Advances in Web Development Journal
vol. 1 no. 3, pp. 26–45

*Submitted: 2023-10-13 | Revised: 2023-10-13 | Accepted: 2023-10-13*

*Keywords: cybersecurity, 2fa, authentication*

*Sebastian FLORCZAK [1], Adrian JASIAK [1], Izabela SZCZYGIEŁ [2*]*

# TWO-FACTOR AUTHENTICATION (2FA) COMPARISON OF METHODS AND APPLICATIONS

**Abstract**

*In this document, the investigation delves into the realm of two-factor authentication (2FA), exploring its applications and comparing various methods of implementation. Two-factor authentication, often referred to colloquially as two-step verification, serves to enhance credential security during login processes across platforms such as Facebook and online banking, among others. While 2FA has significantly improved the security of the login and registration processes, it is noteworthy that its adoption tends to be more prevalent among younger individuals. Unfortunately, an increasing number of financial scams target older individuals who may be disinclined to engage with what they perceive as the complexity of multi-step authentication and password confirmation. Subsequent chapters provide a discussion of the various types of two-factor authentication, furnish detailed descriptions, and offer a summary of the benefits and gains achievable through the deployment of 2FA.*

## 1.INTRODUCTION

The following project task will examine the topic of authentication two-factor authentication, what applications it has and the methods for doing so will be compared. Two-factor authentication is also colloquially known as two-factor login or two-factor login which secures credentials, for example, during the login process for platforms such as Facebook or any type of banking, but not only. Thanks to two-factor authentication logging in or registering has become safe for the user. It is worth pointing out, however, that it is mainly young people who simply use this power. Unfortunately, more and more material frauds result from older

1. University of Information Technology and Management, Poland
2. Rzeszow University of Technology, Department of Complex Systems, Poland

people being attacked because they are afraid of the 'complicated' login and confirming all passwords. The following sections will cover the types of two-step authentication, a description and a summary of what could be achieved or gained from this feature [1].

## 2.BASIC TERMS AND CONCEPTS

The basic question to ask yourself is, *are you sure this is you*? The process of identity verification, known as authentication, holds a paramount role in safeguarding our digital information. Ensuring that only authorized individuals can access our private resources is of utmost significance. A prime illustration of this necessity is in the context of email security. Moreover, authentication plays a critical role in scenarios such as mobile payments, where access to one's bank account is contingent upon a secure confirmation of identity. [3]

Users can prove their identity in several ways, the first of which is to enter a password, show proof of identity, and confirm with biometrics (eg. fingerprint, face). The most popular method is still the password. It proves that users are the person that they claim to be. Unfortunately, there is also the danger that if someone guesses or obtains our password, they could pass themselves off as us and gain access to all our confidential information that is protected by this password. Therefore, in our specialization, it is very important to teach loved ones to defend their passwords well, by using so-called strong passwords, which are difficult for hackers or attackers to obtain.

The problem with passwords is that it could be difficult to remember considering the fact the password for each service should be unique. With advances in technology, it is becoming very easy for attackers to check popular passwords and ultimately guess them or steal them en masse using techniques such as recording a log of keystrokes on a person's mobile device or keyboard. Leaks of password databases are also not uncommon [2].

Two-step authentication, which is also known as two-factor authentication, is a more secure way to confirm user identity. Instead of the required only one entry usually of a password, something that users are responsible for and they have determined, a second step is required. The second step is to enter a one-time code, which can come from different communication channels, e.g. SMS, mobile apps, emails or keys coming from hardware solutions [4].

One of the clear leaders in online authentication is Google. This company uses a wide range of free online services, such as Mail. This company needed to provide a secure authentication solution for many millions of people, and so it was Google that introduced two-step verification. Not only does this company provide us with the security of two-step verification, which is of course free of charge, social networks also secure themselves through two-step verification. It works in the following way, which means that, as standard, you need a username and password as on every platform, but once this is entered, users also need a mobile device in the form of a smartphone, which Two Factor Auth (2FA) is the second part of our verification, there are also two different ways in which users can use

phone for the login process. The first step is to register a phone number with Google. When a user authenticates using a name and password, the company will send an SMS message, or more precisely a unique code to be entered into our smartphone. The second method is to install a Google authentication application on our phone. This application then generates unique code, which is an advantage as users do not have to be connected to the network because the phone generates the code for the user. Two-factor authentication is not enabled by default and must be enabled by the user. Most applications do not support logging in using two-factor authentication for online services. An example of how 2FA works using SMS codes is shown on Fig. 1.

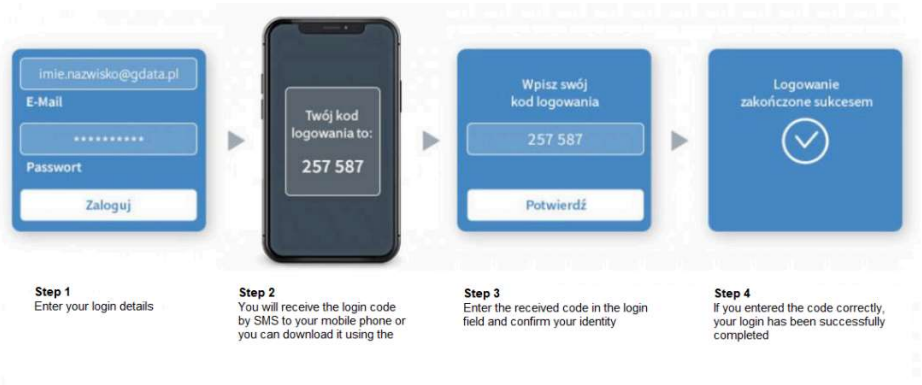


Fig. 1 - Example of 2FA operation scheme using SMS codes as an example [5]

Another example of two-factor authentication is the popular firewall "FortiGate." FortiGate includes authentication of users or groups of users. Once a user is verified, it applies certain security policies to allow or deny access to the network. Authentication is necessary in the following situations:

- Access to the device management platform,
- VPN access an example is given below in the screenshots,
- Traffic filtering policy on user groups [6].

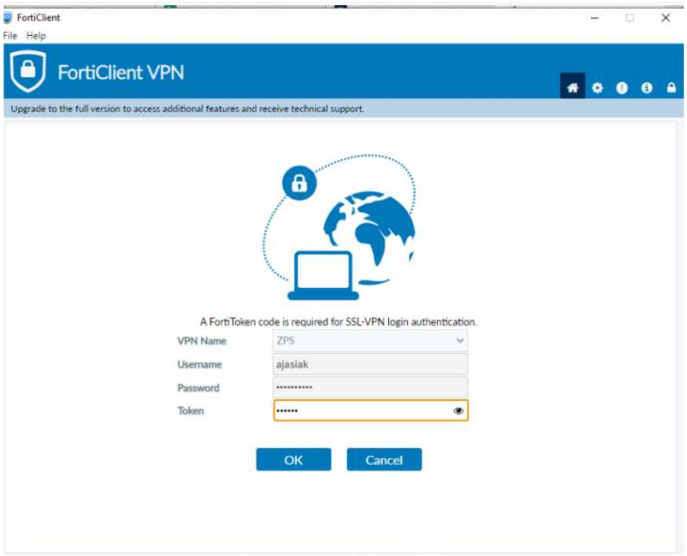


Fig. 2 - Logging into the FortiClient VPN with token

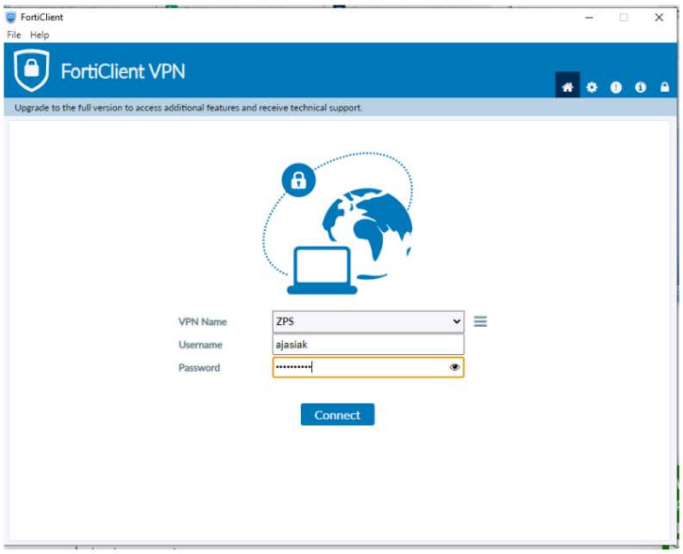


Fig. 3 - Logging into the FortiClient VPN with login and password

After logging in through the VPN (Fig. 2, Fig. 3), users first enter the username and password configured in the FortiGate management panel, and then a token is retrieved via the application on the phone, which must be entered at the authentication site.

Another example of two-step verification that is used on a daily basis in the medical structure are prescriptions, shown on Fig. 4 or e-referral issued to a patient. The patient who receives these two certificates is required, using the above, to provide a unique 4 digit code, which is downloaded from the nationwide P1 platform.


Fig. 4 - Example of e-prescription

In this case, in order to collect the administered medicine, the patient must, as a second condition, provide their unique PESEL number together with the prescription code.

## 3.DESCRIPTION OF ISSUES AND MECHANISMS

This chapter will present the most common two-factor authentication methods. It will discuss how they work and learn about the advantages and disadvantages of the respective solutions. Biometric authentication methods will not be described, as in most cases they can be circumvented by entering a password or PIN, and scratch cards with generated codes, as this method is very archaic. At 2FA page [7] users can easily check whether a particular service enables 2FA and how.

## 3.1. SMS CODE AUTHENTICATION

In this case, it uses a generated one-time code which was sent via SMS. This is a very convenient method of log-in confirmation. Convenient because users do not need to install any additional software but only need to associate a telephone number with our service and currently have access to a mobile network. In Poland, this method has become very popular due to the implementation of the PSD2 directive which came into force in 2019 in September. Banks were forced to implement 2FA and quite a few decided to implement it precisely through this method. This method allows the implementation of additional information in SMS codes informing about the operation being performed, e.g. the amount to be transferred. One-time SMS codes are used for:

- Login confirmation,
- Confirmation of operation [8].

SMS codes in "multiple" form are also often used when opening electronic documents sent by email, when SMS messages are sent with generated passwords to open documents such as credit agreements .

SMS codes are practically a free method for the user, as they do not force the for developers, however, they are not necessarily so cheap, as demonstrated by the example of Twitter, which, after its takeover by Elon Musk, cut free users off from using this confirmation, leaving only the other methods. In order to continue using SMS codes as a 2FA method, users need to purchase Twitter Blue for only around 44£ per month. Interestingly, Facebook and Google have not disabled the possibility of authentication via SMS codes, but always suggest confirmation via their mobile apps as a first step, considering the SMS method as a fallback. Popular Polish webmail services also do not offer an authentication method via SMS codes. Such authorisation requires the use of SMS gateways which, in connection with the server, send specific codes, and the producer of a given solution has to pay for the SMS [8a].

The login time increases minimally, which depends on a number of factors such as

- Network coverage
- Operator
- Server manufacturer load

Usually the extension is minimal, but from time to time the codes like to get lost somewhere get lost and then, after repeated requests, several come up. This is particularly noticeable especially in Chinese services of various cheap gadgets.


Fig. 5 - One-time SMS code

However, the inclusion of this 2FA method requires linking a cell phone number to a specific service, which undoubtedly constitutes the transfer of another person's data to a specific company, about whose security or extent of data processing users are always unsure.

An example of the list of services that allow authorisation by SMS codes is as follows:

- Google,
- Microsoft,
- Twitter (paid),
- Trusted Profile,
- Snapchat,
- Instagram,
- Tiktok,
- Facebook,
- Banks.

The solution is simple but not ideal in terms of safety. In August 2018, 7 fake apps appeared on the official Google Play shop impersonating Bank Zachodni WBK all of which asked for access to notifications and intercepted SMS codes and credentials by which the criminal gained access to the account [8]. SMS codes can also be intercepted via malware, e.g. widely used in 2011 was ZitMo and later TrickBot [9], which simply intercepted SMS messages and passed them on to criminals. 2FA is also subject to the method of Simswaping which involves impersonating the victim and making a duplicate SMS. When a duplicate SIM card is created, the basic SIM card stops working, so that all authentication codes go to the criminal.

## 3.2. AUTHENTICATION BY EMAIL CODES

This method is based on sending one-time codes by email shown on Fig.6. This method is not very common but is very cheap to implement, as all users need to do to use it, for example on non-standard equipment, is to set up an email server and allow them access to the internet. Rarely used in popular services rather as a last resort, e.g. still by Microsoft. In services that do not belong to the IT giants, however, it is used quite often, precisely because of its cheap implementation. It is often used by all Chinese services and also, as previously mentioned earlier, it is also used by various hardware such as Qnap.

However, the time for logging in increases quite considerably, emails do not always arrive immediately even though it seems obvious. Add to this the fact that many ordinary 'gray' users do not have mail configured on their mobile device, which results in the need to recall very complicated passwords or switch on the computer.

This method is easy to crack by gaining access to an email inbox or eavesdropping on communications via man-in-the-middle attacks.

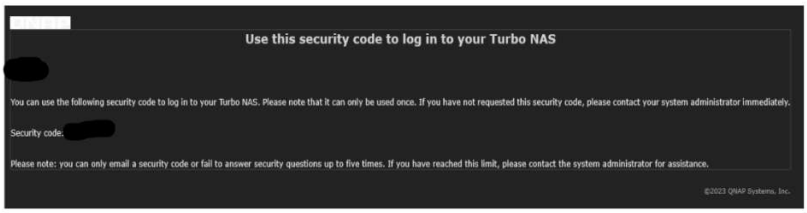


Fig. 6 - One-time code Email

## 3.3. AUTHENTICATION VIA MOBILE APP

In this case, users could use a specific application from the manufacturer of the service in question to confirm the operations performed. For example, when logging into Facebook on a new device, if a user is logged in to this portal on e.g. a mobile phone, he will receive an appropriate notification that someone is trying to log into our account. Very often users also obtain information about the approximate location from which the user is logging on and the operating system from which he or she is logging in. The location is, however, very approximate and is used rather in the context of country and region, although very often the location is stubbornly given in the very often when confirming logins on Apple devices, the location Warsaw is stubbornly given. If a VPN or Tor network is used, the user will also not obtain reliable results.

An example list of services using the above method is as follows:

- Google (Fig. 7),
- Facebook,
- Trusted profile,
- Banks.

This approach exhibits a high level of convenience and self-configuration. When setting up an Android phone, the user is virtually prompted to log into their Google account, and by enabling two-factor authentication (2FA) within the Google account settings, they gain the immediate capability to authenticate using the Google mobile application. A similar scenario applies to Facebook.

This method has virtually pushed banks' one-time SMS codes into the background. After implementation of the PSD2 directive, when Polish banks started to use massively one-time SMS after some time it was realized that this was not the safest method. In principle, every operation, e.g. transferring funds, signing a contract, logging in to a bank account requires confirmation of this operation on a trusted mobile device, where users could additionally confirm it with a PIN or biometrics.

Widely employed within the Apple ecosystem, the process of signing into various services with Apple ID entails a location-based verification step. This procedure typically initiates with a user confirmation to proceed with the login and subsequently necessitates the input of a six-digit code.

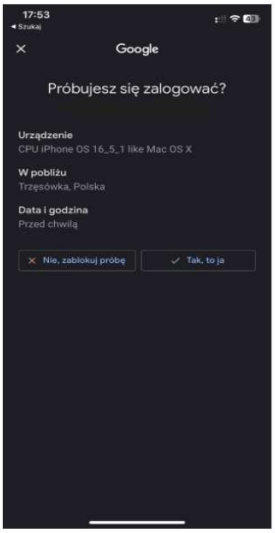


Fig. 7 - Example of Gmail login confirmation

When a device (usually a mobile phone) is lost due to theft or lost, users could lose the ability to log on to untrusted devices. If users only had one trusted device in the case of banks, this triggers various procedures that are tedious and time-consuming.

This method is also not immune to phishing, as evidenced by successful thefts of bank accounts using methods like Blik or by simply making transfers. In such cases, perpetrators posing as sellers or bank employees may instruct individuals to click through all notifications.

## 3.4. AUTHENTICATION BY TELEPHONE CALL

In general, this method is mainly only used during the first activation of the mobile applications at banks when users do not have access to another method of confirming their identity. It often works in combination with one-time passcodes sent by SMS or email as an additional security measure. When activating the mobile applications, users are called by an automated machine which, after informing us of the risks, gives us a one-time access code. Due to its time-consuming and inconvenient nature, it is only used in specific cases. It is used to scan a QR code generated on the site of interest.

## 3.5. AUTHENTICATION BY MEANS OF A ONE-TIME CODE GENERATING APPLICATION

The method, like previous methods, is still based on the generation of single-use codes used. However, the way they are generated and delivered changes diametrically. In this case, users need an application that does not have to be a specific manufacturer's application. Very importantly, it works without internet access. This application can be thought of as something like a random number generator, which regularly and frequently generates a sequence of new random numbers, every 30 seconds. A random number generator can have a 'seed' value to start the sequence, so that a given seed will always generate the same sequence of numbers. Pairing two 'versions' of the application makes the seed the same at both ends and synchronizes the clocks at each end. As long as the two clocks remain synchronized (modern devices usually have internal clocks that synchronize with the global time standard, so this is usually not a problem), the authentication pair will always have the same number and can 'recognise' each other.

The solution does not significantly increase login time, but it does force us to have a phone with the application installed at all times, as most applications run on mobile systems. However, the devices do not require constant internet access.

A very widely used solution in fact every major service allows the use of this solution. The exceptions, however, are banks, which probably stay with their applications for formal reasons. The same is true for government applications, the exception being the SIMP

system (pl. *System Informatyczny Monitorowania Profilaktyki*). The SIMP information system is dedicated for prevention monitoring.

A sample list of service providers offering this solution is as follows:

- Google,
- Microsoft,
- Twitter,
- Facebook,
- Instagram,
- Snapchat,
- SIMP,
- Polish Posts (WP, Onet).

An important aspect is that users can use any app from any manufacturer, it is sensible however, it is obviously advisable to choose a trusted application from a trusted source. An example list is as follows:

- Google Authenticator (Fig. 9),
- ESET Secure Authentication,
- Authenticator Plus,
- Authy,
- Aegis.

In terms of security, this is one of the better methods, only by stealing user devices and learning user login data, of course, gives the possibility of unauthorized access for a criminal. Usually phones are secured by PIN codes or biometrics and access to applications can also be blocked by the same methods. This method is not immune to phishing, as the criminal can simply force us to enter a one-time code. Simply intercepting the code with malware is much more difficult and here possible weaknesses are to be found in the applications that support this method. Even after interception, the criminal must act quickly, as the code expires after 30 seconds.

Facebook, after adding the application as a U2F method, additionally generates one-time codes for in the event of damage, loss or theft of the phone on which the application generating the codes is installed on.

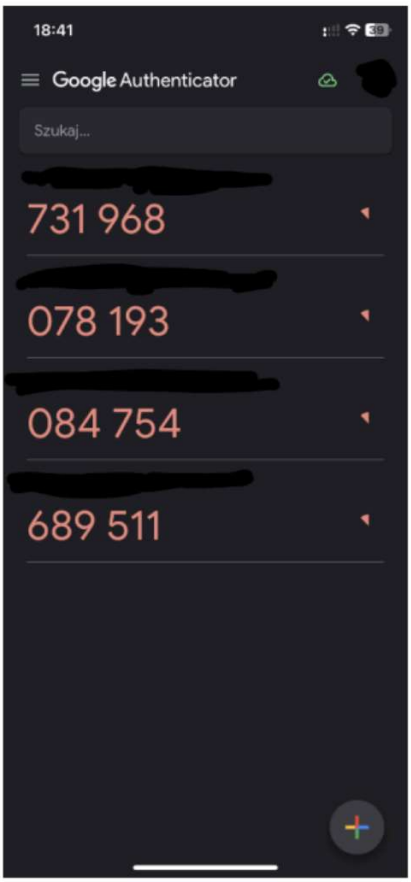


Fig. 9 - Screenshot from the Google Authenticator application

## 3.6. AUTHENTICATION WITH HARDWARE KEYS

There are two types of two-factor authentication by means of hardware solutions. In one, users generate one-time codes; in the other, a unique key pair is generated during configuration and a unique key pair is generated.

## Hardware tokens

These are small, lightweight devices that generate one-time access codes - Fig.10. They work similarly to mobile apps that generate one-time access codes, with the difference that generation takes place on dedicated hardware. When logging in, users need to read code generated by the service, enter it into the token and then enter the generated key to perform the desired operation. This is a very specific login method used practically only when performing operations on online bank accounts in companies. Hardware tokens work only with a specific service and their cost fluctuates around PLN 200. Service providers such as Google, Facebook and Microsoft do not offer this 2FA method. This method is not immune to phishing like the mobile application.


Fig. 10 - Hardware token from Millennium Bank [13]

## U2F keys

U2F keys are very interesting and innovative compared to the previously presented method of two-factor authentication. Practically all previous solutions were based on the generation of single-use codes, which were valid either until use or for a specific period of time. In the case of U2F keys, the principle of operation is radically different.

U2F keys are small devices that communicate with our device without the need to install additional drivers and software. When adding a U2F key to a service of our choice, a private and public key pair is generated. The public one is stored on the server of the service in question and the private one on the U2F key and never leaves this location.

The U2F dongle connects to a computer via a USB port, but there are versions with a USB-C port, Lighting, NFC interface so they work with basically any hardware. They have a high resistance to drops and water spills. In fact, the only manufacturer of U2F dongles is Yubiko [10].

The U2F key can operate in two modes:

- U2F,
- FIDO2.

In U2F mode, one typically enters their username and password when logging into the desired service. Afterward, the U2F key is inserted into the USB port or pressed into the phone. The PIN may also be entered, or biometrics, such as a fingerprint, can be used. In this manner, access to the desired service is obtained.

In FIDO2 mode, there is no need to input a login and password for the service, or sometimes, only a login is required. The entire authentication process is facilitated by the FIDO2 key.

Authentication with U2F keys is in principle the most secure method of authentication two-factor authentication. It eliminates the risk of phishing, as a criminal will not be able to extract the private key from the U2F key. It is also a very convenient method to use, as users do not have to enter or search for authorization codes, but only plug the key into the device. Only the configuration process can make it a little difficult.

As proof of the high level of security, the example of Google, which has massively started to implement U2F keys among its employees. As a result, the number of phishing incidents has decreased significantly.

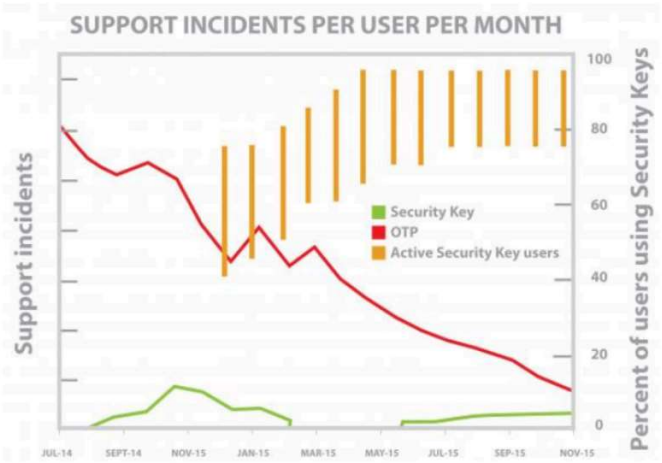


Fig. 11 - Results of Google's U2F launch among employees [10]

It is considered a best practice to acquire two U2F keys: one for regular use and the other to be securely stored in a safe location. This is a crucial precautionary measure, as the loss of the primary U2F key, particularly when it's the sole method of authorization and no trusted devices are registered, could potentially result in permanent loss of access to the service.

U2F keys are unfortunately not as common a method of 2FA as at least applications that generate single-use codes for several reasons. First, lack of knowledge, in fact most people still don't use 2FA, and if they do, it's through a banking app or SMS codes, so the word U2F still doesn't tell people much. Secondly the price, unfortunately it is not free, YubiKey [12] 5 NFC which is one of the most popular versions costs in the range of 250 PLN which, if two keys are purchased, generates a cost of 500 PLN.

However, the popularity of YubiKey is growing and more sites are choosing to implement them [11]. Unfortunately, however, banks in Poland still do not allow the use of U2F keys, only ING Bank [15] has such a possibility.


Fig. 12 - Yubico's U2F keys [10]

# 4. COMPARISON AND ANALYSIS

In this chapter users will put together a selection of two-factor authentication methods. In the form of a table - Tab.1, users will compile ourselves selected methods and then evaluate them with the following criteria:

- Security - how strongly a particular method protects users from hacking attacks and phishing,
- Universality - how many service providers enable a given 2FA service
- Convenience - whether using a given 2FA method significantly impedes the login process,
- Cost of implementation - how much does it cost for the user to implement the given method.

The following 2FA methods were selected:

- SMS codes,
- Mobile applications,
- Applications that generate one-time codes,
- U2F keys.

The analysis will not include authorizations by talking to a payphone and e-prescription codes due to their use in specific situations. Also omitted are also hardware tokens, as they are mainly used in online banking. Not also included in the analysis were codes sent via email, as they are less common than SMS codes and differ only in the way one-time use codes are sent.

A scale of 1 to 6 was used, along with a brief explanation, where 6 means best and 0 means worst. The ratings are the subjective assessment of the authors of the study and should not be drawn from them average.

| | **SMS codes** | **Mobile applications** | **Applications that generate one-time codes** | **U2F keys** |
|---|---|---|---|---|
| Security | Rating 3<br><br>Ability to capture codes, Sim Swapping, lack of immunity to Phishing. | Rating 5<br><br>No resistance to Phishing. | Rating 5<br><br>Lack of resistance to Phishing,<br>limited capabilities code interception. | Rating 6<br><br>Resistance to Phishing no possibility of code interception. |
| Universality | Rating 4<br><br>Common, however, slowly pushed aside more as emergency methods. | Rating 4.5<br><br>Very popular in online banking Internet banking. | Rating 4.5<br><br>Possible to use in quite a number | Rating 3.5<br><br>Still low awareness among users, in Poland only one bank supports U2F keys. |
| Convenience | Rating 4<br><br>All that is required is connection to a mobile phone and access to the network. requires rewriting the code. | Rating 5<br><br>Internet access required, only required to click on notification | Rating 5<br><br>Does not require access to the<br>Internet, requires rewriting code | Rating 5<br><br>It only requires inserting the U2F key into the device |
| Implementation cost | Rating 5<br><br>No cost to the user, however, requires access to the network. | Rating 5<br><br>No cost to the user, however, requires access to the network | Rating 6<br><br>No cost to the user. It does not require network access | Rating 4<br><br>This requires spending about 250 PLN on a "good day." |

**Tab. 1. Overview of selected two-factor authentication methods.**

## 5. SUMMARY AND CONCLUSIONS

The obvious fact is that the use of 2FA keys significantly increases the security of user data and, in general, where it is possible it should be included. The main criterion users should be guided by when choosing a method should always be to what extent it increases user security.

The most secure method is U2F keys, and they should be used whenever it is possible. In second place should be applications that generate one-time codes or mobile applications mainly in cases of online banking. The last method people should decide on SMS codes, but better such a method than none at all.

U2F keys may be a deterrent because of their price, but the paper's authors believe they would become more common if banks started implementing them. People are most are concerned when using the Internet about their money, and this would push them more toward buying a key.

Just as banks, through the PSD2 directive, have forced the use of 2FA in online banking, so other service providers should not only encourage but even force 2FA in their services.

**Author Contributions**
*All authors declare equal contribution to this research paper.*

**Conflicts of Interest**
☑ *The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.*

☐ *The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:*

……

**REFERENCES**


[1] Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. 2009 IEEE/ACS International Conference on Computer Systems and Applications, 641–644. doi:10.1109/AICCSA.2009.5069395

[2] Schneier, B. (2005). Two-Factor Authentication: Too Little, Too Late. *Commun. ACM, 48(4), 136*

[3] Simmons, G. (1988). A survey of information authentication. Proceedings of the IEEE, 76(5), 603-620.

[4] Ali, G., Ally Dida, M., & Elikana Sam, A. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. Future Internet, 12(10), 160. MDPI AG. Retrieved from http://dx.doi.org/10.3390/fi12100160

[5] Czym właściwie jest uwierzytelnianie dwuskładnikowe?, gdata, https://gdata.pl/przewodnik/czym-wlasciwie-jest-uwierzytelnianie-dwuskladnikowe

[6] Network Expert, https://networkexpert.pl/cyberbezpieczenstwo/fortigate/metody-uwierzytelniania-wurzadzeniach-fortigate-fortigate-firewall-authentication/

[7] 2FA Directory, https://2fa.directory/pl/

[8] Strona Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl

[9] Trickbot pushing a 2fa bypass app to bankcustomers in Germany https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bankcustomers-in-germany/

[10] Yubico, https://yubico.com

[11] Fido2, Webauthn and U2F Supported Sites (Full List), https://buybitcoinworldwide.com/dongle-auth/

[12] Kunnemann, G. (2013). YubiSecure? Formal Security Analysis Results for the Yubikey and YubiHSM. In Security and Trust Management (pp. 257–272). Springer Berlin Heidelberg

[13] Bank Millenium, https://www.bankmillennium.pl/przedsiebiorstwa/bankowosc-elektroniczna/bank-winternecie/millenet/bezpieczenstwo/token-sprzetowy-z-czytnikiem

[14] Two Factor Auth (2FA), https://brainstation.io/cybersecurity/two-factor-auth

[15] Klucz zabezpieczeń U2F, ING, https://www.ing.pl/wiem/bezpieczenstwo/klucz-zabezpieczen-u2f-jak-to-dziala


.