



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 D2.1

Survey of existing (non-governmental applications) and emerging biometric applications

Final version

Dissemination level: PU

Date of submission: 1 September 2010

Table of contents

1. Summary	3
2. Introduction	4
2.1 Scope	4
2.2 Structure of the document	4
3. Methodology	4
3.1 General Methodology	5
3.2 Sources	5
3.3 Limits of the deliverable	5
4. America	6
4.1 Banking	6
4.2 Commercial services/retail	8
5. Asia	10
5.1 Banking	10
5.2 Commercial services/retail	12
6. Europe & Middle-East	13
6.1 Banking	13
6.2 Commercial services/retail	14
7. Main teachings	15
8. Conclusions	19
9. References	20
10. Appendix	22
Appendix 1: PayCheck Secure	22
Appendix 2: Fujitsu's hand vein technology	24
Appendix 3 : Biometrics regulation of the French CNIL (Commission Nationale de l'Informatique et des Libertés)	26

1. Summary

The deliverable is an, exploratory survey of existing and emerging commercial biometric applications related to banking and commercial services/retail. We started by contacting BEST Network members in order to gather as much information as possible. After discussing with them, we made a list of criteria which will help us compare the applications and underline their main characteristics. Then, we started looking for applications in retail and in banking on the internet. We also tried to ask biometric specialists about emerging applications they would have heard of. Furthermore, contacting people developing biometric solutions didn't really help up because they wouldn't reply or they had no information to share. Eventually, we organized our different projects following a pre-defined plan.

For each chosen application we found, we tried to detail the way it works, who provides the solution and the equipment and the potential problems it could create. After doing so, we began to analyse the distribution of these applications all around the world. We found that their implementation was very unequal depending on the regions and each country. Finally, we started to think about the reasons why there are so few applications in Europe for example and why there are so many in Japan.

2. Introduction

The goal of this research is to provide a state-of-the-art analysis of biometric commercial applications in Europe and to explain the main reasons of 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 is still explanatory, i.e. validate the interests and opportunities for such biometrics solutions in retail (viewed globally, banking and retail). It will mainly be based upon qualitative research 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 make a survey of existing and emerging commercial biometric applications (banking and commercial services/retail). We will not study access control systems or final products (laptops, cars, USB keys, etc). The main reason is that these applications are already working and widespread; they're not facing the problems we want to highlight for example the adaptation to a third party. Each application we found will be detailed as much as possible for a better understanding of the position of both the firm and the customer using it. We will not explain the technical and technological characteristics of the applications in order to increase readability.

2.2 Structure of the document

The applications will be ordered according to their location (the continent where the firm uses it) and then their nature. The deliverable is divided into three parts corresponding to each continent. Each of these parts is then structured according to the nature of the application: banking or commercial services/retail.

3. Methodology

The work we do is to create a list of the projects of 'commercial biometric applications'. This stage turns to be fundamental for the remaining of the project as it gives us a base to work on.

We use a methodology relevant for our ongoing explanatory research.

3.1 *General Methodology*

First, we defined the topic and the scope of the study with BEST Network members. Then, we started looking for applications in retail and in banking on the internet and with the help of biometric specialists. We also tried to get in contact with people developing biometric solutions in order to gather as many data as possible. Finally we ordered our projects according to our plan and started detailing them as much as possible.

3.2 *Sources*

For the first part of our work, the survey of commercial applications, we exclusively relied on secondary data from the internet whether it was technological news, websites of installators, retailers, banks and biometric specialists. We will interview people in charge of applications and collect primary data for the next deliverable.

3.3 *Limits of the deliverable*

As described earlier, we have concentrated on commercial services and retail and banking which represent a focused subject area. In fact, a large part of the commercial applications of biometrics concern access control for small, closed user groups. These applications are rather straightforward and do not impose large technical and/or legal challenges. For that reason we have chosen to focus on more challenging areas, such as payment systems in banking and retail. In order to use the available resources as efficiently as possible, this survey has relied primarily on desk research. The internet has proven to be the major source, as it has allowed us to compile a good overview of the sector (commercial services/retail & banking) without using travel or other timely resources. Interviews and other direct contact will be undertaken during the next iteration of our deliverable.

4. America

4.1 *Banking*

First United (USA 2010)

The United-States are currently evaluating and studying the potential benefits of biometric solutions in the banking sector as specialised firms providing the banks with solutions are struggling to find customers. The issue of ATM fraud is very important as hackers are more and more technologically aware of the security systems used in the machines. Biometric authentication appears to be one of the solutions to this problem.

First United is currently testing new ATM machines with increased security thanks to fingerprint authentication in the New York metropolitan area. The technology is provided a Delaware-based firm named Hawk Systems which registered a patent that covers "using scanning five layers deep in the epidermal layer of the finger to authenticate a financial institution customer and permit an ATM transaction". With its ATM Touch & Go service, the firm aims at proving the efficiency and the security of their system to the banks. The Company will have the capability to produce the ATM unit in a variety of configurations ranging from just the scanner to both scanner and logic board up to the full system with RFID communication between the ATM card and the ATM. The ATM T&G technology is composed of the machine itself (ATM machine) and the software which allows communication with the fingerprint database (POS) and the bank. In order to use T&G, the card owner must go to the POS location and register multiple fingerprints which will be attached to the account of his or her choice (Visa, MasterCard, etc).

If the pilot is successful, First bank is ready to adopt this ATM technology across its fleet.

Zions (USA, 2006)

Zions First National Bank, a subsidiary of Zions Bancorporation, and Pay By Touch have announced in 2006 the introduction of biometric check-cashing to 12 locations throughout Utah and Idaho. The service, powered by Pay By Touch, uses a finger scan to quickly and securely identify customers when they are cashing a government or payroll check.

This new service, Zions Express powered by Pay By Touch is easy to use. Customers must first register at any participating Zions Bank branch. A bank employee will confirm the customer's identity using a government-issued photo ID, then digitally scan his fingerprint and take an electronic photograph. The one-time signup process takes only minutes, and at subsequent visits to the bank the customer only needs to place his/her finger on the Zions Express scanner to safely and securely cash payroll checks.

With this service, users can cash checks in a more simple and secure way and save time doing so (see appendix 1).

By July 2006, more than \$8 billion in checks had been cashed using Pay By Touch's biometrically initiated check-cashing system. Pay By Touch acquired BioPay, the developer of the biometric check cashing system. More than 2.5 million consumers were using the system to cash checks -- primarily in retail locations. Zions Bank was the first retail banker to



implement the system in branch locations and was in 2006 Pay By Touch's first retail banking customer.

In 2008, Pay By Touch which filed for chapter 11 sold its BioPay Paycheck Secure business to AllTrust Networks, a Phoenix-based management group for \$4.2 million. Pay By Touch paid \$82 million for the business in 2006 when it acquired it from BioPay.

With more than six million registered consumers, AllTrust Networks is actually the most widely used biometric financial transaction database and provides key risk analytics tools for walk-in financial services.

With their Paycheck Secure® check cashing software, AllTrust provides a risk management system available with national networks for both biometric identity and check history.

In South America, Biometrics has been widely used for almost 10 years because there is less resistance to its application and consumer acceptance is a lot higher. In fact, Citizens already are accustomed to the use of fingerprints for general identification, such as the ID cards they own. Here are few examples of the banking applications South Americans have developed since 2000.

BanCafe (Colombia, 2004)

At the end of 2002, BanCafe, Colombia's fifth largest bank implemented biometrics ATMs for the coffee growers and to make them open accounts. It is important to understand that the problem of security in South America is a lot more important than in the USA and so, banks need to find new solutions for their customers. Biometrics is more secure than standard credit/debit cards, and this increases the user's satisfaction but it can also allow people to use ATMs without a card. In Colombia, BanCafe allowed its customers to use its ATM without carrying cards, which can be a lure for thieves. The user only has to put his finger on the fingerprint reader which would check his identity. Many users found that using the machines was more secure and also more convenient.

When the system was installed, ATM failed to recognize fingerprints which weren't clean enough. The elderly and construction workers for example saw their prints rejected or not recognized by the machine. At the beginning of the application of the biometric ATM, the enrolment/authentication failed for 30 percent of the customers which was very high. Thanks to technological progress made by NCR Corp. the American firm selling the machines, the figure fell to 8 percent in 2004 which was still problematic.

However, BanCafe chose to continue its collaboration with NCR Corp. pursuing the implementation of their machines across its entire ATM network.

In order to use the automatic teller machine, a customer places a finger on the fingerprint, enters an ID number and accesses his or her cash. In order to implement finger scanning, the bank needed to create a register of customers' fingerprints. When customers use the ATM, their fingerprints are compared to the centrally stored images.

The ATMs still retain the card and PIN option, however, about 50 percent of BanCafe's customers have signed up for the new technology. The bank had high expectations for the success of biometrics in banking activities and showed a lot of motivation in the application process.

In fact, it initially piloted the biometric scanners on 170 ATMs in 2002 and finally adopted the technology when it was reliable and secure enough. Biometrics allowed the bank to reach new types of customers who needed easier and more secure way of handling their money.

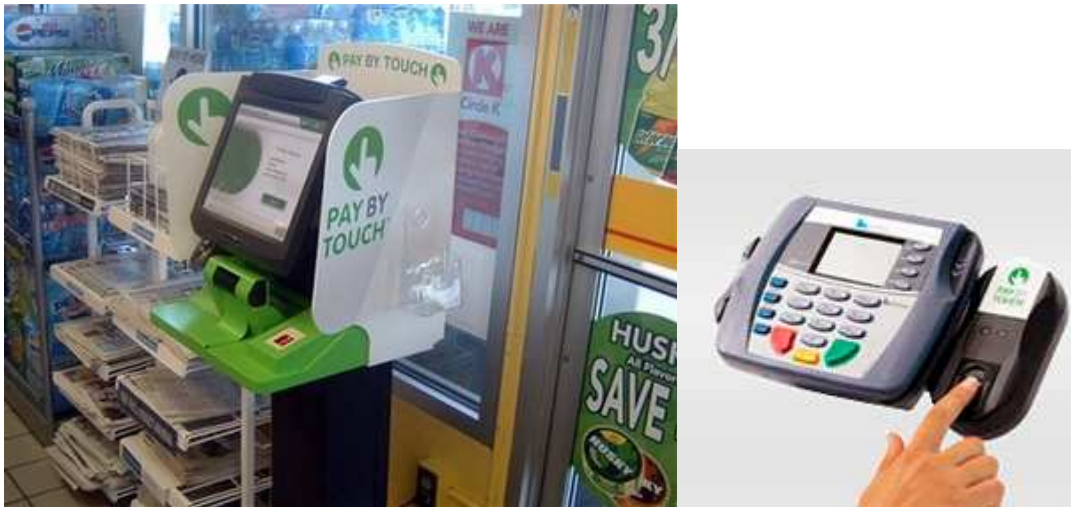
The same type of technology and applications (biometric ATM and check cashing) can be found all across South America. Banco Falabella (Banco de Chile) in Chile uses fingerprint authentication to verify the identity of the consumer in its ATMs or before making operations with a teller (the technology used is made by L1-identity solutions formerly Identix), Grupo Financiero Banorte in Mexico also uses biometric ATMs. Banco Bradesco, Brazil's largest private bank, was incorporating palm-vein technology into its ATM in 2008. The bank tested the solution in 2006.

American banks had already tested the adoption of such solutions but it wasn't as successful. In 1999 national Bank United in the USA installed biometric authentication in three ATM outlets in Houston, Dallas and ft. Worth. The scheme employed an iris recognition system created by DieBold Inc., a company specializing in iris recognition. Citibank has been piloting eye-scanning technology on some 500 employees at its development test centre. If the public accepts it and deployment makes business sense, eye scans could be incorporated into ATMs.

4.2 Commercial services/retail

Shell, Jewel-Osco, etc. (USA, 2008)

The most obvious commercial service retailers can provide their customers with is a simple and convenient payment method. Shell, Jewel-Osco and other retailers allowed their clients to pay with their finger thanks to a biometric technology named "Pay By Touch". Unfortunately, the company behind this payment method, Solidus Network Inc, filed for bankruptcy in 2008 and thus the biometric service was discontinued. The company founded in 2002 had created a payment method based on the user's fingerprint and which was a substitute to credit cards, cash or checks. "Pay By Touch" provided its clients with kiosks (for enrolment) and biometric readers (for payment) they had to install in their shops in order to allow their customers to pay with their finger.



In order to use this payment method, Jewel-Osco customers could register online or directly in their store. On the net, the user only had to register and choose a 7 digit Personal search code which allowed the software to find their fingerprint easily. After doing so, the user was to go to one of the department stores to have his fingerscan registered and he was ready to go. Or, if he didn't register online, he could simply use the Pay By Touch kiosk in his store in order to register his fingerprint and choose his search code. Jewel-Osco also provided the Pay By Touch members with online services such as a payment method and card management webpage. Of course, users of the biometric system were still able to pay with their cards or their cash, it was only voluntary.

When the user goes to the checkout, all he has to do is to put his finger on the biometric reader and enter his 7digit code. The order is then sent to his bank which allows the access to his bank account and the payment is done.

Now that the company has been dismantled and its assets bought by investors, it seems that most stores using "Pay By Touch" kiosks got rid of them but Jewel-Osco is still advertising it in its shops. At its peak, the company provided more than 2000 stores across the United-States in more than 40 states.

There are very few commercial services/retail applications of biometrics in America and even globally. Other than the failed attempt of Pay By Touch, NCR considered selling finger readers to stores in 2005. The technology was designed to speed up checkout and to prevent theft. The scans verified which cashiers were operating the registers in case there was missing cash and the identity of managers who approved customer checks.

5. Asia

5.1 *Banking*

Central Bank (India, 2007)

In India, poor workers who can't read have to go to the bank and queue for hours in order to get the cash they want. In order to help those people, the Government-owned Central Bank has installed new ATM with fingerprint scanners and voice instructions in the state of Bihar in the Vaishali district.

"When the user inserts a cash card into the machine, he is greeted with a voice instruction in Hindi: "Please put your thumb on the specified space." When he does that, crisp currency notes roll out of the machine with the voice saying, "Your cash is ready. Please accept it."

The biometric cash machines are custom-made for people who cannot read or write and use features like fingerprint verification and voice guided animated screens and easy navigation.



The federal government has now announced that everybody in Vaishali employed under its ambitious new National Rural Employment Guarantee Scheme will get their wages through these new cash machines.

The biometric cash machines work through a series of processes.

First, the fingerprint of an account holder is captured through a scanner at the time of the opening of the account. A template is created for each fingerprint and stored in the cash card given to the customer.

When the user goes to the cash machine and inserts the cash card, his fingerprint is captured using an inbuilt scanner and it is matched with the impression stored in the cash card.

This application of biometric technology is fundamental because about 70 percent of the Indian population lives in small rural towns.

Payment through cash machines will also protect the workers from local contractors who routinely extract a cut from their wages in return of getting them on the list of government employment schemes.”

This biometric ATM solution allows the poor who can't read to get cash thanks to the voice instructions and it allows them to save some time.

“Biometric banking” in India is developing steadily because the need for more simple and secure ways to handle money is obvious and so, most of the banks invest in these applications. In early January 2007, the State Bank of India (SBI) announced plans to set up 5-6,000 rural kiosks and started a new rural pilot initiative to encourage banking habits among the rural masses. In early February 2007, Dena bank launched a Biometric ATM in Balwa village near Gandhinagar and Andhra Bank announced their plans to open 150 biometric ATMs in India during fiscal 2007-2008. Axis Software Pvt. Ltd and Citibank have launched two biometric automated teller machines (ATMs) in Hyderabad and Mumbai in 2006. The bank intended to set up 25-35 biometric ATMs in the country during 2007.

Bank of Tokyo-Mitsubishi (Japan, 2007)

After 2000, ATM fraud became a very big problem and the estimated loss was too big for the banks to let go. In reaction to that, banks in Japan chose to adopt biometric technology to improve the security of their teller machines. As a result, the Financial Services Agency proposed the standardization of biometric identification systems to confirm account holders' identities when they use automated teller machines.



The Bank of Tokyo-Mitsubishi installed biometrics-based automated teller machines at 267 outlets in 2007 so as to verify the identity of depositors by scanning their palm vein patterns. Unlike South American ATMs, BTMs use a bank card with integrated-circuit chips to store the customer's palm vein data. The technology used in the machines is developed by Fujitsu (see Appendix 2).

In order to use the ATMs the user must first enrol in a BTM office which will provide him with the bank card containing his biometric data. When he wants to withdraw money for example, the user uses his card and then places his hand above the biometric reader which proceeds to the identity verification. The palm vein patterns replace the old PIN codes that were too easy to pirate because people chose too simple codes and which weren't secure enough.

The major commercial bank plans to offer the technology to other banks, including UFJ Bank which will integrate operations with the Bank of Tokyo-Mitsubishi next year, to help them upgrade their security systems.

Suruga Bank, a regional lender based in Numazu, Shizuoka Prefecture, Hiroshima Bank and Bank of Ikeda also adopted Fujitsu's palm-vein technology in 2004 and 2005. In 2006, Suitomo Mitsui Banking Corp. introduced the same system. Today, more than 92 percent of Japan's banks use vein-pattern recognition. Since then, the number of criminal cases has been falling. As a consequence, the amount of stolen money has also been decreasing.

It seems that user acceptance was higher in South America than in Japan where people were reluctant to having contact based systems for hygienic reasons and felt like criminals when asked to enrol their fingerprints.

Biometrics in Japan are becoming a problem with banks using different technology that cannot be unified which creates compatibility problems for grocery stores and other shops which have to install new expensive devices.

There are now over 80,000 biometric ATMs in Japan, currently used by more than 15 million customers.

Woori (South Korea, 2004)

South Korea also started a massive use of ATM using biometrics for the same reasons. For example, Woori, one of the largest Korean banks announced in 2004 that it would use Veridicom's fingerprint technology for more secure banking transactions. The fingerprint sensors are used to authenticate bank customers at bank machines throughout Korea, as well as for banking transactions on the Internet.

Veridicom's fingerprint sensors have been integrated into the bank's ATM and cash dispensing machines across its branch network.

Woori Bank has 750 branches and approximately 15,000 users are enabled for its Bio-Banking Internet service. In addition, fingerprint sensors are being deployed at 4,000 bank machines to secure cash transactions. The integration of the Veridicom sensors was completed by Real ID Technologies, Veridicom's Korean partner who supports the company's technology to a diverse Korean customer base.

5.2 Commercial services/retail

Citibank and Zouk, etc. (Singapore, 2006)

Before it filed for bankruptcy (in 2008), Pay By Touch, the American company had time to develop several services for international firms such as Citibank in Singapore. The customers of Citibank have the opportunity to be premium members and obtain the Clear Platinum card for several exclusive advantages. In 2006, when Citibank launched this card, it also announced a partnership with Pay By Touch (Solidus Networks) in order to allow their users to have access to the biometric payment method. At launch, Citibank Clear Platinum cardholders were able to make cardless credit card transactions at retail outlets such as music and IT stores, as well as clubs, restaurants and cinemas. Participating merchants included Zouk, Gramophone epiCentre, Coffee Bean & Tea Leaf and Shaw Theatre.

This partnership was "Pay By Touch" first step outside of the US, in Singapore.

The service was available free-to-card for Clear Platinum cardholders which were to enrol at specified locations. They only needed a clean fingerprint, a Government-issued Photo ID and

of course the Clear Platinum card. As their American counterparts, participants had to register a 7 digit Personal search number in order to make the process faster and more convenient. When it launched, biometric enrolment kiosks were only available in selected places.

6. Europe & Middle-East

6.1 *Banking*

BPS Bank (Poland, 2010)

At the beginning of summer, Poland's cooperative bank BPS was proud to announce it was the first in Europe to install a biometric ATM in the Polish capital of Warsaw. The bank chose the technology developed by Hitachi which allows the user to withdraw cash using the tip of his or her finger. As with other biometric solutions, the scanned fingertip veins are then compared to the data saved in the database or in the bank card and the machine allows or declines the transaction. Finger veins don't leave a trace and so cannot be reproduced which is more secure than fingerprints. Customers still use the same credit/debit card as before and the biometric authentication serves as an alternative to their 4-digit PIN code. In fact, each user can choose the way he wants to authenticate at their ATM. If he already enrolled his finger vein scans, then the user is able to use biometrics as a password.



The advantage of this technology is also that it doesn't work with fake or chopped-off fingers making it very hard for thieves to lure the system. Another reason why the Polish bank is so motivated by the idea of using biometrics for banking is because of the role of these institutions in Poland. According to one of the bank's representatives, "banks have a responsibility to perform various social functions like dispensing welfare checks and pensions. These cause long queues at the cashier and many people find it inconvenient and even debilitating.

Thanks to Hitachi's research, finger vein scanning is very fast and simple. The application of such technology will help BPS to reduce queues, customers' waiting times and simplify the whole process for them. BPS plans to install a biometric ATM at every one of its branches by the end of the year, where they will also function as a collection terminal for state benefits.

Barclay's Bank (UAE, 2007)

In 2007, Barclays Bank UAE introduced biometric-enabled ATM's in the United Arab Emirates. The provider of the solution and of the machines is the American NCR Corp which will also take care of the maintenance. Here, ATMs use fingerprint scanning for the authentication of the bank's customers. The main motivation was the need of an increased security for banking transactions in the UAE.

At the end of 2007, Barclays' local network included two branches, three service centres and an ATM network. In the Middle-East region which is famous for its innovative and highly technological progress, biometrics is seen as a solution to make transactions in a safer and more convenient way. The goal is to have a working and satisfying ATM network.

6.2 Commercial services/retail

Officecom, EDEKA, METRO, etc. (Germany, 2006)

German firm It-werke has developed the digiPROOF solution at the beginning of the 2000s which can be considered as a virtual EC-Karte that German consumers use for payment.

This payment technology is based on fingerprint authentication. It is developed by Toshiba tec and relies on the biometric characteristics of the fingertip.

This solution is already well implemented in the retail industry. Since 2005, EDEKA allows its customers to pay without a credit card or cash, using the digiPROOF method in all its facilities. The user only has to enrol in the store of his choice and then he can pay by scanning his fingertip at checkout.

In 2006, It-werke innovated again by dematerializing the fidelity system with its iCARD solution. As long as the consumer is authenticated with its fingerprint, all the operations linked to his fidelity program are automatically done. At the end of 2006, more than 450 stores were equipped with It-werke solutions and tens of thousands of consumers had been enrolled.

It-werke's digiPROOF customers include EDEKA (food retailer chain), Globus Warenhaus (supermarket chain), Gewandhaus Gruber (clothes retailer), METRO (hypermarket, high tech retailer, and food retailer chain), Officecom (computer retailer) and Wagener which uses the virtual loyalty feature especially.

Pay by VINGADO (Germany, 2008)

The METRO group also chose It-werke for implementing a new payment method based on biometry. In its "Future Store" METRO evaluates customers' response to

innovation before implementing new technology in its main shops (“real-,” and “Extra”). Among the pilot projects is a new version of digiPROOF: “Pay by fingerprint”.

This new biometric payment method allows all METRO group stores and brands to use a single fingerprint database. It would allow the customer to enrol only once and pay without card in more than 650 stores: more than 400 “real-,” hypermarkets in Germany, Poland, Romania, Turkey and Russia and about 250 “Extra” supermarkets in Germany.

In 2010, It-werke launched its “pay by VINGADO” service which creates a unique database for all the stores using the solution.

With VINGADO, It-werke offers its customers the access to its large database and the possibility for end users to enrol only once in one of VINGADO Issuing Partners (VIP) for all of them. Contrary to the first solution used by EDEKA, VINGADO is available for any store in Europe. This solution uses It-werke’s digiPROOF technology so the way it is used does not change. The solution provider promises that biometric data isn’t mixed with personal consumer data and guarantees a very high privacy and security. Because it launched very recently, we do not have information about VINGADO’s first users.

As Le Monde noted in 2007, interestingly enough the average biometric payment user is over 40. It seems that it is more convenient for those who have trouble remembering their PIN code or need to look for it in their bag for example.

Carrefour and several other hypermarket chains in France are actually implementing or piloting biometric solutions of access control to their stocks for their employees and partners or timesheet management. This could allow them to increase their productivity and secure their facilities.

7. Main teachings

This deliverable shows that commercial biometric applications are unequally spread all around the world. There seems to be more applications in Asia and in South America than in Europe and the USA. The contrast is even bigger if we consider each country one by one with European having almost no applications on their land and Japan and Korea which have accepted the idea of biometrics for a long time especially in the banking sector.

Our methodology also allowed us to compare each continent and each country in terms of potential for biometric development and user acceptance of such technologies. There most certainly are cultural and social reasons which explain the high presence of biometrics in Asia and the fact it is easier to implement. Here is a comparison between the three studied zones in terms of biometrics in banking and commercial services/retail:

	America		Asia		Europe & Middle-East	
	Banking	Commercial services /retail	Banking	Commercial services /retail	Banking	Commercial services /retail
Country of application	<u>USA (2)</u> <u>Colombia (1)</u>	USA (1)	<u>Japan (1)</u> <u>India (1)</u> <u>Korea (1)</u>	Singapore (1)	<u>UAE (1)</u> <u>Poland (1)</u>	<u>Germany (2)</u>
Application date	Colombia: 2002 - ... USA: 2006 - ... USA: 2010 - ...	2002 → 2008	Japan: 2004 - ... Korea: 2004 - ... India: 2007 - ...	2006 → 2008	UAE:2007 - ... Poland: 2010- ...	Germany: 2005 - ... Germany: 2010 - ...
Application results	<u>USA: 1 Pilot - 1 Deployed</u> <u>Colombia: 1 Deployed</u>	1 failure	<u>3 deployed</u>	1 failure	<u>UAE 1 deployed</u> <u>Poland 1 pilot</u>	<u>Germany: 1 pilot 1 deployed</u>
Type of technology used	1 Fingerscan (contactless) 2 fingerprint	1 fingerprint	1 palm vein scans (contactless) 2 fingerprint	1 fingerprint	1 finger vein scans 1 fingerprint	<u>2</u> fingerprint
Main motivations	Security & new product to reach new customer	Simplicity to use	Simplicity, easiness to use, security, fraud reduction	Simplicity, easiness to use, security	Security, easiness to use, reducing queuing	Easiness to use, homogenous solution
Deployment scale	City, state, country	Country	State, Country	City	City, Country	Country
Advantages	secure, convenient, less fraud, faster, new customers, no card needed	Faster and more simple checkout	very simple, faster, more secure and convenient	Faster and more simple checkout	faster method, contactless, no more PIN code, more secure and convenient	more convenient, no card needed, unified fingerprint database
Drawbacks	Needs clean intact fingerprints, different solution owners in 4 years, needs clean good quality fingerprints, high user reject rate	Solution provider's liability, 7-digit search code needed, need good fingerprint quality	Targeted to people likely to have worn hands, compatibility problems between the different solutions, Solution provider's liability, reliability, need good fingerprint quality	Solution provider's liability, 7-digit search code needed, need good fingerprint quality	maintenance by NCR could create delays, need good fingerprint quality	enrolment needed for each retailer group, need good fingerprint quality need good fingerprint quality



Solution provider	Hawk Systems AllTrust Networks NCR Corp.	Pay By Touch	Unknown Fujitsu Real ID Technology	Pay By Touch	Hitachi NCR Corp.	It-werke (2)
Equipment provider	Unknown MorphoTrak NCR Corp.	Pay By Touch	Unknown Fujitsu Veridicom	Pay By Touch	Hitachi NCR Corp.	It-werke (2)
Size of the company using the solution	<u>FU</u> : 26 full-service offices and a Customer Service Centre in the New York Metropolitan Area <u>Zions</u> : 500 offices and 600 ATMs in 10 Western states <u>BC</u> : 5 th largest bank in Colombia, 1300 ATMs	182 Jewel Osco stores and Shell fuel stations across the USA	<u>CB</u> : 3563 branches and 195 extension counters <u>BTM</u> : 772 domestic branches <u>Woori</u> : 2 nd Korean bank in terms of asset size	One of the biggest banks in Singapore <u>Zouk</u> is a nightclub and Gramophone a chain of 7 music retailers <u>Epicentre</u> sells high-tech products and has 6 outlets in Singapore	<u>BPS</u> : unites 359 credit unions, accounts for more than 60% of banks in the cooperative sector <u>Barclays</u> : operating in over 60 countries	<u>OEM</u> : 1 Officecom shop, <u>EDEKA</u> 12,000 stores <u>METRO</u> 2,100 outlets in 34 countries

The first element we can see is that one of the first commercial biometric applications was Pay By Touch's payment method in the USA. Biometrics-enabled ATMs were launched the same year in South America and especially in Colombia for the first time. Then, Japanese banks decided to fight credit card fraud with the installation of more secure ATMs using Hitachi's finger vein or Fujitsu's palm vein technologies between 2004 and 2006. Pay By Touch continued its development outside the USA (in Singapore for example) during the same period. One year earlier, It-werke had launched its Pay by fingerprint service as a pilot in selected EDEKA or METRO stores and in single shops. They even improved the technology they provided by implementing fidelity management. The UAE and India felt the need to provide their inhabitants with biometric ATMs for different reasons such as security or convenience in 2007. Finally, in 2010, the USA and Europe start piloting and implementing biometrics in their ATMs long after Japan and South America. In the retail sector, It-werke launches its VINGADO service which creates a unified fingerprint database for all the solution users.

If we analyse the chronological order of the development of biometrics in banking, we observe that biometrics-enabled ATMs first appeared in South America then in Japan and Korea and a little after in the UAE. After being the first to pilot biometrics just before 2000, the USA and Europe finally start to consider a real application of the technology they have been developing (fingerprint recognition, iris scanning, etc). Japanese firms such as Hitachi or Fujitsu seem more technologically advanced than their European and American counterparts. But, we can note that most of the solution providers are based in the USA, and with NCR Corp. being the biggest ATM suppliers in the world, American firms account for most of biometric banking market share.

Thanks to the BanCafe Colombian example, we can say that it is crucial for companies applying the biometric solutions to be patient and motivated whether it is financially or even in the literal sense of these words. Biometrics isn't a mature technology; it keeps evolving to provide the best service to the banks and the retailers using it. At first, BanCafe had to cope with very high reject rates for its customers but, by pursuing its pilot applications, it showed that firms which are really focused on biometrics could create a working and popular system. BanCafe showed great confidence in NCR Corp the provider of both the solution and the equipment. In the end, technology evolved and the machines became more and more efficient dividing the customers' reject rates by more than three. Of course, in order to do mid or long term investments, you need to be financially powerful and be able to take the time needed for a successful application of biometric technology. The solution provider also needs to be financially healthy and support these long term investments. For example, Pay By Touch which filed for bankruptcy after selling biometric solutions for 6 years was a Silicon Valley start-up. We can wonder if the mismanagement which conducted to its bankruptcy could be explained by the lack of experience and knowledge of the company's managers and by the small size of the firm in itself.

Besides the maturity of the technology and the involvement of the firm, the unequal distribution of biometric solutions around the world might possibly be explained by cultural and legal factors.

In Japan, people are very reluctant to have contact-based biometrics because of hygiene matters. As a result, Fujitsu and Hitachi were forced to develop contactless hand and finger vein technology in order to begin the application of biometrics in the ATMs.

In Europe where there are almost no biometric applications, data privacy and security legislation is a very limiting factor. The French CNIL is very strict to make sure that civil liberties and privacy is guaranteed, the legislation about fingerprint is very demanding for firms which develop them and those wanting to implement them. It is almost the same in the other European countries and for the EU.

Pay by VINGADO is a biometric payment system based on a unified European database. The firm guarantees the privacy and the security of the fingerprint data it stores, but we may wonder if the German legislation is more lenient in terms of data management than its French counterpart. It could explain why Germany is a lot ahead of the other European countries in terms of commercial biometric applications.

It seems that the density of biometric applications very much depends on the legislation and consumer acceptance of the technology in each country.

8. Conclusions

After detailing how we did the survey of the applications, we will now explain how we plan to continue our study for the next deliverable.

Firstly, we will define the topic and the scope of the study with BEST Network members. Then, we will define the main advantages, drawbacks and shortcomings of biometrics solutions to be used. Secondly, we will conduct exploratory research to understand and evaluate current and future technologies and services available for biometric commercial applications, the state-of-the-art in the implementation on such solutions. Then, we will proceed to the third stage of our research: from a sample of carefully selected experiments, we will conduct an exploratory survey based on in-depth personal interviews in order to understand their perceptions of biometric commercial applications, the organisation of the project, the actors involved as well as their expectations and the expected technical and business implementation issues.

We have identified potential sources of information that have and will help us building the state-of-the-art and illustrate business logics:

- 1- Secondary data, collected from companies web sites and electronic databases (reports, surveys, articles).
- 2- Primary data based on in-depth interviews of people in charge of commercial biometric projects.
- 3- In-depth interviews of members of the selected projects. The companies we came in contact with were put in focus because they were active partners on projects that seemed relevant to study due to their nature and objectives which were quite similar to ours.

9. References

→ 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

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

AllTrust Networks

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

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

X

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

<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://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.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.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/>

10. Appendix

Appendix 1: PayCheck Secure

How Paycheck Secure Works...

Signing up to cash checks using Paycheck Secure is quick and easy. Customers simply provide a photo ID; two finger scans, and a smile for a digital photograph. In about one minute, the customer can be ready to cash checks in your store or any store in your chain.

When the customer returns to the store to cash a check, all they need to do is put their finger on the scanner, and the fingerprint scanner verifies the customer's identity. The customer's complete check cashing history appears on the screen, and Paycheck Secure provides clear recommendations about whether you should accept or reject the customer's check. The entire process takes as little as 15 seconds.

Enrolling in Paycheck Secure

Customer hands clerk a photo ID.

The clerk scans the front and back of ID, and the information is entered automatically in the Paycheck Secure system. No data entry required.



Take the customer's picture.

Using the PC camera, the clerk takes a digital photo of the customer. The customer's picture will appear on screen every time they cash a check, so you can easily verify their identity.



Customer scans fingers.

The customer's two index fingerprints are captured. Using fingerprints is much safer than passwords or PINs, because fingerprints cannot be lost, stolen or duplicated.



Cashing Checks with Paycheck Secure

Customer scans a finger and their record appears.

The customer places either index finger on the finger scanner. Within seconds, the customer's picture, driver's license and check cashing history appear on the screen.



Run customer's check through the scanner.

The bank account and routing information will automatically be entered into the system. Paycheck Secure detects correct MICR levels so it will not populate data from any suspect checks.



Enter check number and date.

You can tell Paycheck Secure to automatically reject checks that fall outside dollar amounts or date limits you set. And the system automatically calculates check cashing fees for you.



Appendix 2: Fujitsu's hand vein technology

Palm Vein Pattern Biometrics Authentication System

World's first "Contact-Less" palm vein pattern biometrics authentication.

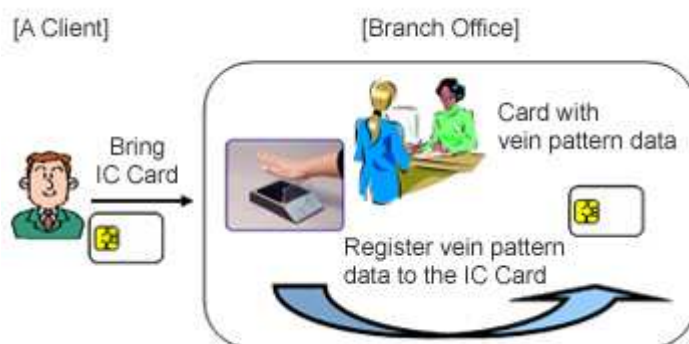


- The pattern of blood veins is unique to every individual and will not vary over the course of a person's lifetime.
- The fact that this pattern lies under the skin makes it almost impossible for others to read, so palm-vein pattern biometrics are essentially secure method of verification.
- High authentication precision: Fujitsu's sampling test showed a result that false acceptance rate was 0.013%.

Fujitsu's Solution

Register the vein pattern data

A client registers the vein pattern data onto the IC card.



Transaction using IC Card with vein pattern data

A client inserts the IC Card onto which vein pattern was registered in advance. A client can make a financial transaction only when verified by the authentication device at the branch office or ATM.

[A Client]



1. Bring IC Card →
2. enter one's PIN →
3. put palm over the device →

[Branch Office]



[ATM]



Appendix 3 : Biometrics regulation of the French CNIL (Commission Nationale de l'Informatique et des Libertés)

Biometric IDs

- [Biometric visa or VISABIO](#)
- [Biometric passport](#)
- [Research programmes](#)
- [Voice recognition and vein pattern recognition](#)
- [An analytical scale for the use of fingerprints](#)
- [Cross perspectives on the analytical scale](#)

Biometric visa or VISABIO

On 10 July 2007, CNIL issued an opinion (Decision No.2007-195) on a draft decree referred by the Ministry of Home Affairs, relative to the creation of a master record of foreign nationals applying for a visa.

The new biometric visa system called VISABIO, implementing the experiments conducted since 2004 under the BIODEV pilot project, should concern over two million foreign nationals from countries subject to visa obligations each year. The system under consideration provides for the collection and retention of biometric data in a centralised base (digitised facial photos and ten fingerprint scans), combined with identity data previously collected during the visa application procedure.

While noting that the use of biometric data may offer strong benefits to check the identity of ID card holders and authenticate IDs, the Commission felt however that the system should be framed by strict guarantees. CNIL regretted in particular that no consideration was given to the possibility for card holders to simply retain their own biometric data on their personal ID card, an option that would raise fewer problems from the personal data protection point of view, since in this case, only the data subjects own the device onto which their personal data are recorded.

The Commission also stressed that the collection of fingerprints of minors from the age of 6 could not be regarded as a mere technical measure and that its very principle deserved to be broadly debated.

Biometric passport

The issue of biometric passports was referred by the Ministry of Home Affairs to CNIL for review in the autumn of 2007 and the Commission issued its opinion on the draft decree on 11 December 2007 (Decision No.2007-365).

The decree intends for France to be in a position, prior to 28 June 2009, to issue passports fitted with an electronic component containing not only the digitised facial picture but also images of two fingerprints, in compliance with the provisions of the European Council Regulation of 13 December 2004.

Concurrently, it provides for the retention of the passport applicant's digitised facial and eight-fingerprint images in the existing passport management record called "DELPHINE", which would lead to significant changes to this database.

The Commission expressed a number of reservations about this project, finding that the system under consideration would lead to the implementation of the first centralised bank of biometric data on French nationals for administrative purposes.

CNIL reminded in particular that processing of such data, in an automated and centralised form, would be acceptable only to the extent that it may be justified by a compelling necessity linked to national security or public order.

In this respect, the Commission considered that the purposes claimed, however legitimate, i.e. improving the procedures for issuance and renewal of passports along with combating ID

fraud, failed to justify the national-scale retention of biometric data such as fingerprints, and that the type of data processing involved would cause excessive prejudice to individual liberties.

Furthermore, the retention of digitised facial and fingerprint images in a central database appears disproportional with the purposes, in spite of assurances from the Ministry of Home Affairs who stressed that it would be impossible to conduct any identification searches from the digitised fingerprint images (i.e. it would not be possible to retrieve civil registry data on individuals based on their fingerprints) and that the system contained no facial recognition device based on the digitised photos (i.e. it would not be possible to retrieve civil registry data on individuals based on their facial image).

Lastly, CNIL regretted that this new procedure framework was to be defined via a regulatory rather than legislative process (i.e. Government decree versus law voted by Parliament), since the changes introduced by this draft decree are much more substantial than actually required by France's European commitments. The scope of this reform and the significance of the issues at stake would undoubtedly have justified a law to be proposed before Parliament, enabling a broad public debate on the subject.

Research programmes

On 18 January and 4 October 2007, CNIL authorised for the first time three research programmes in the field of biometrics. The first 2 approvals concern public research projects submitted by the University of Evry Val d'Essonne and the Groupement des Ecoles de Télécommunications (GET). These programmes address the following topics :

- assessment of biometric recognition processes;
- compilation of "multimodal" biometric databases, i.e. combining the use of several biometric techniques (2D and 3D facial images, iris, fingerprints, hand geometry).

The third authorisation was granted to a European project coordinated by Sagem Défense Sécurité in a consortium with 12 partners. The purpose of this research project is to improve 3D facial recognition systems and the security of biometric data.

These research programmes, relying on volunteer participation, are of major importance since they provide CNIL with sources of reliable assessments on state of the art techniques. The reports published on research findings will be made available to the Commission.

Voice recognition and vein pattern recognition

In 2007, CNIL also investigated its very first request for installation of a voice recognition system, designed to secure and facilitate the management and resetting of passwords used to access the IT system at Michelin. The process can generate and reset the passwords automatically, in particular in the event of forgotten passwords. The Commission reviewed the system to ensure that adequate information was supplied to the personnel and that all efforts were made to guarantee data security and prevent any risks of identify theft.

Similarly on 8 November 2007, CNIL reviewed for the first time five devices based on finger vein pattern recognition (VPR) designed to control access to premises or IT systems. Following an in-depth technical expertise of the vein recognition technology, the Commission reached the conclusion that, in view of the current state of the art, vein pattern recognition is a traceless biometric process generating data that can be recorded in a database without any particular risks in terms of data protection.

An analytical scale for the use of fingerprints

CNIL issued its very first opinion in 1997 regarding a device based on fingerprint recognition. A decade later, the Commission felt it was necessary to clarify its position on the subject.

A document was therefore published recently, presenting the major criteria grounding the Commission's decisions to authorise or reject the use of systems based on fingerprint recognition with recording of data in a scanning/matching device or on a server.

The analytical scale derives from the following observations:

- fingerprinting is a traceable biometric process. Each person leaves traces of fingerprints in most circumstances of daily life (e.g. on a drinking glass, a door handle, etc.), which can be exploited with variable ease;
- such “traces” may be captured unbeknownst to data subjects and may be used among other for purposes of identity theft (a copy of the fingerprint can be used to fraudulently deceive a fingerprinting recognition device).

Consideration for these characteristics and for their related risks has led CNIL to differentiate between the various devices based on the fingerprint storage method:

- Storage on an data subject device (e.g. chip card or USB key) = limited risk since the data subjects keep full control over their biometric data which cannot be used for identification purposes without their knowledge.
- Storage in a scanning/matching device or on a server = higher risk, since data subjects lose control over their data held by a third party. In the event of intrusion into the system, all fingerprint data can be accessed.

Accordingly, the Commission does not authorise the use of devices based on fingerprint recognition with data recording in a database, unless the use of such devices is duly justified by compelling necessity of security and fulfils the following four prerequisites :

- the purpose of the device must be restricted to access control for a limited number of persons to a specifically delimited area constituting or containing a major concern over and above the basic interests of the organisation, such as protection of physical integrity of persons, property and facilities, or integrity of certain data.
- proportionality: it is important to know whether the proposed system is the most suitable for the previously defined purpose with regards to any risks it may involve for personal data protection and as compared with other potentially usable systems;
- security: the device must enable both a reliable authentication and/or identification of data subjects and offer all guarantees of security to prevent any data disclosure;
- information of data subjects : it should be conducted in full compliance with the Data Protection Act and, as appropriate, with the Labour Code.

Cross perspectives on the analytical scale

François Giquel

Vice-President, Honorary Legal Counsellor to the Cour des Comptes
Commissioner in charge of the Justice sector

Didier Gasse

Legal Counsellor to the Cour des Comptes
Commissioner in charge of Telecommunications & Networks and European & International Affairs sectors

What were the triggering factors that drove the Commission to clarify its doctrine on fingerprint databases?

F. Giquel : In view of technological breakthroughs in biometrics and of the diversity of circumstances, it was felt essential to clarify, as a reminder, the main criteria used by CNIL to investigate applications for authorisation.

It was also necessary to help companies, public administrations or local authorities considering the installation of such systems to ask themselves the relevant “Data Protection”-related questions prior to the decision making and application filing processes.

What justifies such special attention from the Commission to this type of devices?

D. Gasse : Unlike any other identity-related data or any other personal data, biometric data are not assigned by any third party or chosen by the data subject: they are generated by the

human body itself, they designate or represent the human body as unique and immutable, unlike any other. Such data therefore belong to the person who generated them.

Hence, it is easy to understand that any possibility of misuse or misappropriation of these data would engender a major risk for that person's identity. Entrusting a third party with your biometric data and allowing that third party to retain them is therefore never a trivial or inconsequential matter, particularly since fingerprints are traceable biometrics that can be captured and used without the person's knowledge.

What are the criteria selected by the Commission to evaluate the proportional nature of a system based on the recording of fingerprints in a database?

F. Giquel : As a general rule, the purposes of fingerprint storage in a database can always be achieved via a different technology based on fingerprint storage on an individual device (e.g. smart card). Nevertheless, a centralised database may be of benefit whenever access must be provided at any time and immediately, or to respond to emergency situations requiring a timely intervention.

D. Gasse : It should also be noted that, whenever we deal with situations where security is the key issue, we also look at the relevance, adequacy and non-excessive nature of fingerprint database systems, as compared with the number of data subjects: the more restricted the area and the smaller the number of data subjects, the more limited are the drawbacks of fingerprint databases.