary developments, either because of technology insufficiency, lack of correct implementation or correct use procedures. Such adaptations take time and would require from the project managers to invest time and resources. The capacity of both users and suppliers to invest time and resources is a key-issue to ensure success or failure, whereas it is difficult to forecast the adaptations to be made.

Technology adaptation is needed to make sure it is fully compatible with the current ones it will co-exist with, i.e. within a company. See for instance the case of BanCafe a financial institution in Colombia. BanCafe wanted to implement NCR Corp. biometric ATMs. At the beginning of the project, the enrolment/authentication process failed for 30% of customers, a rejection rate unacceptable for the bank. After two years of continuous improvements, the failure rate had fallen to an 8%. Still, BanCafe pursued the use of biometric ATMs and their implementation with NCR Corp., along with card and PIN options. Without the strong support of BanCafe top managers for such solution, the implementation would have been interrupted<sup>14</sup>.

---

<sup>12</sup> RAHMUN Fahes, HICK Sibylle, « Towards Best Practices for Biometrics Enrolment », pp 121-126 in BROMME Arslan, BUSCH Christopher (Eds), BIOSIG 2010: Biometrics and Electronic Signatures, Proceeding of the Special Interest Group on Biometrics and Electronics Signatures, Lectures Notes in Informatics, Vol P-164, 09-10 September 2010, Darmstadt, Germany, 161 pages, ISBN 97-3-88579-258-1, GI, Bonn.

<sup>13</sup> BanCafe

<http://www.msnbc.msn.com/id/9660429/>

<http://www.atmmarketplace.com/article/134252/Columbia-s-Bancafe-Bank-introduces-ATM-finger-scanning-technology>

<http://www.bancafe.com.co/>

Pay By Touch

<http://biometricpayments.blogspot.com/2008/01/pay-by-touch-update-on-cardline.html>

<sup>14</sup> cf. footnote 13.

## **5.7 Technology Safety and Privacy assurance**

One additional key factor for delivering a successful biometric project is its capability to assure safety and privacy of the involved end users. Biometric systems during their design and execution phases, should take care of safety issues (i.e. handling identity fraud or theft, to provide countermeasures for biometric data breaches, etc.) in order to avoid errors or misuse of the biometric system. Thus, a safety assessment should be always in mind during the extensive evaluation of a biometric system (except other critical factors such as performance or usability) as the biometric technology itself is easy to mislead or to be misused.

To avoid identity fraud, several countermeasures have been proposed such as the simultaneous use of several biometric technologies (multimodal biometrics<sup>15</sup>) and their possible combination in order to eliminate the successful imitation of all of them by the identity fraudster. As the effect of identity theft<sup>16</sup> is more critical in large-scale applications, the biometric products shall meet specific privacy and “safety” requirements that will further assist the social acceptability of such projects, thus rendering them as viable business cases and appropriate technology choices for increased security.

---

<sup>15</sup> Victor Lee, Biometrics and identity fraud, *Biometric Technology Today*, Volume 16, Issue 2, February 2008, Pages 7-11.

<sup>16</sup> Grijpink, J.H.A.M., (2008). Biometrics and security: Trend report on biometrics: Some new insights, experiences and developments, in: *Computer Law and Security Report*, vol. 24 (3) 2008, pp. 261-264. Oxford, UK: Elsevier Science Ltd

## 6. Business consumer dimension

The business consumer dimension deals with all the organisational aspects required to implement and use a biometric commercial application.

The time frame, in which the deployment of an application takes place, depends on both, the business consumer and the supplier of the application. Once the deployment begins the planning may be adjusted accordingly to account for all necessary changes and developments to assure a successful implementation, and this adjustments may end up stretching the time frame allocated. Therefore, it is crucial that on the consumer side, top level management is engaged and supporting all along the project, while the supplier is fully committed to deliver.

Once a business consumer is determined to implement such application, the project should be ranked as priority. In order to make that happen, a risk and benefits assessment shall be correctly done from the very beginning. The business consumer also needs to continuously monitor the activities being carried out to apply any relevant corrective actions and conduct the project successfully; in particular, assessing both positive and negative impacts on processes and the evolution over the project duration.

Based on what we observed, we consider several factors to be determinant within the organization:

- Support over time of top level management, in particular when complementary adaptations are required
- Good assessment of benefits, risks and limits of the project along its duration, i.e. good project management
- Involvement and motivation of all stakeholders, i.e. top level management and employees
- Training employees, customers, and all types of users
- Compatibility of new technology with current portfolio of technologies.

There are also a few complementary factors to take into account regarding the involvement of partners. Again, what we observe is that because biometry is a complex technology to be used in companies, there are strong requirements to enable the correct implementation of projects. The very first one is to secure at least two suppliers to ensure project follow-up, in the given case one of them cannot continue with the project or to be sure that alternative compatible solutions exist. Having two or more suppliers, will enable the user to go on even if there are casualties during the process, if there is only one supplier, there is an eminent risk of a complete disruption of the project for instance as in the case of First National Bank ATM deployment in the USA with Pay By Touch supplier.

Another issue is to be sure that everything is ready when the time comes to implement the application and use it, i.e. at the business consumer shops, or its partner facilities. For instance, the full process of end users enrolment has to be fully controlled, which requires from the business consumer partners to fully understand the solution. Eventually, there will be needed a long term involvement and continuous engagement of these partners, for them to train their employees, and adapt their own working environment. The case of a large retailer chain with franchisees may be cited. If it wants to propose a loyalty based-card program to customers, the project has to be implemented at franchisees. The retailer will need sufficient control over the franchisees to be certain that everything is acting according to the book, and that the final customer will be offered with the same service regardless of the franchisee.

The more numerous the number of partners involved in the process, the more control is required to have the work done correctly.

## 7. User interaction dimension

User interaction dimension deals with every aspect regarding the continuous use of application by end users. Based on what we observed, we consider two cases, according to the degree of control over the participants:

1. When the project is solely intended for employees or internal participants (within the limits of the business consumer organisation, i.e. for access control)
2. When the project involves external partners, outside the organization (as in the case of franchisees and customers for a loyalty program).

For the first case, the control exerted by the business consumer organization over its employees make things simpler for there is a direct relationship among the parties during the implementation process (direct control), and among the related tasks, such as promoting benefits, training employees, adapting processes, etc.

In the second case, where partners are involved, things get more complex. Based on what we observed in deliverable D2.1, the very first factor to explain success is to be sure that customers know what they gain, compared to existing solutions<sup>17</sup>. That is why, benefits have to be clearly promoted and demonstrated, such as, security, convenience, simplicity to use, no card needed, etc.

The second case is about making the biometric application easy-to-use for the end user/customer. Firstly, the processes of enrolment, data storage and purse, as well as account cancellation steps, have to be clearly understood by customers. Secondly, the overall process has to be perceived as both easy and secure. If there is too much complexity and/or the process highly differs from what is being explained, there will be a high risk of rejection. All procedures must facilitate the customer interaction with the application, which in the end results in a rewarding experience for him or her.

Furthermore, a critical factor for the success or failure of a biometric project is the active participation of the end users to various phases of its design and development. Both, the biometric vendors and end users/customers, will benefit when a user-centred design approach (ISO 13407:1999) is followed<sup>18</sup>. By following an iterative, user-centred design approach, biometric vendors and the biometric industry as a whole can achieve a measurable impact on the usability and ease-of-use of the COTS (Commercial off-the-self) biometric management systems.

Based on what we preciously observed (deliverable D2.1) as in the case of BanCafe in Colombia or Zions in USA<sup>19</sup>, the careful monitoring of pilot experimentations and the implementation of corrective adaptations enable the company to save up money and time when it comes to full scale deployment.

Nonetheless, being a solution highly sensitive in respect to all the parties involved in its deployment, there is always a need to reassure the end user that existing solutions are still in order.

---

<sup>17</sup> Cf. footnote 13 for websites.

<sup>18</sup> M. Theofanos, B. Stanton, and C.A. Wolfson, Usability and Biometrics: Ensuring successful biometric systems, NIST, June 11, 2008, available at [http://zing.ncsl.nist.gov/biousa/docs/Usability\\_and\\_Biometrics\\_final2.pdf](http://zing.ncsl.nist.gov/biousa/docs/Usability_and_Biometrics_final2.pdf)

<sup>19</sup> Zions

[http://www.paymentsnews.com/2006/07/zions\\_bank\\_embr.html](http://www.paymentsnews.com/2006/07/zions_bank_embr.html)  
<https://www.zionsbank.com/>

## 8. The importance of negotiation and clear business drivers

Another approach on assessing the potential success or failure of a biometric project is the analysis of the stakeholders and their respective interests. These interests are divided in three main categories: security, convenience and efficiency. Our field experience and the on-going analysis we make as part of our professional activities of a wide variety of biometric projects and deployments (whether they have been successful or not), indicates that these three categories form the main drivers of any biometric deployment. Based on the previous statement, the selection of biometric technology suggests an a priori assumption of a significant contribution to any of the drivers or a combination of them.

In many cases these three drivers actually represent different stakeholders, or the different interests within a stakeholder. These stakeholders and their interests together have to decide on the overall requirements and specifications of a project. Technical elements such as FRR (false reject rate) and FAR (false acceptance rate) have a profound impact on the design and implementation of the project; they are to be considered as of strategic value. This view is being supported by the European Data Protection Supervisor (EDPS) Peter Hustinx, who stated the following during his keynote speech at the RISE Conference "*Ethics and Governance of Biometrics and Identification Technologies*" (Brussels, 9 December 2010):

*"Biometric systems are inherently based on probability. This is why one needs to apply false-rejection and false-acceptance rates. In this respect, I have always emphasised that those who are responsible for data processing must proceed on the assumption that a biometric system is not perfect. False-rejection and false-acceptance rates should be matched to the ultimate purpose of the system."*

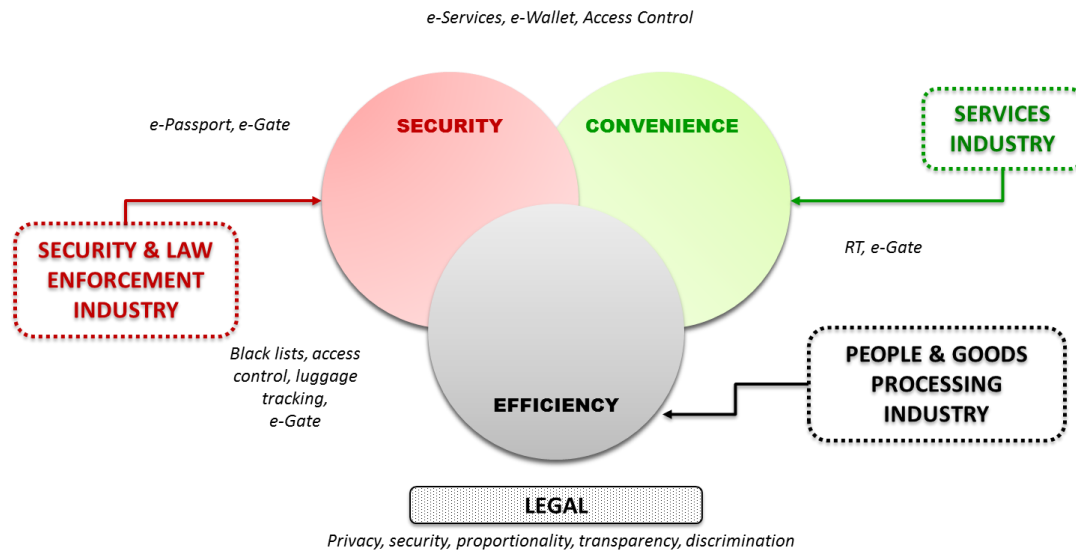
The setting of these elements (i.e. the FRR and FAR) should be a result of negotiated requirements. For that reason it is of utmost importance that all stakeholders are being actively involved via the project management from the very beginning of the design process. The final requirements must be clear and unambiguous, demanding an open and thorough negotiation process with and between the stakeholders.

All stakeholders need to have the same understanding of the relationship between the technology and the goals to be achieved by its deployment, as well as of the consequences for the organization of its application and related processes and procedures.

A program of requirements, which is the consolidation of the overall negotiation process on the final requirements of an end to end system, should at all times be defensible and explainable based on realistic and quantifiable arguments. This ensures that, during the preparation and execution of the project plan, the requirements and specifications will remain stable. To achieve this, it will be necessary that the primary drivers for the deployment of a biometric application are well understood from all relevant stakeholders perspectives. These drivers should be described in their specific context and need to represent the focus of all efforts followed towards the realization of the project, including the financing and tendering phases.

If from the very beginning the desired achievements are not clear, the system viewed as an entity will in the end not function properly or as expected. Internal discrepancies can easily lead to contradictory interpretations of the desired FRR and FAR. The only way to avoid that is to make a choice between them while bearing in mind the inherent trade off. It is important to realize that different usages of biometrics within a single application may lead to opposite requirements.

The choices need to be based on a final agreed balance between those arguments which drove the stakeholders to the use of a biometric application in the first place. The three main drivers, as mentioned before, are *security*, *convenience* and *efficiency*. The following figure (Fig. 2) provides an overview of them.



**Figure 2.** Biometric business drivers.  
<http://www.eubiometricsgroup.eu/>

With many biometric deployments there is a combination of all three drivers; all drivers play a role, for the positive or the negative side. It is important to understand the interdependencies of the different drivers and to decide which of these drivers is dominant to the envisaged application.

Nowadays *security* is the dominant driver in most of the current applications. In the justice domain, biometric applications are being used to help solve and reduce crime, thus increasing the safety of the citizens. Also access control applications are driven by security. Depending on the level of security to be achieved, the importance of the other two main drivers, convenience and efficiency of the process flow, can be higher or lower. Meaning that e.g. adding iris recognition to an existing access card application, would add certainty about the relationship between access card and the truthfulness of the owner, while at the same the process of passing a door or gate will be less convenient and slower. The lowest acceptable level of convenience and/or efficiency will rely on the balancing and negotiation between the stakeholders. If security is the main driver, the final investment decision will be mostly based on a risk analysis.

There are scenarios where *efficiency* is the main driver. The leading advantage of using biometric applications in such a case will be the extent of delivered automation. In these cases decisive factors are the increase of the throughput of an existing process or system, or the reduction of the costs of operating the system. (e.g. by reducing the number of personnel) In the end higher efficiency might also increase the convenience, e.g. if waiting times for the users are being reduced. Therefore, the investment decision will most likely be based on the amount of cost reduction that can be achieved, or the increase of capacity/transaction per time unit. These factors are and should be definable and measurable.

Another system which can be seen as driven by efficiency is an AFIS (Automated Fingerprint Identification System). This system itself is capable of performing high numbers

of database searches in a short time, something which cannot be achieved by manual inspection, either for costs reasons or simply because there are limitations to the size of biometric databases that can be searched manually.

Finally *convenience* can be the main driver when applying biometrics. The related commercial applications we can think of are, for instance, replacing the four digit pin-code or a smart card to get access to services. Biometric payment is also an example. In such scenarios the quality of service delivered to the user represents the key to the success of implementing biometric applications. The added value of using biometric applications must be evident to the end-user, as he or she will use the system on a voluntary basis and should be willing to pay extra costs that may come with it. The commercial merit of such applications creates a very different kind of balance between the related costs and benefits. The system should be perceived as a trusted one, otherwise privacy issues may represent a drawback. Being the reason why, privacy may become an important success factor for a full uptake of the service.

Below three different appearances of an application are described, which all seem to have one single purpose: crossing the border at an airport. Further analysis will show that in fact this application may be driven by three different drivers, which each go along with different underlying business cases and objectives.

### ***Example 1. Manual Border Control***

The main objective of the biometric passport is to prevent 'look alike' fraud at border check points. The primary driver is security, although it is also of general concern whether the biometric check will delay the process too much. A long delay will result in decreased efficiency and may represent a loss of convenience for the travellers. Too much pressure on both of these drivers (i.e. efficiency and convenience) might even, in the end, put the security at risk, and therefore the whole business case.



*Image 1. Border control at Schiphol Airport*

### ***Example 2. ABC – The e-Gate***

The continuously growing stream of air flight passengers causes longer queues. At the same time the operational surface of an existing airport is not growing, while deploying more personnel is too costly. Nevertheless, these growing numbers of passengers still need to be processed safely and conveniently. If not, a chaotic situation can occur resulting in complaints from the passengers. None of those are beneficial to an airport's or airline's business. Biometric applications here are meant to facilitate processes providing higher efficiency, and at the same time keeping an appropriate level of security. Therefore, the most important driver in this case is efficiency.

### **Today**



*Image 2. Growing air flight passengers at an airport*

### **Tomorrow**



*Image 3. e-Gates in Portugal (RAPID)  
<http://www.rapid.sef.pt/>*

Gates for automated identity verification based on the e-passport to facilitate Automatic Border Control (ABC), standards and interoperability, as well as common security requirements are critical factors for success. right picture: the e-Gates in Portugal (RAPID),

### **Example 3. Privium**

Privium at Schiphol Airport is an automated border passage service program. Besides a quick flow through the Privium Gates, the program offers other several services, like parking facilities, and free usage of a luxurious lounge (incl. food and beverages). The program targets the frequent flyers (mostly business) and charges € 185 per year.

Privium program uses an iris scan biometric system that compares a picture of the member iris stored in his/her Privium Card with the scan performed whenever the member passes through the border control. The smart card contains biometric data (left and right iris) and some other information like membership and personal data. The smartcard is issued under direct supervision of the border policy.

The primary driver here is convenience, given that the added value of the application is focused on providing convenience to the flyer. It is offered and marketed as a commercial service.



*Image 4. A transparent gate*



*Image 5. The luxurious Privium Club Lounge*

These examples show that the role of biometrics from a business case perspective can differ, although we speak about the same application, in this example border control. The different business cases are resulting in different designs of the processes and procedures, as well as different technology choices. The three cases will have different factors of success, different privacy assessments and different funding schemes. The latter is certainly important: whoever pays gets to decide.

Those cases where stakeholders with multiple interests are to reach an agreement based on compromises can become a risky matter. Compromises, although unavoidable in many cases, may lead to unclear requirements and vague criteria for success. This will lead to a project that will be hard to evaluate since success factors need to be clear and measurable. These are strong ingredients for a project failure. On the other hand, if the requirements are clear, thoroughly negotiated and understood by all stakeholders, the project will have a higher potential for success.

## 9. Main teachings

There are three types of innovation decision-process: collective, optional and authority. Commercial applications represent option decisions, industry-based applications, collective, and government applications authority. As for the use for commercial applications, it is up to the company to make decisions; therefore, even if norms and standards are defined and agreed upon, but there is a limited number of suppliers, risk may be perceived as too large regarding the benefits.

On the contrary, whenever a government decides to implement such a solution, it should be in a position to force every participant into the adoption process. But governments are not isolated from each other when it comes to cross-border applications for instance. The case of USA is representative for immigration control policy, and is the only one to make the decision<sup>20</sup>. On the other hand, dealing with border crossings in the Schengen area, comes to collective decisions to adopt, for all governments involved may have something to say.

In WG2, we deal with commercial applications. So as shown in table 1, the decision is rather optional than authoritarian and rather more individual than collective. As for biometric commercial applications, there are necessary factors to be considered when implementing them.

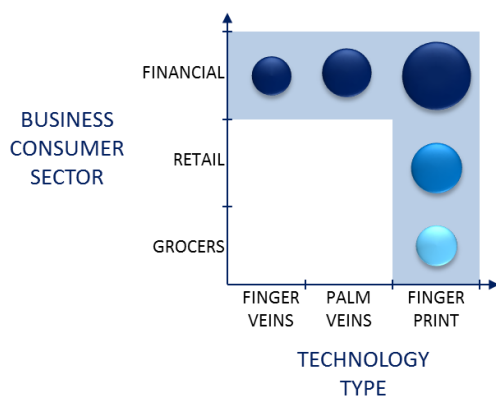
---

<sup>20</sup> AL-KHOURI Ali, « Facing the Challenge of Enrolment in National ID Schemes », pp 13-28, in BROMME Arslan, BUSCH Christopher (Eds), BIOSIG 2010: Biometrics and Electronic Signatures, Proceeding of the Special Interest Group on Biometrics and Electronics Signatures, Lectures Notes in Informatics, Vol P-164, 09-10 September 2010, Darmstadt, Germany, 161 pages, ISBN 97-3-88579-258-1, GI, Bonn.

## 10. Conclusions

The model here proposed based on three dimensions (Technology, Business Consumer, and User interaction) to assess the factors that will determine the success or failure of a biometric commercial application mapped with the projects described in the previous deliverable, help visualize mostly the success factors for such applications. It is important to notice that, as it was mentioned in the beginning of this deliverable, the size of the sample and the lack of access to detailed information restrict the breadth and depth of resulting analysis.

The following maps aim to depict the conclusions of the analysis here made in a visual way, for a better and easier understanding.

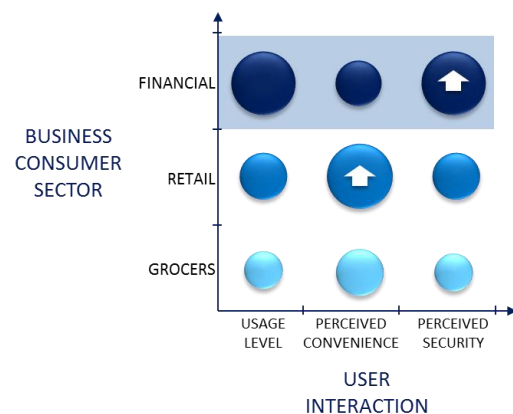


**Map 1.** Business Consumer sector vs. Technology type

Map one in the left, shows the business consumer sectors utilizing biometric commercial applications and the type of technology implemented based on the research conducted in D2.1. The size of the spheres is linked to the level of adoption and use of a certain technology for each business consumer sector. As we can observe, the financial sector has widely deployed biometric applications in their operations and it is familiar with three different types of technologies. While the technology type standing out is the finger print biometric one, for the three sectors here showed.

It is also important to emphasize that the use of finger print biometric technology in the financial sector specially is mostly related to security issues as we will further discuss in the following map.

There are different drivers that lead to the use and implementation of biometric commercial applications. For the business consumer sectors represented in this analysis, there are two main drivers, security and convenience. The level of security and convenience may be linked to the sector nature itself, the socio-cultural and demographic characteristics of the users and the politic and regulatory frame to mention a few. But in order to have a high level view of the current situation of such drivers and their place in the market, map 2 in the right helps us depict convenience and security weighted perception once they have been implemented and in use.



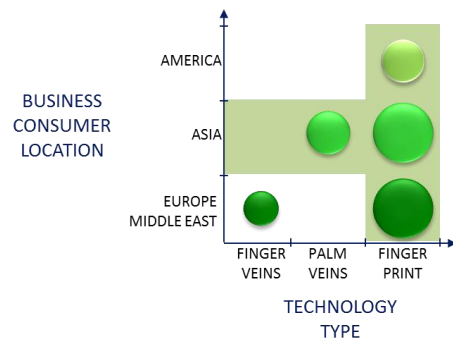
**Map 2.** Business Consumer sector vs. User Interaction

The size of the spheres represents the assessed weight of each element in the horizontal axis for each of the business consumer sectors. We can observe that security has a higher weight in the financial sector compared to convenience and the usage level is also high. Whether in the retail sector, convenience shows a rather big sphere than security, while the use of biometric applications in this sector is still growing and becoming more adopted. Finally for the grocer sector the behaviour is similar to the one seen in retail, but still the adoption and usage of biometric applications in this one has room for diffusion and improvement.

The biometric commercial applications described in deliverable D2.1 were grouped according to their geographic area, which represents another influential factor to use and implement a biometric application. To easily visualize this, in map three a comparison of the business consumer location and the technology type is made.

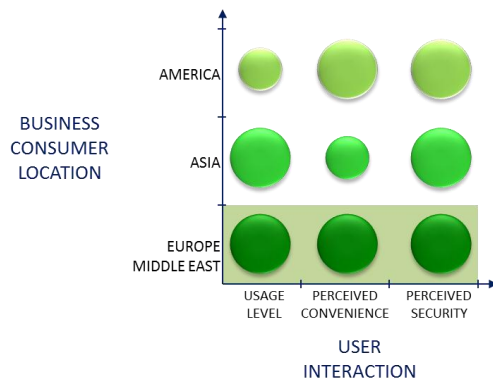
The finger print biometric technology type, stands out once more, within the three regions, although given the size of the spheres in Asia and Europe Middle east locations, the level of adoption and usage of such technology shows a higher weight.

For the case of Asia, we can observe that overall they are used to this type of technology and therefore the level of adoption and diffusion is higher than in the other two locations.



**Map 3.** Business consumer location vs. Technology type

While there may be a type of technology more widely used among the business consumer locations here depicted, an assessment of the drivers to use biometric applications shall be done in order to make a second correlation.



In map four, we can see the different locations of business consumers that are currently using biometric commercial applications in their operations, and the user interaction measured by the level of usage, perceived convenience and security. The size of the spheres represents again a weight, in this case, the one assessed to each of the elements in the horizontal axis in each location accordingly.

**Map 4.** Business consumer location vs. User interaction

For the case of America we can observe that the perceived convenience and security of the users interfacing with the biometric technology has similar weights, which we may attribute to the drivers of the business consumer itself and the resulting perception on the end users. As it was described in deliverable D2.1, the projects within America were mostly related to financial institutions which main driver is security and in a smaller portion to grocers which tend to vote for convenience. From the end user perspective, the behaviour attached to the use of financial or retail (grocers) services requires both convenience and

security, which may be equally important given the cultural habits and lifestyle in such location.

From the information gathered in the previous deliverable D2.1, the implementation of biometric application is in the financial sector, therefore security is the main driver, and the level of usage is greater compared to America for instance, given the high adoption and diffusion rate in the location. The convenience weight here shown is also linked to the fact that there are some societies that are not that comfortable using finger print based biometric applications, because of hygienic issues or because they feel they are being mistreated, which is again a socio-cultural and demographic factor specific to this location and differs from other locations.

In the case of Europe Middle East, the level of usage, perceived convenience and security is quite high, we may explain those given the fact that both financial and retail business consumers are both quickly adopting and therefore increasing the diffusion of biometric applications (i.e. finger print) in their operations to increase security and convenience of their customers. Also, it seems that the end users interfacing with such applications are less reluctant and therefore adopting their behaviours to the use of such technology.

Based on the four maps described above, we can observe that the finger print type of biometric technology is the one most highly adopted and diffused, irrespective the sector and the geographical location. Since this technology reunites a wide network of providers, developers, buyers, users, etc. the network surrounding it is quite larger than the one around the other type of biometric applications.

We have also observed that there are many drivers to adopt and use a certain type of biometric application, but among those drivers one will prevail being the one that will most likely dictate the type of technology to use and in the end facilitate the success path of such technology. It is therefore important for technology developers and suppliers to identify such drivers to better accommodate their applications and/or solutions in the market.

Lastly the environmental factors surrounding us are also dictating the pace, at which a new technology is adopted and diffused, location, demographic, socio-cultural, politic-economic factors are also determinants on the use of biometric technologies. The adoption stages shall be considered to avoid misuse of the application and misleading.

## 11. References

### Books

- BROMME Arslan, BUSCH Christopher (Eds), BIOSIG 2010: Biometrics and Electronic Signatures, Proceeding of the Special Interest Group on Biometrics and Electronics Signatures, Lectures Notes in Informatics, Vol P-164, 09-10 September 2010, Darmstadt, Germany, 161 pages, ISBN 97-3-88579-258-1, GI, Bonn.
- ROGERS Everett, Diffusion of Innovations, 3<sup>rd</sup> Edition, The Free Press, 453 pages, New York, 1983.

### Research Reports

- EPINETTE Olivier, VIOLETTE Jean, DORIZZI Bernadette and al, Survey of existing (non-governmental applications) and emerging biometric applications, BEST NETWORKS Grant n°238955, WG2 D2.1, September 2010, 28 pages, working on progress.

### Websites

<http://www.eubiometricsgroup.eu/>

<http://www.rapid.sef.pt/>

#### → AMERICA

First United

<http://www.finextra.com/news/fullstory.aspx?newsitemid=21373>

<http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/now.html>

<https://www.mybankfirstunited.com/>

Zions

[http://www.paymentsnews.com/2006/07/zions\\_bank\\_embr.html](http://www.paymentsnews.com/2006/07/zions_bank_embr.html)

<https://www.zionsbank.com/>

AllTrust Networks

<http://www.alltrustnetworks.com/Default.aspx>

<http://www.alltrustnetworks.com/Product/HowPaycheckSecureWorks/tabid/58/Default.aspx>

BanCafe

<http://www.msnbc.msn.com/id/9660429/>

<http://www.atmmarketplace.com/article/134252/Columbia-s-Bancafe-Bank-introduces-ATM-finger-scanning-technology>

<http://www.bancafe.com.co/>

Pay By Touch

<http://biometricpayments.blogspot.com/2008/01/pay-by-touch-update-on-cardline.html>

<http://biometricpayments.blogspot.com/2008/03/final-postpay-by-touch-shuts-down.html>

<http://www.jewelosco.com/eCommerceWeb/SaveAction.do?action=beginPBT&target=showPBTPage>

<https://www.jewelosco.com/eCommerceWeb/PbtAction.do?action=beginPBT&target=showFAQ>

<http://www.shell.us/>

→ **ASIA**

Central Bank of India

[http://news.bbc.co.uk/2/hi/south\\_asia/6478627.stm](http://news.bbc.co.uk/2/hi/south_asia/6478627.stm)

<https://www.centralbankofindia.co.in>

Axis Citibank

<http://www.axistech.com/Products/Technology/Technology-Biometrics-Who&How.asp>

Bank of Tokyo Mitsubishi

<http://www.atmmarketplace.com/article/129761/ATM-security-in-Asia-moves-to-veins>

[http://edition.cnn.com/2010/WORLD/europe/07/05/first.biometric.atm.europe/index.html#fbid=fTJVUI\\_rzUA&wom=false](http://edition.cnn.com/2010/WORLD/europe/07/05/first.biometric.atm.europe/index.html#fbid=fTJVUI_rzUA&wom=false)

<http://reports.celent.com/PressReleases/20060329%282%29/BiometricsJapan.htm>

<http://www.bk.mufg.jp/english/>

Woori

<http://www.allbusiness.com/banking-finance/banking-lending-credit-services-cash/5220823-1.html>

<http://eng.wooribank.com/>

Citibank

[http://www.paymentsnews.com/2006/11/citibank\\_singap.html](http://www.paymentsnews.com/2006/11/citibank_singap.html)

<http://www.citibank.com.sg/>

→ **EUROPE/MIDDLE-EAST**

BPS

<http://www.finextra.com/news/fullstory.aspx?newsitemid=21384>

<http://www.bankbps.pl/>

Barclays Bank

[http://www.kuwaittimes.net/read\\_news.php?newsid=NDg1NDMwMzEy](http://www.kuwaittimes.net/read_news.php?newsid=NDg1NDMwMzEy)

<http://www.barclays.ae/>

EDEKA, METRO, Officecom, etc

<http://www.it-werke.com/en/references/index.html>

METRO real- Future Store

<http://www.future-store.org/fsi-internet/html/en/7670/index.html>

<http://vingado.eu/http://vingado.eu/vingado/pay-by-vingado/>

<http://libertesinternets.wordpress.com/2007/09/17/en-allemande-les-supermarches-edeka-accepte-le-paiement-des-achats-sous-la-forme-dempreinte-digitale/>

<http://www.zalix.fr/references.html>

CNIL

<http://www.cnil.fr/english/topics/regulating-biometrics/>