OBSERWATORIUM.BIZ

E-BANKING SECURITY

IDENTIFICATION, AUTHENTICATION AND AUTHORISATION TOOLS IN A NEW REALITY

SPECIAL REPORT
01 / 2016
APRIL

PLATINIUM SPONSOR
HID

MEDIA PATRON :
Bankier.pl

CONTENTS

E-banking is becoming the basic channel many people's daily transactions. In Poland, there are already over 30mln electronic accounts. The figure does not only refer to Internet banking, but also mobile services, which we have been using more and more often, a trend which has made banks come up with another approach to customer authentication. Another step is to change authorisation methods because customers expect a safe electronic payment and declaration of intent system. Sophisticated security threats require authorisation to be convenient and support customers in the area of key data verification. Building awareness of correct behaviours and responses to threats is another important element in the development of electronic banking.

Wojciech Boczoń
bankier.pl

One of the greatest challenges that the banking industry will face in the nearest future is efficient identification of customers and instructions that they submit. In an era of developing electronic financial services there are new risks, fraud crimes, and identity theft methods to be deal with. The so called "human factor" still remains the weakest link in the security chain, for users are susceptible to social engineering and tricks used by cybercriminals. Examples from foreign markets show that biometrics will hopefully become an effective identification method.

Michał Olczak
OBSERWATORIUM.BIZ

Electronic banking can take a further huge step forward as far as the number of users and the volume of all kinds of transactions are concerned but only provided that progress is also made in the area of identification, authentication, and authorisation. To have this accomplished, it is necessary to implement a universal approach to security from a customer's point of view (ergonomics and omni-channelling) as well as internal banking systems and processes.

Miłosz Brakoniecki
OBSERWATORIUM.BIZ

EXECUTIVE SUMMARY

GENERAL REPORT CONCLUSIONS

Customer identification and authentication, and payment authorisation areas in e-banking will be undergoing key changes because:

- there is an increase in the number and kind of channels through which customers access and apply for financial products, a trend which requires universal ergonomic solutions to be introduced that would still meet security requirements;
- the number and complexity of cybercrime attacks related to on-line banking is on the rise for which social engineering and malware are the most often used tools. For this reason customer awareness of how login and authentication methods are employed is so much crucial;
- using banks as “gates” through which customers access public digital services leads to a considerable increase in the sensitivity of mechanisms used to a new functional area;
- new regulations such as the eIDAS and the PSD2 are opening up new opportunities for using authentication and identification banking tools.

When a federated identity model has been introduced in Poland, banks will have a key role to play by making their identification and authentication tools available in practice to new both public and commercial services. Following from that, banks will have to consider whether they need changes both in the range of tools made available to customers (e.g. by providing better login protection and extra solutions) and whether they require "internal platforms" to be developed to ensure fraud and malware protection and, in general, customer e-banking activity monitoring.

The PSD2 regulatory package will create a new business area – that of security measures between institutions which will act as intermediaries for sharing customer identification data based on a service to access an account or initialise a payment transaction. We will be faced with a challenge to come up with detailed solutions in this area.

The banking sector sets standards for identification, authentication, and authorisation, but it will slowly start to adopt external standards, especially those related to the convenience of privacy use and management from other digital services, mainly social media and e-commerce. Combining those experiences with banks' operational risk requirements and the regulator perspective will remain a considerable challenge.

Quite importantly, it is possible to use authentication and authorisation tools employed by banks in trust services. The eIDAS brings about significant changes to the regulations and the electronic signature market, which leads to a valid question as to the creation of digital signatures that could be used in non-financial commercial and public services.

- Today SMS codes are the most frequent authentication tools used by banks. The total cost of SMS codes sent is estimated to stand at 60-70 million PLN, which already constitutes quite a serious burden for banks. We estimate that in the first place banks will try to replace this method with other less money-consuming mechanisms based on, say, PUSH notifications from applications.

- We predict that the coming years will continue to see banks exploiting biometric tools with emphasis placed on employing those that enable solving the problem of strong authorisation in mobile channels and attempting to standardize a framework for these types of solutions at the level of the sector's self-regulation.

- Customer identification, authentication, and authorisation must be part of a wider approach to e-banking security in a financial institution. A complex approach that includes both the system's external elements visible to customers, namely their education in tools and incident handling, the ergonomics of the tools used, the provision of omni-channelling and internal elements to ensure an organization's knowledge is built in a consistent way, to create algorithms of risk response, and to put flexible and quick measures in place to respond promptly to a cybercrime threat.

CHAPTER 1 - OVERVIEW OF IDENTIFICATION, AUTHENTICATION, AND AUTHORISATION TOOLS IN THE POLISH BANKING MARKET

1. Introduction

The process of identification and authentication in applications made available to customers is key from the viewpoint of e-banking security and ergonomics. Banks have to catch up with changing technological trends e.g. by adapting these tools to the needs of more and more popular mobile devices and customer expectations as to the continuing simplification and raising the intuitiveness of services.

The increasing number of customers that access their bank products over the Internet also means a growth in the number of cybercriminals that attempt to steal the resources. These threats are quite real, although customers have a limited awareness of them and do not understand how cybercriminals use social engineering, malware, and other tools. Such a situation puts banks in a relatively challenging position because, on the one hand, they have to be determined to offer their customers the most convenient and widest range of services and products possible in remote channels, yet, on the other hand, it is them that have to take care of security and not only be a guardian of the internal security of their systems, but also a teacher to their users.

The fact that banks have to combine these two seemingly opposing requirements often means they are making greater and greater use of state-of-the-art and innovative customer identification and authentication solutions based on biometrics and purely mobile tools. In the case of banking contemporary omni-channelling treated as a requirement to be met by service portals is manifested in the requirement for e-banking services to develop rapidly, which gives rise to extra challenges for banking institutions:

▶ Ergonomics – the necessity to use various authorisation tools, introduce various data during login, especially when technology is not a customer's forte or he or she seldom uses such tools. This often creates a situation in which customers specify a trivial password or passwords similar to those used in other applications and services, which makes them more susceptible to cybercrime. Employing current tools in new contexts is also an ergonomic problem. SMS codes are a widely accepted tool in Internet banking, but they do not perform well in mobile applications, because firstly they are received on the same device, which objectively means that they are hardly an example of two-channel authentication. In addition, it is difficult to copy the code between open applications in some devices.

▶ Implementation of new authorisation devices may be technically challenging when it is necessary to make changes at the back-end of a bank, a central system or a fraud-detection system. Moreover, new tools cannot always be successfully used in various channels – using biometrics is a really convenient tool in mobile banking, but it poses a considerable problem for traditional Internet banking.

▶ Costs of developing, implementing, and maintaining authorisation tools are an extremely significant aspect during pre-implementation analysis. Banks are increasingly faced with greater and greater challenges related to the cost side of customer service.

In the last twelve months banks have been confronted with regulatory and business changes that have led to a major drop in their revenues. Hence they see the need for cost optimisation also with regard to authorisation tools, if only because the basic authorisation tools, namely SMS codes, cost them millions of zlotys per year.

- Security of new tools expressed in the question as to whether they will be resilient enough to technological and social engineering attacks that are more and more often taking place in the Polish market despite the fact that the solutions are more user friendly and more cost-efficient.

2. E-banking identification and authentication – current state

Identification and authentication – e-banking

Customer identification and authentication in e-banking services is the first process encountered by a customer that is interested in gaining Internet or mobile access to his or her resources. Internet banking login has evolved over the years, and yet in fact it still looks quite similar. Customers enter their login and password, in some cases answer an extra question or enter the password that they have received in a token or in a one-time code SMS.

Apart from standard elements, Internet banking login differs among various institutions. Additional security measures, both optional and required, are divided in a few groups and their specific implementations in individual banks may differ from one institution to another.

Password requirements may concern its length, composition, and way of it being entered. Initially, a masked password was used for Internet banking login purposes by a considerable number of banks and the solution gained popularity quite fast. Today, a masked password is still present as a login element, yet it is usually an optional component which a customer can opt out of by selecting the correct option in his or her system settings. Apart from the fact that masked passwords did not improve security considerably they made login difficult and encouraged behaviours that were far from safe such as jotting down passwords on a piece of paper etc. Users also had to re-try logging in because of entering incorrect characters.

Another protection from hackers is the possibility of users logging in with additional information that they have provided. For example Bank Millennium's customers need to enter randomly selected digits from their PESEL (Polish Resident Identification Numbers), passport or personal ID numbers. Another possibility is to log in using a token or SMS code password. Such an option is made available by several banks e.g. BZWBK and Raiffeisen Polbank. It is a security measure against login data loss or theft and allows customer data security to improve considerably, although this of course happens at the expense of his or her convenience.

The option of customers' specifying their own logins is another way of increasing security and improving their convenience. Such a solution makes it possible for especially new users to log in.

Table 1. Identification and authentication – e-banking

E-BANKING AUTHENTICATION	ALIOR BANK	Bank Zachodni WBK Grupa Santander	eurobank	GET IN BANK	ING	mBank	Millennium bank	Bank Pekao	PKO Bank Polski	Raiffeisen POLBANK
LOGGING IN WITH AN ACTIVE CREDIT CARD NUMBER	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
ADDITIONAL PASSWORD FOR LOGIN (SMS CODE, TOKEN)	✗	⇔	✗	✗	✗	✗	✗	✗	✗	⇔
» WHICH ONES?		SMS								SMS
MASKED PASSWORD	✓	⇔	✗	⇔	✓	✗	✗	✓	✗	✗
SECURITY IMAGE AFTER INTRODUCING IDENTIFICATION	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗
ADDITIONAL QUESTION FOR LOGIN	✗	✗	✗	✗	✗	✗	PESEL PASSPORT PERSONAL ID NUMBER	✗	✗	✗

Identification and authentication – mobile banking

User identification and authentication in mobile banking have evolved substantially over a couple of years as the channel itself has advanced, too. At first, like in the case of Internet banking, customers had to enter both their logins and passwords each time they wanted to access the service. Now most of the applications we examined remember a customer's login and he or she simply enters his or her password or mobile password. This change has resulted from the introduction of mobile device trust processes, or in fact the overriding authentication of an application in a smart phone.

Application registration has been used in all the applications that we looked at. In most cases, compared with the previous years, the process is fully executable inside the application without users having to log on to their computers to access e-bank services in order to confirm or even initiate the process. In most banks, registering requires an SMS code to be entered that a bank has sent to the customer's device. Thanks to this, banks minimize the risk of unauthorized access to their customers' resources by means of third-party devices. Mobile banking registration not only simplifies logging in, but also provides a solution to the transaction authorisation problem when combined with mobile limits and passwords.

Table 2. Identification and authentication – mobile banking

AUTHENTICATION IN A MOBILE APPLICATION	ALIOR BANK	Bank Zachodni WBK Grupa Santander	eurobank	GET IN BANK	ING	mBank	Millennium bank	Bank Pekao	PKO Bank Polski	Raiffeisen POLBANK
APPLICATION REGISTRATION	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OPTIONAL	OPTIONAL	REQUIRED	OPTIONAL	OPTIONAL	REQUIRED	REQUIRED	OPTIONAL	REQUIRED	REQUIRED
» ACTIVATION AUTHORISATION	SMS	SMS	CALL CENTER / BRANCH	SMS	SMS	VOICE MESSAGE	SMS	SMS	VOICE MESSAGE OR AN INTERNET BANKING CODE	NONE (ONLY NIK, PIN AND DOB)
» CHANNELS IN WHICH AN APPLICATION IS ACTIVATED	MOBILE + INTERNET	MOBILE	CALL CENTER OR BRANCH + MOBILE	MOBILE	MOBILE	MOBILE OR INTERNET	MOBILE	MOBILE	MOBILE AND INTERNET OR VOICE MESSAGE	MOBILE
REMEMBERING LOGIN	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓
MOBILE PASSWORD	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓
LOGGIN IN WITH A GRAPHIC SYMBOL	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗
MASKED PASSWORD	✓	↔	✗	✗	✗	✗	✗	✓	✗	✗
BIOMETRIC LOGIN	✗	✗	✓	✗	✓	✓	✓	✗	✗	✗

Changes to ergonomics have made a significant contribution to the promotion of the mobile channels among those who are non-tech savvy. The simplified login process means logging in to mobile banking services is fast and hassle-free, considering the context it is used in – on the go, which is the defining feature of the channel. Banks offer several basic methods for logging in to their mobile applications:

▶ Shortened mobile password – the most popular method that mobile banking customers are offered. Customers themselves specify a dedicated password that usually has four to eight digits. This solution is extremely convenient and intuitive, combined with the customer login being remembered after the application has been registered.

▶ Biometrics – biometric solutions seem to be a global trend not only in mobile banking, but also in the operation of ATMs or branch networks. Today, mobile banking biometric solutions are used by e.g. the banks Bank Millenium, ING Bank Śląski, Eurobank, and mBank, and several other institutions are preparing to implement them. Fingerprints or voice seem to be natural tools not only for customer authentication during login, but also for authorising a transaction or communicating with an application. Unfortunately, biometric solutions are mainly available to IOS users and only Bank Millenium has decided to implement their equivalent in Android-supported devices.

▶ Symbol – it is a solution more widely associated with blocking telephones and non-banking applications. Despite this such a solution is now used in Alior Bank and Getin Bank. The solution consists in users defining their own “mark” on a board consisting of 16 or 25 dots and use the mark to log in to their mobile application.

▶ Standard password – despite the numerous solutions available in the market some bank services still make their customers log in to their mobile banking service using full passwords encountered in Internet banking. The bank Pekao SA uses a masked password for access to mobile banking and this is one of the few cases in the market in which a bank has not facilitated logging in to their mobile applications.

REPORT EXPERT

ROBERT TRĘTOWSKI
DIRECTOR OF THE IT INITIATIVES AND TESTING DEPARTMENT, PKO BANK POLSK

Customer behaviours are changing so banks have to keep pace with their expectations as to not only product offers, but also multi-channelled processes of sales and contact by adapting security mechanisms. Today, a customer has Internet and mobile banking password, PIN code debit and credit cards, a Call Centre password and transaction authorisation tools. The multiplicity of solutions makes us think about seeking mechanisms that do not require additional digits to be remembered or a piece of paper with login data to be kept in our wallets. In search for safe, economically viable and convenient solutions two directions are examined in the first place: mobility and biometrics.

The dynamic mobile banking development may create the opportunity to change customer transaction authentication and authorisation. Banks are considering use of technologically advanced telephone components (e.g. phone, touch ID) for voice biometrics, facial and fingerprint scanning. The flexibility of the platform ensures safe implementation of mechanisms for client identity being stored in a phone e.g. encoded shortened identity documents. It is also a good idea to use mobile payment systems such as Blik/IKO that make it possible to authenticate a customer in and outside of banking e.g. in e-Administration.

ATMs, VTMs, and Call Centres are undergoing changes, too, in which biometric solutions such as biometric signature, finger, hand, face and voice recognition will be increasingly used. The changes will simplify remote sales processes through customer video-verification (comparing a photo of his or her ID and a photo of him or her) and signing of the agreement electronically. But in branches, too, document readers are more often to be found to authenticate a customer, verify the authenticity of a document, and speed up customer service.

And let us not forget about corporate clients. Making use of Web services enables full automatisation of a two-channel flow of information about account transactions, balances, and turnover between a company and a bank. In order

> to achieve STP (Straight-Through Processing), we need an efficient and safe tool such as a qualified electronic signature (QES), yet without the present drawbacks (e.g. legal issues, context identification, rising implementation demands, costs). Corporate managers also expect mobile solutions in order to manage their companies' finances and authorise key transactions. To my mind, such a tool will be developed based on solutions for retail customers.
>
> This area will see a lot happening in the nearest future. We are going to see the implementation of the PSD2, the eIDAS, and the Polish administration going digital. Are banks interested in becoming an identity provider in the public administration? In my opinion, they have no choice, because they play a crucial part in the system as institutions of public trust. This will create a win-win for everyone: the administration, Polish citizens and banks. A well-thought-out concept of a federated identity model in e-Administration makes it possible to look even further – to use digital identities of natural and legal persons in the commercial sector, including the banking industry.

3. E-banking authorisation – current state

Authorisation of transactions and other instructions submitted in remote channels are the fundamental way of safeguarding customers from financial abuse and theft. Authorisation tools used by banks differ from one another even with regard to one method, e.g. the kind of information sent in an authorisation code SMS. As for e-banking there are visible differences between what authorisation tools customers can choose from.

Table 3. Authorisation of financial operations – Internet banking

AUTHORISING A BANK TRANSFER TO ANY ACCOUNT IN INTERNET BANKING	ALIOR BANK	Bank Zachodni WBK Grupa Santander	eurobank	GET IN BANK	ING	mBank	Millennium bank	Bank Pekao	PKO Bank Polski	Raiffeisen POLBANK
SMS CODE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MOBILE TOKEN	✗*	✗	✓	✗	✗	✗	✗	✓	✓	✗
PHYSICAL TOKEN	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗
CALL CENTRE	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
LIST OF ONE-TIME PASSWORDS	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓

****Available in T-Mobile; Banking services provided by Alior Bank***

Table 4. Pay-by-link authorisation

AUTHORISATION OF INSTANT TRANSFERS (PRZELEW24)	ALIOR BANK	Bank Zachodni WBK Grupa Santander	eurobank	GET IN BANK	ING	mBank	Millennium bank	Bank Pekao	PKO Bank Polski	Raiffeisen POLBANK
NO AUTHORISATION FOR "SOME" TRANSFERS	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗
SMS CODE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MOBILE TOKEN	✗*	✗	✓	✗	✗	✗	✗	✓	✓	✗
PHYSICAL TOKEN	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗
CALL CENTRE	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
LIST OF ONE-TIME PASSWORDS	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓

Available in T-Mobile; Banking services provided by Alior Bank

One-time codes received in short messages are the most popular authorisation solution. The method is used by all the banks we looked at and it is clear and convenient for customers, too. With Polish mobile phone penetration having long reached or even exceeded 100%, it is safe to say that virtually all bank customers are able to use this transaction authorisation method. One major advantage of SMS codes in terms of security is that it is possible to include in them the details of the operation that the customer is authorising. Apart from their authorisation codes, customers may also receive the number of their transactions, date, recipient, and amount. For this reason it is more difficult to steal the customer's authorisation code using fake login pages or e-mails from his or her “bank”.

The remaining methods are far less popular both in banks and among customers. Mobile tokens are becoming a more and more noticeable trend in e-banking. They are used both in Internet and mobile banking. Now there are two models for providing customers with this type of solutions – stand-alone applications or as a feature embedded in a mobile banking application. The banks Pekao S.A. and PKO BP provide their customers with an application dedicated to generating authorisation codes, whereas Eurobank has a token embedded in its mobile banking application. Another interesting example is Raiffeisen Polbank, which has had a token built in its mobile application. Users cannot access the token directly. It is there only to authorise mobile banking transactions. In this case, users simply enter the PIN code that they have specified.

Physical tokens and scratch cards provide another way of authorising Internet banking operations. These tools generate codes which are not directly related to a particular transaction, which means they are more susceptible to fraud and phishing. This is somewhat different for transactions authenticated in mobile banking. Banks approach the problem in a variety of ways and, as a consequence, customers are offered different models in different institutions. The fact that a customer is accustomed to the way operations are authorised in one bank does not necessarily mean that the information will come handy in another bank that he or she has moved his or her account to, as is the case for for example SMS codes, which are universally used in Internet banking.

Table 5. Authorisation of financial operations – mobile banking

AUTHORISING A BANK TRANSFER TO ANY ACCOUNT IN A MOBILE APPLICATION	ALIOR BANK	Bank Zachodni WBK	eurobank	GET IN BANK	ING	mBank	Millennium	Bank Pekao	Bank Polski	Raiffeisen POLBANK
NO ADDITIONAL AUTHORISATION UP TO A CERTAIN LIMIT	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓
MOBILE PIN CODE	✓	✗	✗	✓	✗	✓	✓*	✓	✓	✗
MOBILE TOKEN	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓

**BOTH REQUIRED (BELOW LIMIT + MOBILE PIN CODE)*

The first thing customers need to deal with when it comes to mobiles application protection is to register his or her device. It is a feature that all the banks we analysed share, yet the registration, or “trusting”, of a device is very different. The most significant distinction is that whether the process is compulsory and whether it takes place inside the application only or whether users need to use another contact channel e.g. Internet banking or the bank's information line then or later in order to complete the process. To take an example, the bank PKO BP enables customers to use mobile banking services without having to register, yet no registration means that they cannot carry out transactions using this feature. Banks also differ in that customers must authorise such an order. Most banks also require their customers to copy their authorisation code from the SMS they have received.

The first thing that a customer does after installing his or her mobile application is to register his or her device. For this reason it is a crucial process not only from the perspective of security but also ergonomics of applications. Sophisticated processes that require him or her to know how to operate a smartphone or use another channel may discourage him or her and make him or her abandon the process because he or she may not be able to complete it during one session. As a result, it may mean that some customers will simply give up the registration or mobile banking in general.

Authorisation of transactions themselves also differs from one bank to another, yet it is possible to pinpoint three dominating manners in which systems function in this respect:

- No extra authorisation up to a certain limit (e.g. BZWBK, ING), in which case banks assume that device registration and login provide enough protection to carry out transactions up to a limit set by the bank or the customer himself or herself.

- Transactions authorised with a mobile password (e.g. Pekao SA, Getin) – the password may be either the same as for simplified login or an entirely different one specified by the customer.

- Transactions authorised with a mobile token (e.g. Raiffeisen Polbank, Eurobank); from the viewpoint of a user the process is in fact identical as in the case of using a mobile password, the difference being that a token authorisation code is provided in the background.

REPORT EXPERT

WOJCIECH DWORAKOWSKI
SECURING

Authorisation and authentication tools may be used on mobile platforms both as an element of a mobile banking application and a stand-alone application designed to authorise transactions and authenticate users in other channels (the so called “mobile tokens”). When developing applications key to mobile systems, account needs to be taken of a totally different risk profile in the devices compared with PCs. There is a wide range of threats characteristic of only mobile devices e.g. theft, loss, or temporary access. The problem of malware cannot be overlooked, either. It is somewhat different from that encountered in a PC because of the sandboxing offered by an operational system, but it needs to be kept in mind that contemporary mobile platforms may facilitate a seemingly innocuous application to access sensitive information (e.g. sent in SMSs, displayed on the screen, or entered by users). It also needs to be remembered that telecommunication and platform operators (e.g. Apple, Google, Microsoft etc.) rely on infrastructure security. To take an example, in a recently described attack scenario one operator's banking and portal passwords were overheard. Having gained access to the operator's portal, the attacker was able to read the victim's short messages, including the ones with one-time codes for transaction authorisation.

We need to consider all these aspects when designing secure mobile solutions for banks. Yet let us also bear in mind safe implementation that considers the nature of a platform, potential vulnerabilities, and extra protection specific to the Android, iOS, or Windows operational systems. Solutions concerning the safe implementation of an application on a platform may prove handy. I recommend our company's report on creation of higher-risk mobile applications and a check list developed as part of the OWASP Mobile Security Project.

4. Estimation of the authorisation tool market value and potential savings

The popularity and the convenience of using SMS codes have greatly contributed to the rapid development of Polish e-banking. The tool has allowed introducing other active transactional and sales functionalities. Unfortunately, the rapid development and promotion of electronic banking and its basic authorisation tool in Poland has its weaknesses, too.

First, the authorisation method is a specific cost factor for banks. In their price policies, at least several first authorisation SMSs that customers receive in a given month are free of charge, which in practice means high costs incurred by banks, which have suffered considerably in the wake of new regulations and other market factors for the last two years. We estimate that banks pay between 60 and 70mn zlotys to provide the service.

60-70mn PLN

is the estimated amount that banks spend to send authorisation codes in SMS messages in the Polish market.

SMS messages sent to authorise transactions – Elixir transfers, eCommerce and card payments over the Internet (3D Secure). The estimates show that banks pay about 5 zlotys to deliver the service to one active Internet banking customer.

The number of transactions carried out through remote channels is bound to rise, a trend which will lead to banks paying higher charges to intermediaries and mobile phone operators. Now that banks are coming under greater regulatory and cost pressure, the problem will only be exacerbated. Even today the institutions are continuing to attempt to limit the cost of sending SMS codes e.g. by promoting adding recipients to favourites or introducing algorithms that limit the possibility of authorising pay-by-link transfers. Such activities, however, cannot be treated as a long-term strategy, and banks need to seek alternative solutions.

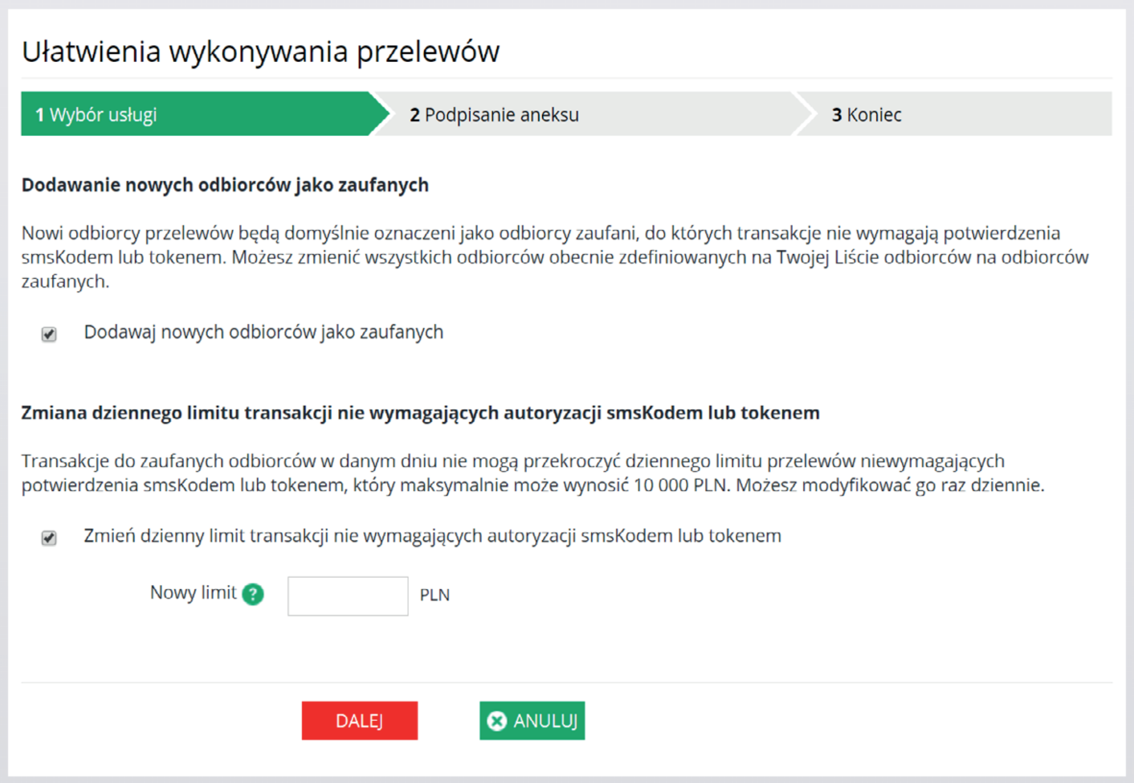
The fact that this tool is popular among and convenient for customers in fact has another drawback for banks – it is extremely hard to change customers' habits especially related to the sensitive issues of finances. For this reason, customers may find it especially difficult to shift to new authorisation methods such as tokens, especially that these methods are less convenient for customers, because first, to put it colloquially, they need to “install something”, then “turn something on” and have access to the Internet in order to carry out a transaction, whereas an SMS message arrives “by itself”.

So what are the alternatives to SMS codes? Nowadays, mobile tokens are becoming more and more widespread. More and more banks are using the solution to authorise both mobile and Internet banking transactions. Mobile tokens are quite an obvious choice here, yet the cost of the implementation is relatively high and business advantages mainly depend on customers migrating to the new solution. Changing customers' behaviours and patterns takes a long time and simply being interested in introducing the solution is not enough. Long-term marketing and educational campaigns are also money- and time-consuming. Customers have been migrating to mobile banking for several years now and the process has been the subject of a number of marketing campaigns, also on television, the consequence of which is that slightly below 40% of customers use the channel. Migration to an entirely new authorisation tool could take less time, yet we need to keep in mind that for customers the change in the way transactions are authorised is not an advantage per se, as was the case for mobile banking.

Other possible authorisation methods could include codes used in the BLIK mechanism created by the Polish Payment Standard and PUSH notifications generated by mobile applications. This method, however, has never been tested in Poland. Both methods have their own advantages and disadvantages but what they do have in common is that they have become known to customers. BLIK payments, or in fact codes with which transactions are carried out, have been around already for more than six months in Poland's six biggest banks. Quite a lot of customers have already used the method to make payments in shops or withdraw cash from an ATM. BLIK codes generated individually for each customer and changed every two minutes may be a viable and cost-efficient option for transaction authorisation. This method would require the already existing mechanisms to be adjusted, but it appears to be a natural direction that banks should pursue because of the fact that a number of investments in the area have already been completed. As a method, BLIK is already in use and customers are increasingly aware of it.

The other tool that could stand a chance of becoming a real alternative to SMS codes is PUSH notifications, or messages that a user receives into his or her phone directly from the applications installed without actually having to launch them. Even now many of the most popular applications are using this sort of communication, which means that in practice users have already know it. This method would have another strength, too, in that the mobile banking customer database is already extensive, because the services are delivered to as many as about five million customers. These are those who are in fact ready to switch to another solution. Clearly, the cost of such a solution being implemented is quite high in the beginning, because of the suitable and secure infrastructure to send such messages that has to be built and maintained, but in the long run such an investment may prove profitable, especially for banks which already have mobile solutions used by a large group of customers.

EXAMPLE FROM THE MARKET



Ułatwienia wykonywania przelewów

Dodawanie nowych odbiorców jako zaufanych

Nowi odbiorcy przelewów będą domyślnie oznaczeni jako odbiorcy zaufani, do których transakcje nie wymagają potwierdzenia smsKodem lub tokenem. Możesz zmienić wszystkich odbiorców obecnie zdefiniowanych na Twojej Liście odbiorców na odbiorców zaufanych.

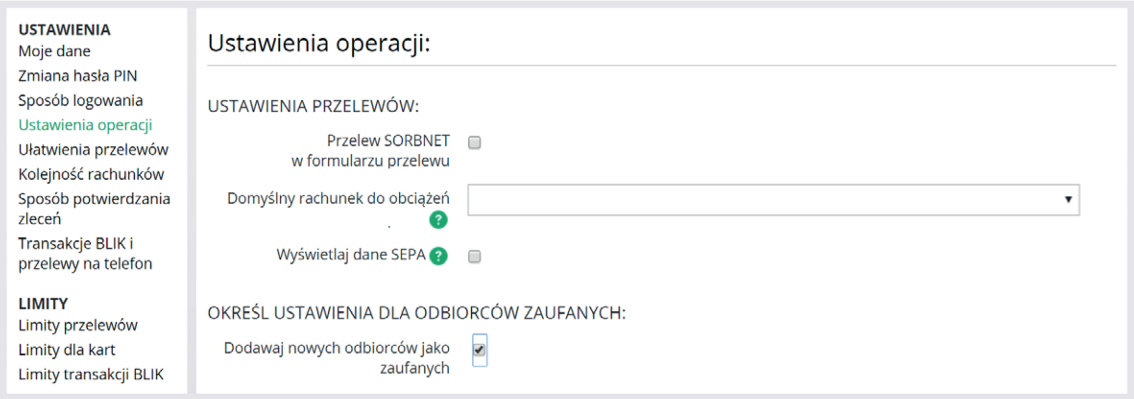
☑ Dodawaj nowych odbiorców jako zaufanych

Zmiana dziennego limitu transakcji nie wymagających autoryzacji smsKodem lub tokenem

Transakcje do zaufanych odbiorców w danym dniu nie mogą przekroczyć dziennego limitu przelewów niewymagających potwierdzenia smsKodem lub tokenem, który maksymalnie może wynosić 10 000 PLN. Możesz modyfikować go raz dziennie.

☑ Zmień dzienny limit transakcji nie wymagających autoryzacji smsKodem lub tokenem

Nowy limit ? ______ PLN



Ustawienia operacji:

USTAWIENIA PRZELEWÓW:

Przelew SORBNET w formularzu przelewu □

Domyślny rachunek do obciążeń ? ______

Wyświetlaj dane SEPA ? □

OKREŚL USTAWIENIA DLA ODBIORCÓW ZAUFANYCH:

Dodawaj nowych odbiorców jako zaufanych ☑

> Bank Zachodni WBK has made it possible for its customers to manage their trusted recipients more easily by being able to add them automatically and make a number of recipients trusted with just one click.

5. E-banking fraud estimates

Poland's electronic payment system has been developing rapidly over the last decade. It is so advanced it can already be compared to the one in countries that have been enjoying economic freedom for a far longer period of time than we have. The number of active Internet and mobile banking users have already reached 13 and 5 million, respectively. In Poland, over 1.6bn Elixir transfers are made yearly, and the value of the e-Commerce value is estimated to stand at 20-25bn Polish zlotys. It is a staggering number of transactions and customers doing their daily shopping, paying their bills or just checking their account balances. For many years, these figures have attracted both individual criminals and organised crime groups.

The last five years have seen a surge in the intensity of e-banking-related attacks. Only in 2014, almost 1300 such incidents were reported (source: CERT Polska). There is a marked tendency for cybercriminals to depart from simple DDoS attacks designed to block and hinder access to electronic services and move towards more and more sophisticated attacks using malicious software and targeted attacks. Social engineering attacks have evolved, too, from the randomly sent e-mails and scattered web pages to better and better targeted attacks designed to reach the groups of customers or employees in a particular institution. These attacks are fully professional and extremely hard to detect by an ordinary customer. The fact that such crime activity has gone professional shows that defence mechanisms and vulnerabilities in electronic systems are understood better and that cybercriminals are now using advanced tools to achieve their goals. In order to counteract this phenomenon, banks will have to become increasingly engaged in creating new and developing existing security mechanisms. They will also have to engage in a continuous and proactive processes of educating and protecting their customers, because they themselves are the most powerful weapon in a cybercriminal's hand through their carelessness and little security awareness.

	Characteristics and possible consequences	Threat level	Frequency
Denial of Service (DDoS)	Attacks designed to block access to services and affect a company's business operations and image	Low Such attacks are relatively easy to detect and apart from affecting a company's image they are harmless	High There is a marked change from network towards application attacks
APT (Advanced Persistent Threat)	Latest types of dedicated attacks that consider the specific nature of a particular institution. They also make use of other methods such as malware and phishing.	High Such types of attacks require a high degree of sophistication and preparation on the part of the hackers, yet this activity may result in identity theft, surveillance, money theft or laundering	Average Rising number of campaigns; in 2014 at least one active campaign per one institution during a period of time in Poland

	Characteristics and possible consequences	Threat level	Frequency
Malware	Malicious software that automatically executes operations that cybercriminals are interested in, e.g. swapping account numbers or sending an SMS code to an unauthorised account	Average Threat levels dependent on security measures used by a particular institution or network operators	High Malware attacks have been known and used for many years now. It is a relatively popular method of attack due to the low cost of criminal activity.
Phishing	A massive social engineering attack that consists in imitating a legitimate site and sending users fraudulent e-mails	High The level of threat is dependent on an action that a victim is encouraged to carry out. If authentication and authorisation data are stolen, the victim may lose his or her money	High Noticeably upward trend towards making it difficult for banks to block such attacks; better and better social engineering methods
Spear phishing	Like in phishing, the result being that a specified target group or institution is selected	High The level of threat is dependent on an action that a victim is encouraged to carry out. If authentication and authorisation data are stolen, the victim may lose his or her money	High Growing, because of the greater detection problems than in the case of massive attacks

According to a recent NBP (the National Bank of Poland) regular report titled “Assessment of the Polish payment system” prepared in September 2015, the number of fraud crimes targeted at credit cards has been rising quite dynamically. In the last five years the number of attacks has risen almost threefold – from 13,000 in the first half of 2010 to over 45,000 in the first half of 2015. It is the biggest number of credit card fraud crimes ever recorded since the study was launched in 2005.

The transactions that banks describe as Internet-related have the biggest share in these figures. The percentage of the incidents in the number of all reported fraud crimes amounted to 43%. The value of fraud transactions reached over 21mn zlotys in the first half, a rise of almost 45% against the second half of 2014. The share of Internet transactions in the value of fraud crimes was almost 49%. The trends that have been the most noticeable for the last decade are the growing numbers of cybercriminals and the greater interest they take in electronic service channels. More and more bank accounts are being targeted because of the high number of clients that use the Internet on a regular basis to make their transfers, do their shopping, or merely check their account balances. Tools and solutions that cybercriminals make use of are more and more sophisticated and banks need to find a way to combat them in order to maintain customers' trust. Customers' carelessness, lack of knowledge and awareness are the greatest threats that banks have to combat, which means they will be forced to use better and better authorisation and authentication tools and continue to educate their customers on safe behaviour not only in e-banking, but all Internet activity in general – from checking their e-mails, through browsing, to data that they provide visiting web pages.

CHAPTER 2 - CHANGES IN THE MARKET AGAINST NEW REGULATIONS ON E-IDENTITY AND TRUST SERVICES AS WELL AS THE PSD2

1. Introduction

It appears that the banking identification, authentication, and strong authorisation will face a regulatory tsunami. For years these areas have not had any distinguishing features and have not seen significant developments, an exception being the necessity to create mobile banking solutions, which we have covered in detail in the previous chapter. In business the change was initiated in the area of mobility and the ensuing requirements to ensure customers the best solutions. As for regulations, it was started with the SecurePay Recommendation, which specifies the requirement of strong authorisation for certain electronic transactions (which has mainly translated into a wide range of 3D Secure solutions implemented for credit card payments). At present, the eIDAS implementation accompanied by changes to domestic regulations and the PSD2 Directive may produce momentous changes in the market, taking the discussion context and range much further beyond the banking industry.

REPORT EXPERT

PAWEŁ WIDAWSKI
DIRECTOR IN THE POLISH BANKS ASSOCIATION

STRONG AUTHENTICATION AND eIDAS AND PSD2 IMPLEMENTATION

Implementing the eIDAS regulation will create a federated model of authentication services in Poland. Banks will be faced with the possibility of developing an inter-bank eID system, which has already happened in e.g. Scandinavian countries (Denmark, Sweden, and Norway). The bank eID is not only designed to authenticate bank customers in a standardised way, but also citizens in e-government services or a client in the public sector (e-commerce platforms, private health service). Embedded in a suitable business model, the plan may help banks generate fresh revenue and the state speed up the development of e-administration. Using authentication tools will of course have to comply with the PSD2 Directive, meaning they will have to rely on strong authentication.

2. Changes in regulations on identification and trust services

The eIDAS regulation implemented directly into the Polish domestic law is a European Union act that lays down regulations on electronic identification in transborder transactions and trust services. It appears that Polish laws implementing the eIDAS will be limited to a small number of issues to be decided upon by Member States and to make the domestic law compliant. At the same time the way in which national electronic identification systems will be organised is left to the Member States' decision, so, naturally, it is necessary to determine the strategy and the final model according to which electronic identification will function in Poland.

In practice, the eIDAS regulates and creates the market for e-Identity and trust services in Europe, a process that is exemplified in a lot of countries implementing commercial and public systems that encompass the areas and that are in demand among both users and merchants/providers of such services (e.g. in Estonia, Sweden, Italy, and the Czech Republic). In addition, when it comes to identification, new technological standards are being introduced by the world's biggest players – both technological giants, the so called GAFAS (Google, Amazon, Facebook, Apple) and telecommunications operators (the standard created by the world's telecommunication operators, Mobile Connect). The notion of e-Identity itself and identity is the key regulatory and social challenge and, looking ahead, it may also be crucial to the emerging market of the Internet of things.

The eIDAS introduces identification standards, but at the same time organises or at least provides a chance of organising trust services, namely submission of declarations of intent remotely, which can include a variety of electronic signatures, electronic stamps, electronic registry services and validating services that allow verifying the validity and correctness of signature and stamps by electronic providers. The eIDAS is designed to ensure the transborder dimension of e-Identity services at Member States level by introducing the notification of national e-IDs on EU level and, finally, requirements for their acceptance on the level of digital public services in all EU Member States. The regulations also provide for various strengths of e-IDs, offering the possibility of classifying services provided by e-services providers according to what level of trust is necessary. The laws have also introduced such descriptors as “low”, “substantial”, and “high”, which a particular tool should be characterised by. It is worth mentioning that the directive does not impose e-IDs' technological media for particular “levels”, which seems reasonable considering the rate of technological changes that we are witnessing. Considering the existing solutions, it seems that the level “low” will be matched by tools requiring only customers' ID/login and password; the level “substantial” will require second factor authorisation, whereas the level “high” will be based on e.g. microprocessor cards (but not only). At the same time the directive can be seen as the basis for the emerging e-Identity and trust services markets and a chance of the massification of services and commercialisation of this business area. It is obvious that this may become a leverage for the dynamic development of Polish e-Administration services, the potential of which is not properly utilised yet.

DEFINITION

FEDERATED E-IDENTITY MODEL

According to the e-Identity federated model, it will be possible for customers to make use of various e-Identities functioning in the market. e-Identity providers

> and hubs/brokers that would deliver the services to end portals must be subject to supervision at national and/or international level, creating the so called circle of institutions of trust. In the model, a Member State may both be an e-Identity provider and organise one of the hubs/brokers (for example the one dedicated to integrating public digital services), but does not have monopoly of the business areas. Yet it does perform an important supervisory and educational function in the market.

Implementing international frameworks also means creating and codifying the idea of a domestic identification system and trust services in Poland. All this is there to be able to use the potential of domestic e-Identity providers who have already issued those identities on a massive scale, as is the case of banks or who have the potential to do so – for example thanks to a considerable customer database, an extensive network of physical branches and popular customer service and transactional portals in an electronic channel, in the case of which telecommunication operators, insurance providers, post institutions can become potential players. At the same time space for fintech sector start-ups appear which can offer a brand new and creative solution to e-Identity and trust services distribution, promotion, and use in a virtual environment.

Projected schedule of implementing regulations on e-Identity and trust services in Poland

July 1 2016	Till the end of 2016	2017	September 2018
Implementation of eIDAS / new regulations on trust services	Introducing the framework for national identification systems	Implementing the obligatory dimension for acceptance of commercial e-IDs in public digital services in Poland	Obligatory dimension for notified acceptances of e-IDs in public EU services (eIDAS Reg.)

*Commercial and government e-IDs can be notified

REPORT EXPERT

ARTUR MIĘKINA

INDEPENDENT E-IDENTITY MARKET EXPERT

> The development of the e-ID market and services results from the interaction of two opposing factors: security and convenience.

Transferring a physical identity to the virtual reality is key to eID security. The world has become an inseparable part of most people's everyday reality in which we work, talk, exchange views, and build interpersonal relations, so we also rebuild ourselves and our e-identity.

It needs to be kept in mind that an e-identity that has been stolen one allows the hacker to use it in the entire virtual world. Yet e-identity should not be avoided. It should merely be managed properly by promoting openness to new technologies and services that keeps pace with global technological advancements and enables using electronic services (in administration, banking, telecommunication, e-shops etc.) in both a secure and convenient way. In the market, there is a demand for mechanisms ensuring that eIDs can be used regardless of the medium- cards, telephones, information and communication systems. Ways of making electronic identities, however, should be regulated by the market considering known legal and security requirements.

For the last couple of years, the public administration has undertaken efforts in the area of e-identity, yet the experiences have not resulted in citizens using it on a massive scale both due to its low usability and no framework for cooperation with commercial solutions. As Poland is building a citizen-centric approach, it should leave its citizens a choice of the way in which they will manage their e-identities and which devices they will use to access electronic services. Only synergy between e-identity, business, and administration providers can ensure that the e-identity market will function properly in Poland and Europe.

EXAMPLE FROM THE MARKET

SUBMITTING OF APPLICATIONS FOR THE +500 CHILD BENEFIT VIA BANKS

Using electronic channels to apply for a benefit to which over 2.5mn households are to be entitled is in fact the first solution that employs the so called federated identity model in which legitimate entities (literally, under a dedicated legislation that specifically sets out e-ID providers) that are found in the so called “trust circle” make massive identification and authentication to an also massive public service available. Provisional data show that for two days over 90% of the 120,000 applications were submitted via

> banking channels. A dozen or so banks have implemented or declared implementing the mechanism as soon as possible. If the solution proves successful, it may pave the way for other implementations of this type, and finally, a long-expected breakthrough in using e-administration by Polish citizens and entrepreneurs.

To conclude this chapter in the context of the development of transaction identification, authentication, and authorisation tools by banks, specific strategic objectives are being formulated that need to be achieved in the area:

▶ Using the potential of e-Identity in administration services.

If the solution of applying for the Program 500+ benefit via banking channels is successful, this may mean other services for citizens and entrepreneurs being added (let us imagine a "Public services" tab in electronic banking systems), introducing "single sign-on" services (cooperation between PKO BP and ZUS – Poland's Social Insurance Institution – can be used for reference), and introducing authentication via banks on digital services pages (currently aggregated via the ePUAP portal and at obywatel.gov.pl and biznes.gov.pl). Frameworks for such cooperation must be created at the level of sectors, rather than individual institutions, and supported by relevant regulatory changes.

▶ Using the e-Identity and trust services potential in the context of a commercial market.

Banks may also become a business beneficiary of a commercial market in this respect. Offering authenticated user identities to service providers and new services of remote identification and remote submission of declarations of intent (changing service providers, applying for a job remotely, signing B2B agreements, and many other options) to their customers, banks are able to generate a brand new revenue line, mostly leveraging the infrastructure that they already have and the customer database they have already acquired. What is still left to be created is a model of offering services to dispersed entities, which will certainly call for the need of creating a hub/a broker of the services, as is the case for payment institutions and gateways. Also, decisions need to prepared as to whether uniform services should be built on a sector level (banking ID, banking digital signature) or the level of individual banks as providers, as is the case of e-transfers (pay-by-links) for the electronic payment market that emerged nearly 15 years ago.

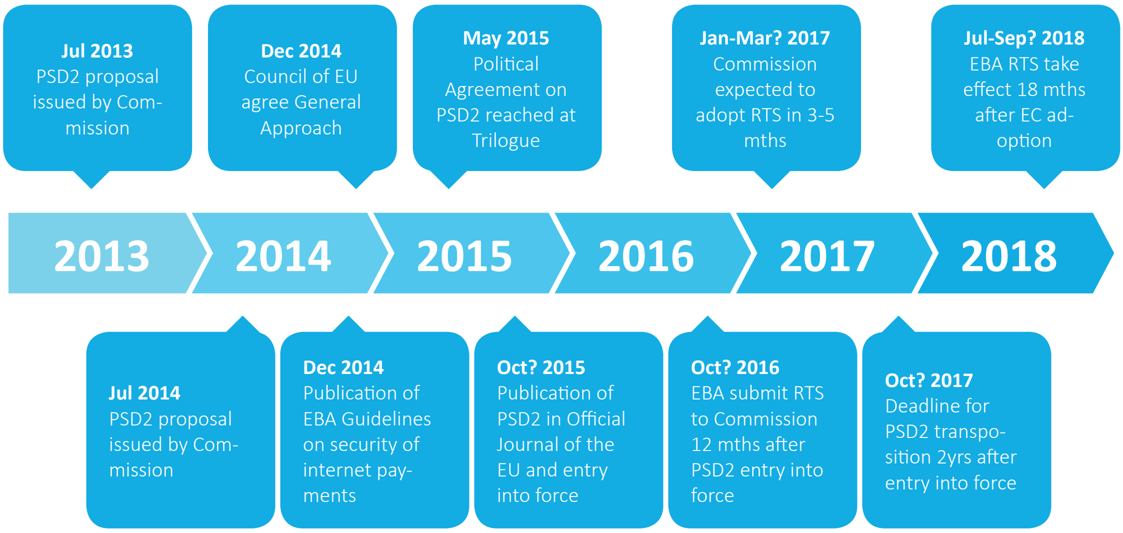
▶ Widening the security perspective.

As for security, the above changes will necessitate a review of both policies and infrastructures related to electronic operational security. Both the internal tools related to an electronic banking security management platform and the external ones provided to users will have to be employed for new purposes related to identities and remote submission of declarations of intent being made available. For this reason they will have to be reviewed for their adequacy, costs (other applications will generate volumes and costs in the case of for example SMS codes), and ergonomics of use.

3. Regulatory changes ensuing from the PSD2 and the resulting consequences for authentication and authorisation services

The PSD2 Directive is another regulation that will affect banks. Everyone says that it will bring about fundamental changes in the financial market, as it will allow – under certain conditions – non-banking entities to provide financial services. The Directive is also designed to ensure greater transparency in the market. In the area of authentication, identification, and authorisation it is key, too, as the banking industry and its customers may be removed from their comfort zones and be challenged with having to assess the reliability of such institutions outside of the banking industry and solutions that they offer as they provide customers with access to accounts and resources.

Projected schedule of implementing PSD2-related regulatory changes



Jul 2013 PSD2 proposal issued by Commission

Dec 2014 Council of EU agree General Approach

May 2015 Political Agreement on PSD2 reached at Trilogue

Jan-Mar? 2017 Commission expected to adopt RTS in 3-5 mths

Jul-Sep? 2018 EBA RTS take effect 18 mths after EC adoption

2013 2014 2015 2016 2017 2018

Jul 2014 PSD2 proposal issued by Commission

Dec 2014 Publication of EBA Guidelines on security of internet payments

Oct? 2015 Publication of PSD2 in Official Journal of the EU and entry into force

Oct? 2016 EBA submit RTS to Commission 12 mths after PSD2 entry into force

Oct? 2017 Deadline for PSD2 transposition 2yrs after entry into force

Source: Payments UK

The key notion in the Report is Strong Customer Authentication, which is to be compulsory in the case of:

- access to a bank account in on-line channels;

- initiating a payment transaction in an electronic channel (also considering the dynamic combination of the transaction data with the amount and the payer's identification);

- other activities carried out via remote channels which require such a level of security due to fraud threats. SCA parameters are still being developed by EBA in the RTS formula.

Lawmakers have responded to the fact that individual customers in mature markets use a number of financial services and may want to manage them from his or her perspective, almost a cockpit of services. For this reason, the notion of Account Information Service, or AIS, is covered in the Directive. The service is designed to deliver users aggregated information on-line that concerns them or a number of payment accounts maintained by one payment services provider or more. Such access could be enabled by a provider's portal, so in this case the organisation of an e-ID that a customer could use to log in remains an open question. In a federated model notified methods, e.g. banking-related, could be used for identification and authentication. AIS providers will be able to have access to information from designated accounts and only payment transactions in them. They will not be able to demand access to particularly protected data related to payments in a payment account, either. Nor will they have any right to use and store any data apart from those related to AIS service provision. Quite importantly, banks will be obliged to introduce standardised and safe communication with an AIS provider, which introduces a new dimension – that of the necessity of creating universal APIs complying with RTSs that make such an integration possible. Banking institutions will not be allowed to discriminate against AIS entities, by, say, making it impossible for them to handle enquiries.

Another definition that the PSD2 Directive introduces is Payment Initiation Service (PIS) that refers to initiating an on-demand payment ordered by a user of a payment account maintained and provided electronically by another payment services provider. In this case, a PIS provider does not to have to conclude an agreement with a bank which does have to communicate with him or her in a secure manner following RTS and on-line requirements and deliver or make available all information related to initiating a transaction after receiving a payment from the PISP. Also in this case, no discrimination is allowed against transactions initiated by any entity with a PISP, or Payment Initiation Service Provider status. From the viewpoint of authentication and authorisation safeguarding a user's own protection measures is key, which is the responsibility of a PISP under the new law. Crucially, both PIS and AIS services are based on the authentication procedure made available by a bank and according to the Directive strong authentication is laid down as obligatory.

The last service that the PSD2 regulation covers is about providing users only with access to card-based payment instrument based on a card without Payment Instrument Issuing. In this case, money comes from the account maintained by a payment account provider (e.g. a bank), and transactions are carried out only after verifying whether the required amount is kept in the payment account.

Finally, it is worth mentioning that in the context of security the PSD2 Directive additionally sets out the obligation on the part of financial institutions to implement procedures in the area of operational risk related to payment services provisions, including procedures of handling incidents. This will lead to financial institutions having to report significant security incidents to KNF (Polish Financial Supervision Authority), which in turn will be obliged to report relevant information to ECB and EBA. Quite importantly, the Directive also introduces the obligation to inform users of incidents that may impact or do impact their financial interests and measures they should take to avoid the effects of such incidents. Like in other cases, EBA will issue detailed guidelines on reporting incidents at a later date, before the regulation becomes effective.

REPORT EXPERT

PHILIP HOYER
SENIOR DIRECTOR STRATEGIC INNOVATION AND ALLIANCES, WITH HID GLOBAL

The publication of PSD2 will provide financial organisations with a business case and strong incentive to implement a security strategy that is scalable and cost-effective, yet is sufficiently robust to ensure high assurance of the customer identity in the shift of the customer authentication process, during payments, from the merchant to the financial organisations. The suggested approach is to implement multiple layers of security that strengthen against various vectors of attack. These layers can include traditional user- and device-based authentication methods, while incorporating other aspects including browser protection and application security including more continuous and frictionless forms of authentication such as behavioural biometrics. In addition to more secure customer data and a higher degree of confidence in the customer identity, financial institutions would also make themselves less vulnerable to attacks by fraudsters, saving money and their reputation in the process.

REPORT EXPERT

PIOTR BREWIŃSKI
COORDINATOR FOR THE LEGAL TEAM, POLISH BANKS ASSOCIATION

One of the most important changes that the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, introduces on payment services in the internal market is the strong authentication requirement apart from account information services, and payment initiation service. “Strong customer authentication” means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data; In line with the 2015/2366 Directive strong customer authentication will be required when a payer accesses his or her payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. In addition, strong authentication will be required whenever payments are initiated through a payment initiation service provider or when the information is requested through an account information service provider. The 2015/2366 Directive sets out that EBA shall submit the draft regulatory technical standards by 13 January 2017. No doubt, the new regulation will force the market to introduce new, not always previously used security solutions considering that the market of payment transactions will open up to new entities and services and that there will be a change in principles relating to a payer's responsibilities where no strong customer authentication has been used.

CHAPTER 3 - ERGONOMICS OF INDENTIFICATION AUTHORISATION TOOLS – HOW A CUSTOMER APPROACHES IT

1. Introduction

The need to adopt a user-centred approach has permanently entered the consciousness of people responsible for the business, development, and Informational Technology dimension to electronic banking. Examining the ergonomics of the solutions that have already been introduced together with relevant professionals engaging in the design stage of services has in fact become an integral part of design methodology and transactional portals development. It seems, however, that only now is ergonomics expanding into the area of identification, authentication, and authorisation. On the one hand, it is happening because so far this area has been the exclusive security domain with little space for businesses to engage. On the other hand, the area has never been such an important development before as it is now.

For this reason an approach is becoming more and more popular according to which final solutions that customers are provided with must reconcile the business aspect (e.g. the cost of maintenance of a give method incurred by a financial institution), security and user convenience. Let us take a look then at how customers assess today's authentication and authorisation tools. It is all the more important in view of the fact that identification and authentication is a prerequisite for each login activity as well as Internet banking and mobile services. Customers' experiences of using such a service have a definite impact on the total assessment of satisfaction with remote access to a given financial institution. In addition, the area is going to face major changes in the nearest future because of

- the growing popularity of mobile banking, which has introduced the obligation of further adaptation of tools to the specific nature of a mobile solution;

- the appearance of such solutions as identification, authentication, and authorisation in the background, in which these processes are for example elements of payment in a shopping platform (an example being making purchases via the PayU account service, and, ultimately, payment organisations' portfolio in the future. Other changes in the area may also be brought about in the wake of PSD2 implementation);

- the implementation of biometric identification, authentication, and authorisation tools.

This is exactly why it is worth finding out customers' current views and perceptions of what they see as a secure solution and what they find convenient about the processes in order to design new solutions efficiently.

2. Assessment of the existing identification and authentication solutions in the market

When research was carried out into the usability of Internet and mobile banking in the area of identification, authentication, and authorisation, interviews were conducted with almost 200 users of systems in Poland's leading banks.

The results we obtained made it possible to formulate conclusions on customers' attitudes and opinions of the transaction identification and authorisation methods they used. As for Internet banking, 18 systems were looked into. 108 tests were conducted for a mixed user base (current and new users), for which the following results were obtained:

Table 6. Average time of logging in to Internet banking

IDENTIFICATION METHOD	Number of portals	Average login time (in sec)
LOGIN AND PASSWORD	10	32
LOGIN AND MASKED PASSWORD*	8	60

in Millenium Bank customers' PESEL, passport or personal ID numbers are used as an additional way of their identification

In the case of mobile banking 15 applications were studied and 90 tests were carried out in a mixed group, too.

Table 7. Average time of logging in to mobile banking

IDENTIFICATION METHOD	Number of portals	Average login time (in sec)
PIN (4-6 CHARACTERS, WITH NO LOGIN)	8	18
OTHER COMBINATIONS	7	54

Password errors occurred only for masked passwords in desktop interfaces and concerned almost 50% of the cases under investigation. The research results show unanimously that the simpler login method, the less time is devoted to the activity. Logging in to a mobile device should be made much easier, but in as many as 7 banks tested, the way of login was so complicated that on average it took almost a minute (54 seconds).

The login time is for general information purpose only, because the studies we carried out were not quantitative. It is also worth remembering about various circumstances that affected the results: respondents often used login data that they had not known before, they often were not customers of the banks under investigation, they did not set up the way of login and authorisation themselves (if such an option was provided by a given bank). Respondents' comments and remarks received during the study proved to be much more important. We are citing some of them below. We have also used them to attempt to define the “ideal” identification and authorisation set.

VOICE - IDENTIFICATION AND AUTHENTICATION

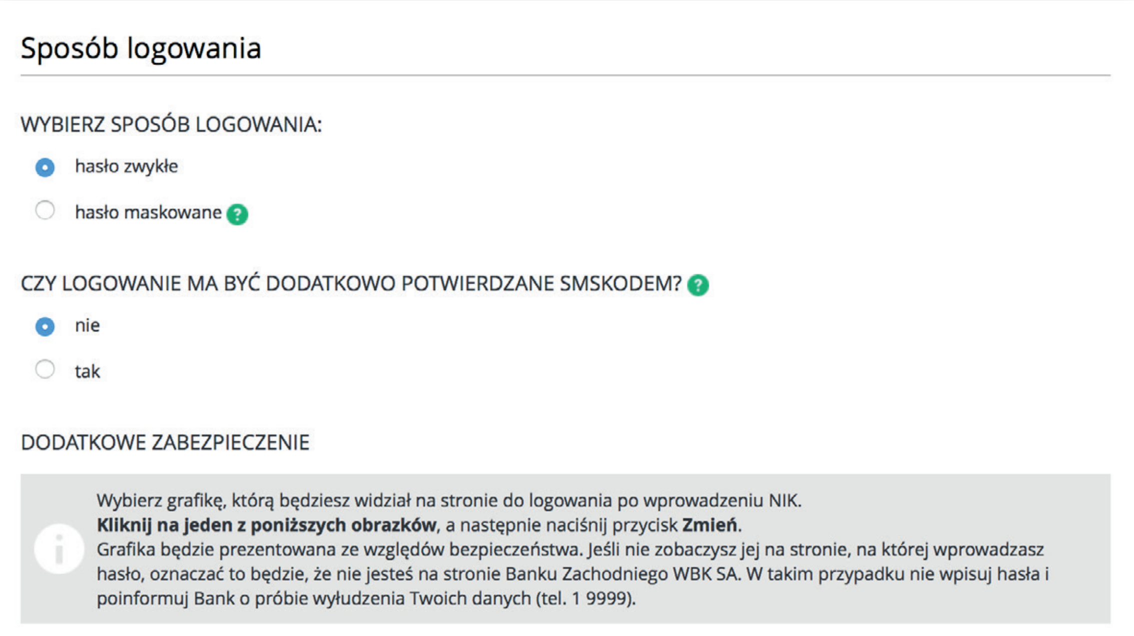
ABOUT MASKED PASSWORDS:

> *“Well, I can't stand it.”*
>
> *“They say the password is so secure, yet I must jot it down on a piece of paper anyway.”*
>
> *(after entering the incorrect password) ”Strange, it appears in the same combination."*
>
> **ABOUT PASSWORDS:**
>
> *„It is a good thing there are no longer stringent password requirements, I don't have to write it down.”*
>
> **ABOUT ADDITIONAL IDENTIFICATION AND AUTHENTICATION TOOLS:**
>
> *„I'm not really sure whether it's safe to use your PESEL, everybody can find it out.”*
>
> **ABOUT LABELS, DESCRIPTIONS AND BUTTONS:**
>
> *“Where am I supposed to log in??” (about applications with no button “Login”)*
>
> *“Is my ID my login?”*
>
> *“NIK, it sounds so funny.”*
>
> *“It's a good thing it's OK here, I missed that in other applications.”*
>
> *“The strange thing was that when I entered my PIN I did not have to click OK. I'm not sure it's safe.”*
>
> **ABOUT SECURITY:**
>
> *“It must be made secure somehow, I'm OK with this.” (masked password)*
>
> *“Such a short PIN code? Doesn't seem safe to me.”*
>
> *(login method) “Doesn't influence the way I assess the system.”*

In principle, users do not disregard the necessity to protect their accounts properly. There are some elements, however, that could be corrected or eliminated, which would contribute greatly to raising the comfort of using both services and applications. These elements certainly include the possibility of login configuration (choosing a masked password as an option) and the detailed and comprehensive description of and usage of proper names for standard terms (such as login and password). Because when it comes to customers of various institutions, the multitude of terms used by banks is puzzling: identity number, login, customer number, NIK, MilleKod; password, p@ssword, key.

Based on respondents' opinions we tried to figure out what an ideal identification and authentication solution should look like in bank systems. First of all, we believe that users themselves could set up their own logins. As an example, we used a functionality available in the Bank Zachodni WBK system.

EXAMPLE FROM THE MARKET



Sposób logowania

WYBIERZ SPOSÓB LOGOWANIA:

● hasło zwykłe

○ hasło maskowane ?

CZY LOGOWANIE MA BYĆ DODATKOWO POTWIERDZANE SMSKODEM? ?

● nie

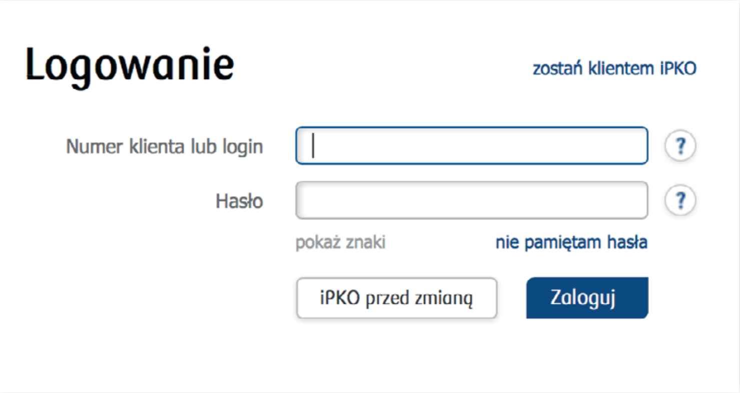
○ tak

DODATKOWE ZABEZPIECZENIE

Wybierz grafikę, którą będziesz widział na stronie do logowania po wprowadzeniu NIK.
Kliknij na jeden z poniższych obrazków, a następnie naciśnij przycisk **Zmień**.
Grafika będzie prezentowana ze względów bezpieczeństwa. Jeśli nie zobaczysz jej na stronie, na której wprowadzasz hasło, oznaczać to będzie, że nie jesteś na stronie Banku Zachodniego WBK SA. W takim przypadku nie wpisuj hasła i poinformuj Bank o próbie wyłudzenia Twoich danych (tel. 1 9999).

The correct and unambiguous description of fields and buttons means that users do not have pause and think what information to enter. The PKO Bank Polski login page may serve as a good example of a user-friendly login panel in a desktop service. As far as applications are concerned, the Bank Millenium application seems to be the best tool in this respect.

EXAMPLE FROM THE MARKET

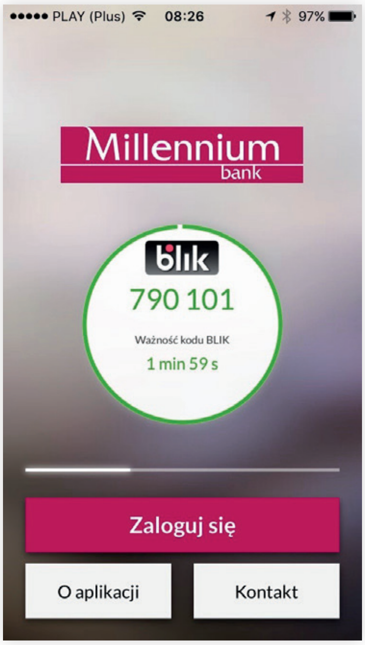


Logowanie

zostań klientem iPKO

Numer klienta lub login ?

Hasło ?

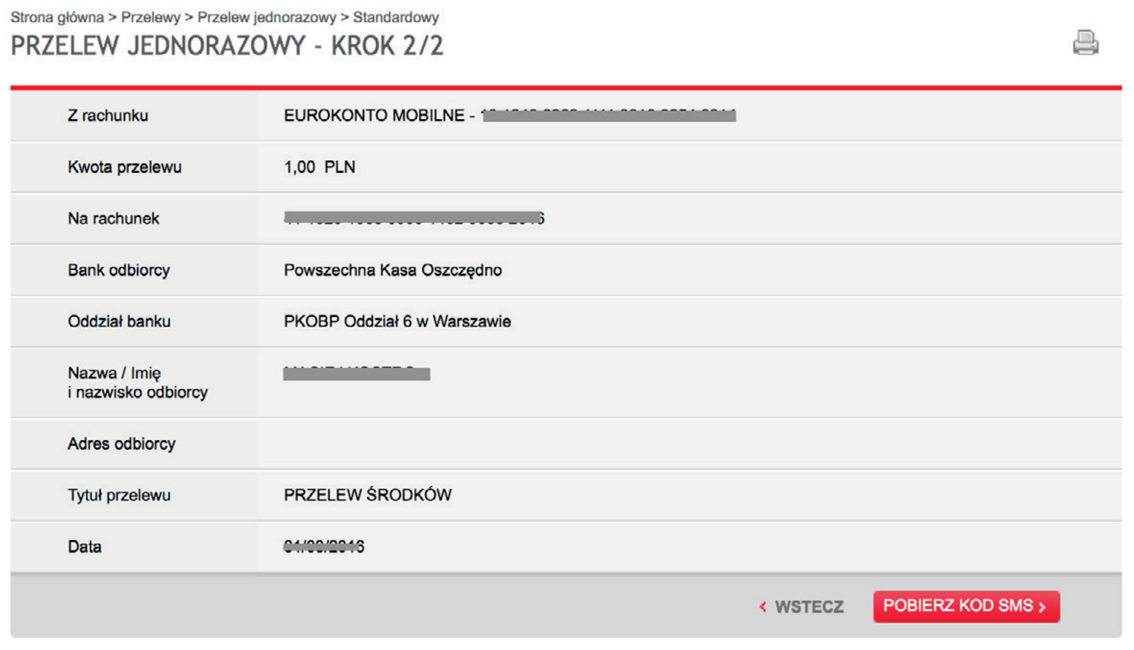


3. Assessment of the existing strong authorisation solutions in the market

As for on-screen transactional systems, a one-time password sent in an SMS is still the most widespread authorisation method. The authorisation method does not pose too many problems to users, yet during our study we received some significant remarks. They referred to the global numbering (not according to “Operation x of...”) of one-time passwords sent, which explains why we received comments such as “how come it's 16th operation today?” (users responding to the necessity of entering one-time code no 16). Users also pointed out to the fact that their previous codes had been remembered in the field.

Users also reported that it is inconvenient having to click a button to send the code. They say the code should be sent automatically. This inconvenience also appears in a situation caused by the description on the button: making a transfer consists of 3 steps. If the button “Get an SMS code” instead of “the Accept button”, the process becomes longer for users. They comment: “Why do I have to get the code? Shouldn't it be sent automatically?”.

EXAMPLE FROM THE MARKET



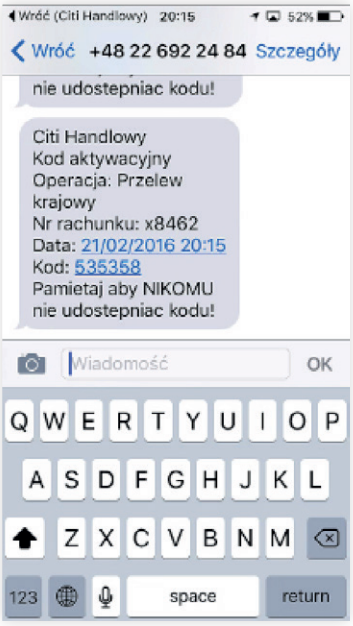
Strona główna > Przelewy > Przelew jednorazowy > Standardowy

PRZELEW JEDNORAZOWY - KROK 2/2

Z rachunku	EUROKONTO MOBILNE - [redacted]
Kwota przelewu	1,00 PLN
Na rachunek	[redacted]
Bank odbiorcy	Powszechna Kasa Oszczędno
Oddział banku	PKOBP Oddział 6 w Warszawie
Nazwa / Imię i nazwisko odbiorcy	[redacted]
Adres odbiorcy	
Tytuł przelewu	PRZELEW ŚRODKÓW
Data	[redacted]

Authorising transactions in mobile applications is slightly more diverse. During the process the same PIN code is used as the one for login or some other. Also, a one-time SMS password can be used, like in desktops. The last method is evaluated unambiguously badly by our respondents: they have to remember, copy or write down the password from their messages and enter it into the appropriate field in an application form, which is hard and time-consuming on these types of devices.

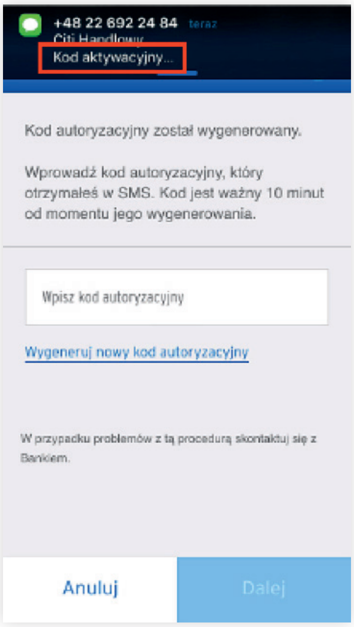
EXAMPLE FROM THE MARKET



Wróć (Citi Handlowy) 20:15 52%
Wróć +48 22 692 24 84 Szczegóły
Wiadomość
OK
space
return

nie udostepniac kodu!

Citi Handlowy
Kod aktywacyjny
Operacja: Przelew krajowy
Nr rachunku: x8462
Data: 21/02/2016 20:15
Kod: 535358
Pamietaj aby NIKOMU nie udostepniac kodu!



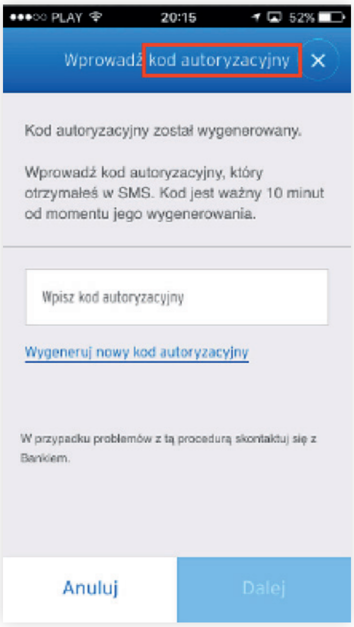
Kod autoryzacyjny został wygenerowany.

Wprowadź kod autoryzacyjny, który otrzymałeś w SMS. Kod jest ważny 10 minut od momentu jego wygenerowania.

Wpisz kod autoryzacyjny

Wygeneruj nowy kod autoryzacyjny

W przypadku problemów z tą procedurą skontaktuj się z Bankiem.



Kod autoryzacyjny został wygenerowany.

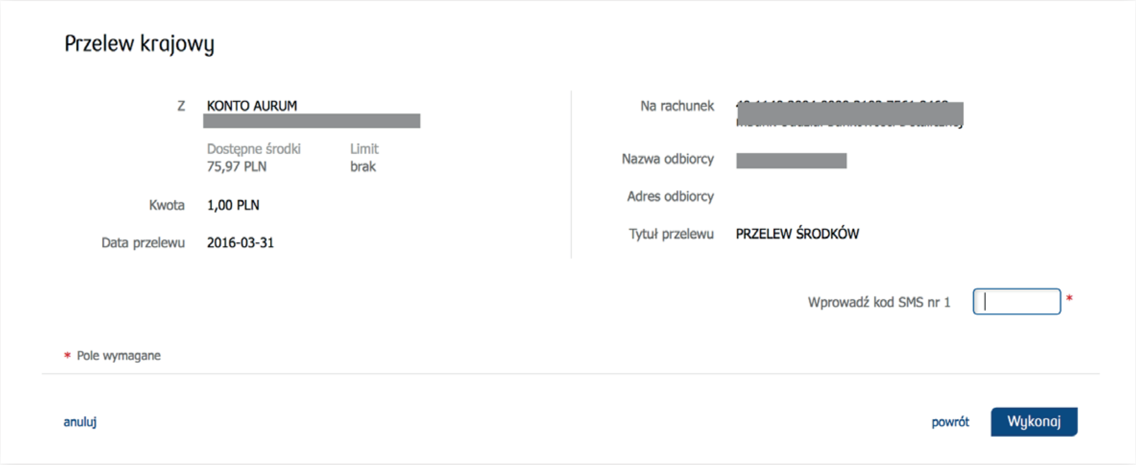
Wprowadź kod autoryzacyjny, który otrzymałeś w SMS. Kod jest ważny 10 minut od momentu jego wygenerowania.

Wpisz kod autoryzacyjny

Wygeneruj nowy kod autoryzacyjny

W przypadku problemów z tą procedurą skontaktuj się z Bankiem.

As far as one-time codes go, a lot of incoherent terms appear: code, smscode, sms p@ssword, authorisation code, activation code, the last two appearing even in the same institution. During authorisation when money is being transferred, sending a one-time SMS code should be done automatically in step 2. This would shorten the process and be intuitive for users.



Przelew krajowy

Z KONTO AURUM [redacted]

Dostępne środki 75,97 PLN

Limit brak

Kwota 1,00 PLN

Data przelewu 2016-03-31

Na rachunek [redacted]

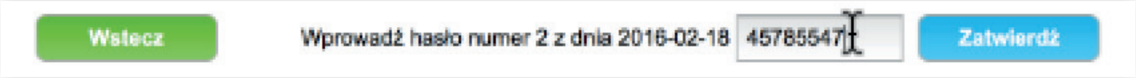
Nazwa odbiorcy [redacted]

Adres odbiorcy

Tytuł przelewu PRZELEW ŚRODKÓW

Wprowadź kod SMS nr 1 *

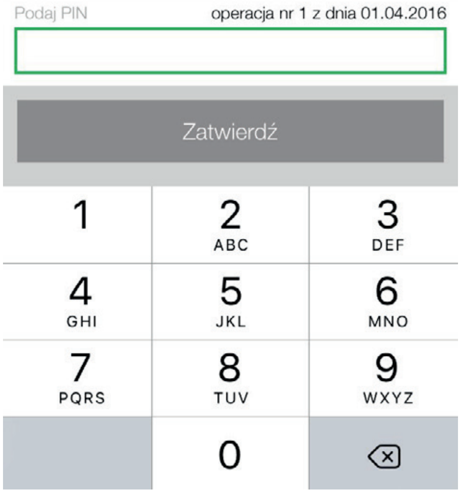
* Pole wymagane



Wprowadź hasło numer 2 z dnia 2016-02-18 45785547

A description of a one-time code should include information about the next number of transactions on a particular date.

In users' view, it would be best if a transaction carried out via a mobile application was authorised by the same PIN code which is used for login.



Identification and authorisation are a seemingly small part of the functional world of electronic banking solutions. Yet, we must not forget that security related to access to money is one of the biggest concerns among customers in the banking industry. What is more, it is the login page or screen that is the first contact point in the case of which banks may make customers more interested in and happy about using their services and electronic access channels more efficiently.

4. Perspectives for the development of identification, authentication, and authorisation tools from the perspective of ergonomics

Customers opinions presented above reveal the current problem with awareness among Internet and mobile banking which is the combined results of previous experiences of solutions used in banks, their own need of security and the current need to control the solutions and make them convenient. There is no denying the fact that by promoting and maintaining specific solutions such as SMS codes and the absence of events or incidents that would undermine trust in them on a massive scale and in people's consciousness, it is becoming an indisputable standard expected by customers. Certain solutions put in place to raise security (as is the case of masked passwords or the lack of shortened/simplified login in to mobile and Internet banking) lengthen considerably the time needed to complete a given process and are thought of badly by customers, also in terms of how they are perceived from the perspective of security (e.g. having to write down a password to enter it into the system). In the course of assessment of the process that takes place in banks customers also paid attention to the fact that names of various solutions should be optimised, the number of stages to be completed should be lowered and customers should be provided with the possibility of selecting their own way of identification, authentication, and login, since this would enable them to choose the best solutions for themselves and they would not have the impression that their banks imposes solutions on them.

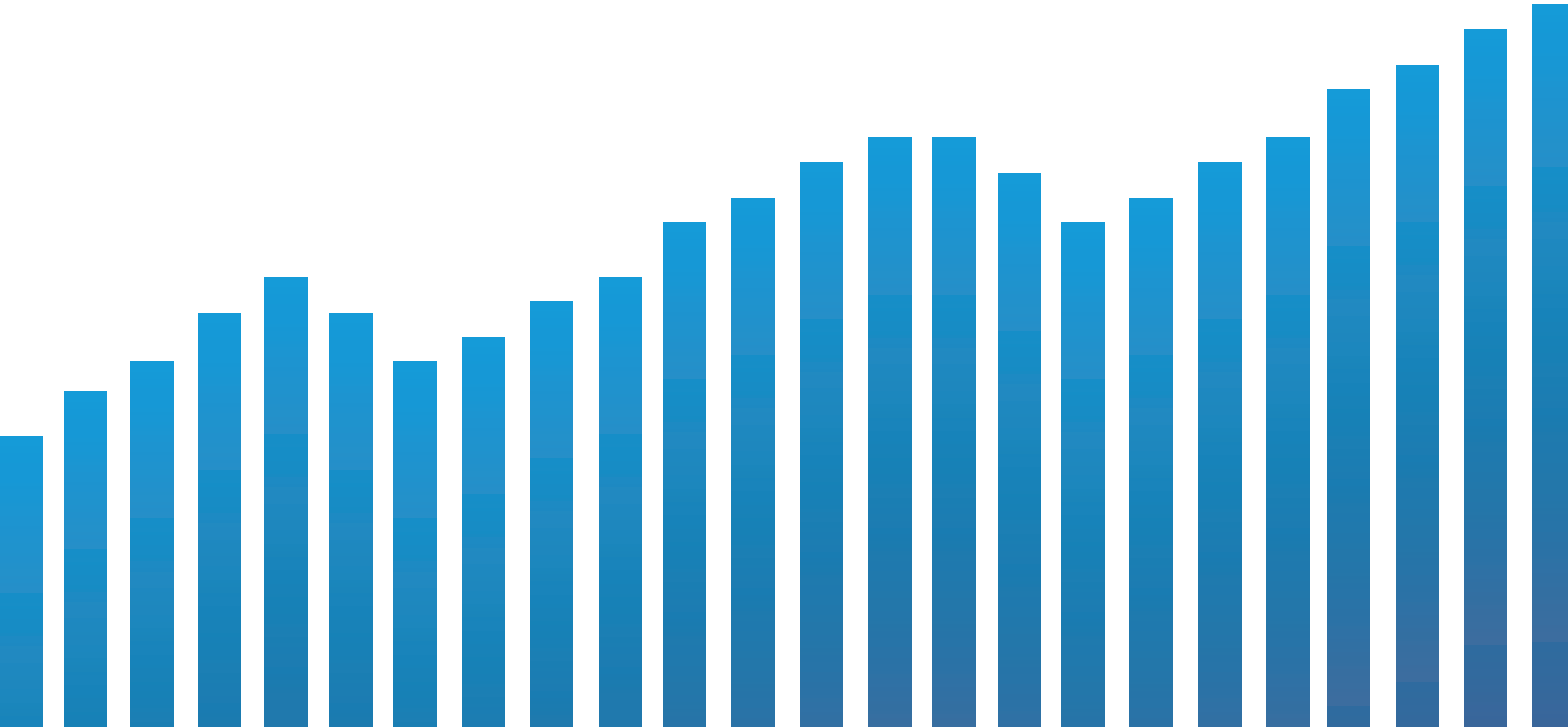
As pointed out in Chapter 1, more and more banks are employing or testing the use of biometrics during login and transaction authorisation, which can be exemplified by certain banks using fingerprints (mBank, Bank Millenium). According to the available studies, Poles are open to biometric solutions. They say they are convenient and trust them “conditionally” in terms of security. Implementing these solutions into massive systems has to be, however, preceded – apart from the obvious functional analysis (expressed as a percentage of correct identification) – by security tests as well as ergonomic analysis comprising complex tests with users. The solutions that are being put in place now may become a point of reference to customers and an actual market test. If they turn out to be unacceptable because of functional, security or convenience reasons, their development may be halted for an extended period of time.

Since we consider the triangle of security, financial results, and ergonomics when designing identification, authentication, and authorisation solutions, it is worth looking for those that improve one of these aspects, leaving the remaining ones at the same high level. For this reason we suggest striving for usability optimisation in tools that are already used, but also seeing the potential of services, which are of the same quality as the current ones in terms of security and usability, yet they may produce substantial cost savings.

To sum up, what all the remarks presented so far have in common is that it is necessary to consider the ergonomics of a tool's usability already at the stages of design or modification planning. Usability tests are about examining various solutions with users and experts from a given organisation. When it comes to the research presented here, a more ethnographic element is brought into focus, namely our ability to elicit customers' standpoint on the security of solutions that are designed, because in the area even users are aware that simplifying the process to the best possible extent is not always an optimum solution either for customers or for institutions.

UM USABILITY MONITOR

THIS CHAPTER WAS CO-CREATED BY MACIEJ KOSTRO, WHO IS THE OWNER OF THE USABILITY MONITOR SERVICE AND DEALS WITH THE ERGONOMICS OF TRANSACTIONAL SERVICES IN FINANCIAL COMPANIES. USABILITY MONITOR IS A RESEARCH SERVICE THAT CONSISTS IN ONGOING COLLECTION OF OPINIONS FROM CUSTOMERS OF TRANSACTIONAL BANK SYSTEMS, BOTH INTERNET AND MOBILE ONES, AND APPLICATIONS FOR NEW BANKING PRODUCTS.



CHAPTER 4 - NEED FOR STRONG INTERCHANNEL AUTHORISATION – A WAY OF APPROACHING IT

1. Introduction

In the previous chapters we have reviewed identification, authentication, and authorisation methods that are being currently used in the market. We have also pointed to upcoming regulatory changes which will have a substantial impact on the market. Now it is time to pose a question as to in which direction these methods should be developed, also in the context of technological changes and experiences from other markets, too. Proper protection of digital processes is key to convincing customers to migrate to remote channels and this is the core of many digital strategies implemented by financial institutions – but also other organisations e.g. in the public administration – all over the world. As we have also described above, ensuring the balance between ergonomic, economic, and protection quality dimensions is the success factor in the area. Selecting customer identification and authentication as well as transaction authorisation methods are key and interrelated elements for contemporary financial institutions. The methods and practices used so far turn out to be insufficient both due to the growing sophistication and determination on the part of cybercriminals. Another important element that will determine changes is the growing number of users that could be called “digital natives”. They have much higher expectations of the costs and ergonomics of security measures that they are offered. They do not accept non-ergonomic solutions, especially in the mobile channel and generally prefer to contact their service providers remotely. Since the group of customers is becoming increasingly active and their revenues are going up, service providers will attempt to meet their expectations, an effort that requires them to adopt an innovative approach to digital security.

REPORT EXPERT

WOJCIECH BOCZOŃ
BANKING MARKET EXPERT AND BANKIER.PL JOURNALIST

DIRECTION OF DEVELOPMENT – BIOMETRICS

E-banking customer authorisation methods are evolving as new technologies are becoming more widespread. Today's standard is authentication using SMSs, through which it is possible to conclude an agreement with a bank or to confirm instructions in Internet banking. One-time password scratch cards, which have been popular over the years, are becoming a thing of the past. It seems the same fate will be shared by equipment tokens. Customers are interested in authorising instructions using tools that are always available. They are provided with such a comfort by a phone and... their own bodies. It appears that in the nearest future biometrics will have a big role to play in customer identification. Biometric solutions are already used to authenticate customers' identity in institutions and ATMs. With just a single tap of your finger against a reader, you can order a transfer to be made or collect cash from an ATM. Apart from biometrics that maps the blood vessels under the skin used so far banks are starting to take advantage of other forms of biometric identification. Voice biometrics is used by call centres to identify a customer with his or her voice sample. This means that he or she does not have to remember all his or call centre passwords. Fingerprints, in turn, are used in mobile banking and payments by users of the latest smartphones. New services are beginning to appear that identify a customer with a photo of his or her face. You simply take a selfie and blink your eyes to authorise a transaction.

The Polish electronic banking market already has a logical model that takes account of the nature of the two main currently used channels of access to electronic banking – the Internet channel and the mobile channel. Such solutions are detailed in Chapter 1 and the table below gives an overview of them:

CHANNEL / PROCESS	AUTHENTIFICATION / IDENTIFICATION	CHANNEL ACTIVATION	TRANSACTION AUTORIZATION
INTERNET / WEB MOBILE	Unique ID + Password; OPTIONAL: Strong authentication with a mechanism used for authorisation	Assigning a unique password based on an "activation code"	SMS codes, mobile tokens, scratch cards, equipment token Trusted recipients – no extra authorisation
MOBILE APPLICATION	Unique ID + Password; RELATED (TRUST) DEVICES, OPTIONAL FOR RELATED DEVICES: Remembered ID and simplified digital PIN for an application (so called mobile PIN code)	Additional process with an additional authorisation tool (SMS code, telephone) or user-specific data	Trusted recipients – with no additional authorisation (or possibly up to a certain limit); Untrusted recipients – daily limit and/or mobile token and/or simplified digital PIN for an application (the so called mobile PIN)

REPORT EXPERT

CEZARY PIEKARSKI
DIRECTOR OF THE SECURITY DEPARTMENT, BANK MILLENNIUM

For many years the banking sector has sought an optimum model for two-factor authentication that could be used in a massive market. The widespread use of

> mobile phones, especially smart phones, and inconvenience have made one-time SMS passwords become a standard used by retail customers almost in the entire market. Unfortunately, the method has a number of disadvantages and is becoming obsolete in the context of current banking trends, such as multi-channelling and mobile banking. In addition, the method is ceasing to be secure due to the increasing number of efficient attacks on one-time SMS passwords. The changes and the expectations on the part of customers that access to electronic banking should be simplified are causing banks to search for new, secure, and convenient methods of identity confirmation. The attempts to adapt dedicated mobile applications or QR codes are not very much successful mainly because of the limited functionality, security, and the diversity of various mobile platforms, which makes it hard to implement them.
>
> It is my belief that new security mechanisms will come our way based on simplified biometric methods and mobile devices being integrated with the so called wearables. Promoting these authentication technologies will be dependent on cooperation with mobile devices producers and customers' attitudes to biometric technologies. I am convinced that this direction is the one enabling us to combine high security, convenience of use and contemporary technological trends. Irrespective of what the new standard multi-factor authentication model will look like, we can be sure that in the next couple of years both banks and their customers will face a great number of changes in the area.

2. Development direction – standardisation, behaviourism, and biometrics

In our opinion, the basic trends in the development of identification, authentication, and authorisation protection measures in remote processes include:

- Standardisation of general technical rule
- Biometric of various kinds
- Analysis of users' behaviours
- Complex solutions that combine the "external" side, i.e. that of users and the "internal" side, i.e. that of an institutioni

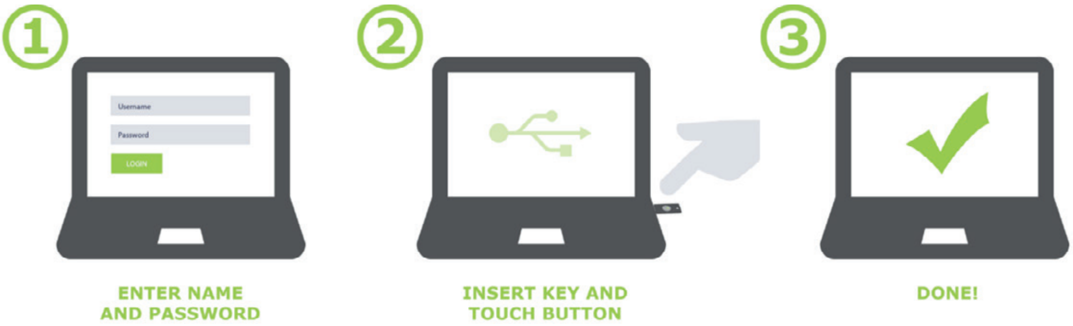
Standardisation of technical rules

EXAMPLE FROM THE MARKET

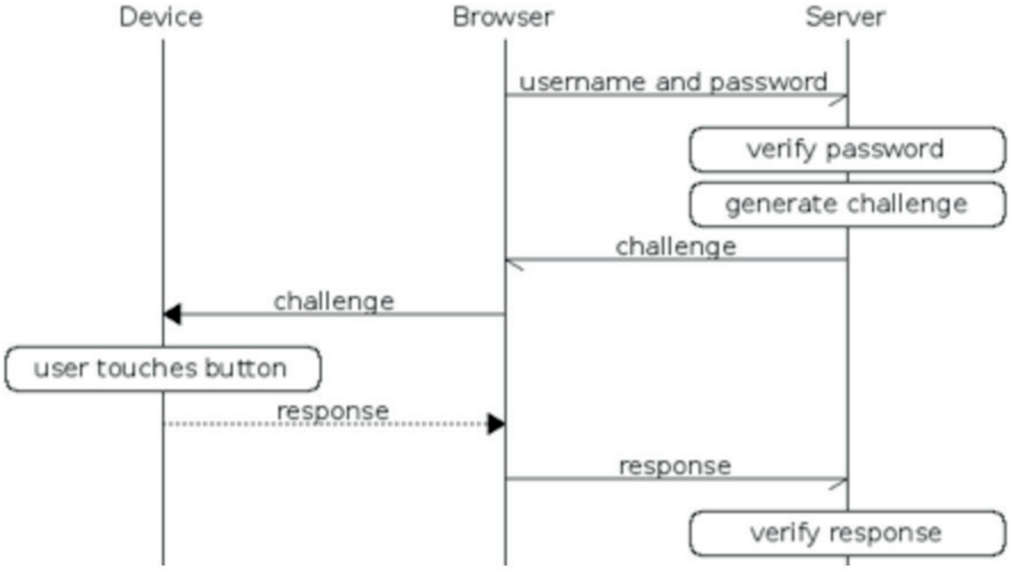
As many as 150 devices have been certified to the FIDO standard.

From the regulatory point of view the most interesting thing when it comes to authentication and authorisation systems and tools used is that customer strong authentication must be introduced. FIDO (Fast Identity Online) is the standard that is in use in the American market. It was created by over 250 companies, mainly American ones from the financial and technological sectors (e.g. PayPal, Bank of America, Google, MasterCard, Visa, Qualcomm, RSA, Samsung, and Lenovo). FIDO has the potential of becoming a widely used standard comprising the tools that already exist, emerge, or beginning to emerge and those that have not been created yet. The standard is sure to comprise biometric tools like those based on fingerprints, blood veins, voice or face as well as technical and equipment security measures, like tokens (including USB tokens), microprocessor cards, NFC modules and embedded secure elements. FIDO is ultimately designed to enable integration between two standards of two-factor identification that have been worked out – Universal 2nd Factor (U2F) and Universal Authentication Framework (UAF). The former was initially created by Google and Yubico and is now open. It specialises in using tools such as USB and NFC media as authentication tools

Examples from the market include YubiKey NEO tokens, and upgrades such as YubiKey 4 (Nano).



Schemat działania urządzeń U2F



Generally, the advantages of two-factor authentication (U2F) are presented in the arguments below:

- **Strong security** - strong two-factor authentication by means of public and crypto key with native support in a browser (starting with Chrome). Protection from phishing, session hijacking, men-in-the-middle type of attacks and malware attacks.

- **User friendly** - works out-of-the-box, allowing instant authentication of any number of services. No codes for another kind of services and no drivers to install.

- **High level of security** - allows users to select and control their own identities on-line. Each user may also decide to choose many identities, including an anonymous one (i.e. with no personal data matching his or her identity).

- **Multiplicity of options** - designed for telephones and computers for various authentication (mobile phone, fingerprint reader etc.) and communication (USB, NFC, Bluetooth) methods.

- **Interoperability** - an open standard supported by leading Internet and financial services providers, including Google, Bank of America and 250 companies in Fido Alliance.

- **Cost-efficiency** - service providers do not bear operational and support costs for safe distribution of U2F tools. Users are free to choose from a range of inexpensive devices from various suppliers available on Amazon and in other shops around the world.

- **E-Identity** - for services requiring a higher level of certainty as to identity, both services are developed both on-line and in the real world to tie a U2F solution to a user's true identity.

- **Secure recovery** -- it is recommended that users register at least two U2F devices for each service provider, one of whom can deliver a user with a backup code.

Biometrics

It is not a new phenomenon that a great deal of hope is being placed in the resolution of basic dilemmas related with safe and secure customer identification and authentication methods. In practical applications, biometric techniques are mainly used for identification of people (they compare the obtained features with a previously collected sample; in other words, they choose one over the many others, and verify it), and, to a lesser extent, identify them when it is necessary to compare the characteristics after measurements and compare with the already recorded sample.

Biometric methods have a disadvantage in that not everyone has a feature that can be measured and that almost all characteristics change during life. An important part is played by the so called quality of touch points, in other words, reading biometric parameters, which comprises both the characteristics of such sensors (e.g. a microphone in a laptop or a fingerprint reader in a smartphone) and the quality of Internet and telephone connections by means of which communication takes place. After a particular biometric method has been implemented, it also needs to be assessed for resilience to repeated attacks. In particular, new requirements need to be introduced correctly, such as information processing in a cloud (which is offered by some solution providers and which may end up leaking sensitive data through an unsecured communication channel).

Over the last two years, state-of-the-art and disruptive technologies in the area of authentication and authorisation have given rise to a greater number of mobile devices equipped with various biometric sensors and use of the already existing ones together with mobile devices themselves to build security systems and platforms. Examples of biometric sensors in telephones include a fingerprint sensor in the iPhone 6 and the Samsung S7 or an iris sensor in the ZTE Grand S3.

REPORT EXPERT

ŁUKASZ DYLĄG
CEO & FOUNDER AT VOICEPIN.COM

> Biometric technologies are becoming an integral part of identification and authentication processes in the financial services industry. For it is single innovations that are in a position to change the banking reality.
>
> Voice biometrics has been in use in banking for a couple of years now. Using it for authorising access to an account will ensure a high security level and faster and

simpler customer service. It is a personal verification technology based on differing voice characteristics of an individual which are virtually impossible to emulate. The solution gathers almost a hundred voice features to create a phonoscopic registration of an individual (VoicePIN). A simple phrase spoken by an individual is replaced by a number of digits, banking identifiers, and control questions.

The technology is also designed to detect fraud and proves an effective solution in this respect. Eligible customers are authenticated by the system seamlessly, which makes a significant contribution to identifying criminals. Consultants may monitor and analyse fraud risks in real time thanks to system indicators that inform them of a potential interlocutor being found in the BlackList database. The anti-fraud mechanism protects against attack attempts efficiently.

The fact that so much emphasis is now being placed on user convenience means that a financial institution has to phase out the traditional and currently used method of verification using passwords and PIN codes, because not only are they inconvenient for customers, but also generate costs for the company itself. Voice identity verification makes it possible to shorten the time during which a user is authorised by a couple of times and increase security level of the process. As opposed to passwords, which may fall into unauthorised hands, our voices are inimitable, and so are our fingerprints and irises.

Voice biometrics uses multichannel banking system solutions which enable providing customer service using the same voice password in such communication channels as IVR, call centre, a web page, and a mobile application without having to carry out another verification.

The growing interest on the part of banks and other financial institutions may stem from business advantages after the implementation of voice biometrics. The fact that the amount of time spent on connections is smaller, many channels are operated at the same time, and the number of consultants is decreased ensures fast ROI, and the user friendly and always available solution raises customer service standards. A biometric password implemented by a company is an excellent showcase for a company which is focussed on advanced security systems, comfort assurance and shorter customer service times. It is also an excellent marketing communication tool that enables a company to secure a competitive advantage.

Now we are going to discuss a voice password that will enable using mobile banking with no limits, at any time and place. This solution determines the direction in which safe access to personal data will be developed.

EXAMPLE FROM THE MARKET

The virtual Atom Bank uses face and voice biometrics, and machine learning to authenticate their own customers.

Apart from sensor-based solutions we would also like to pay attention to the ones entirely based on widely available devices which combined with innovative software create state-of-the-art ideas that raise the security in the multichannel world:

- **Voice biometrics** – for example a platform created by VoicePIN, which has experience of call centre system integration and is ready for mobile platform integration, also in the SaS model.

- **Universal authentication platform** – for example HID ActivID, which is a response to an increasing risk of digital process customer identity being attacked and resources being stolen as a result of social engineering attacks which compromise authorisation security measures.

- **Remote identification based on identity documents using state-of-the-art technologies** – this allowed Identt to build a tool for remote customer registration automatically and securely.

- **Eye biometrics**¸ especially such solutions as EyeVerify or IdentityX

Behavioural analysis of users

Another biometric factor that is approved of by lawmakers is behaviourism, which can be used as a way of operating a device (a keyboard, touch devices) or to create a user profile based on his or her behaviours in the system.

EXAMPLE FROM THE MARKET

BIOMETRIC ANALYSIS OF USERS' BEHAVIOURS

TeleSign has introduced an option of identifying users' behaviours. It is a new solution for Internet and mobile applications to measure and analyse the

> biometric data related to the behaviour of a particular user in order to ensure his or her continuous authentication, even when he or she has been identified through traditional security methods, such as passwords.
>
> The tool gathers and assesses the combination of the dynamics of an individual's mouse, keyboard, interaction GUI, and advanced behavioural algorithms to specify a unique user profile, save it, secure it, and thus avoid fraud and taking over the customer's account.

REPORT EXPERT

TIM PHIPPS
VICE PRESIDENT OF STRATEGY, IDENTITY AND ACCESS MANAGEMENT SOLUTIONS WITH HID GLOBAL

> To achieve desired revenue growth targets, meet risk and compliance challenges, and improve operational effectiveness banks must, in part, drive adoption of mobile channels and deliver a superior experience with increased convenience whilst improving security. This can be addressed through a multi-layered approach. The user, device, channel, transaction and back-end banking application are all authenticated with end-to-end trust.

3. Elements of the target identification, authentication and authorisation model – "internal" and "consumer" systems

In an attempt to build a target security model for institutions and users in mobile banking, we need to take account of both the consumer, and internal side, based on risk analysis for service providers. There are three areas to be mentioned from customers' perspective:

- **ergonomcs of usability**, or legibility as well as ease of authentication and authorisation (quick login and access to information/payments);

- **omni-channelling of solutions** – protection against attacks and ensuring the coherence of solutions for various channels from a user's perspective, ultimately also with a view to preparing for payments in the Internet of things (IoT/IoV); a multi-channel approach, authentication security, and increasing control over authorisation (secure channel, challenge-response with sensitive data verification);

- **the need for remote service should a transaction be blocked** (unblocking by users themselves vs. their visit to the branch);

- **education of and communication for customers**, including instructions on how to behave when security-related incidents occur from the perspective of a user and/or an institution.

The following areas are crucial to a service provider: protection from :

- fraud/unambiguity of action (secure confirmation/notification);
- costs of the tools (push rather than SMS; a mobile application instead of a dedicated device);
- ease of integration of other channels and tools, procedure of assigning access/ management (API oriented/security in the cloud).

EXAMPLE FROM THE MARKET

Wells Fargo combines various biometric features to increase security to a great degree and at the same time simplifies mobile access to banking. Wells Fargo offers two new options: voice and face biometrics, as well as scanning of eye lens. Authentication takes less than 15 seconds. User-friendly and quick CEO Mobile service.

In an attempt to balance security and convenience, it is vital to manage authentication and authorisation processes in a complex way in a number of channels that are made accessible by banks. For this reason, on the one hand, we can see more and more comfortable methods of customer biometric authentication in the mobile channel, a trend which will result in these methods being standardised and popularised in other channels. From the perspective of the system this requires an architecture that is open to integration, which will raise the level of requirements for the maturity of digital services, combined with the eIDAS and PSD2 directives.

In order to meet such requirements, electronic banking needs a flexible platform to manage customer identity that will combine the existing authentication methods and new biometric services so that they can be used in various channels of access to banks. Extended to include state-of- the-art authorisation methods and customer patterns, such a platform will enable banks to develop even more mature digital services.

ABOUT OBSERWATORIUM.BIZ

Obserwatorium.biz is a Polish independent counselling company set up in 2015. It specialises in developing and implementing digital strategies, especially for financial, IT, and government institutions. Our business activity is focused on the following:

- Business, technological, and strategic counselling for financial and IT sector companies in the area of optimising and implementing communication products, processes, and operations in Internet and mobile businesses and electronic payment systems; Audit of and consultancy in cybersecurity for e-businesses;

- Market research and analysis of mobile and Internet banking systems, electronic payment systems, and self service solutions, as well as non-cash payments considering the security aspect of using such solutions;

- Fintech market analysis and activities that coordinate cooperation between the sector and the sector of mature financial institutions;

- Co-organising conferences and preparing factual reports on e-business issues.

AUTHORS

dr Miłosz Brakoniecki
Obserwatorium.biz Board member

Co-founder of and Board member at Obserwatorium.biz. A Ph.D. in humanities, Department of Sociology, Adam Mickiewicz University, Poznań, Poland. He completed a post-graduate course in business strategy and planning at the University of Economics, Poznań, Poland. Between 2006 and 2014 he was the electronic banking manager at Bank Zachodni WBK, where he was responsible for business development of electronic banking, sales via electronic channels, and electronic payments in the bank. Between 2012 and 2014 he was a member of the Electronic Banking Council in the Polish Bank Association (ZBP). He has co-created Poland's biggest crowd-founding service Siepomaga.pl and is one of the founders of Siepomaga.pl foundation.

Michał Olczak
Obserwatorium.biz Board member

Co-founder of and Board member at Obserwatorium.biz. He has ten years' experience in developing safe applications. He is a security architect, the organiser of OWASP Poland, and a member of the Electronic Transactions Security Forum at ZBP

Piotr Sterczała
Obserwatorium.biz Board member

Co-founder of and Board member at Obserwatorium.biz. He graduated from the Department of IT and Electronic Economy at the University of Economics, Poznań, Poland. tBetween 2010 and 2014 he worked for Bank Zachodni WBK S.A., where he implemented and developed mobile and Internet banking in a business environment.

EKSPERCI

Tim Phipps
VP of Strategy, IAM Solutions, at HID Global

Tim Phipps is the VP of Strategy, IAM Solutions, at HID Global. He is responsible for defining market strategy and vertical solutions that help keep people safe in a digital world by providing a seamless, convenient and trusted experience.

Target markets include banking, healthcare and enterprise with a focus on securing end-to-end trust across mobile and cloud infrastructures using frictionless multi-layered user identification and authentication.

Mr. Phipps has spent over 25 years working in the Security and IT industry across a variety of sectors including major government projects, banking, defence, oil & gas, healthcare, telecommunications and transportation.

Mr. Phipps was born in the United Kingdom and graduated with a Joint Honours Degree in Physics and Computer Science at the University of Hull in 1989

Phil Hoyer
Director of Strategic Innovation at HID Global

Philip Hoyer is Director of Strategic Innovation at HID Global. His main responsibilities are driving Strategic Innovation projects specifically in Mobility Security Solutions, managing and creating new strategic alliances and business unit strategy. Philip represents HID Global on standards bodies such as GlobalPlatform (Strategic Director and Chair of Identity Task Force), Smart Card Alliance, IETF and OATH. He is a recognised subject matter expert on NFC, TSMs, Mobile Security, Identity, Cloud Security and Payment Standards, especially in financial services and e-government, who regularly speaks at major conferences. He has over 20 years experience architecting, building and delivering IT solutions, much of which was gained working as a solutions architect for a large consultancy. He holds a first class honours degree in Software Engineering from Westminster University

Wojciech Boczoń

Journalist at Bankier.pl

He is an expert on banking. He explores and reviews the latest financial products and services, tests electronic and mobile banking systems, and deals with personal finance security. He has written a number of comments, guide books, papers, and reports on banking for both the industry and its customers. He is the leading editor of the PRNews.pl portal. In 2013, he won the journalist of the year award from the jury of a competition held during the 9th Congress of Electronic Economy organised by the Polish Bank Association (ZBP). He is also a winner of the Marian Krzak journalist reward for the year 2014.

dr Paweł Widawski

Manager of the Team for Electronic Payment Systems and Banking, the Polish Bank Association (ZBP)

He is an expert at regulations on payment services and systems, electronic banking, and electronic economy. He is a law graduate at the University of Warsaw, where he obtained a University of Cambridge British Centre for English and European Legal Studies certificate. He has written publications on payment services regulations (Glosa, Bank – a monthly). He is a lecturer at the Chair of Administrative Economic and Banking Law at the Institute of Legal and Administrative Sciences at the University of Warsaw. He participates in sessions of the Council of the Payment Systems at NBP Board, is a member of the European Payments Council Board, and a member of the Payment Committee at the European Banking Federation.

In the European Commission, he was a member of the Payment System Expert Market Group and he participated in the Ad-hoc Group on revising the Directive on Electronic Money. He was a member of the Legal Support Group and the Programme Management Forum at the European Payments Council.

He participated in legislative works on financial services regulations.

Łukasz Dyląg
CEO & Founder at VoicePIN.com

He is a private entrepreneur and invests in interesting ideas in the IT industry. Łukasz specialises in corporate and project management, as well as investments and finances. He has an extensive knowledge of information and telecommunication technologies and rich experience in the IT industry.

He compares his work to an endless and exciting journey. He is quick at taking decisions and is not afraid of risk.

He has worked for Wind Telecom S.A., Pirios S.A., Bahaa Studio Sp. z o.o., and Connection One Sp. z o.o., being responsible for project management, supervision over technical divisions, and companies operational management.

On a day-to-day basis he runs VoicePIN.com, an innovative company that develops voice biometrics technologies.

Since September 2009, he has been President of the Board at Media Connection. Education:

Financial market analysis and investment consultancy, Kraków University of Economics;

Electronics and Telecommunications, Kraków University of Science and Technology

Robert Trętowski
Director of the IT Initiatives and Testing Department, PKO Bank Polski

He is an IT expert in for example retail and corporate banking, having worked in the sector for a dozen or so years. Between 2001 and 2011, he worked for BRE Bank S.A. and was responsible for electronic banking as well as business and IT cooperation. Since 2011, he has been the Director of the Application Developing and Maintenance Department at PKO BP S.A.. His responsibility include arranging new IT initiatives with the Bank's business entities and working out an approach to running tests. He is an Executive member of key projects for PKO BP S.A. such as migrating Inteligo into the PKO structures, Nordea Polska S.A. migration, setting up a German PKO BP branch, preparing PKO BP for delivering services to Zakład Ubezpieczeń Społecznych (Poland's Social Insurance Institution), new iPKO, development of the Cash Management and PKO Biznes offers for the Bank's corporate clients, the launching of PKO Życie, and many others. His work was key to implementing the IKO project at PKO BP and in the inter-banking initiative to develop and implement the BLIK mobile payment standard. Lately, he has been the main coordinator for the implementation of the Rodzina 500+ benefit programme for PKO BP S.A. and commercial banks that take part in the project.

Cezary Piekarski
Director of Security Department, BANK MILLENNIUM

Before he started working for the bank, he had spent more than 10 years in one of the biggest global advisory companies. His responsibilities included business security related services. He specialises in transforming the area of security, managing technological abuse, and rationalising operational risk costs. He is an experienced tutor and lecturer who runs classes during the post-graduate course “Zarządzanie Bezpieczeństwem Informacji” (“Information Security Management”) organised by Warsaw School of Economics.

Wojciech Dworakowski
Leader of the Polish branch of the OWASP foundation

He is an IT security consultant with a dozen or so years' experience. He is a partner in SecuRing, which has dealt with tests and consultancy in the area of IT applications and systems security. He has managed a number of projects in audit, assessment, and testing of IT systems and applications security, for example for leading companies in the financial sector and many public institutions. He has been a speaker at a significant number of conferences devoted to IT security. He holds the title of “the leading auditor of IT security management systems”. Since 2011 he has been the leader of the Polish branch of the Open Web Application Security Project foundation.

Artur Miękina
Independent e-identity market expert

He graduated from Lazarski University. He is an ENISA expert, and PIIT and PKN (Polish Committee for Standardization) member. For 13 years now, he has been dealing with public key architecture (PKI), including electronic signature. His areas of interest now include electronic trust and identification services under the eIDAS regulation. He has co-created the qualified Centre for Certification in PWPW S.A. and participated in key IT projects in the area of identification and its authentication in Poland

Piotr Brewiński
Coordinator for the Legislative Team, Polish Banks Association

He is a a solicitor and coordinator for the Legislative Team at the Polish Bank Association (ZBP), a member of a working group for physical security of the European Bank Federation. For many years, he has taken part in legislative works on the most significant regulations concerned with the banking sector and the payment services market. He coordinates works of the Banking Law Council at the Polish Bank Association.

He is a legal expert in banking, payment services and systems, electronic banking, outsourcing, new technologies and economic information. He is a law graduate at the Department of Law and Administration at the University of Warsaw, Poland. He obtained a Diploma in an Introduction to English Law and the Law of the European Union at the University of Cambridge. He completed legal counsel training in Warsaw and is a member of the District Chamber of Legal Advisers in Warsaw

ABOUT OBSERWATORIUM BIZ

his Report has been prepared based on desk research analysis that consisted in gathering information on web pages, via information lines and in bank branches, exploring mobile banking applications and Internet transactional services as well as data from the press and made available by financial and public institutions. The authors of the Report set up accounts and had access to electronic services in all the banks under investigation. Analysis was carried out in March 2016.

LEGAL NOTE

Opinions found in this report have been expressed based on the knowledge gained from market research and the authors' experience. The authors do not take responsibility for decisions based on opinions expressed in this report.