MUNI
FAKULTA
SOCIÁLNÍCH
STUDIÍ

MUNI
FAKULTA
INFORMATIKY

User Testing of Mobile Banking Authentication Methods

UX Testing, User Interviews, and Quantitative Survey

Technical report for TA ČR project *Innovation and adaptation of authentication technologies for secure digital environment (TL01000207)*

Authors:

Mgr. Agáta Kružíková

Mgr. Lenka Knapová

Mgr. Ondřej Gabrhelík

Prof. PhDr. David Šmahel, Ph.D.

Mgr. Lenka Dědková, Ph.D.

Prof. RNDr. Václav Matyáš, M.Sc., Ph.D.

Mgr. Petr Doležal

Mgr. Martina Šmahelová, Ph.D.

MUNI Interdisciplinary Research Team on Internet and Society

CROCS

KEY FINDINGS

This report describes the results of testing of authentication methods and applications for smartphones, including the methodology that was used. We want to determine the authentication methods that are perceived as secure and user-friendly by the end users, and which methods users would prefer. This technical report may be of interest to security experts, IT security managers, UX experts, and researchers in the field of usable security. The report can help them understand user evaluation of the methods and the factors that influence it.

The document has three parts: (1) Security and the threats of selected authentication methods: Technical specifications; (2) UX testing and interviews with users; and (3) a quantitative survey of the adult and elderly populations. The following is a summary of the key points of these three parts. Links in the text will take you to more detailed information further in the technical report.

(1) Key facts: Security and the threats of selected authentication methods: Technical specifications

The following authentication methods have been implemented for use on smartphones (with Android OS): a one-time SMS code, a PIN code, a fingerprint, a FIDO token, an identification smart card (i.e., a payment card) that is attached to an NFC reader or inserted into a card reader, and an NFC token. The strengths and weaknesses of these methods are described in detail here. The technical specification of the methods can be summarized as follows:

- One-time SMS code: one of the most commonly used methods within two-factor authentication. Its advantage is a simple implementation. The disadvantage is the cost for each SMS and susceptibility to having the SMS redirected to an attacker.
- PIN code: a commonly used method, which is insufficient for certain financial operations in terms of security because of its susceptibility to simple attacks, such as observation, social engineering, correct guesses, the use of a key logger, overlay, or eavesdropping.
- Fingerprint: a promising method thanks to its user-friendliness but it does not provide high security due to the lack of quality implementation on smartphones (e.g., no liveness detection) and the existence of masterprint attacks.
- FIDO token: a method based on strong asymmetric cryptography that is subject to certification. By definition (i.e., storing arbitrary cryptographic keys on an arbitrary FIDO token) the bank has no control over who the token owner is and for which services it is used.
- Smart card (i.e., payment card): a rarely used method, both when used via NFC smartphone reader and when inserted into a card reader. Its security always depends on the specific implementation of the cryptographic algorithms, functions, and keys. In general, smart cards are the strongest authentication method.
- NFC token: security of this method depends on the specific chip used in the token. Thus, the level of security can be the same as for a FIDO token and for smart cards.

(2) UX testing and interviews with users

The aim of the user interviews and UX testing was to determine a detailed evaluation of the application and the selected authentication methods on a sample of selected end users. This study was necessary to test the appearance and the clarity of the applications and to ensure their maximum user-friendliness. We conducted the study on a sample of 33 users of all age groups. The methodological procedure of this study is described in detail here. Detailed results of this testing are described here.

Key findings: UX testing

Among the most fundamental findings of the UX testing are the following:

- The consistency of control elements and terminology is essential for easy orientation in the applications. Inconsistent use of the terms *username*, *login*, and *client name* often creates confusion.
- Text in applications should briefly and concisely inform the user about the state of the application. This can be achieved by highlighting keywords and shortening detailed text that discourages reading.
- Animations and graphics throughout the applications are helpful. They should correspond with reality (e.g., a realistic depiction of the token).
- New and technical concepts need to be explained. For example, the use of a 5-digit PIN code (unlike the more common 4-digit code) was problematic. The labels FIDO and NFC token were also confusing. Therefore, only the word *token* with a demonstration of this hardware was later used. The term *transaction*, meaning any operation that needs to be authenticated, was also unclear because the users assumed that the term meant a financial transaction only. In the end, the term *request* was chosen.

Key findings: Interviews with users regarding the evaluation of authentication methods

The main recommendations for developing and implementing authentication methods that came from the user interviews include the following:

- New methods of authentication should be offered as a complex service that involves the relevant institutions (e.g., banks) and services (e.g., technical support during an attack).
- The product owner of the authentication method must understand the needs and concerns of the user and consider them during the design phase.
- New methods and combinations should build upon and incorporate existing methods and devices that are commonly available.
- Eventual new methods could be used for more operations outside of online banking in order to increase their usefulness and acceptability for the user (e.g., a token as a memory disk).
- The relative stability of preferred authentication methods requires the continuous monitoring of the state of attacks and security of these methods and constant improvement of their security solutions.

Reasons for user preference of fingerprint authentication (based on the interviews):

- Users believe that every fingerprint is absolutely unique.
- Potential risks, such as kidnapping or chopping off a finger, are perceived as unlikely, and thus do not concern users.

- Users believe there is no need for special security-related behavior when using fingerprint authentication.
- Fingerprint authentication is now supported by most smartphones, so users generally believe in the future of this method, which reduces their motivation to adopt other novel technologies.
- Users do not need any additional devices. The method is fast, simple, and intuitive. If fingerprint authentication is not possible, a backup method (usually a PIN) is always available.

(3) **Quantitative survey of the adult and elderly populations**

The aim of the quantitative survey was to investigate the current user experience with online banking and to test the selected authentication methods (PIN code, fingerprint, smart card inserted into a card reader, and NFC token) with a focus on perceived user-friendliness and security, and the preference for these methods. A quantitative survey of a sample of 500 users (250 adults up to the age of 54, further referred to as "adults"; and 250 people aged 55 and older, further referred to as "the elderly") built upon the UX testing and interviews with users. The methodological procedure of the quantitative study is described in detail here. Detailed results are described here.

Key findings: Quantitative survey

Experience with online banking and authentication methods (detailed results here)

- The vast majority of respondents has used some form of online banking (97% of adults, 86% of the elderly).
  - Most respondents accessed online banking by computer, followed by mobile banking applications used especially by adults.
  - Most of both populations accessed internet banking several times a month or several times a week. A few did so daily.
- The most common authentication methods for logging in to online banking were username and password (87-88% for both populations) and a PIN code (73% of adults, 76% of the elderly). Adults had more experience with fingerprint authentication (29%) than the elderly (12%).
- When confirming payments in online banking, most respondents had experience with an SMS code (more than 95% in both groups), followed by a PIN code and a password (50% of the adults, 36-39% of the elderly).

Two-factor authentication (2FA) (detailed results here)

- Most of those surveyed (84%) had previous experience with 2FA.
- At least three-quarters said that they would like to use 2FA for online card payments and confirmation of online money transfers. They seem to realize the importance of asset protection and appreciate these security features.
- Although almost all of the respondents had previous experience with the SMS code, more than half would not mind if this method was replaced. On the other hand, replacing the SMS code would bother about a third of the respondents. Thus, prior experience does not necessarily imply a preference.

Evaluation of tested authentication methods (detailed results here)

Based on practical experience gained during interaction with the authentication methods on a smartphone, respondents rated them in the following categories: *ease of use*, *practicality,* and *security*.

- Respondents perceived the specific methods (PIN code, fingerprint, smart card inserted into a card reader, and NFC token) positively in all three categories.
- The fingerprint was perceived as the easiest to use, the most practical, and the most secure method by both populations.
- The elderly evaluated the authentication methods based on the ownership of an object (i.e., token, card reader) similarly in all categories. Adults, on the other hand, felt that inserting a card into a reader was more complicated and less practical than using a token.

Preferences for authentication methods for payment confirmation (detailed results here)

We evaluated the preferences of individual authentication methods and their combinations for online banking payments, depending on the amount of the transaction:

- Almost half of the respondents would like to use fingerprint authentication to confirm payments of higher amounts, which is in line with its positive evaluation (e.g., easy to use, practical, and secure).
- The second most preferred one-factor method for paying both lower and higher amounts was the PIN code, which had high ratings for ease of use and practicality (both second to the fingerprint).
- In the case of the proposed two-factor combinations, approximately one-fifth would never want to use the specific combinations. However, this is probably due to the preference for other combination of methods.
- The majority of respondents (51-72%) would like to use individual 2FA combinations of methods to confirm payments of higher amounts.
- In both the adult and elderly populations, the 2FA combination including fingerprint authentication (i.e., fingerprint + token) was slightly preferred.

Summary

The testing with users focused on the evaluation of authentication methods (PIN, fingerprint, inserting a smart card into a card reader, and token) and showed a clear preference for fingerprint authentication. It was rated as the easiest to use, the most practical, and the most secure by our respondents. The reasons were indicated in interviews. Users perceive the fingerprint as unique and difficult to misuse (they perceive physical risks as unlikely). They also positively evaluate its current availability and the presence of a backup method.

Due to the stability of the perception and preference of the authentication methods, it is recommended, among other, to strive to increase the security of the methods that users prefer, like the implementation of more secure fingerprint readers.

Although the other tested methods were assessed as less practical (especially those based on the ownership of an additional piece of hardware, like the token and the reader), their evaluation was still overall positive.

Please cite this report as:

Kružíková, A., Knapová, L., Gabrhelík, O., Šmahel, D., Dědková, L., Matyáš, V., Doležal, P., & Šmahelová, M. (2020). User Testing of Mobile Banking Authentication Methods: UX Testing, User Interviews, and Quantitative Survey. Brno: Masaryk University. https://doi.org/10.13140/RG.2.2.16528.97288

TECHNICAL REPORT

(1) Security and the threats of selected authentication methods: Technical specifications

Authentication is the process of verifying that a user is who they claim to be. The best-known authentication methods include logging in with using a username and a password. As the number of online services and devices grows, so does the number of authentications a user has to perform daily. The usability of authentication methods is one of the key aspects for their proper, trouble-free, and secure use. This report discusses specific examples of one-factor and two-factor authentication. For single-factor authentication (1FA), only one authentication method is used as the single factor (e.g., a numeric code). Two-factor authentication (2FA) uses a combination of two independent authentication methods, often a combination of different types of methods, including "something I have" – a token; "something I know" – a numeric code/password; and "something I am" – biometrics.

The most common authentication methods in the banking sector include a numeric code (PIN), a fingerprint, and a one-time SMS code. Although some of these methods have long been considered hard to compromise, their security may not be sufficient for some financial operations (e.g., transferring large amounts of money between accounts).

After a mutual dialogue between security experts from AHEAD iTec, s.r.o. and researchers in the fields of computer security and psychology at Masaryk University, the following methods were implemented as the functionality of a smartphone authentication application:

1. one-time SMS code,
2. numeric code (five-digit PIN),
3. biometrics (fingerprint),
4. hardware token (FIDO token, NFC token), and
5. smart card (inserting the card into a reader or attaching it to the NFC reader on a smartphone).

The methods were chosen with regard to the prevalence of different options. The aim was to compare methods with different levels of security and to include methods that are not yet widely used but that have great potential for future use by different user groups.

SMS code

The SMS code is still the most used method for two-factor authentication for most Czech banks. The reason for the spread of this method was the expansion of mobile phones (not just smartphones). The main competitors for SMS codes were OTP (One-Time Password) calculators and other specialized hardware, which represented high initial costs. Another advantage for SMS codes was the relatively simple implementation into the bank systems. The disadvantages are the price for sending the SMS and the security of this technology. Attacks on bank accounts that redirect authentication SMS codes to an attacker are well known and quite common in the Czech Republic (although they are not often publicized). The attack consists in installing an application that sends incoming SMS codes from the bank to the attacker's phone number in real-time. The Android platform allows for the development and distribution of such applications.

Numeric PIN

Attacks directed at PIN codes are generally known and, in the most common cases, simple. A PIN can be compromised in several ways:

- Visual observation (i.e., shoulder surfing) when the user enters the PIN code, or possible detection from the usage marks left on the screen.
- Social engineering (e.g., phishing emails).
- An overlay attack (e.g., the user enters data into a fraudulent application that poses as an official service).
- A brute force attack (e.g., attempting all possible combinations of the PIN), or a guess.
- A keylogger (e.g., a program that records the pressed keys on the keyboard).
- Reading the PIN from the device memory or intercepting or eavesdropping the communication.

Nevertheless, if the PIN is compromised, it can be changed. Some of the above-mentioned attacks can be prevented by a well-chosen PIN and its storage in an encrypted or a hashed form.

Fingerprint

A fingerprint authentication resolves some of the issues with the previous authentication methods, and its security level is sufficient for most use cases. Another advantage is its speed, price, and usability. However, this technology has its weaknesses as well, so it is more suitable as a complementary method:

- Inadequate hardware and software implementation on Android devices (especially on cheaper models, but also on some high-end smartphones) (Paul & Irvine, 2016).
- The absence of liveness detection (i.e., the reader is not able to determine if an animate person's finger is being used or its counterfeit; this applies to both Android and iOS platforms).
- Masterprint attacks (i.e., a fingerprint that is similar to multiple fingerprints; this attack is possible because only some markers, and not the entire fingerprint, are compared during the authentication process).

FIDO token

FIDO tokens are based on strong asymmetric cryptography that uses elliptic curve technology (ECDSA). Every hardware manufacturer who supports the FIDO protocol must meet demanding certification standards to protect the private keys generated and stored directly in the token, thus significantly eliminating the possibility of key disclosure. For banks and similar entities, however, the openness of the solution is still a major problem that prevents its wider use among end clients. The FIDO protocol allows arbitrary keys to be stored on any FIDO token; the bank, therefore, cannot, by definition, have any control over who owns the physical token or for what services the token is used.

To use FIDO tokens, it was necessary to implement an official SDK (software development kit) for Android, which proved to be inconvenient during development and subsequent testing, both in terms of application stability and user interface. The SDK contains visual components that were confusing for the users and that could not be changed or omitted.

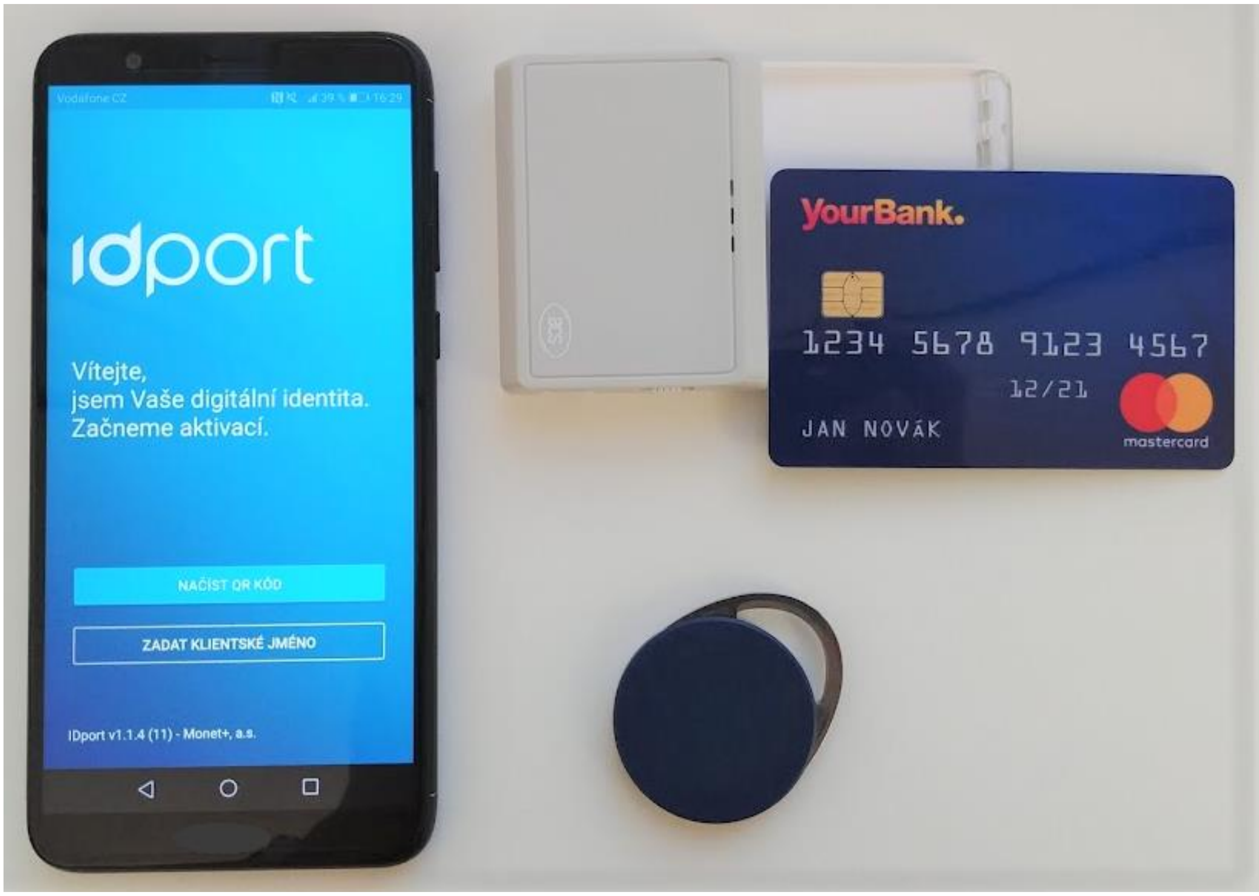


Figure 1: Hardware used for testing: smartphone, card reader and payment card, NFC token.

Smart card

The security of smart cards is dependent on the implementation of authentication functions, the algorithms used, cryptography, and parameters of keys (Mayes & Markantonakis, 2017). In general, smart cards are the strongest method of authentication. Using asymmetric algorithms (ECDSA, RSA) in combination with properly configured smart card processes (e.g., personalization, distribution, activation, PIN setup) creates ecosystems that can be used in environments with the highest security demands.

However, the use of these systems in combination with smartphones is still rare, so this project explored two ways of using a smart card in communication with the smartphone:

1. Contactless smart card that communicates via NFC technology.
2. Contact smart card inserted into an external card reader that communicates via Bluetooth technology.[1]

The security itself is comparable. Both cards contain the same algorithms, the same keys, and the same type of chip technology. Both NFC and Bluetooth communication can be tapped or modified. The difference in security arises with (non)use and the length of the PIN.

NFC token

The NFC token can contain several types of chips, including chips that are compatible with the FIDO protocol and chips that correspond to the conventional smart cards mentioned in the previous section. Furthermore, there are many proprietary NFC chips that contain symmetric and / or asymmetric cryptography (Mayes & Markantonakis, 2017). For our implementation, we chose the NTAG[2] chip from the NXP company. This chip is designed to best support communication with a smartphone and meets the essential security requirements. The security of this solution does not reach the level of smart cards; it is based on the verification of the token originality by means of elliptic curves (ECC).[3]

[1] The ACS contact smart card reader (ACR3901U-S1) was selected for communication with the payment card. The ACS SDK was implemented as part of the mobile authentication application.

[2] Detailed description here: https://www.nxp.com/products/rfid-nfc/nfc-hf/ntag:MC_71717

[3] Detailed description here: https://www.nxp.com/products/rfid-nfc/nfc-hf/ntag/ntag-for-tags-labels/ntag210-ntag212-ntag-21x-nfc-forum-type-2-tag-ic-with-multiple-user-memory-sizes:NTAG210_NTAG212#documentation

(2) UX testing and interviews with users

Methodology

Description of the study

UX testing and interviews with users consisted of the iterative testing of the authentication method prototypes and the individual applications with users and subsequent modifications and innovation of the applications based on user evaluation and behavior. The primary tested application was the IDport digital identity application. The application was used for user authentication and the authorization of requests and supported the selected authentication methods. Users also interacted with a fictitious online bank, YourBank, through a mobile application and a web interface.

Four separate rounds of testing took place. After each round, the findings were implemented into the relevant software. Such iterative testing and development ensured the necessary quality of the authentication methods to enable further testing in a large-scale quantitative survey. The first and second rounds mainly included UX testing. The third and fourth rounds focused primarily on a detailed evaluation of the authentication methods, their perceived user-friendliness and security, and ways of thinking about these topics. In addition to the PIN and fingerprint, the following methods were tested in each round:

First round: one-time SMS code, hardware token (FIDO token), and payment card inserted into a card reader.

Second round: hardware token (FIDO token) and payment card inserted into a card reader.

Third round: hardware token (NFC token) and payment card inserted into a card reader.

Fourth round: payment card (read by smartphone via NFC).

The change in authentication methods between rounds (e.g., the transition from a FIDO token to an NFC token) was due to the technical aspects and the user evaluations of each method. In the case of the FIDO token, it was necessary to redirect to an external service and it was not possible to ensure a stable flow of the authentication process for all users. Moreover, the users themselves rated this external service as problematic and not user-friendly. Therefore, we decided not to test the FIDO token and replaced it with a token that communicated with the smartphone via NFC.

Testing procedure

During testing, the users tried out at least three separate authentication methods and then were interviewed about the perceived user-friendliness and security, and preferences for these methods. They also completed questionnaires (demographic questions and user-friendliness of the methods). The whole procedure for one respondent lasted from 45 to 90 minutes and was conducted in Czech language. Before testing, the respondent signed an informed consent form. The testing was approved by the *Ethics Committee for Research* at Masaryk University.

At the beginning of the testing, the respondents were told that their bank recommended them to use a new application to confirm requests in online banking (i.e., a mobile authentication application). The users were instructed to activate the application and then log into the online banking and eventually pay for a vacation. In both cases, the users were redirected from the online banking to the authentication application to confirm the request.

During the testing, respondents went through the activation and authentication scenarios. The activation scenario (activation of the authentication application, i.e., identity confirmation) used the methods of sending a one-time SMS code, using a smart card (a payment card inserted into a card reader), or using a hardware token (FIDO or NFC). The authentication scenario (i.e., confirming the online banking login and sending payment) used both 1. a PIN or a fingerprint; and 2. inserting a payment card into a card reader or using a hardware token.

Sample and its selection

The user study targeted the adult population, including the elderly. The inclusion criteria were to be an active user of a smartphone and online banking, and to not have studied or worked in IT.

The sampling method was convenience sampling combined with the snowball method (i.e., referrals from other respondents themselves).

A total of 33 users were tested in the user study: 8 in the first round; 8 in the second round; 7 in the third round; and 10 in the fourth round. Of the 33 respondents, 17 were women and 12 were over the age of 60.

Results and recommendations from UX testing and user interviews

UX testing of the authentication methods and applications addressed user-friendliness and user satisfaction. The subsequent user interviews focused on how users think about security and how they make related decisions.

UX testing

In the first two rounds, the emphasis was primarily on aesthetics and the clarity of the visual and textual elements.

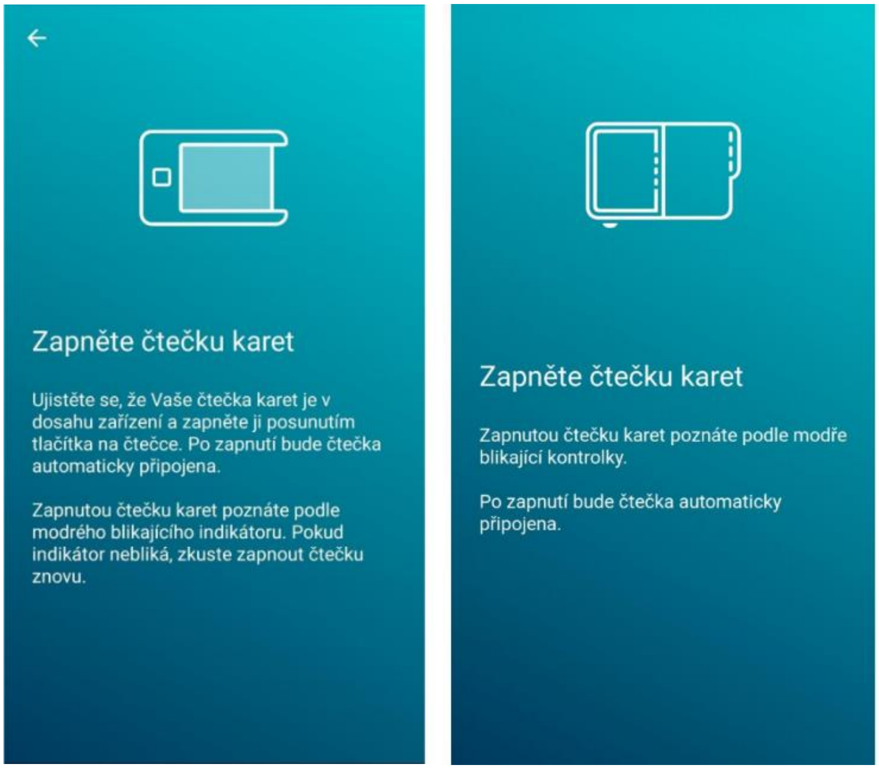
Consistency

Although the completion of the tasks in the application was a relatively short process, users quickly developed habits and perceived it to be confusing if the application was inconsistent (e.g., a label was at the top on one screen and at the bottom on another). Care should also be taken to ensure consistency in naming and terminology. The biggest problem for users was the term *username* because it was labelled as *client name* in a letter from the bank. Users also mentioned the existence of *login* (this term was not mentioned anywhere in the testing) and the fact that different services use these terms to mean different things. Users were also not sure if they were synonyms. In later versions of the applications and test materials, only the term *client name* was used, which no longer caused any problems.

The amount of text

Users commented on the amount of explanatory text in the application. In general, they want to keep track of what is happening because they want to have the application and payment process under control, but text blocks that are too long discourage reading. In later versions of the application, the texts were reformulated to be short and concise. Information that users did not find helpful was dropped, and the keywords were highlighted in bold.

For example, instead *of "You will use the PIN in your e-banking. Therefore, do not use personal or easy-to-guess data"* we used *"You will confirm incoming requests with your* ***personal PIN****. Do not use easy-to-guess numbers.*" Another example is the replacement of the text *"Your device qualifies for confirming operations by fingerprint. You can use your fingerprint instead of your chosen PIN code. To continue in the application, scan your index finger on the fingerprint reader.*" with the text *"To complete the activation, verify your identity with a fingerprint*." Another example can be seen in Figure 2.



Zapněte čtečku karet

Ujistěte se, že Vaše čtečka karet je v dosahu zařízení a zapněte ji posunutím tlačítka na čtečce. Po zapnutí bude čtečka automaticky připojena.

Zapnutou čtečku karet poznáte podle modrého blikajícího indikátoru. Pokud indikátor nebliká, zkuste zapnout čtečku znovu.

Zapněte čtečku karet

Zapnutou čtečku karet poznáte podle modře blikající kontrolky.

Po zapnutí bude čtečka automaticky připojena.

Figure 2: Screen adjustment based on iterative testing (shortening the text and realistic animation).

Realistic animations

The authentication application contained animations that depicted the use of the novel authentication methods (e.g., pressing the button on the FIDO token, attaching the NFC token / NFC payment card to the smartphone, turning on the card reader and then inserting the payment card into the card reader; see Figure 2). Most users were encountering these methods for the first time during the testing and their feedback showed that the animations were helpful, but it was important that they were as realistic as possible (e.g., it was important that the icon representing the card reader looked as close as possible to the actual card reader; oversimplification of the icon was not understandable for respondents).

Representatives of the elderly had difficulty scanning their finger on the fingerprint reader, although it had been presented to them beforehand. They often placed their finger on the smartphone screen where the respective icon resembled a button.

Unusual or expert concepts

Users encountered a few uncommon concepts during testing that they found problematic. The first example was the choice of a 5-digit PIN instead of a more usual 4-digit one. Users were surprised and particularly elderly users had trouble typing in 5 digits (either because they had not noticed that they were to enter an additional digit or because it was more difficult to come up with 5 numbers than just 4). Users also expressed concerns about remembering a PIN code that was one digit longer, although they did rate it as more secure.

Another new concept was the use of hardware tokens: *FIDO* and *NFC tokens*. Especially elderly users had trouble remembering the word *token*. *FIDO* and *NFC* were confusing for most of the users because they did not know what the abbreviations meant. In later stages, when the *FIDO token* was no longer tested and only the *NFC token* was used, the term *token* was used exclusively along with the demonstration of this hardware.

The IDport authentication application is basically a versatile application for confirming diverse actions. Naming these actions required several suggestions and iterative improvements. For technical reasons, it was not possible to name each action differently, such as *login* and *financial transactions*. However, users understood the term *transaction* to mean a financial transaction and thus the need to confirm a login *transaction* seemed confusing. In the end, we chose the term *request*, but we still do not consider it the most appropriate term.

Interviews with the users

User interviews mainly focused on the ways of thinking about the security of the authentication methods and what comes into consideration when deciding upon a method.

In the first three rounds, where the evaluated authentication methods were a hardware token or a card reader, we found that users had great reservations towards owning an additional device that seemed otherwise useless (this could be resolved by extending the use of the device). In particular, the main objections were the impracticality of the ownership of additional hardware and the risk of loss. Therefore, we decided to prepare user testing with an NFC payment card – a common payment card that users receive to use with their bank accounts.

When comparing the authentication methods, users make relatively complex decisions, consider many different contexts, and do not evaluate the security of the method only based on technical parameters. To the respondents, usability is defined not only by how the method or application behaves, but also by its potential widespread use and the available technical support during a failure. In terms of security, they consider individual components, their reliability, and the availability of back-up solutions. One of the reasons that fingerprint authentication surpassed the contactless payment card in the user rating was because users perceived the fingerprint within the context of their previous use along with the PIN code, and they would know what to do if one of these methods did not work. Users did not know such crisis scenarios for the use of the payment card, which reduced the subjectively perceived security and usability. Similarly, it was important for them to know who was responsible for the risks and who would deal with security problems (e.g., card theft). For users, security is represented not only by the technical solution but also by the institutions, services, and other actors that accompany these solutions.

The fingerprint was rated as user-friendly due to its speed and promptness. At the same time, users considered it secure due to its uniqueness and the fact that it cannot be easily stolen or lost. When using payment / smart cards, users were concerned that they were not physically connected with them, that they might be stolen along with the smartphone, and that someone could see and misuse the information printed on them. However, users did not consider that they normally use a contactless payment card in stores, and no one mentioned worries about the same risks during these activities.

In their assessment, and possibly in their security behavior, users based their actions on scenarios that highlight physical threats, such as theft. However, this model is inaccurate and does not allow them to adequately assess digital threats, although it may motivate them to behave more securely (e.g., conduct transactions in a private location). Although the model is inaccurate, it affects users' willingness to use individual authentication methods. It is, therefore, important that product owners of authentication methods understand these ideas and consider them in their design.

The information provided above is based on our analyses and partly on our article "*How do users think about security in the context of mobile banking?*" published in the Data Security Management journal, issue 2/2019 (Doležal, Dařbujanová, & Knapová, 2019).

(3) A quantitative survey of the adult and elderly populations

Methodology

Description of the quantitative survey

The aim of the quantitative survey was to investigate the current user experience with online banking and to test selected authentication methods with a focus on perceived user-friendliness and security, and the preference for these methods. The quantitative testing was conducted on a sample of 500 users (250 adults up to 54 years of age, and 250 people aged 55 and older) and built upon the UX testing and the user interviews and the acquired findings.

The tested authentication methods were consistent with the third round of UX testing and user interviews:

- PIN code
- fingerprint
- hardware token (NFC token)
- payment card inserted in a card reader.

The primary tested application was again the IDport digital identity application. This application was used for user authentication and the authorization of requests and supported the selected authentication methods. Users continued to interact with the fictitious YourBank online banking.

During the preparatory phase, a series of steps were taken to ensure the smooth running of the quantitative survey. First, the changes in the tested applications (i.e., IDport authentication application, YourBank online banking) were implemented based on the UX testing described above. For extensive standardized testing of the authentication methods, it was also necessary to ensure the functionality and consistent behavior of all the test scenarios, even in the case of a missing or insufficient internet connection. Therefore, a native mobile banking application for the Android operating system was created that did not require an internet connection. Last, the printed materials used in the survey were modified. These included letters from a bank to describe how to activate IDport, a fictitious invoice for payment, and instructions for the devices (see Figure 3). Similarly, a highly standardized testing procedure and detailed training materials were developed for interviewers.

Testing procedure

The testing process and the tasks on the smartphone were based on the experience of the UX testing and the user interviews. Testing within the quantitative survey was conducted individually (i.e., one interviewer with one respondent) and consisted of performing tasks on a smartphone and completing questionnaires. The whole procedure with one user lasted about 30-90 minutes and was conducted in Czech language. Before testing, the respondent signed informed consent. The testing was approved by the *Ethics Committee for Research* at Masaryk University.

Respondents were presented with a hypothetical situation where their fictitious bank, YourBank, recommended them to use the IDport authentication application to confirm online banking requests. The user was instructed to activate the application and then log into their online banking and pay for a vacation. In both cases, the user was redirected to the authentication application to confirm the request.

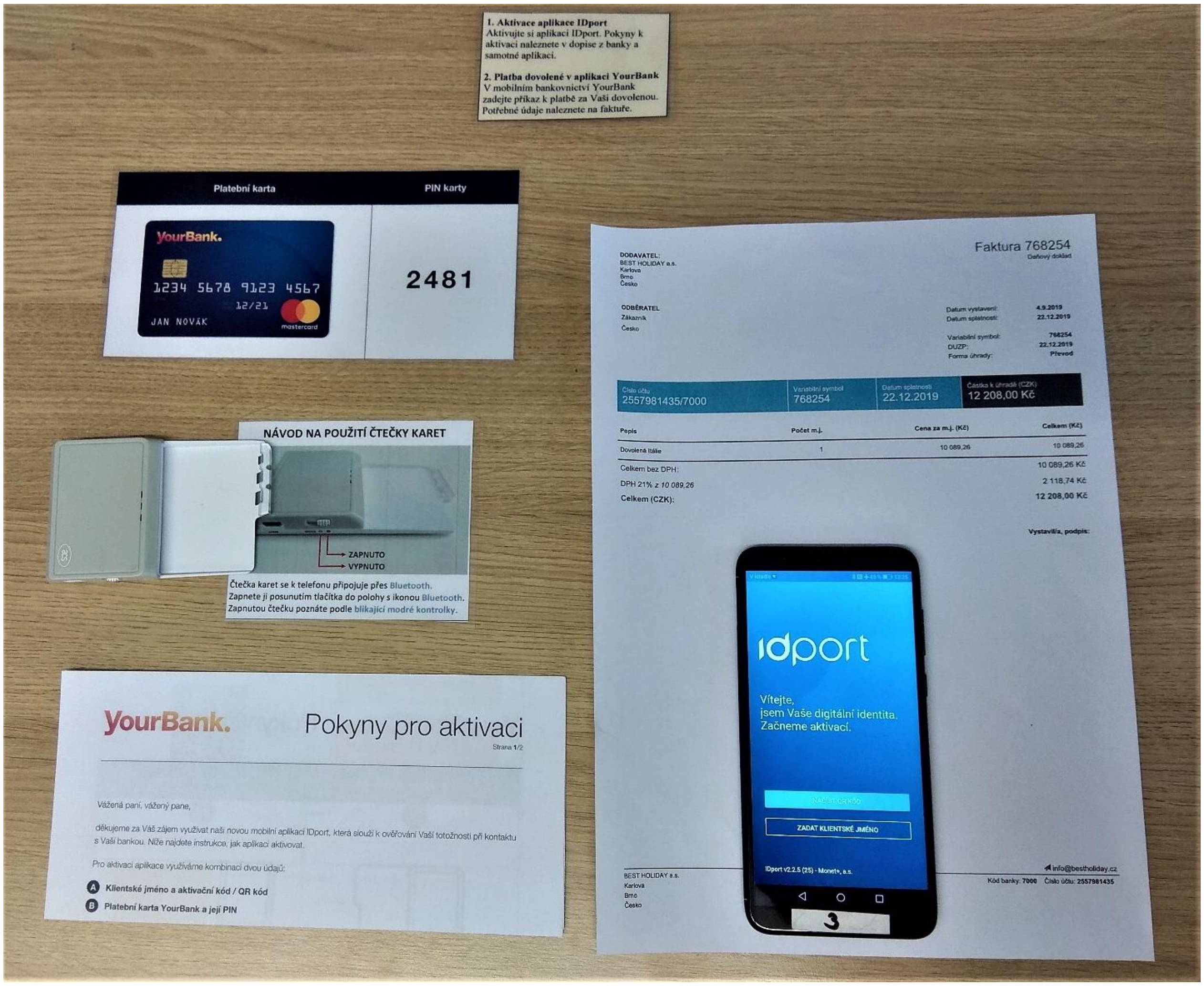

1. Aktivace aplikace IDport
Aktivujte si aplikaci IDport. Pokyny k aktivaci naleznete v dopise z banky a samotné aplikaci.
2. Platba dovolené v aplikaci YourBank
V mobilním bankovnictví YourBank zadejte příkaz k platbě za Vaši dovolenou. Potřebné údaje naleznete na faktuře.
Platební karta
PIN karty
YourBank.
1234 5678 9123 4567
12/21
JAN NOVÁK
mastercard
2481
NÁVOD NA POUŽITÍ ČTEČKY KARET
ZAPNUTO
VYPNUTO
Čtečka karet se k telefonu připojuje přes Bluetooth.
Zapnete ji posunutím tlačítka do polohy s ikonou Bluetooth.
Zapnutou čtečku poznáte podle blikající modré kontrolky.
YourBank.
Pokyny pro aktivaci
Strana 1/2
Vážená paní, vážený pane,
děkujeme za Váš zájem využívat naši novou mobilní aplikaci IDport, která slouží k ověřování Vaší totožnosti při kontaktu s Vaší bankou. Níže najdete instrukce, jak aplikaci aktivovat.
Pro aktivaci aplikace využíváme kombinaci dvou údajů:
A Klientské jméno a aktivační kód / QR kód
B Platební karta YourBank a její PIN
Faktura 768254
Daňový doklad
DODAVATEL:
BEST HOLIDAY a.s.
Karlova
Brno
Česko
ODBĚRATEL
Zákazník
Česko
Datum vystavení: 4.9.2019
Datum splatnosti: 22.12.2019
Variabilní symbol: 768254
DUZP: 22.12.2019
Forma úhrady: Převod
Číslo účtu
2557981435/7000
Variabilní symbol
768254
Datum splatnosti
22.12.2019
Částka k úhradě (CZK)
12 208,00 Kč
Popis
Počet m.j.
Cena za m.j. (Kč)
Celkem (Kč)
Dovolená Itálie
1
10 089,26
10 089,26
Celkem bez DPH:
10 089,26 Kč
DPH 21% z 10 089,26
2 118,74 Kč
Celkem (CZK):
12 208,00 Kč
Vystavil/a, podpis:
idport
Vítejte,
jsem Vaše digitální identita.
Začneme aktivací.
NAČÍST QR KÓD
ZADAT KLIENTSKÉ JMÉNO
IDport v2.2.5 (25) - Monet+, a.s.
BEST HOLIDAY a.s.
Karlova
Brno
Česko
info@bestholiday.cz
Kód banky: 7000
Číslo účtu: 2557981435
3

Figure 3: Standardized layout of materials for the card-reader scenario.

During testing, the users tried out activation and authentication scenarios. As part of the activation scenario (activation of the IDport authentication application, i.e., identity confirmation), they set up and used all of the tested authentication methods. They then went through two authentication scenarios: logging into YourBank and confirmation of sending a payment. When confirming the login, they used one factor according to their own preferences: a PIN or a fingerprint. The payment was confirmed by two factors depending on the variant of the testing: either the PIN or fingerprint (according to individual preferences) and then using the NFC token; or inserting the payment card into a card reader and then entering the PIN for the card.

The quantitative survey procedure was as follows (Figure 4):

- Questionnaire A (5-10 minutes): Administered before testing on the smartphone. It covered demographic questions, attitudes towards online security, and smartphone secure behavior.
- Smartphone testing, TOKEN variant: Activation of IDport application, logging into YourBank, and sending a payment using NFC token, PIN, and fingerprint.
- Questionnaire B1 (2 minutes): Control evaluation of smartphone testing immediately after its completion (ease, perceived length, clarity of instructions).
- Smartphone testing, CARD READER variant: Activation of IDport, logging into YourBank, and sending a payment using card reader, PIN, and fingerprint.
- Questionnaire B2 (2 minutes): Control evaluation of smartphone testing immediately after its completion (ease, perceived length, clarity of the instructions).
- Questionnaire C (15-20 minutes)**:** Administered after the completion of both variants of testing on the smartphone. It included the evaluation of the tested authentication methods in terms of usability and security, the preference for selected authentication methods, experience with authentication methods and online banking services, and experience and preferences for two-factor authentication.

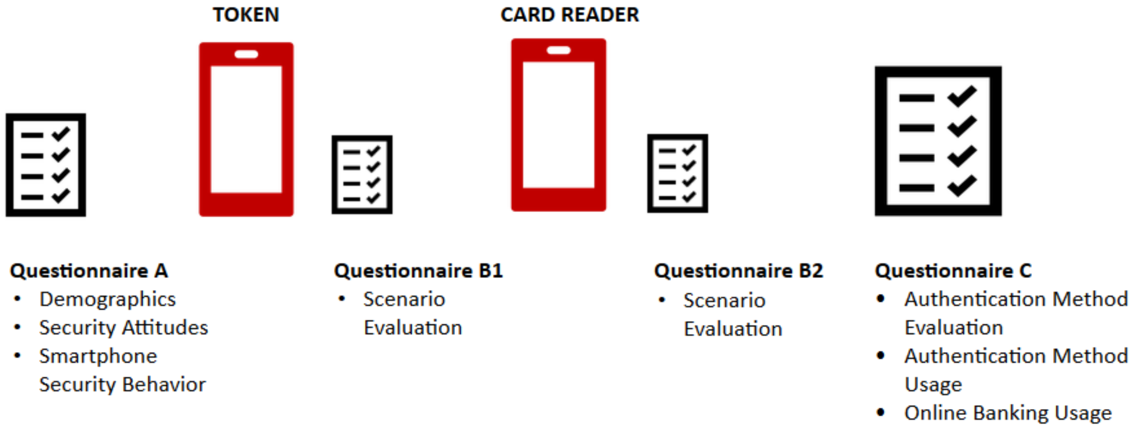


Figure 4: The testing procedure scheme.

Sample and its selection

The quantitative survey was carried out in two independent data collections. The first focused on the adult population (adults up to 54 years of age, N = 250, further referred to as “adults”), and the second focused on the elderly population (aged 55 years and older, N = 250, further referred to as “the elderly”). The inclusion criterion was the use of a smartphone with the Android operating system. In addition, representatives of the elderly population were not allowed to have had professional experience or education in IT.

The survey of the adult population was conducted by a professional survey agency, FOCUS, which provided a representative sample of the surveyed population with regard to gender, age, education, size of residence municipality, region, and socioeconomic status. The testing was carried out by professional interviewers.

The survey of the elderly population was coordinated by the research team of Masaryk University. Interviewers were recruited mainly among Bachelor and Master students. Data collection was performed by a total of 24 interviewers, who were trained by the research team and successfully conducted a pilot testing session. The method of selecting respondents was convenience sampling; the interviewers approached people around them and various senior organizations and third-age university students were contacted. This sampling was complemented by the snowball method (i.e., the respondents could recommend another relevant respondent).

Description of the adult sample

Three cases were excluded from the sample of 250 adults due to poor data quality. The resulting sample of adults included 247 people up to 54 years of age, including 114 men (46%) and 133 women (54%). The mean age was 38.75 years, with a median of 38 years, and a standard deviation of 9.23.

Stratification of the sample according to education was as follows: primary 4%; secondary without a high school diploma 33%; secondary with a high school diploma 30%; vocational 5%; and higher education 29%. (*Note:* In some cases, the total sum of the percentages may not equal 100% due to rounding).

Stratification of the sample according to the size of residence municipality was as follows: up to 1,999 residents 18%; 2,000-4,999 residents 5%; 5,000-9,999 residents 7%; 10,000-19,999 residents 5%; 20,000-49,999 residents 9%; 50,000-99,999 residents 12%; 100,000 and more residents 45%.

The main source of income for the majority of adult respondents under 54 years of age was full-time work (69%), part-time work (9%), or maternity/parental leave (11%). In addition, respondents reported their status as student (3%), unemployed (4%) and pensioner (1%). The remaining respondents (2%) did not want to indicate their source of income.

Five respondents (all men) were excluded from further analyses because they were specifically focused (academically or professionally) on IT security and their data was biased.

Description of the elderly sample

The resulting sample of the elderly included 250 respondents aged 55 years and older, including 98 men (39%) and 152 women (61%). The mean age was 62.58 years, with a median of 61 years, and a standard deviation of 6.70.

In the sample of elderly respondents, there was a higher proportion of people with secondary education with a diploma (42%) and higher education (41%). Significantly fewer people had secondary school education without a diploma (9%), vocational (5%), or primary education (3%).

For half of the respondents (51%), the main source of income was full-time work, for 41% it was pension, and for 6% it was part-time work. The remaining people (1%) were unemployed or did not want to disclose their main source of income.

When interpreting the following analyses, including the comparison between adults and the elderly, it should be taken into account that the sample of adults is representative with respect to the Czech Republic's demographics, while the sample of the elderly is a convenience sample. As the participation criterion was the use of a smartphone, the sample of people aged 55 years and older is probably a technologically proficient subset of the elderly population.

Results and recommendations from the quantitative survey

The following results are based on questionnaire responses. Note that in some cases, the total sum of the percentages may not equal 100% due to rounding.

First, respondents rated their knowledge of secure online and smartphone behavior, online banking skills, and smartphone skills on a scale of 1 (beginner) to 7 (expert). Chart 1 shows that the representatives of the adult population rated their knowledge and skills as better than the representatives of the elderly population. Greater differences can be seen, for instance, in the assessment of online banking skills, where 20% of the elderly identified themselves as complete beginners (value 1), compared to 6% of the adults. Similarly, in the case of the knowledge of secure behavior on the smartphone, 19% of the elderly rated themselves as beginners (value 1), and a further 42% as below average (value of 2 or 3). For adults, 5% of the respondents considered themselves to be beginners in terms of secure behavior on a smartphone, while a further 28% as below average.

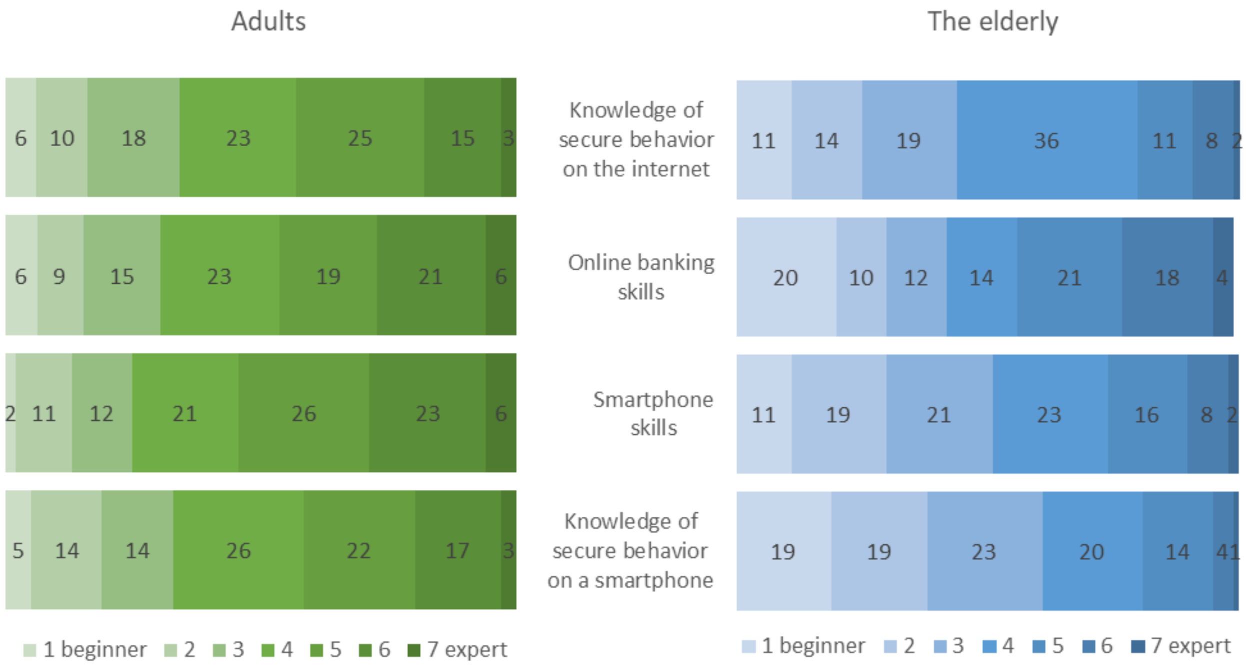


Chart 1: Self-assessment of selected knowledge and skills with technology.

Experience with online banking and authentication methods

The vast majority of respondents in both populations had a bank account (97% of adults, 99% of the elderly) and most reported using some form of online banking (97% of adults, 86% of the elderly). Almost all of adults (98%) and the elderly (97%) had a payment card for their account.

The most common form of online banking was computer-based internet banking, which was used by 81% of adults (i.e., 84% of those using some form of online banking) for an average of 8.5 years (standard deviation 4.5) and 84% of the elderly (i.e., 98% of those using some form of online banking) for an average of 9.2 years (standard deviation 5.1). Adults and the elderly used internet banking on a computer with a similar frequency. Most of them reported using it several times a week (33% of adults, 32% of the elderly) or several times a month (39% of adults, 43% of the elderly). Only 6% of adults and 7% of the elderly respondents reported using online banking daily. Therefore, it is necessary to offer authentication methods that users will be able to use repeatedly and, at the same time, after a long period of inactivity.

Using a mobile banking application on a smartphone or tablet was reported by 52% of adults (i.e., 54% of those using some form of online banking) for an average of 4.4 years (standard deviation 2.9). Among the elderly it was 30% (i.e., 35% of those using some form of online banking) for an average of 5 years (standard deviation 4.2).

Accessing online banking through the browser on a smartphone or tablet was reported by 20% of adults (i.e., 21% of those who used some form of online banking) for an average of 4.7 years (standard deviation 3.2). For the elderly it was 11% (i.e., 13% of those who used some form of online banking) for an average of 5.5 years (standard deviation 4.4).

Thus, the most common form of online banking for both populations was internet banking on a computer. Among the elderly, almost all of them used computer-based internet banking. On the other hand, online banking on a smartphone or tablet was characteristic of the younger age group: two-thirds of adults used banking on their smartphone or tablet (whether in the form of an application or via a browser), which is approximately twice as much as among the elderly.

Regarding online banking, the authentication methods most adult and elderly users had previous experience with were username (87% of adults, 88% of the elderly); password (87% of adults, 88% of the elderly); and PIN (76% of adults, 73% of the elderly) (Chart 2). Both populations have experienced the above methods on an approximately equal basis. However, there are differences, specifically in fingerprint authentication, with which adults had more experience (29% of adults, 12% of the elderly); the certificate, with which the elderly had more experience (15% of adults, 21% of the elderly); and gesture, which only a few of the elderly had tried (9% of adults, 2% of the elderly). The fact, that users had experience with these methods does not necessarily mean that they are currently using them or prefer them. However, experience with individual authentication methods can affect the perception of these and other methods.

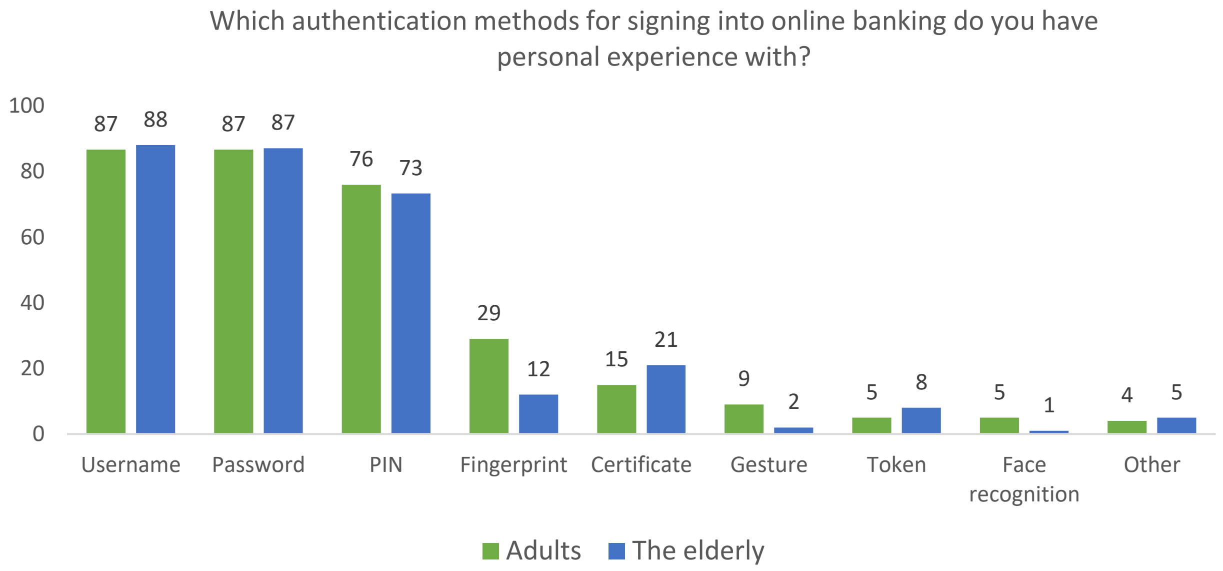


Chart 2: Experience with authentication methods for signing into online banking.

For confirming payments in online banking, most online banking users had previous experience with the SMS code, similarly in both populations (95% of adults, 96% of the elderly). This was followed by PIN (50% of adults, 39% of the elderly) and password (51% of adults, 36% of the elderly), where we can see differences between adults and the elderly (Chart 3). Population differences can also be observed in the case of fingerprint authentication, with which more adults had experience (26% of adults, 11% of the elderly). Adults had more personal experience than the elderly with most forms of online payment confirmation.

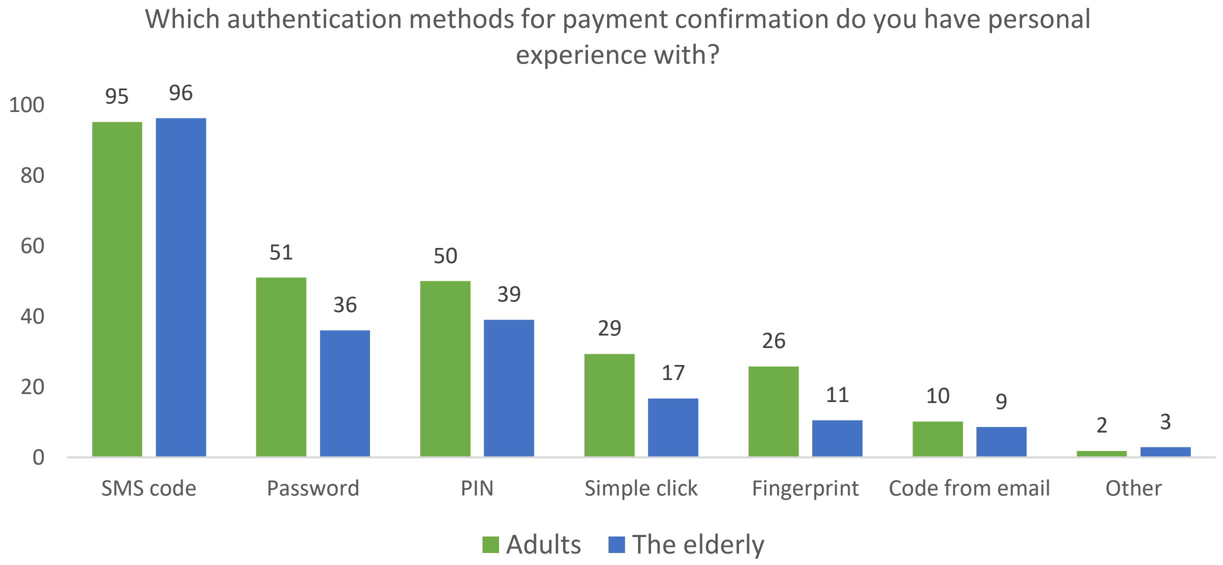
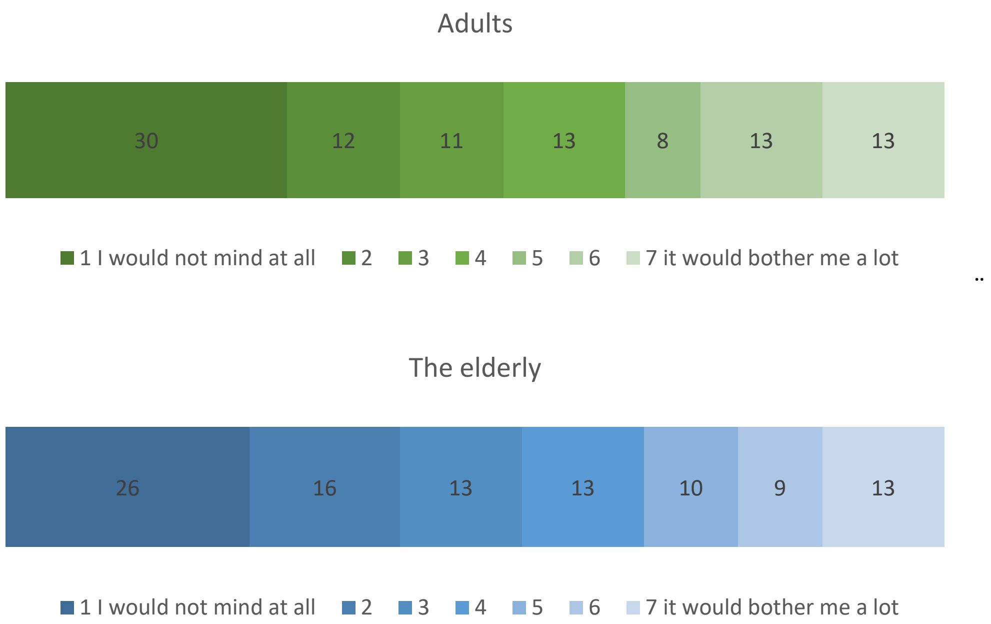


Chart 3: Experience with authentication methods for payment confirmation in online banking.

The majority of respondents had previous experience with paying online (e.g., using a card to pay online or transferring money in online banking) (95% of adults, 82% of the elderly). Most online banking users said they pay online several times a month (43% of adults, 41% of the elderly), 24% of adults and 25% of the elderly pay online several times a week, with only 4% of adults and 2% of the elderly users paying online daily. Another 28% of adults and 27% of the elderly reported paying online only once a month or less.

With regard to the security risks of the SMS code for confirming payments in online banking (see details here), respondents evaluated the hypothetical situation where this authentication method would be replaced by another, on a scale of 1 (*I wouldn't mind at all*) to 7 (*It would bother me a lot*). About half of both the adults (53%) and the elderly (55%) reported that they would not mind such a change (value 1, 2, or 3), as shown in Chart 4. Such a change would significantly bother 26% of adults and22% of the elderly (value 6 or 7), and it would rather bother 8% of adults and 10% of the elderly (value 5). The rest (13% of both adults and the elderly) hold a neutral attitude (value 4). Thus, it can be said that there are less who would mind replacing the sending of the SMS code with another authentication method than of those who would not mind a change. However, this question did not consider the particular authentication method that would replace the SMS code.


Adults

The elderly

Chart 4: Evaluation of the replacement of SMS code by another authentication method.

Two-factor authentication

Further questions focused on the experience with 2FA and the willingness to use it for different scenarios.

Most respondents (84% of both adults and the elderly) have used two-factor authentication in online services, so the concept was not entirely unknown. Specifically, the use of 2FA in online banking was reported by 71% of the surveyed adults and 69% of the elderly, while using 2FA for card payments was reported identically by 59% of both groups. Although 2FA was explained to the respondents in the questionnaire, it is uncertain whether all users were aware that they might already be using 2FA, for example for online banking.

Adult users reported that they used two-factor authentication several times a month (32%) or several times a week (29%). Furthermore, 11% of adults use some form of 2FA daily, the rest (27%) use it once or twice a month or less. The same is true for the elderly population: 38 % of the elderly use 2FA several times a month and 28% do so several times a week. Daily use of some form of 2FA was reported by 8% of the elderly. Another 25% said they used 2FA once or twice a month or less often.

The most commonly used combination of factors by both adults and the elderly using 2FA was login credentials and confirmation SMS code (73% of both adults and the elderly), and payment card credentials and confirmation SMS code (59% of adults, 62% of the elderly). Respondents reported two-factor combinations using fingerprint or token significantly less frequently, as can be seen in Chart 5. The confirmation SMS code in combination with another method (e.g., login credentials or payment card credentials) is still one of the most widespread authentication methods used by both surveyed populations.

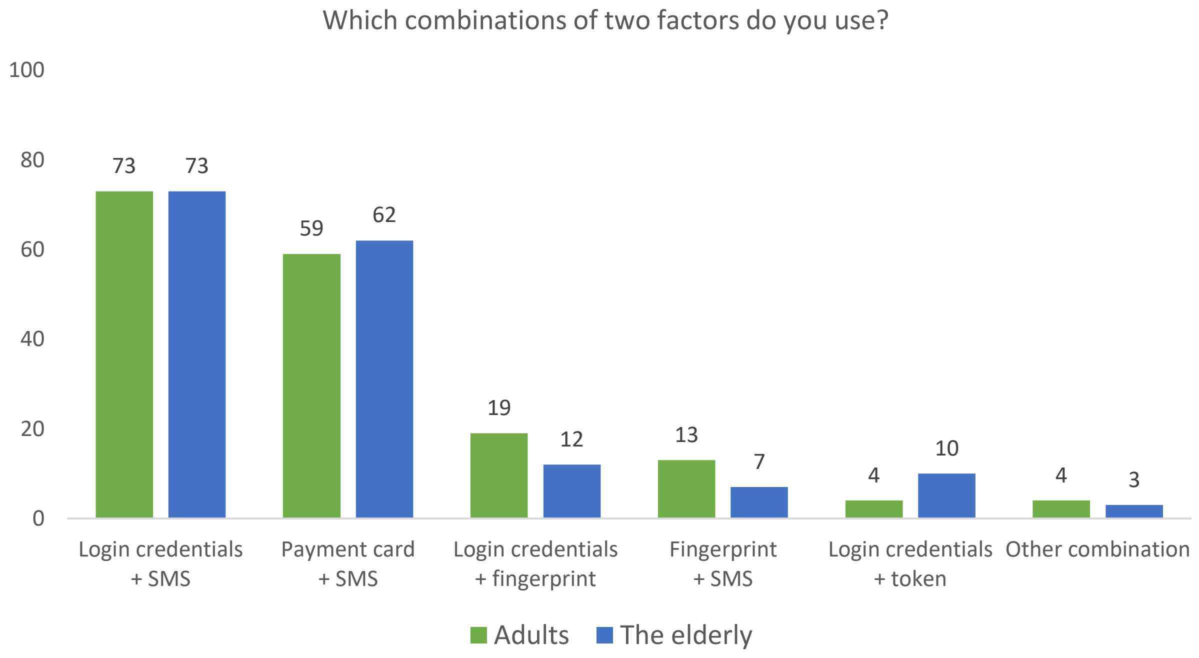


Chart 5: Frequency of use of selected two-factor combinations.

Subsequently, respondents were asked if they would like to use two-factor authentication for online card payments and online payment confirmation (Chart 6). Fully 78% of adults said they would like to use 2FA for both online card payments and online payment confirmation. Similarly, the majority of the elderly (74%) would like to use this method of authentication for online card payments, and even more for online banking (88%). These percentages are higher than the proportion of respondents who had already used 2FA for online card payments or online banking (see above). These responses, therefore, indicate a generally positive attitude towards 2FA for financial transactions across the age groups and interest to use this form of higher security, even by users that did not have previous experience with 2FA for financial services. The surveyed users seem to realize the importance of protecting their financial assets.

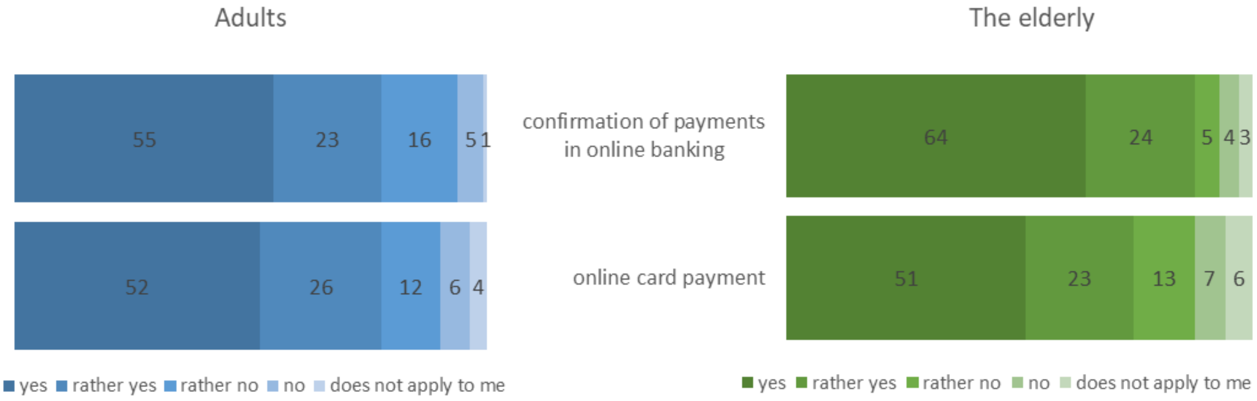


Chart 6: Willingness to use 2FA to confirm payments in online banking and for online card payments.

Evaluation of the tested authentication methods

Respondents also assessed the authentication methods they had tried while performing tasks on a smartphone. They evaluated how *easy to use*, *practical*, and *secure* they are.

Evaluation of the *ease of use* of each method is shown in Chart 7. Fingerprint authentication was rated as the easiest to use. For most respondents in both populations, using a fingerprint was *totally easy* (74% of adults, 80% of the elderly). For more than half of the adult population (54%), the token was *totally easy* to use. Among the elderly, 47% of respondents rated the token as *totally easy* to use. The PIN was rated as easy to use as the token in both populations. Inserting a payment card into a card reader was rated as the least easy to use by both populations: only 44 % of adults and 38 % of the elderly rated it as *totally easy* to use. On the other hand, 19% of adults and 22% of the elderly rated it as rather or *totally complicated* to use.

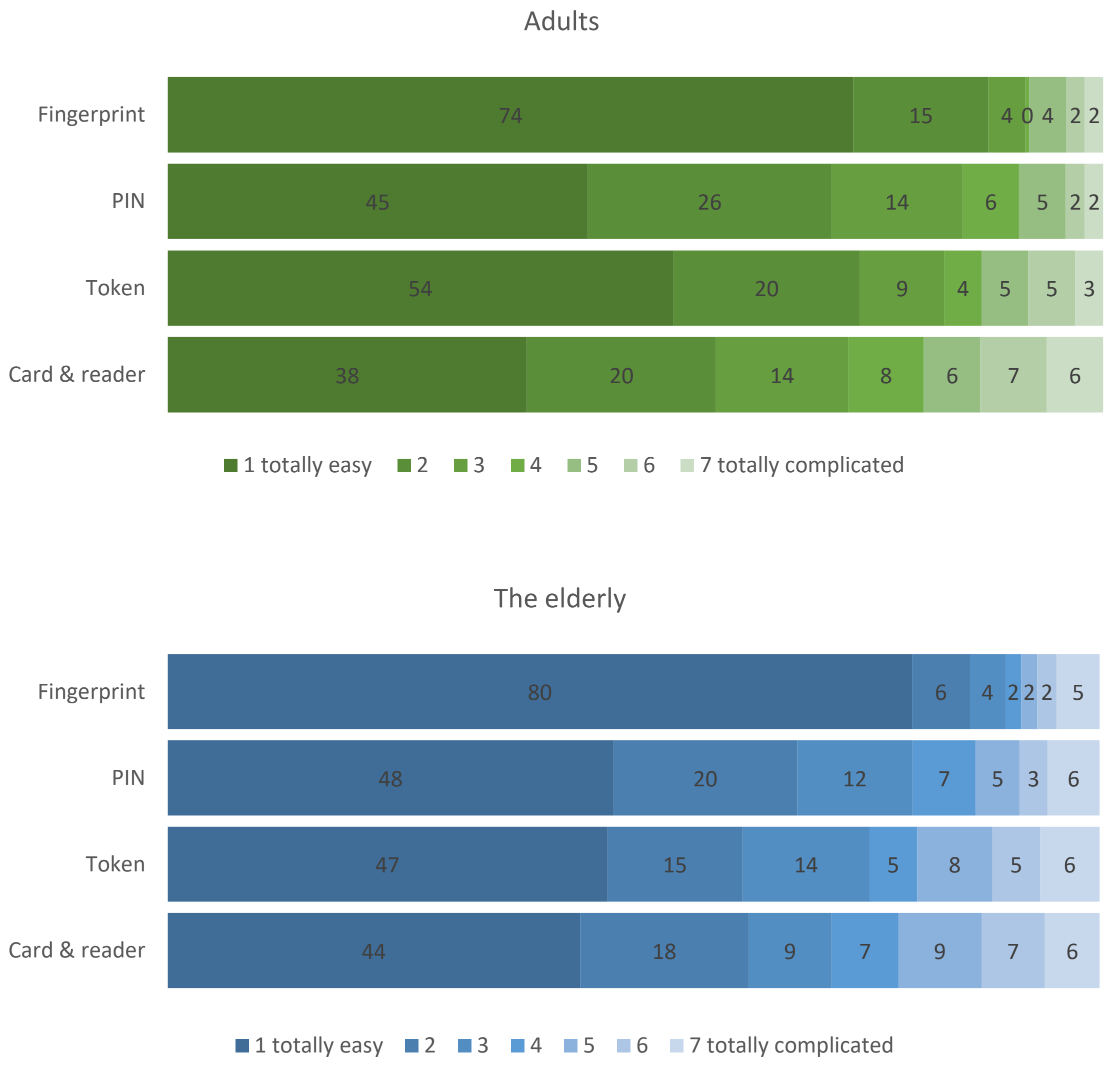


Chart 7: Evaluation of the ease of use of the tested methods.

Chart 8 shows the evaluation of each method regarding its perceived *practicality*. The fingerprint came out as the best-rated method in this comparison as well. It was perceived as *totally practical* by the majority of both surveyed populations (73% of adults, 80% of the elderly). Fully 44% of both populations rated the PIN as *totally practical* and a further 40% of adults and 34% of the elderly rated it as rather practical (value 2 or 3). Although more of the elderly considered inserting a payment card into a card reader as *totally practical* (22% of adults versus 37% of the elderly), when added together with the scoring of rather practical, 59% of adults and 62% of the elderly perceived the practicality of inserting a payment card into a card reader positively. However, more adults rated the card reader as *totally impractical* (15% adults versus 8% of the elderly). Similarly, in the case of a token, more of the elderly (34% of adults versus 41% of the elderly) considered it to be *totally practical*; summed together with the rather practical rating, the token was perceived positively in terms of practicality by 69% of adults and 64% of the elderly.

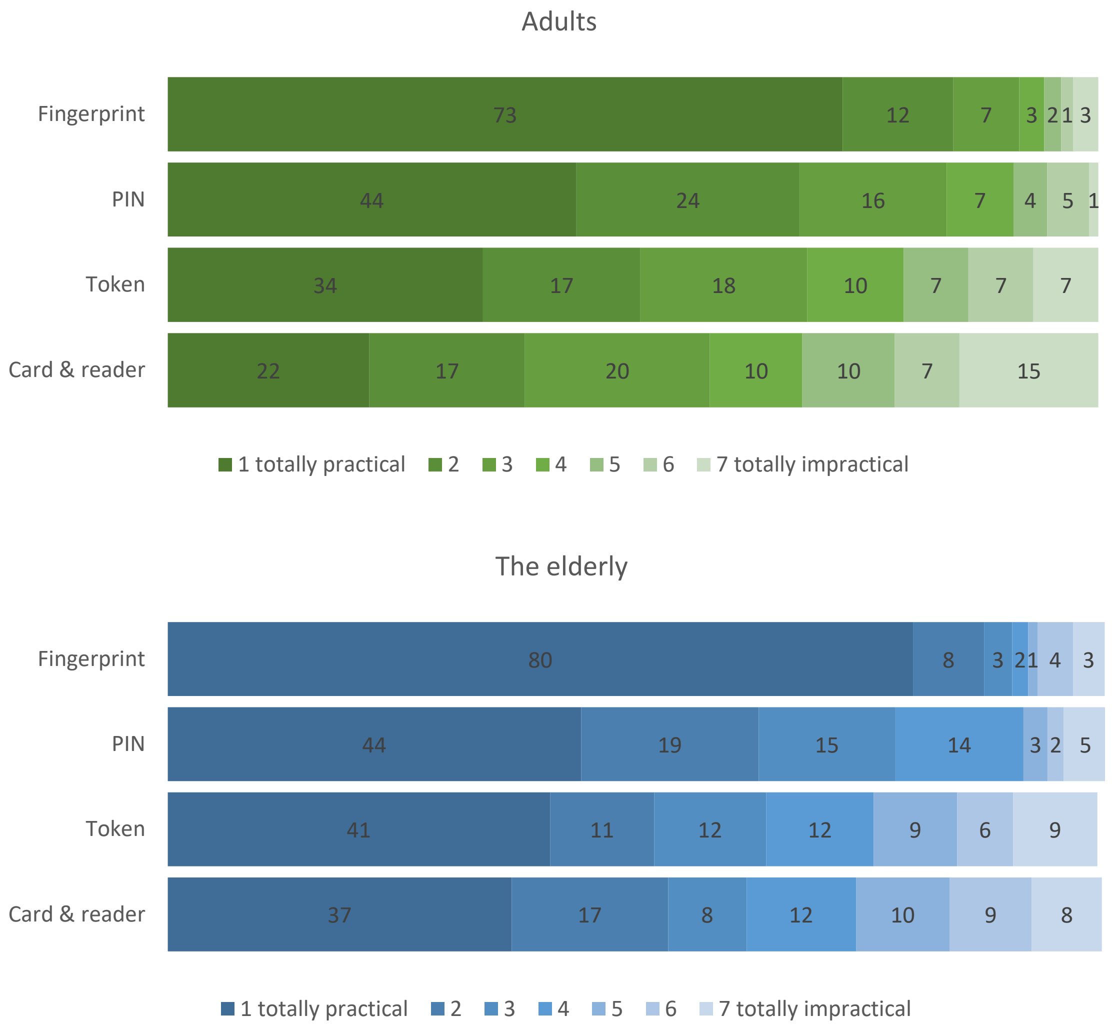


Chart 8: Evaluation of the practicality of the tested methods.

The last category was the perceived *security* of each of the methods, as shown in Chart 9. The fingerprint was once again evaluated as the most secure by both populations. Fully 64% of adults and 69% of the elderly assessed it as *totally secure* and another 21% of adults and 18% of the elderly assessed it as rather secure (values 2 or 3). The elderly population perceived the other three methods similarly in terms of security. Somewhat less of the elderly respondents rated the PIN as *totally secure* (23% versus 29% for both the token and inserting a payment card into a card reader); summed together with the rather secure rating, 66% of the elderly considered the method of using the PIN as secure, while it was 63% for the token and 66% for the card reader. The adult population perceived inserting a payment card into a card reader and using a PIN as more secure methods than the token. Fully 28% of adults considered the card reader to be *totally secure*, 25% in the case of a PIN and 24% for a token. Summed together with the rather secure rating, 75% of adults viewed the card reader positively, 71% in the case of using a PIN, and 66% for a token. In the case of a token, the largest proportion of respondents rated the method as rather or *totally insecure* in both populations compared with other methods (17% of adults, 24% of the elderly).

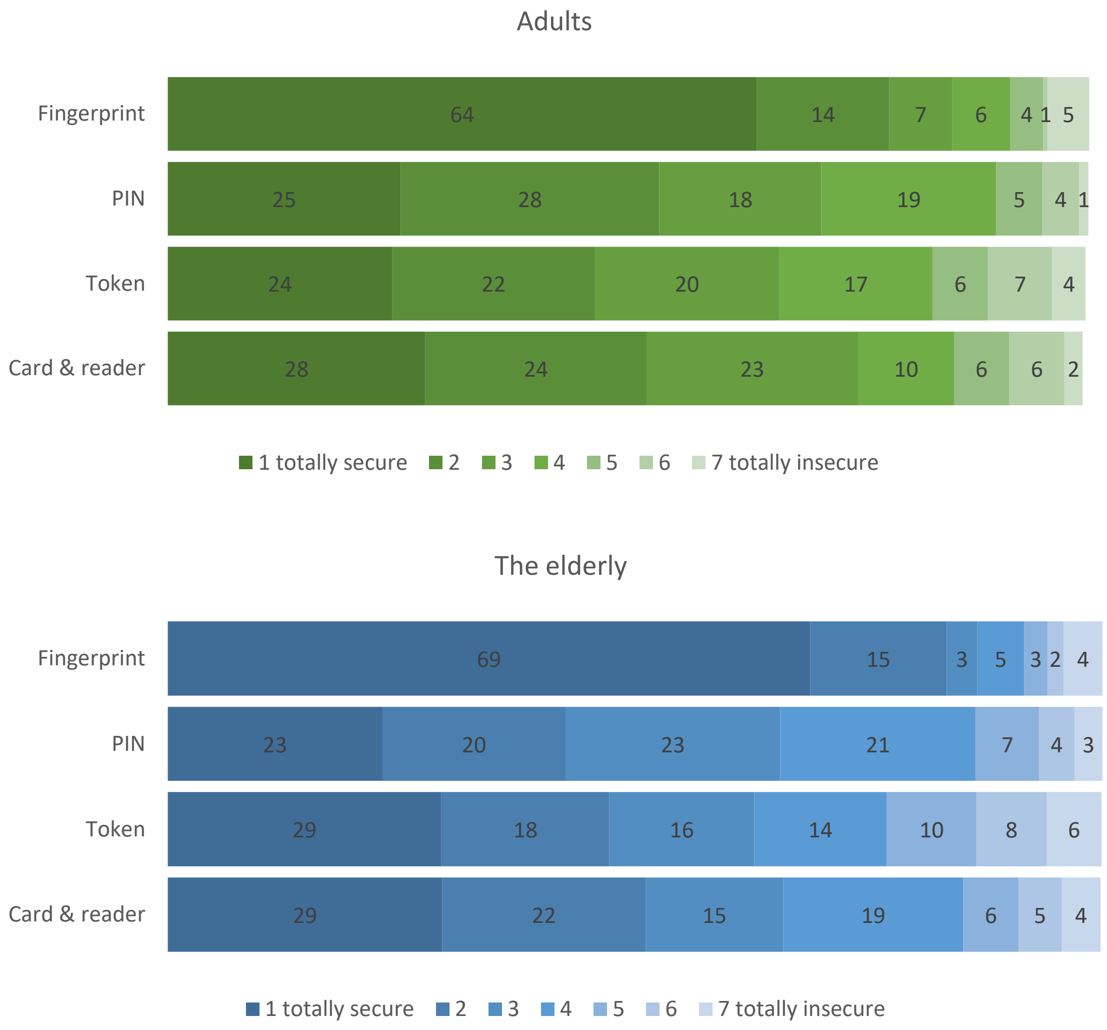


Chart 9: Evaluation of the security of the tested methods.

Chart 10 shows the average scores for each method on a scale of 1 (best) to 7 (worst). Overall, both populations perceived the individual methods positively in all three areas. The fingerprint was perceived as the easiest to use, most practical, and, at the same time, the most secure method by both populations, despite the fact that its actual security is not very high (details here). Other methods were also generally assessed positively.

Authentication methods based on object ownership (namely a token and a card reader) were evaluated very similarly in all three areas by the elderly population. In contrast, the adult population perceived inserting a payment card into a card reader as more complicated and less practical than using a token. The use of a PIN code was assessed by both populations similarly: less easy to use, less practical, and less secure than fingerprint authentication, but more practical and similarly secure as using a token and inserting a card into a card reader.

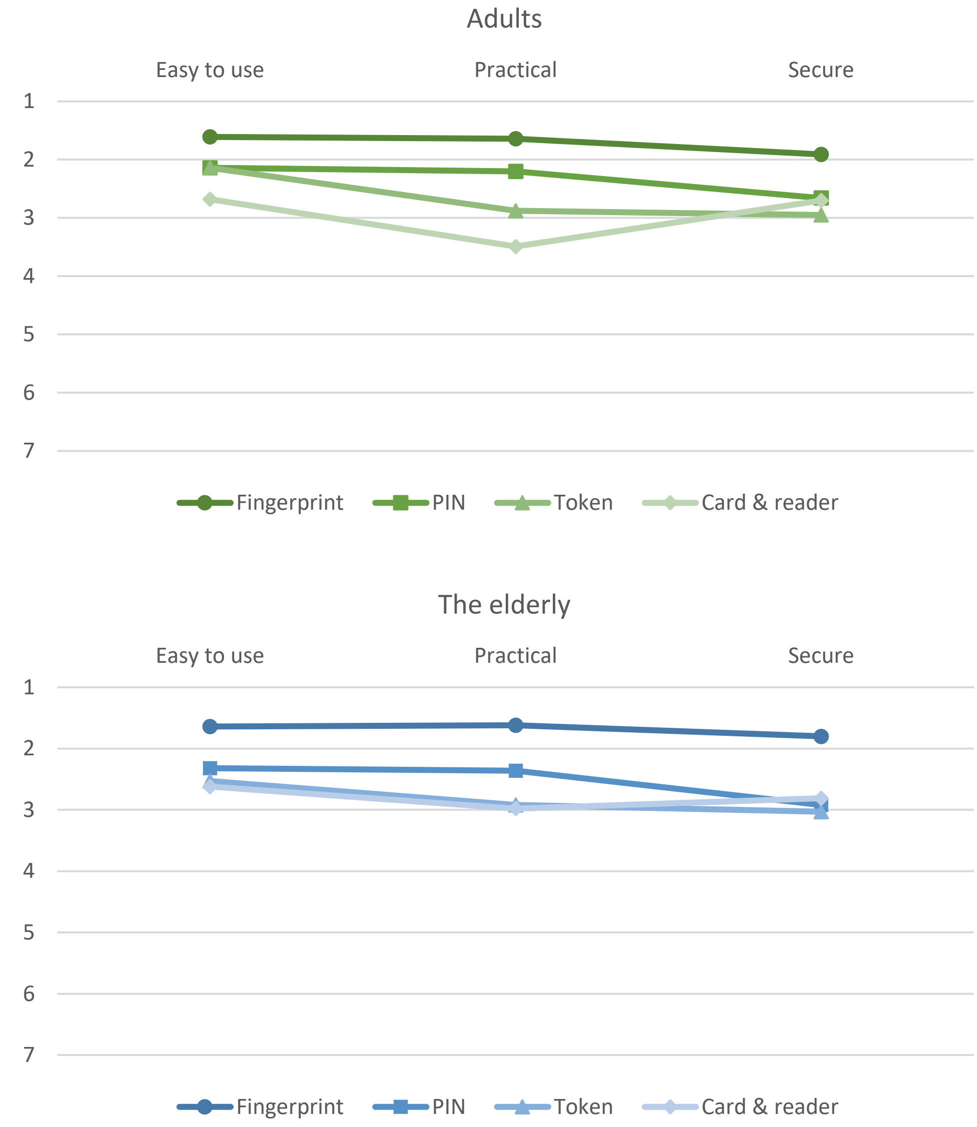


Chart 10: Comparison of the average evaluation of ease of use, practicality, and security of selected methods.

Preferences for authentication methods for payment confirmation

Finally, we asked the respondents for what amounts they would like to use the given authentication methods to confirm their transactions after logging into online banking. In addition to the tested methods, other untested combinations were added that users knew from their smartphone or could imagine based on their experience gained during the testing. They could choose from the following options: *I would never want to use this method*; *only for lower amounts*; *only for higher amounts*; *for both lower and higher amounts* (i.e., for confirming all financial transactions). The line between the lower and the higher amount was not explicitly set and was, therefore, the subjective perception of the respondents. The full results are described in Chart 11.

The use of an authentication method for confirming payments in online banking is desirable because confirmation of the payment by simply clicking a button (i.e., without using another authentication method) was the most rejected form of payment confirmation: 38% of adults and 45% of the elderly users would never want to just click to confirm the payment. On the other hand, there were also people for whom it was enough to just click to confirm, although they would rather use it for lower amounts (37% of adults, 41% of the elderly). Further, 28% of adults and 35% of the elderly would never want to use the token without another factor. On the contrary, a one-factor method that the respondent would like to use to confirm transactions of any amount was the fingerprint (46% of adults, 43% of the elderly), which is in line with the evaluation of the method as easy to use, practical, and secure. The second most preferred 1FA method for transactions of any amount was a numeric PIN code (35% of adults, 32% of the elderly), which had the second highest average ratings regarding easiness to use and practicality.

The evaluation of two-factor methods was more balanced. In general, for all 2FA combinations, there was more than one-fifth of the people (21-27%) who would never want to use the given combination. However, this is probably due to the preference of other combinations. At the same time, for a majority of the respondents (51-72% in total), it would make sense to use the given combinations of methods for the confirmation of payments of higher amounts. Specifically, 33-45% of the respondents would want to use the mentioned 2FA combinations for all payments and 24-31% only for payments of higher amounts. Furthermore, it was apparent that the use of 2FA only for lower amounts does not make sense to respondents, and this was preferred by a minority (5-15%). In both the adult and the elderly populations, the combination of fingerprint + token was slightly preferred: 39% of adults and 45% of the elderly would like to use this combination to confirm all payments, while 31% of adults and 27% of the elderly would use it only for high-amount transactions. The other two 2FA combinations, PIN + token and card with a reader + PIN for the card, were rated similarly by both populations.

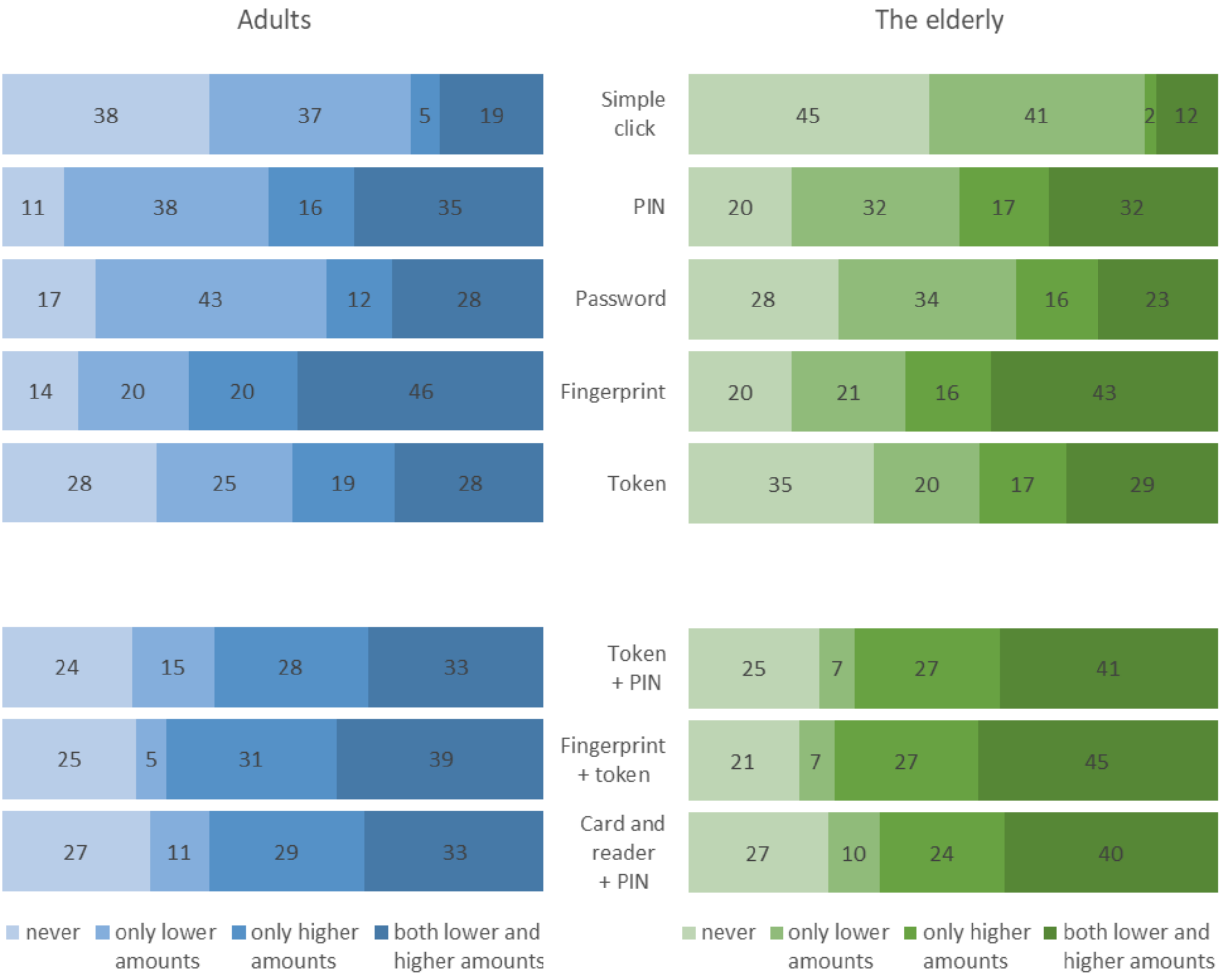


Chart 11: Preferences for authentication methods for payment confirmation.

Sources

Doležal, P., Dařbujanová, A., & Knapová, L. (2019). Jak uživatelé přemýšlejí o bezpečnosti v kontextu mobilního bankovnictví. *Data Security Management, 2019*(2), 11-15. Available at: https://tate.cz/archiv-2019/893-dsm-2019-2

Mayes, K. & Markantonakis, K. (2017). *Smart cards, tokens, security and applications.* Cham, Switzerland: Springer.

Paul, G., & Irvine, J. (2016). IEDs on the Road to Fingerprint Authentication: Biometrics have vulnerabilities that PINs and passwords don’t. *IEEE Consumer Electronics Magazine, 5*(2), 79–86.

Acknowledgements

We would like to thank all those who helped with this research. In the first place, we thank all the respondents who participated in user testing. We would also like to thank all the interviewers and assistants who helped us with data collection and processing.

The technical report was supported by the Technology Agency of the Czech Republic within the project TL01000207 Innovation and adaptation of authentication technologies for secure digital environment.

Contact

prof. PhDr. **David Šmahel**, Ph.D.

Institute for Research of Children, Youth and Family, Faculty of Social Studies
Department of Machine Learning and Data Processing, Faculty of Informatics
Masaryk university, Brno

E-mail: smahel@fss.muni.cz
Phone: +420 604 234 898

Mgr. **Ondřej Gabrhelík**

AHEAD iTec, s.r.o.
Team Leader

E-mail: ondrej.gabrhelik@ahead-itec.com
Phone: +420 731 196 750

Interdisciplinary Research Team on Internet and Society

http://www.irtis.muni.cz/

Center for Research on Cryptography and Security

https://crocs.fi.muni.cz/

AHEAD iTec, s.r.o.

https://idport.cz/tacr/

AHEAD

MUNI Interdisciplinary Research Team on Internet and Society

CROCS