Warsaw, 2016

Report

Biometrics in banking – key aspects

Związek Banków Polskich

FORUM TECHNOLOGII BANKOWYCH

CENTRUM PRAWA NOWYCH TECHNOLOGII

Editor:

Tadeusz Woszczyński

Co-authors:

Michał Czechowski, Łukasz Hnatkowski, Artur Krystosik, Zbigniew Marcinkowski, Mariusz Sudoł, Jarosław Wójtowicz

Table of contents

Table of contents 1
1. INTRODUCTION 2
2. RECOMMENDED AREAS OF USING BIOMETRIC TECHNOLOGIES 3
3. BIOMETRICS IN THE POLISH BANKING SECTOR (DETERMINANT FACTORS, IMPLEMENTATIONS) 4
3.1. IMPLEMENTATIONS, STATISTICS, BUSINESS BACKGROUND 4
3.2. LEGAL ASPECTS 6
4. BIOMETRIC TECHNOLOGIES IN BANKING 7
4.1. FINGER VEIN BIOMETRICS 7
4.2. VOICE BIOMETRICS 8
4.3. HANDWRITTEN SIGNATURE BIOMETRICS 9
4.4. OTHER BIOMETRIC TECHNOLOGIES IN BANKING, LESS COMMONLY USED IN EUROPE 10
5. CRITICAL PARAMETERS OF CHOOSING THE RIGHT TECHNOLOGY FOR A SPECIFIC USE 12
6. RESISTANCE TO FRAUD, SECURITY MECHANISMS, THREATS, EXCLUSIONS 14
7. BENEFITS 16
8. BIOMETRICS VS. ELECTRONIC SIGNATURE 17
9. CONCLUSION 18
10. AUTHORS 19
10.1. EDITOR 19
10.2. CO-AUTHORS 19
10.3. SUPPORT FOR INTERNATIONAL VERSION 19

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

1. INTRODUCTION

The development of modern technologies used in banking, the increasing automation which enables simplifying, raising the efficiency and transparency of banking processes, the continuing need for minimising the operating risk are just a few examples of phenomena related to the fundamental – and yet still relevant and challenging – **obligation of banks** to **ensure the safety** of deposits held with them, protect information covered by banking secrecy, apply appropriate security measures for ICT systems and banking operations performed using such systems.

> Market practice shows increased interest in new security methods

Despite the development of various security systems, the risk analysis suggests that the currently used measures are still not fully satisfactory. This is why market practice shows **increased interest in new security methods**.

Our experience shows that only 5 years ago bankers perceived biometric technologies as an interesting "technological innovation", which might come into use in some distant, undefined future. Yet today, **the use of biometric technologies is a fact**.

It turns out that **over 30 banks in Poland** perform selected banking processes using biometrics, and providers of biometric technologies are conducting talks about the possibility of using such technologies with nearly every bank.

The goal of this white paper is to present an outline of the most useful biometric technologies with a view to preparing a strictly **practical document to be used by senior management**. It is another document prepared by the Biometrics Group, which has been operating in the Bank Technology Forum (FTB) of the Polish Bank Association since 2007. Unlike other documents we have published previously, this one is not intended to be a thorough, exhaustive report. This time our intention was to prepare a short paper presenting the **elementary yet important information** addressed at decision makers who consider the use of biometric methods in their organisations.

Individual biometric methods have been selected based on market trends we have observed and taking into account biometric features that are expected to offer **the most universal, interesting and socially acceptable application, increasing the security level in banks**.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

2. RECOMMENDED AREAS OF USING BIOMETRIC TECHNOLOGIES

The image below presents our recommendations concerning the application of individual biometric technologies in specific functional areas of a bank:

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

3. BIOMETRICS IN THE POLISH BANKING SECTOR (DETERMINANT FACTORS, IMPLEMENTATIONS)

3.1. IMPLEMENTATIONS, STATISTICS, BUSINESS BACKGROUND

Fig. Advertising campaign of biometric ATMs of the Planet Cash network
Source: IT Card S.A.

In 2007, a Biometrics Group was established in the Bank Technology Forum of the Polish Bank Association, with a view to educating the banking sector about biometric applications. In 2009, thanks to intensive efforts of the group, the Polish Bank Association and biometric solution providers, the first banks decided to test the use of biometrics in ATMs. They were Podkarpacki Bank Spółdzielczy (PBS) and Bank Polskiej Spółdzielczości (BPS).

In 2010, PBS was the first bank in Europe to implement a biometric technology (more specifically: finger vein recognition) in their ATMs to facilitate withdrawal of social security benefits. Currently, the bank offers biometric solutions (finger vein) to all its clients. The biometric functionality is implemented throughout the network of ATMs (biometric withdrawals without a card) and bank branches (authorisation of operations in a branch). The cooperative banking sector is currently the largest recipient of biometric solutions in Poland. Apart from PBS, biometric solutions are used by clients of such banks as Krakowski Bank Spółdzielczy, Bank Spółdzielczy in Kielce, Bank Spółdzielczy w Radzyniu Podlaskimand many others.

In June 2010, Bank PEKAO SA introduced biometric readers for its corporate clients, based on fingerprint biometrics with PKI cards. Since that time, clients using the PekaoBIZNES24 online transaction platform have been able to log in to the system and authorise orders based on their fingerprints.

> In 2009, first banks decided to test the use of biometrics in ATMs

In September 2012, Bank BPH S.A. introduced biometric authentication in all of its branches. The bank's clients can have their identity verified and authorise bank teller transactions using their fingers (finger vein technology). According to BPH, more than 55% of bank customers are using Finger Vein. Currently, Bank BPH is implementing the solution in the entire franchise chain, and biometrics has become the main authentication method in the bank.

The same solution was deployed in 2013 by Getin Bank in all its new branches. In February 2014, Getin Bank introduced pilot of the revolutionary Getin Point virtual teller machines, enabling clients to log in to their accounts, authorise operations and sign documents using finger vein biometrics. Biometric signatures were also

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

implemented in traditional branches, where biometrics had been applied before.

In May 2014, IT Card S.A. announced the launch of the first independent network of biometric ATMs in Europe: Planet Cash. In February 2015, Bank Smart announced the introduction of voice biometrics for logging in to the mobile banking system.

Voice biometrics is also used by Meritum Bank. Meritum Bank and Bank Millennium introduced the possibility of logging in to the mobile banking system using a smartphone fingerprint reader.

In April 2015, one of the largest banks in Poland, Bank Zachodni WBK, introduced in its branches, on a pilot basis, a biometric signature solution based on finger vein biometrics. Clients of BZ WBK in Lubin and in selected branches in Warsaw, Wrocław and Poznań, were able to have their identity verified and to sign agreements with the bank related to personal accounts using their fingers. In November 2015 BZ WBK has introduced voice biometrics in call centre channel.

In June 2015, PKO BP announced its research project, prepared in cooperation with the Gdańsk University of Technology. The bank wants to develop a solution enabling its clients to confirm their identity with their voice, palm or face image instead of a PIN or password. The first results are expected in 2018.

There are already over 1300 biometric ATMs in Poland: 300 belonging to the cooperative banking sector (BPS Group and SGB), and 1000 to the independent network Planet Cash. In the following months, the Planet Cash network will increase the number of biometric ATMs to 1780.

The higher the popularity of biometrics among clients, the easier it is for the bank to limit frauds

The higher the popularity of biometrics among clients, the easier it is for the bank to limit frauds

Bank BPH has 256 branches with biometric readers (ca. 1700 readers). Biometric readers will also be introduced in approx. 172 partner branches in 2016. Bank BPH already has over 266 thousand clients who use Finger Vein biometric features actively, and the PBS bank – ca. 30,000 clients. Biometric solutions have been implemented in Poland in 6 commercial banks and in over 30 cooperative banks. It is anticipated that the number may at least double in 2017. Banks announced a number of procurement proceedings and pilot programmes to apply biometrics in call centres, mobile banking, online banking and in branches. According to public opinion surveys ordered by two leading commercial banks in Poland (in 2010 and 2013), the acceptability of using biometrics (more specifically: finger vein biometrics) in bank branches amounted to ca. 85%.

The main reasons for the popularity of biometrics in Poland are increased threats and the increased number of frauds in banks. By using biometric solutions in bank branches to authenticate operations performed both by clients and branch employees, a bank is able to eliminate internal frauds in branches, which are becoming an increasingly common problem, almost completely. The higher the popularity of biometric technology among clients, the easier it is for the bank to limit frauds committed using stolen documents or resulting from false identity (e.g. a forged ID card). The use of biometrics together with an electronic signature for signing docu-

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

> Projects implemented in Poland were widely discussed not only in our country, but all over the world

ments can significantly reduce their costs (including the cost of paper, printouts and archiving). Cooperative banks have streamlined the work of their branches by moving withdrawals of social security benefits to biometric ATMs and limited the costs of card withdrawals by introducing "finger withdrawals". Voice biometrics is a convenient tool in contacting a bank through the call centre, at the same time reducing fraud risk. The marketing aspect of introducing biometric solutions should not be overlooked. Projects implemented in Poland were widely discussed not only in our country, but all over the world.

3.2. LEGAL ASPECTS

The process of analysing the permissibility of using biometric technologies under applicable legal provisions plays a critical role for the possibility of using and implementing these technologies. Such analyses should be prepared on a case-by-case basis for each planned implementation.

Due to the nature of biometric data, work performed so far includes analyses concerning public law, for example related to personal data protection regulations, and (in more advanced projects) private law – due to the necessity of ensuring legal validity of declarations of will made using a specific technology.

Based on experience gained with respect to completed projects, management boards of banks have a positive attitude to the analyses conducted so far. To the best of the authors' knowledge, a selected scope of implementation of a biometric technology in a bank operating in Poland was also inspected by the Inspector General for Personal Data Protection, who issued a positive opinion in this matter.

It should be emphasised, however, that each assessment of permissibility of using a particular biometric technology should involve – apart from a detailed analysis of legal norms – a thorough analysis of the facts, including a detailed description of biometric data to be applied, a specification of the scope and manner of using biometrics, processes for which it should be applied, influence of the selected biometric method on the privacy of biometric system users, technical aspects and safety considerations, as well as the manner of implementing such a technology by the provider.

It seems that a successful implementation requires conducting a comprehensive analysis covering, among other things, all the indicated areas necessary for legal assessment of the permissibility of the given implementation and regular cooperation with the provider of the biometric technology.

This is why, when assessing legal risks, it seems reasonable not only to assess the legal (regulatory) permissibility of using a given biometric technology and the cost effectiveness of the given solution, but also to consider the experience and resources of the given provider of biometric technologies and to assess implementations performed by such a provider. When modifying processes such as identity authentication, which are extremely important for the bank's operations, it is not possible to neglect practices proposed by the providers and shape these processes without applying such practices.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

Furthermore, a comprehensive approach to the project and legal analysis provides more assurance to the bank that the provider's commitments under implementation agreements will be met on time and in due manner, which is critical for a successful implementation.

4. BIOMETRIC TECHNOLOGIES IN BANKING

Biometric technologies are gaining popularity and their scope of application is expanding. Every year new biometric technologies are introduced, using various unique physical or behavioural human features. The best-known biometric technologies in the world are, without doubt, facial and iris recognition and fingerprint biometrics. None of these technologies, however, is commonly used in banking in Europe or in Poland. A biometric technology used in the banking sector must have all the following features:

- High security
- Protection of privacy
- High social acceptability
- Practicality and ease of use
- Universality

Based on market trends observed in Poland, three technologies have been selected and described in detail in this chapter, namely:

- A technology that is most frequently implemented in Poland in branches and ATMs (finger vein biometrics),
- A technology that a number of banks in Poland plan to implement or have implemented in call centre and mobile banking solutions (voice biometrics),
- A technology that attracts banks' attention but still raises many doubts (handwritten signature biometrics).

It should be emphasised that the selected technologies are considered in the context of client-bank relations.

> Biometric technologies are gaining popularity and their scope of application is expanding

4.1. FINGER VEIN BIOMETRICS

Finger vein biometrics uses **the unique pattern of blood vessels inside a human finger**. The uniqueness of this technology was proved with comprehensive medical research. The research proved the universality of the finger vein biometrics, which means that it can be used by everybody, regardless of race and age, which was a problem in other biometric technologies (e.g. iris recognition biometrics). The blood vessel pattern used in the authentication process does not change over time, unless it is affected by a disease. The blood vessel pattern is captured by illuminating the finger with near infrared light, which is harmless and widely used in medicine. During enrolment, a unique, biometric reference template is created. The biometric template is created unidirectionally and does not contain any sensitive data. During biometric verification, a living finger is compared with the previously recorded reference template in real time. As the biometric data is inside human body, this technology ensures protection of users' privacy, which has been confirmed by a number of personal data

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

protection organisations (e.g. CNIL in France). The key advantage of this technology is the high social acceptability, which amounts to ca. 85% in Poland, as confirmed by many surveys.

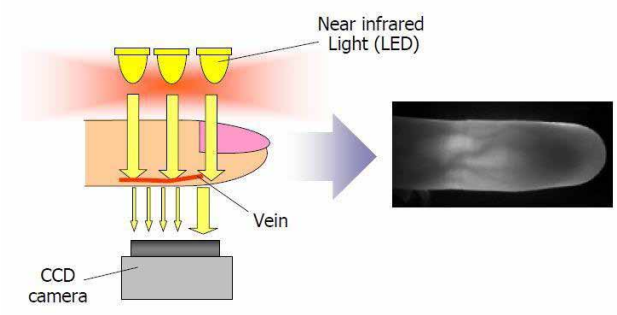


Fig. A unique pattern of blood vessels in a finger used in the finger vein authentication technology

The finger vein authentication technology was created in the late 1990s in Japan. It was developed and patented by the Japanese company Hitachi. The main goal of this technology was to create an alternative for fingerprint biometrics, which – due to many flaws and controversies – did not catch on in the Japanese society. The finger vein biometrics has been used in the largest banking projects around the world. In Japan, it is used in 293 banks (including Mizuho Bank, SMBC, Japan Post Bank, Bank of Kyoto, CITI, HSBC, etc.) and implemented in over eighty thousand ATMs. It is used by over 50 million bank clients in Japan. In 2010, IS Bankasi deployed over 3000 biometric ATMs ("Biyokimlik") based on the finger vein technology. In 2014, Barclays announced that it would implement the finger vein technology in corporate banking and provide tens of thousands biometrics readers for corporate customers in 2016. Since 2009, the technology has been used in Poland. It has been implemented and developed by 2 commercial banks (BPH SA and Getin Bank) and by ca. 30 cooperative banks. Poland also has the first independent network of biometric ATMs employing the finger vein technology – Planet Cash. In 2015, the BZ WBK bank launched a pilot implementation of finger vein biometric readers with touchscreens for clients in six branches for the purposes of signing documents.

4.2. VOICE BIOMETRICS

"At my bank, my voice is my password" – this is what an access password in a modern bank IVR system can sound like instead of a telephone PIN. The password is the same for everybody, so there is no need to keep it secret.

Eliminating IVR services has been a popular trend recently, and voice biometrics can be extremely helpful in such a situation as well. If the client agrees to the creating of a voice profile, he or she will be authenticated automatically during a normal conversation with a consultant, without the need to use a voice password in the IVR system. This voice biometric method is used today by such banks as Tatra Banka, Barclays or, recently, by the Eastern Bank from the US.

Fig. Voice biometrics

Voice biometrics is also a popular feature in mobile applications, as an alternative for PINs or an additional security feature for accessing mobile banking services. The best solutions allow users to use one biometric profile in more than one channel, e.g. a profile created for the IVR system can also be used in mobile banking.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

More and more banks around the world are using voice recognition to identify their clients, since voice is a unique feature that ensures high security and convenient access to services. Examples include the ING bank in Romania, Tatra Banka in Slovakia or Barclays in the United Kingdom.

> The number of abuses is constantly growing, and call centre is accessed not only by our clients, but by impostors as well

Today this is the only practical and effective biometric identification method available for remote communications.

According to a survey conducted by TNS in Poland in November 2014, 54% of the respondents would be willing to use voice biometrics instead of passwords or PINs, and 23% have no opinion on this matter, which means that they could be persuaded to use voice verification with appropriate education measures. This is very good news for all institutions in Poland that plan to implement voice biometrics. Compared to polls conducted in other European countries, the results of the Polish survey are significantly better.

Voice biometric solutions perform well not only in the area of client authentication, but are also used with increasing frequency in anti-fraud processes. The number of abuses is constantly growing, and the call centre is accessed not only by valid clients, but by impostors as well. Apart from threats from organised crime groups operating in the area of electronic banking, there are also crime groups that attack call centres. Thanks to voice biometrics we can effectively prevent such attacks, using recorded call cenrte conversations.

4.3. HANDWRITTEN SIGNATURE BIOMETRICS

Handwritten signature biometric solutions normally use only a couple of features, such as pressure, pen movement above the surface, writing speed, acceleration, writing angle, angle change. The number of these parameters is so large that it is possible to create biometric profiles of signing persons.

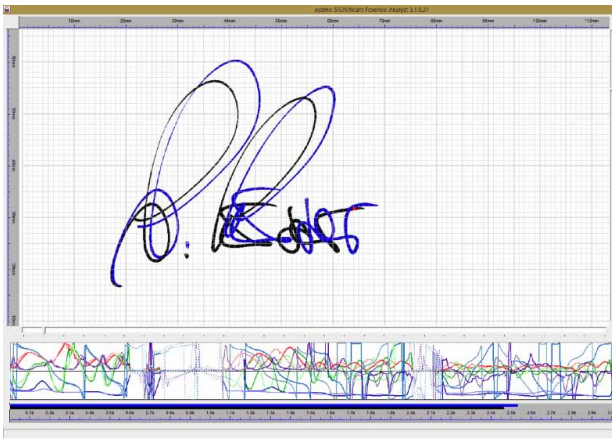


Fig. Biometric data for handwritten signature biometrics

Analysing an electronic handwritten signature is not difficult for a handwriting expert. The expert can successfully work on a printout of the handwritten signature, and if a more accurate analysis is necessary, the above-mentioned additional parameters, recorded electronically, such as pressure or reproduction of pen movement above the surface, provide an additional assistance in the signature analysis.

First and foremost, a handwritten signature makes it possible to eliminate paper from banking processes without modifying business processes – we maintain the signing step and

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

proceed in accordance with the process that is already in place. An important change is absence of processing paper documents, which accelerates processes, reduces costs and additionally secures the transaction thanks to real-time biometric verification. One of many advantages of this method is document standardisation, as the file format used for this purpose is the open timestamped PDF format, which is protected against changes. Such a document has all the features of an original paper document.

One of the banks that has been using electronic handwritten signatures successfully is Tatra Banka in Slovakia. The main goal of the bank was to automate client verification based on a handwritten signature in a branch and, as a result, increase transaction security. Another important factor for the bank's management was the ease of introducing this method in branches and training the client facing employees.

> The increasing possibilities and low costs make the handwritten signature biometrics an increasingly popular technology

An electronic handwritten signature is also used in such institutions as: Italian Post, Unicredit Italy, Intesa San Paolo Bank, GE Money Bank in the Czech Republic, Raiffeisen Bank, T-Mobile USA, KPN, Vodafone. This list is not exhaustive, of course.

The technology is advancing so fast that today we can use not only specialised pads for capturing handwritten signatures, but also mobile devices and tablets. An increasing number of devices have built-in sensors that are sensitive not only to touch, but to pressure as well. If a device does not have such functionality, we can also use a special electronic pen that will record the writing pressure. The increasing possibilities and low costs make the handwritten signature biometrics an increasingly popular technology. Currently, the main barrier to widespread use of this biometric is the security level, which remains low (the false acceptance rate, or FAR, amounts to ca. 1.2%).

4.4. OTHER BIOMETRIC TECHNOLOGIES IN BANKING, LESS COMMONLY USED IN EUROPE

Na There are also other biometric technologies used in banking worldwide, which have not gained significant popularity in banking projects in Europe, including in Poland. One such technology is fingerprint biometrics, which is commonly used in the Brazilian banking sector. In India and African countries fingerprints are implemented to prevent the practice of opening bank accounts based on a false identity. In Europe and in Japan, however, fingerprints are not used due to controversies related to protection of privacy and low social acceptability. Another example is palm vein biometrics. This technology is used by some of the largest banks in Japan (Bank of Tokyo Mitsubishi), Brazil (Banco de Bradesco) and Turkey (Ziraat Bankasi). Several small copperative banks implemented Palm Vein in Poland between 2015-2016. It has not become widespread in Europe, however, mainly for practical reasons. Both technologies are described briefly below:

- **Finger print biometrics**

  This is one of the longest used identity verification methods. It is based on analysing the fingerprint pattern, which is unique and dif-

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

> Fingerprint biometrics is one of the longest used identity verification methods

ferent for each finger on each palm, for each person. Fingerprints can be measured as a biometric feature using a fingerprint reader (ultrasound, capacitive or optical), which may confirm that two fingerprints are identical based on the concurrence of around 12 elements (called minutiae).

The biometric method based on the analysis of fingerprints is easy to use and relatively reliable (small readers capture the fingerprint image with high precision), and additionally it is commonly known. On the other hand, there is a risk of mistakes during the measurement due to mechanical damage (e.g. dry or cracked skin), dirt on the finger (e.g. grease), changes in the finger shape over years or shifting the finger on the scanner. Some of the factors hindering this technology are its negative perception in the historical context and concerns about the possibility of identity theft. Using fingerprint-based biometric data is also controversial due to legal aspects related to the possibility of identifying a person without his/her knowledge. In recent years, however, this biometric technology is experiencing "reincarnation" of a kind, due to the popularity of smartphones and tablets that enable users to log in using this modality..

- **Palm vein biometrics**

This method is based on the analysis of human palm, but instead of examining its external surface it focuses on the blood vessels inside the body, whose pattern is unique and permanent. The biometric data is verified by illuminating the palm with near-infrared light and obtaining information thanks to the properties of haemoglobin. The obtained template cannot be used to reconstruct blood vessels. This technology is considered to be non-invasive and non-interfering in the privacy of users due to the non-indirect examination of data located inside the body of the verified person.

Similar to finger vein biometrics, palm vein biometrics is a convenient and socially acceptable method, it reduces the bank's costs, it is accurate, but at the same time its use does not pose a threat to the user's health. It has not become widespread in financial institutions in Europe, however, mainly for practical reasons.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

5. CRITICAL PARAMETERS OF CHOOSING THE RIGHT TECHNOLOGY FOR A SPECIFIC USE

In order for the implementation in the bank to be successful, it is necessary to choose a biometric technology and solution which meets the criteria for the specific field of use. The table below presents the key criteria required from biometric solutions for the most popular fields of use:

Use	Key criteria of choosing a biometric technology
ATM	• Reader resistant to weather conditions (sun exposure, frost, rain, etc.) • Size of the reader makes it possible to install it on the face of the ATM • High social acceptability • Vandal proof reader • Integration with ATM application possible • High security of the device (incl. anti-tamper feature)
Branch	• High social acceptability • Ergonomic and easy-to-use reader • A solution that does not require modifying the network infrastructure in bank's branches • A solution independent of operating systems installed on the consultants' workstations in branches • High security of the device
Signing documents	• Ensuring the integrity of the signed document through integration with public key infrastructure (PKI) • Secure storage of private keys • High social acceptability
Virtual teller machines (VTM)	• Possibility to install the reader in the virtual teller machine (excluding voice biometrics) • Possibility to perform the biometric enrolment process in a convenient and secure manner, without the need for a consultant to be physically present (resistance to fraud) • High social acceptability • High security of the device • Reader supports liveness detection
Call centre – IVR (authentication in IVR)	• Using natural speech recognition • Voice sample management system • Possibility to integrate the IVR voice password in other channels, e.g. mobile app or web • Paying attention not only to FAR (which ensures security), but also FRR, which ensures user's convenience • Business and security reporting system • Resistance to cut-and-paste replay attacks or attacks using artificial voice timbre modification

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

Call centre without IVR – (authentication during conversation with a consultant)	• Successful speaker verification during the entire conversation on a continuous basis • Convenient collection of voice samples during a conversation with the agent • Voice sample management system • Attention should be paid to selecting a provider with business consultancy competences • Consistent business and security reporting system for all channels: IVR, mobile app, web • Resistance to cut-and-paste replay attacks or attacks using artificial voice timbre modification
Safe deposit boxes	• Convenient for the user • High security ratio
Online banking	• Low price of the device, enabling mass use and high quality at the same time • Small reader size • Secure communication with the bank's system, resistance to attacks • Can be used with Sign What You See technologies • High social acceptability • Supported by the most popular browsers (IE, Mozilla, Chrome) and operating systems (Windows, MacOS, Linux)
Mobile banking (voice)	• Voice sample management system • Possibility to integrate the mobile app password in IVR and in other channels, e.g. web • Paying attention not only to FAR (which ensures security), but also FRR, which ensures user's convenience • Consistent business and security reporting system for all channels: mobile app, IVR, web • Resistance to cut-and-paste replay attacks or attacks using artificial voice timbre modification
Corporate banking	• Device price that enables mass use and ensures high quality at the same time • Small reader size • Ensuring secure storage of biometric data by the user • Possibility of integrating the solution with the public key infrastructure (PKI) implemented in the bank • Secure communication with the bank's system, resistance to attacks • Can be used with Sign What You See technologies • High social acceptability • Supported by the most popular browsers (IE, Mozilla, Chrome) and operating systems (Windows, MacOS, Linux)
Mobile consultant	• Can be used with mobile devices (laptop, smartphone) • Possibility of secure communication via an open network • Allows signing of e-documents

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

6. RESISTANCE TO FRAUD, SECURITY MECHANISMS, THREATS, EXCLUSIONS

The main features of biometric systems are their ease of use and high resistance to authentication-related frauds. Each biometric technology is assessed in terms of many parameters. They include two basic technical parameters:

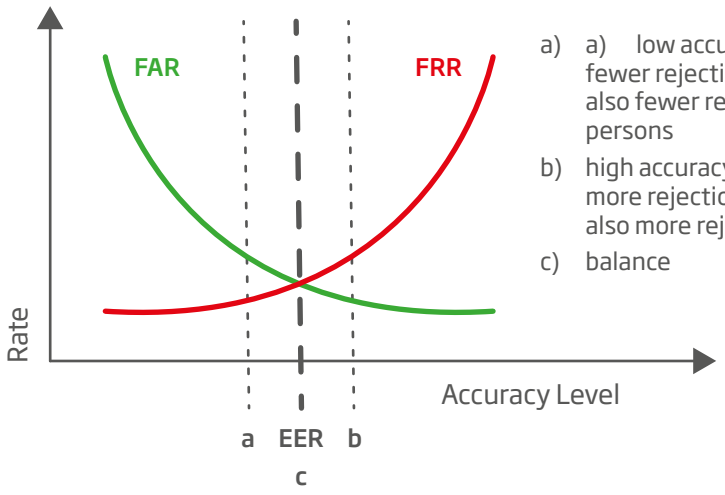
- false acceptance rate (FAR), which measures the probability of authenticating an unauthorised person,
- false rejection rate (FRR), which measures the probability of a failure to authenticate an authorised person.

These rates are opposed to each other – the higher the FAR, the greater the reliability, but also the greater vulnerability to false rejections. A higher FRR results in a smaller number of rejections (greater convenience), at the expense of reliability. In practice, when both parameters are balanced in relation to each other at a reasonable point (called 'equal error rate', EER), it is unlikely that an unauthorised person succeeds to pass the biometric authentication process, and the process remains sufficiently convenient for users.

Like any other IT system, biometric authentication can be a target of attacks. The attacks can be of various natures, from counterfeiting biometric features, to replacing biometric templates, comparison results or attacking the IT system.

> An important parameter when using the biometric technology is its social acceptability

A simple spoofing method is to replace the original biometric feature with its photography. This is the most common method in the case of face or iris recognition systems. Another popular method is to make a gel copy of a fingerprint or to use recordings in voice systems. Attacks against such biometrics are dependent on the availability of the biometric feature – taking a face photograph or obtaining the fingerprint image is not a problem for the counterfeiter. Hidden features, such as blood vessels, and behavioural features, such as handwritten signature, are more difficult to obtain and counterfeit.



a) a) low accuracy level – lower security level, fewer rejections of authorised persons, but also fewer rejections of unauthorised persons
b) high accuracy level – higher security level, more rejections of unauthorised persons, but also more rejections of authorised persons
c) balance

Fig. Illustrative graph or FRR and FAR as a function of accuracy level

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

Of course, manufacturers of biometric devices are aware of these threats and try to eliminate these types of frauds by using liveness detection mechanisms, i.e. verifying whether the sample belongs to a living person. Primitive frauds, like the ones mentioned above, are easy to eliminate, and good (but more expensive) devices have very sophisticated liveness detection mechanisms, which, unfortunately, extend the authentication time.

An attack may also be launched against the IT infrastructure at the time of processing, sending or storing templates. It is, therefore, necessary to use security mechanisms guaranteeing unavailability and integrity of templates, the correctness of their comparison using cryptographic methods, mutual authentication of devices and servers, certificates, signatures.

An important parameter when choosing a biometric technology is its social acceptability. Fingerprint recognition is still associated with "criminality and police forensic methods", although the only thing that systems discussed here and police systems such as AFIS have in common are fingers. Retina recognition is also objectionable – the eye has to be brought close to the eyepiece to be scanned. Such technologies as face, iris, vein, handwritten signature, voice recognition have high social acceptability – they do not have bad connotations, do not evoke negative emotions and are easy to use.

Another important parameter to be considered when choosing a biometric technology is the level of exclusion of a particular group of users. One of the main characteristics of biometric technologies that makes them so easy to use is the universal possession of biometric features. This universality, however, is not absolute. Each biometric technology has limitations which have to be considered. Fingerprints cannot be taken from ca. 4% of the population due to various skin lesions (other than cuts or chafes). Elderly

> Each biometric technology has limitations which have to be considered

people have a tendency to lower their eyelids, making it difficult to use the iris recognition technology. Many people suffer from dysgraphia or parkinsonism, which makes them unable to write a handwritten signature corresponding with the template. There are many people with physical or speech impairments, eye or blood vessel diseases – all of them restrict the use of biometric technologies. A simple solution to the problem of excluding persons with specific impairments is to allow users to choose one of several available biometric technologies.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

7. BENEFITS

The main benefits of using biometrics in banking are presented below:

1. Increased security:
- Eliminating the risk of wrong identity verification or Client identification,
- Eliminating the risk related to unauthorised access to accounts,
- Reduction of internal frauds committed by bank employees,
- Reduction of external frauds, e.g. committed by persons presenting a false identity document.

2. Increased convenience:
- Clients do not need to carry a payment card or an ID card with them, remember a PIN or have any other document to perform all operations,
- Clients do not need to remember the specimen signature made on the Specimen Signature Card at the bank,
- Clients do not need to remember the answer to the security question in the call centre channel,
- The bank can accept clients who do not use payment cards.

3. Cost optimisation:
- Reducing costs of paper document flow – cost of paper, printouts, archiving, FTE (documents processing), etc.,
- Accelerating processes by using digital technology instead of paper documents,
- Reducing customer service costs – eliminating the need to issue an ATM card to clients,
- Limiting the costs of ATM withdrawals (performing operations without a card),
- Building business on benefit payments (commission fees on withdrawals) and reducing the workload of branches at the same time,
- Reduction of costs related to maintaining positions for auditing bank tellers,
- Reducing the time necessary for customer service – reducing the workload of the staff,
- Possibility to open a new client acquisition channel – without using a "wet signature",
- Limiting costs related to call centre maintenance.

4. Image change:
- Innovative and secure institution.

Apart from the above advantages, each institution that implements or plans to implement a biometric technology can certainly find a number of additional advantages during the analysis of its processes.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

8. BIOMETRICS VS. ELECTRONIC SIGNATURE

An increasingly common form of making handwritten signatures is the use of specialised tablets and pens. A handwritten signature made in this way is recorded and stored in a digitised form. Although it has a digital form, it cannot be considered to be an electronic signature within the meaning of the public key infrastructure (PKI) – it is not a function of the document, it does not protect the integrity of the document, it can be easily transferred between documents.

Using biometric data as signatures under electronic documents (similar to a handwritten signature under a paper document) poses significant security challenges and is not regulated by law. Signing an electronic document by simply adding the value of a biometric feature (e.g. a graphic image of a handwritten signature with data describing the dynamics of the signature) to the content of the document results in a combination of the negative features of both solutions, as far as security is concerned. A signature which is not a function of the document does not protect its integrity, and the possibility to copy biometric data from one document to another enables forgeries. To change this, the procedure would have to be extended by a secret known to the signing person, but then it would be pointless to including biometric data in the signature, as the secret itself would be sufficient to sign the document.

However, biometric data can be used to authenticate access to cryptographic keys used for attaching an electronic signature, including a qualified signature. This technology is called BioPKI. In this model, the user's private key can be stored on a crypto-processor card (a variant closest to the classical electronic signature) or in the central Hardware Security Module (HSM) of the bank or an institution of a trusted third party. Biometric data captured at the moment of making the signature is used to authenticate access to the key.

The variant involving the use of a crypto-processor card, with biometric authentication used instead of a PIN, uses the power of biometrics to a limited extent only, as it requires the user to have a card and a reader. Consequently, in terms of costs, ergonomics and the user's convenience, it is a better solution to store the key in the central HSM.

> The BioPKI solution, combining biometrics and PKI, is already used by several banks in Poland

In this model, the user applies biometric methods to authenticate himself to the Bank's server, which uses the user's private key deposited in the HSM to attach an electronic signature on the user's behalf. A document signed according to this procedure can then be time-stamped and signed by an employee on behalf of the bank. The security of the procedure is based on trust in the party to which the keys are entrusted. This solution combines the advantages of biometrics and electronic signature, eliminating to a large extent the weaknesses of both technologies.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

9. CONCLUSION

Thanks to their intensive development and positive reception, biometric technologies can find a wide application in many different areas of the banking sector. Notable benefits can be achieved in corporate, retail and mobile banking, whether in branches, remote service or ATMs.

The scope of potential innovations is expanding all the time. Seen with a modern eye, from the perspective of the 21st century, biometric technologies reveal a completely new dimension of providing banking services.

To be modern, banks need to keep pace with technological progress. Banks' benefit is twofold. Most importantly, biometrics makes the infrastructure more modern and increases the security of banks, elevating it to a new level. At the same time, the implementation of biometric solutions raises the attractiveness of banks for clients, increasing the convenience, effectiveness of service and the awareness of those benefits.

Biometrics brings new opportunities and challenges, which are extremely useful today, will be desirable tomorrow, and indispensable the day after tomorrow.

> To be modern, banks need to keep pace with technological progress

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

10. AUTHORS

10.1. EDITOR

- **Tadeusz Woszczyński** - President of the Biometrics Group, Member of the Presidium of the Forum of Bank Technology of the Polish Bank Association, Regional Manage CEE and CIS, Information Systems Group, Hitachi Europe Ltd. – managing and substantive editor, co-author

10.2. CO-AUTHORS

- **Michał Czechowski** – Member of the Management Board, Noa Tech Sp. z o.o.
- **Łukasz Hnatkowski** – Secretary of the Forum of Bank Technology, Polish Bank Association
- **Artur Krystosik** – Director, Enigma SOI
- **Zbigniew Marcinkowski** – Deputy President of the Biometrics Group, Member of the Presidium of the Forum of Bank Technology, Country Manager at Nuance Communication.
- **Mariusz Sudoł** – Expert of the Forum of Bank Technology
- **Jarosław Wójtowicz** – Institute of Mathematical Machines

10.3. SUPPORT FOR INTERNATIONAL VERSION

- **Peter Jones** – Deputy General Manager, Information Systems Group, Hitachi Europe Ltd.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

All rights reserved. Copying the present report in its entirety or in fragments without the consent of the Polish Bank Association is prohibited.

06.2016