Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Ingunn Langtangen Furuberg & Marie Øseth

From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Lillian Røstad
June 2023

NTNU
Norwegian University of Science and Technology

Ingunn Langtangen Furuberg & Marie Øseth

From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Lillian Røstad
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Title: From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication

Students: Øseth, Marie and Furuberg, Ingunn Langtangen

Problem description:

Password-based authentication is one of the most significant security issues. People have challenges with creating sufficiently complex passwords and memorizing them. As a result, people create weak passwords that are easily remembered. In addition, people reuse the same passwords across multiple services. Security threats increase today, and hackers can easily steal a user's identity. Therefore, other more user-friendly and robust alternatives for authentication should exist. Researchers have found passwordless login to be a more secure and convenient authentication. Despite this, other studies indicate that users still choose passwords as their preferred authentication method.

Fast Identity Online (FIDO) Alliance produces standards intending to reduce the reliance on password-based authentication. Their vision is a passwordless future. Passwordless authentication includes biometric methods like fingerprints, face scans, and physical security keys. On May 5th, 2022, Apple, Google, and Microsoft announced their plans to expand support for FIDO's passwordless login standard. With support from three leading worldwide companies, FIDO is in a position to accelerate the adoption of passwordless authentication. However, studies indicate slow progress in the adoption of FIDO.

This project aims to identify obstacles to a widespread adoption of FIDO's passwordless authentication. A comparative study of the user experience in different services supporting FIDO will be conducted. User testing will be performed to understand how user experience plays a role in adopting FIDO, as a convenient user experience is necessary to ensure proper security. Observations from the study will be used to develop recommendations on what actions may be taken to increase the adoption of the passwordless authentication approach.

Approved on: 2023-02-22
Main supervisor: Bartnes, Maria, NTNU
Co-supervisor: Røstad, Lillian, Simula Research Laboratory

Abstract

The Fast Identity Online (FIDO) Alliance has developed standards to reduce reliance on password-based authentication. FIDO2 is a passwordless authentication standard that allows authentication to online services. This research identifies the obstacles to the widespread adoption of FIDO2, focusing on usability and user perceptions. Previous studies indicate FIDO2 as more secure and user-friendly than traditional password-based methods. Despite this, the adoption has been slow, although major companies like Apple, Google, and Microsoft recently announced their support for FIDO2 authentication.

To explore the obstacles, a usability test and follow-up interviews were conducted with ten participants. The participants performed tasks related to setup and sign-in using passwordless authentication. These tasks were performed on two online services, namely Microsoft and eBay, which both offer FIDO2 as single-factor authentication. The two passwordless authentication methods used for setup and sign-in were fingerprint and security key.

Findings revealed that only two out of ten participants were aware of passwordless authentication on the web. All participants expressed willingness to adopt passwordless authentication but expressed concerns about manually changing security settings and sought a more seamless transition. Our results identify the lack of awareness regarding passwordless authentication as the most significant obstacle to the widespread adoption of FIDO2.

Sammendrag

Fast Identity Online (FIDO) Alliance har utviklet standarder for å redusere avhengigheten av passordbasert autentisering. FIDO2 er en passordløs autentiseringsstandard som tilbyr autentisering mot nettbaserte tjenester. Dette forskningsprosjektet identifiserer hindringene for utbredt bruk av FIDO2 med fokus på brukervennlighet og brukeroppfatninger. Tidligere studier tyder på at FIDO2 er sikrere og mer brukervennlig sammenlignet med passordbaserte autentiseringsmetoder. Til tross for dette har utbredelsen av FIDO2 vært treg, selv om store selskaper som Apple, Google og Microsoft nylig annonserte at de er i gang med å støtte FIDO2 autentisering.

For å utforske hindringene ble det gjennomført en brukervennlighetstest og oppfølgingsintervjuer med ti deltakere. Deltakerne utførte oppgaver knyttet til oppsett og pålogging ved bruk av passordløs autentisering. Disse oppgavene ble gjennomført på to nettbaserte tjenester, nemlig Microsoft og eBay, som begge tilbyr FIDO2 som en-faktor autentisering. De to passordløse metodene som ble brukt i studien var fingeravtrykk og sikkerhetsnøkkel.

Resultater avslørte at bare to av ti deltakere var bevisst over muligheten for passordløs autentisering på nettbaserte tjenester. Alle deltakerne uttrykte at de var villige til å gå over til passordløs autentisering, men uttrykte bekymringer for den manuelle endringen i sikkerhetsinnstillinger, og håpet på en mer sømløs overgang. Våre resultater identifiserte mangelen på kunnskap om passordløse autentiseringsalternativer som den viktigste hindringen for utbredt bruk av FIDO2.

Acknowledgements

We would like to thank our supervisors, Maria Bartnes and Lillian Røstad, for their guidance and support. Their ideas and expertise have been of great value in reaching this stage of our work.

A special acknowledgment goes to Per Thorsheim, who has been a true inspiration to us. Your enthusiasm, ideas, and knowledge have motivated us and ignited our passion for the subject. We are grateful for introducing us to a network of talented and inspiring people, including Maximilian. We want to thank Maximilian Golla for his feedback, advice, and support, as well as for encouraging us to submit our poster to SOUPS 2023.

Furthermore, we are grateful to our families for cheering on us and supporting us throughout our academic journey. Your love and belief in us mean everything to us.

Finally, we would like to thank our classmates for participating in our research and dedicating your time, and thanks to everyone for making our study experience unforgettable. The discussions we've had and the close friendships we have formed over the past five years have been truly adored and have enriched our academic journey in so many ways.

Contents

List of Figures

List of Tables

List of Acronyms

2FA Two-Factor Authentication.

CTAP Client to Authenticator Protocol.

FIDO Fast Identity Online.

HCI Human–Computer Interaction.

MFA Multi-Factor Authentication.

NFC Near-Field Communication.

NIST National Institute of Standards and Technology.

OS Operating System.

OTP One-time Password.

PIN Personal Identification Number.

SFA Single-Factor Authentication.

SSO Single Sign-On.

U2F Universal Second Factor.

UAF Universal Authentication Framework.

UX User Experience.

W3C World Wide Web Consortium.

WebAuthn Web Authentication.

Chapter 1
Introduction

Every day, we find ourselves signing into multiple accounts to access our online services and platforms. Whether accessing a bank account or signing into a social media platform, the process has become a daily routine in our lives. With the increasing complexity of digital systems, the need for authentication has grown. As a result, new authentication methods are being introduced and constantly developed to ensure secure and user-friendly authentication to the end-user.

Password-based authentication is one of the most significant security issues on the Web [PMA22]. However, this traditional authentication method is the most used form for authentication today. Unfortunately, people are forced into dealing with passwords on a daily basis and struggle a lot with using them [PTN+17]. Without a password manager [PZB+19], it becomes almost impossible to create, memorize, and avoid reusing unique and secure passwords across websites [FHV14]. Consequently, the user experience of passwords suffers, highlighting the need for more user-friendly authentication alternatives.

The Fast Identity Online (FIDO) Alliance and World Wide Web Consortium (W3C) have been working with hundreds of tech companies over the past decade to develop a new login standard that works the same way across multiple browsers and operating systems [FA22a]. This authentication standard is known as FIDO2, and consists of W3C's *Web Authentication (WebAuthn)* standard and FIDO Alliance's *Client to Authenticator Protocol (CTAP)*. Web services and apps implementing FIDO2, allow users to authenticate more easily than passwords, through biometrics, mobile devices, and FIDO security keys. Consequentley, FIDO2 is more secure than passwords alone [W3C19]. The purpose of this new approach is to avoid passwords altogether.

Apple, Google, and Microsoft are three leading companies that recently committed to expand the support for FIDO's passwordless login standard [FA22a]. A paradigm shift from password-based authentication to a more unfamiliar authentication method causes questions regarding security and usability. Today, FIDO Alliance is in the perfect position to accelerate the adoption of passwordless authentication on the Web. So far, prior work has focused on various usability aspects of FIDO, from security keys [DDC18; FLS+20], to phones [OAKU21; WPHH23], business use cases [FLPD22], and general user interface issues [OGY+20], or misconceptions [LHGU21].

The scope of this thesis is implementation of FIDO2 on online services on desktop. Consequently, mobile apps are excluded. FIDO2 supports several authentication methods, and this research study assesses fingerprint as a platform authenticator and security key as a roaming authenticator. We will further identify what obstacles exist today that may delay widespread adoption of FIDO2.

1.1 Research Question and Objectives

We wonder why the adoption of FIDO2 authentication has not increased more, and users are still forced to use passwords on online services. To investigate this, we have defined the following Research Question (RQ):

RQ: *What obstacles related to user experience hinder the widespread adoption of FIDO2 passwordless authentication?*

In order to investigate the obstacles related to user experience that hinder the widespread adoption of FIDO2, we have formulated four research objectives. The research objectives are defined to address specific usability factors which will be used to investigate user experience obstacles to adopting FIDO2 authentication [PSPP22]. The four Research Objectives (RO) are as follows:

- **RO1 Effectiveness:** Estimate the success rate of FIDO2 setup and sign-in processes, and identify potential failures.
- **RO2 Ease of Use:** Evaluate the user-friendliness of the FIDO2 setup and sign-in processes, and identify any usability challenges during the two processes.
- **RO3 Trustfulness:** Explore users' security perceptions of passwordless authentication and understand concerns about adopting passwordless authentication methods.
- **RO4 User Satisfaction:** Evaluate overall satisfaction and attitude towards FIDO2 authentication, and identify any obstacles that hinder user satisfaction.

To answer our defined research question and research objectives, we decided to test two online services' websites that have implemented FIDO2, namely Microsoft and eBay. Our aim was to explore how user experience plays a role in adopting passwordless authentication. We studied the following two processes on each website:

1. **Setup:** Switching from password-based authentication to FIDO2 authentication
2. **Sign-in:** Sign-in using FIDO2 authentication

By using Microsoft and eBay's websites to study setup and sign-in with fingerprint and security key, we were able to examine the user experience.

1.2 Overview of the Thesis Structure

The following list of chapters presents an overview of the thesis' structure.

Chapter 2: Background Presents authentication theory, focusing on authentication factors, password-based authentication, and passwordless authentication in general, and presents human factors in computer systems.

Chapter 3: FIDO Passwordless Authentication Introduces background information on FIDO's passwordless authentication standards. It also explores related work in the combined field of usability aspects in authentication.

Chapter 4: Research Methods Our two research methods, usability test and follow-up interview, are presented in detail. Furthermore, a description of how the chosen usability factors contribute to collect data. Limitations of our study are presented in this chapter.

Chapter 5: Results Presents the findings from the usability test and follow-up interview.

Chapter 6: Discussion A discussion of how the findings from results and existing literature link to the research question. In addition, recommendations are provided in this chapter. The discussion will further be a foundation for the conclusion.

Chapter 7: Conclusion and Future Work Provides a conclusion to our research question. In addition, the chapter provides suggestions for future work based on our findings.

Chapter 2
Background

This chapter gives an introduction to the background information needed for the thesis, focusing on different authentication methods in general and human aspects in computer system interaction. It is structured into four main sections, each providing a foundational understanding of authentication and usability aspects. Section 2.1 explores the concept of authentication and different ways to authenticate. Section 2.2 focuses on password-based authentication, presenting its benefits and challenges in the current digital landscape. Section 2.3 introduces the concept of passwordless authentication, presenting passwordless authentication methods used in this thesis and the associated advantages and challenges with these methods. Section 2.4 explains aspects of human factors in computer systems, defining two key terms used in this thesis; user experience and usability.

The state of art and related work were reviewed, and an identification of the relevant background material was carried out in the project preceding this thesis [Øse22]. Some of the relevant background material is therefore included and built upon in this chapter with a citation to the project.

2.1 Authentication

Authentication is the process of validating the identity of a user, process, or device [PMA22]. With the digital age and widespread computer usage in the last decades, authentication has been more important to ensure the security of accounts, networks, programs, and data. On the other hand, authorization determines access rights and permissions, verifying whether an entity has the necessary permissions to access specific data or execute a program [KL17]. To ensure only users with a certain authorization gain access to specific files or accounts, authentication of the users is necessary. In this way, authentication allows users to access their accounts, download a specific file, or modify a program they have permission for.

2.1.1 Authentication Factors

To validate whom a user pretends to be, one or more authentication factors are used. There are different ways of categorizing authentication factors, and one common way is to categorize the authentication factors into the three following categories, which were used in the project preceding this thesis [PMA22; NIST; Øse22].

- **Knowledge-based:** often referred to "something you know," which includes passwords, Personal Identification Numbers (PINs) and security questions, among others.
- **Possession-based:** often referred to "something you have," which includes physical keys, smart cards, phones, and USB sticks, among others.
- **Inheritance-based:** often referred to "something you are" which includes biometrics such as fingerprints, facial recognition, and voice, among others.

2.1.2 Single-Factor Authentication (SFA) and Two-Factor Authentication (2FA)

The following paragraph is taken from the project preceding this thesis [Øse22]. Single-Factor Authentication (SFA) requires the user to have one factor of authentication. The most common way to authenticate a user is to ask them for a correct combination of username and password, where the password works as the single factor of authentication. If the user enters the correct combination, the system will assume the identity is legitimate and grant access. Unfortunately, SFA is often no longer sufficient for some services due to security risks; therefore, people tend to use Two-Factor Authentication (2FA) [NM16]. 2FA considers a stronger authentication because it requires two factors of authentication instead of only one factor. An example is a person withdrawing money from an ATM. Firstly, the person needs a credit card, which is possession-based, and secondly, the person needs to enter a PIN code, which is knowledge-based. Through two authentication factors, the person can confirm their identity. Similar to 2FA, Multi-Factor Authentication (MFA) requires two or more factors of authentication [NM16].

Users using SFA with passwords are unfortunately an easy target for intruders to gain access to systems, accounts, or networks because passwords are easy to obtain these days. Therefore, using 2FA is a more secure alternative as it not only relays on passwords. On the other hand, 2FA often requires a physical authentication token that has to be connected to the client system. Another option is a device supporting in-built authentication methods, such as a biometric scanner [KZ10].

2.2 Password-based Authentication

Passwords are the traditional and most used form of authentication [PMA22]. Passwords are knowledge-based authentication where the knowledge factor refers to a secret only the user knows. In other words, a password is an individual secret, a string of self-determined characters that meet specific requirements. Password-based authentication comes with both benefits and challenges. On one hand, it is straightforward and easy to use as it does not require more than remembering the password, but on the other hand, statistics show that users are concerned about this authentication factor due to memorability problems [YM19; Øse22]. Furthermore, people are using more and more services online, increasing the number of passwords. More information about benefits and challenges is provided in Section 2.2.1. In Section 2.2.2, known threats towards password-based authentication are provided, while in Section 2.2.3, we explain some countermeasures to improve the security of password-based authentication.

2.2.1 Benefits and Challenges

Long and Complex Passwords

From a security perspective, a password is considered safe given that the password is made rugged enough. A user is free to choose between all letters including both upper cases and lower cases, special characters and numbers to create their secret password. In total there are 94 possible characters to use, considering the English alphabet. This includes 26 upper cases, 26 lower cases, 10 numbers and 32 special characters. Utilizing characters from all these categories increases the complexity and strength of the password [Dep12]. For example, a nine character long password with at least one character from each category mentioned, will have $94^9 = 572\ 994\ 802\ 228\ 616\ 704$ different possible password combinations. However, a five character long password only utilizing lower case and numbers will have $36^5 = 60\ 466\ 176$ combinations. A very strong, single computer can test around 2 billion passwords every second, which means the computer will use around 9.1 years to test all combinations of the nine character long password, while only 0.03 seconds to test all combinations of the five character long password [Dep12]. Hence, passwords are a secure choice for protecting an account if the password is long, random and complex.

Memorability Problem

The more complex password, the more difficult the password is to memorize. It is possible to reset and update passwords, but this is considered inconvenient as it is time-consuming and the user has to remember new passwords. Additionally, people rarely create a password complex enough when a password needs to be changed [Sum22]. Instead, people create memorable or similar passwords to what they had before. This postpones today's problems with passwords, such as using easily guessable passwords, but hard to remember several new passwords.

Furthermore, as preceded in the project, some people use the same password among several services, which increases the security risk even more. On the other hand, people who make different passwords for different services have more passwords to memorize. The strategy for memorizing several passwords is often to write them down, but then the security risk increases if someone else gets a hold of a person's password. The memorability issue leads to the reuse of weak passwords and makes them vulnerable to various attacks [YM19]. Due to this, usability decreases, and passwords become less user-friendly [Øse22].

Some examples confirming this are statistics from a survey that showed 76% of the participants needed to use their phone notes to save passwords [PSPP22]. As a result, passwords are being forgotten and stolen. Another result from the survey was that users often do not remember their passwords at first, making them need several attempts to log into a service. 33% of 76% needed to try and fail several times when logging into a service. Furthermore, 60% of 76% need to reset their passwords frequently. Another study [WS19] also indicates that passwords are not very user-friendly by describing passwords as a frustrating and inconvenient part of users' daily life due to the memorability problem.

Compromising Passwords

Passwords have been a widely used standard for authentication, leading to long research on cracking users' passwords to gain insight into private and sensitive information, as indicated in the project preceding this thesis. Some common password attacks are described in Section 2.2.2. When a password is compromised, it is unsafe because the credentials have been leaked in a data breach and shared online [PNP+16]. "HaveIBeenPwned.com" is a tool that allows users to check whether their email or phone is in a data breach where their password has been compromised [Øse22].

Many people today use a password management system, also known as a password manager. The password manager stores multiple passwords, each password linked to its associated service, solving the memorability problem for the user [YM19]. The system requires a master password that protects all the passwords. However, even though it helps the user, it may be problematic; if the master password is cracked, the attacker will access all of the users' passwords [YM19][Øse22].

2.2.2 Threats and Vulnerabilities

Several known threats and vulnerabilities related to passwords cause risk to authentication systems. In this section, we will present common attacks and malware targeting password-based authentication, such as brute-force, dictionary, and phishing attacks, in addition to the keylogger malware.

Brute-Force Attack

Passwords have been a widely used authentication standard for a long time, leading to long research on cracking users' passwords to gain insight into private and sensitive information. One way to crack passwords is to perform a brute-force attack. In this attack, the attacker tries every possible combination of letters, numbers, and special characters to find a combination that matches the password [KMJ18]. Brute-force attacks benefit from short passwords as there are fewer combinations to guess. As seen in Section 2.2.1, the difference in the number of combinations in a five-character long password versus a nine-character long is enormous. Also, using both upper and lower cases, numbers, and special characters will increase the difficulty massively. Typically, a strong computer is used to crack passwords, leading to a lookup of two billion passwords per second [Dep12].

Dictionary Attack

A related attack is called dictionary attack, a type of brute-force attack where the attacker only tests common passwords and words instead of all possible combinations. This is due to a higher probability that a password is a word in a language rather than a random set of characters. Humans remember words easier than random character combinations and, therefore, create these types of passwords. Instead of wasting time trying password combinations like `kgq#zl`, it is more efficient for attackers to first try common password phrases such as `mypassword` [WAMG09].

The internet offers several available tools for password cracking [KMJ18]. John the Ripper is a tool for performing dictionary attacks efficiently, with built-in wordlists with the most common passwords and password phrases. Also, it offers an easy way to add rules that can be employed to the wordlists. Some examples of rules could be adding the number one at the end of the word, changing all o's with zero, or capitalizing the first letter [WAMG09]. If the password does not appear in the wordlist and is not discovered using the rules, cracking it through a dictionary attack becomes challenging. On the other hand, brute-force attacks are often not an option to discover passwords as it is very time-consuming. Therefore, choosing a lengthy and complex password will prevent these password attacks from discovering the password. Therefore, selecting a lengthy and complex password is effective and can prevent such password attacks.

Phishing Attacks

Phishing is a social-engineering attack where an attacker sends forged emails to mislead people into sharing sensitive information or unknowingly installing malware on their computers [Hon12]. These emails are cleverly designed to imitate trusted brands and organizations, leading victims to believe they are genuine and then encouraging them to click on a link. An attacker typically wants to steal sensitive information such as personal identities and credit card information. Unlike direct attacks on computer systems, phishing targets the human element within the system [Hon12].

Figure 2.1 is an illustration of how a phishing attack is performed. First, the hacker sends a phishing mail to the target. Then the target becomes a victim by clicking on the link in the phishing email and visiting a fake website. On the phishing website, the victim typically enters login credentials to an account or credit card information. When the credentials are submitted, they are directly sent to the hacker who designed the email and website. With access to these obtained credentials, the hacker can freely use them to sign in to accounts or even sell the compromised information on the internet [Jen22].

Keylogger

A keylogger is a malware designed to monitor and record a user's keystrokes [SC09]. After the malware is installed on the victim's computer, for example after clicking on an evil link, the hacker can capture every keystroke. This may include sensitive information like passwords, credit card details, or personal messages. While its primary purpose is keystroke monitoring, modern keyloggers have evolved to include additional capabilities like cut, copy, and paste operations with more [SC09].

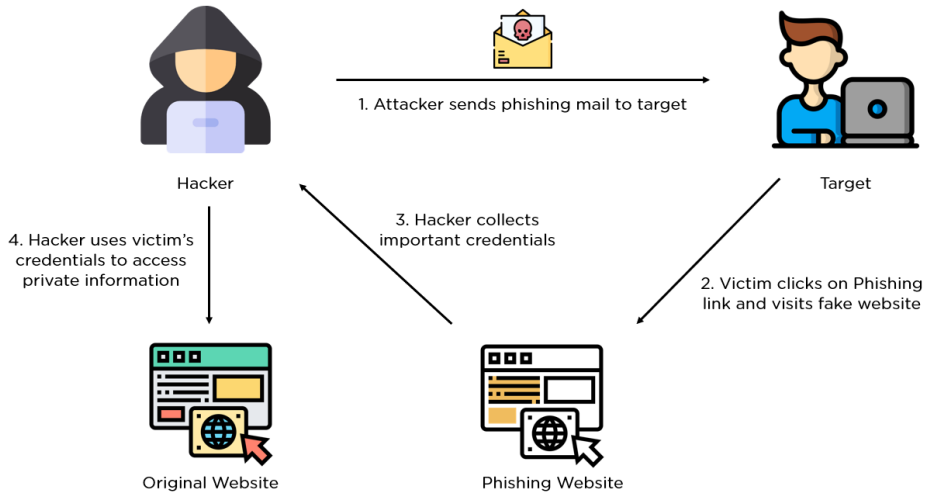


Figure 2.1: How a phishing attack is performed [Jen22].

Keyloggers differ from other types of malware. They operate alongside legitimate programs, utilizing CPU and memory resources while remaining hidden within the system [SC09]. Keyloggers are designed to perform their tasks without attracting the attention of users. The ability to stay hidden makes keyloggers a significant problem, as they are challenging to detect.

2.2.3 Countermeasures for Password Threats

This section provides how password managers and the National Institute of Standards and Technology (NIST) are seen as countermeasures for the password threats provided in this background chapter.

Password Manager

A password manager is a web-based or local software program that helps users securely store and organize multiple passwords [LHAS14]. The login credentials are stored in an encrypted database. It can automatically fill in login credentials for websites and applications that have been previously saved. By allowing for automatic fill-in, there are several advantages; the need for manually entering and remembering passwords is eliminated, and some protection against phishing attacks.

This is because the password manager will not recognize a fake domain and cannot automatically fill credentials into unknown web pages. In addition, many password managers also provide the feature to generate strong password suggestions that are difficult to brute-force [LHAS14]. This feature is usually available when creating a new password and changing an existing password, ensuring sufficiently complex passwords.

To access the password manager, usually, a master password is required. It is important to note that users should still have good password education to create a sufficiently strong and unique master password to ensure their password manager account is secured.

Authentication Guidelines by The National Institute of Standards and Technology

The *National Institute of Standards and Technology (NIST)* is a non-regulatory agency in the U.S [NIS22]. The NIST Cybersecurity Framework helps companies of all sizes comprehend, handle and reduce their cybersecurity risk. The framework is used by companies worldwide and outlines best practices regarding cybersecurity protection.

NIST has a publication called *Digital Identity Guidelines* (SP 800-63-3) with requirement recommendations for user-created passwords. For example, one of the recommendations is that a password should contain at least eight characters to avoid easy brute-force attack attempts [GGF17]. In addition, NIST recommends implementing a password check before committing a new password. This check can inform the user and avoid using passwords from previous breaches, dictionary words, repetitive or sequential characters, and content-specific words. The check may eliminate weak passwords before they are a problem.

Studies indicate that users create more secure passwords if organizations have strong password policies [SKD+16]. In addition, a strong password policy may have a negative impact, making the users annoyed and leading to the memorability problem described in Section 2.2.1. It is up to each organization to choose to follow the NIST recommendations, and some organizations avoid them due to usability, while others follow them due to security [SKD+16]. Applying a strong password policy is a dilemma for organizations, thus, other user-friendly and secure alternatives for authentication should exist without using passwords. Section 2.3 will therefore discuss passwordless authentication.

2.3 Passwordless Authentication

Technology keeps improving, and there are tendencies of a paradigm shift from password-based authentication to passwordless authentication. Today there are more internet connected devices than people. All of these devices need a type of account, and every person active on the internet manages around 90 accounts each [Lor20]. Because of the problems of password-based authentication, written in Section 2.2.1 and Section 2.2.2, passwordless authentication is seen as a more applicable solution for secure logins [PSPP22].

There are several definitions of passwordless authentication. Parmar et al. [PSPP22] describes passwordless authentication as a way for a user to authenticate without a password or other knowledge-based secrets. Examples of passwordless authentication methods are social login (a form of Single Sign-On (SSO); logging into a website with another social networking account instead of creating a new account specifically for that website, for example, "Sign in with Google"), magic authentication link via email, one-time code via email, one-time code via SMS, biometric authentication, hardware tokens like security key or smartphone, pattern lock, and authenticator applications [PSPP22].

From a security perspective, passwordless authentication differs from password-based. The typical challenges with passwords, like reuse, sharing, and hacking credentials, are not major problems when utilizing passwordless authentication. Nevertheless, because there are many different passwordless authentication methods, stating anything general about passwordless security is difficult, as it depends on the method. In this thesis, we will go deeper into the fingerprint and security key, which is two methods offering high security level [LSN+20].

2.3.1 Biometric Authentication Methods

There are several biometric authentication methods, such as fingerprint, facial, iris, voice, and gait recognition. In this thesis, we focus on biometric methods available on everyday devices accessible to most people. We will present facial and fingerprint recognition, however, fingerprint will be the main focus due to our research methods presented in Chapter 4.

Facial Recognition

Facial recognition is used among several devices to verify users' identities. The device verifies an identity of a person from a digital image or video frame [BRAM09]. Facial recognition technology has developed into two areas: Facial metric and Eigen face. First, the facial metric considers the positioning of the eyes, nose, and mouth and the distances between them. Second, the eigen face looks into symmetry patterns of the face, where the patterns point out darker and lighter areas [BRAM09]. Apple has implemented Face ID technology into iPhone and iPad Pro as a passwordless authentication sign-in method. The same has Android and Windows, with facial recognition and Windows Hello. From a usability perspective, it is an easy and efficient factor for authentication. However, some challenges are uncontrolled lighting conditions, wearing glasses, facial expressions, changes in facial hair, and aging [HA15].

Fingerprint

Fingerprint has become the most common biometric form of authentication [FLP16]. A fingerprint is a pattern consisting of ridges and valleys on the surface of a fingertip [PCKT19]. Several smart devices have provided the option to scan a fingerprint for authentication, like Apple with Touch ID, Android with fingerprint recognition, and Windows with Windows Hello. It is easy to use from a usability perspective, but touching other surfaces may lead to our fingerprint being exploited [PMA22]. From a security point of view, it takes work to guess a person's fingerprint pattern. However, it also depends on how the fingerprint is stored and measured. The fingerprint sensor does have impact on security. In addition, it may happen that a device does not recognize a user's fingerprint due to an error. Therefore, a fingerprint is not recommended as a factor for authentication alone [PMA22].

2.3.2 Security Key

A *security key* is a hardware device used for passwordless authentication on devices and web services. To authenticate through security keys, the user must manually put the key into the device or tap the key against a smart card reader. There are various types of security keys; most look like ordinary USB sticks, but there are also keys compatible with other input ports like USB-C or lightning input, see Figure 2.2 for the most common one. Some keys can communicate over Bluetooth and others over Near-Field Communication (NFC). Keys with NFC tags work like a smart card and can be tapped against a smart card reader. As the majority of new phones are equipped with NFC technology and can work as smart card readers, the security key

can be tapped against the phone for authentication, and there is no need to insert the key physically [Yub23b].

Yubico is a provider of security keys, and they recommend having two keys for each online service belonging to a user. One primary key, and one secondary key as a backup, in case of a lost primary key. The purpose of the secondary key is to ensure users won't be locked out of important accounts [Yub23f]. When first using the key, users register it directly on the service they want to authenticate for. Then, they must insert or tap the key, and a cryptographic key pair will be generated to authenticate. After the registration phase of the security key, the key can be used for sign-in by inserting or tapping the key.

Figure 2.2: A security key, more specifically a YubiKey. It is USB-compatible and has a touch sensor in gold on top.

It is easy to find a suitable key for a user's device as the different security keys support a variety of input ports and some even NFC technology [Yub23b]. On the other hand, one key usually supports only one or two input ports. Therefore, if the user has several devices with different input ports, such as a computer with a USB input port and a phone with lightning input, the user will need a key for each of these two devices. As mentioned, backup keys are recommended, so these two devices need at least four keys when following recommendations. It is a disadvantage that using security keys for all accounts, on all devices, may result in a disorganized collection of security keys. Also, unlike passwords, the user must buy the security keys themselves. The price for a personal use security key varies between 25-75 dollars at security key provider Yubico's webpage. For some people, the cost may be a financial barrier.

An advantage of the security key is that the key is independent of the device the user wants to authenticate at and the user itself. This solution differs from biometric authentication methods, which are tied to both a specific device and a user. The key can then be used on different devices if the correct input or NFC is available. As a result, users have the flexibility to bring their key and sign in on a different computer, such as a friend's device. Also, one security key may be registered for several services, such as one single key to authenticate at Google, Facebook, and Microsoft. A new independent cryptographic key pair will be generated for each service to keep all accounts securely separated at the key. If the key is lost, it cannot be identified. A lost or stolen key can also be deleted from account settings. Regarding security, a correctly set up security key is impossible to clone, unlike some authenticator apps [Yub20]. In addition, some security keys have a touch

requirement when authenticating. Touching the key after it is inserted ensures that the authentication is confirmed by a physical user and avoids remote attacks if the key always stays plugged in [Yub23d].

As people today are very dependent on their accounts and unplanned login episodes occur, the user would benefit from carrying the keys at all times to avoid any authentication problems. From a usability perspective, there are some challenges regarding carrying a physical key at all times, like remembering it and not losing it. However, the key is easy to use once it is in possession.

Security Key Vendors

Different vendors provide security keys for strong authentication. Google is one and provides the Titan Security Key [Goo23b]. However, this research focuses on the YubiKey provided by Yubico [Yub23a]. Yubico is a trusted security key vendor and member of the FIDO Alliance [Yub23a]. *FIDO Alliance* is an open industry association with a mission to reduce the reliance on passwords, and more information about FIDO Alliance will be provided in Section 3.1.1. Anyways, the key is compatible with hundreds of applications and online services. In this research, we will use a YubiKey 5Ci to test the user experience of passwordless login. Yubico's keys require a finger to touch the key after inserting it. The touch ensures that only authorized users can authenticate with the key, preventing remote attackers from utilizing it. In addition, all Yubico's keys require a PIN. The default is a four-digit PIN, which can be changed up to eight digits. Yubico produces keys specialized for personal, business, and governmental use.

2.3.3 Public Key Cryptography

The passwordless authentication methods described in Section 2.3.1 - biometrics, and Section 2.3.2 - security key, uses public key cryptography [Yub23c; CT19].

Public key cryptography, also known as asymmetric cryptography, consists of two keys, a public key, which is shared, and a corresponding private key which is kept secret to the user [Okt23]. Figure 2.3 shows how public key cryptography works. The public key encrypts the data, while the private key decrypts the data, and together they form a public key pair. If Alice sends a message to Bob, Alice uses the public key to encrypt the message and forward it to Bob. Further, Bob can use his private key to decrypt the message. An intruder will have access to Bob's public key but not Bob's private key. It is impossible to derive the private key from knowing the public key [Hel02]. Public key cryptography ensures the creation of

unique credentials for each online service, which is only generated and stored on the user's device, and ensures resistance against phishing attacks [FLS+20]. For instance, if a user authenticates using a fingerprint, a unique pair of private and public keys is generated on the user's local device. Therefore, the private key and the fingerprint never leave the device [CT19].

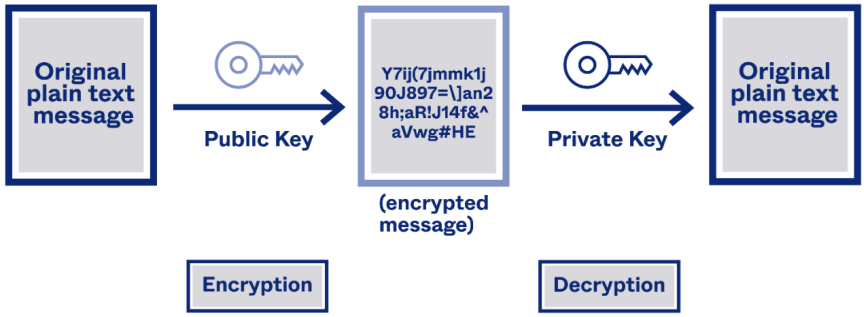


Figure 2.3: Illustration of how public key encryption works [Okt23].

2.3.4 Mitigating Password Threats

Passwordless authentication reduces the risks for the given attacks in Section 2.2.2. One of the reasons for increased security is due to the use of public key cryptography described in Section 2.3.3. Compared to passwords, passwordless authentication methods using this type of cryptography are resistant to phishing attacks which ensure higher security. Passwordless authentication offers the advantage of no leaked information between the user and the website. In this way, it is resistant to phishing attacks and keyloggers described in Section 2.2.2. These advantages are mainly due to the hardware-based authenticators, such as the security key and the fingerprint sensor implemented into a hardware device, where the private key never leaves [LSN+20]. In addition, dictionary attacks are not a convenient method to disclose private keys, and there are no other recognized methods for guessing private keys today, mitigating the chance of guessing and disclosing private keys. Therefore, passwordless authentication, such as fingerprint and security key, provides a more secure authentication compared to text-based password authentication [AWAC20].

Figure 2.4 provides a ranking of different authentication methods given by Microsoft. Passwordless authentication is recommended over password-based due to a more secure sign-in experience. Furthermore, Microsoft suggests passwords to be replaced with more secure authentication methods [Mic23].

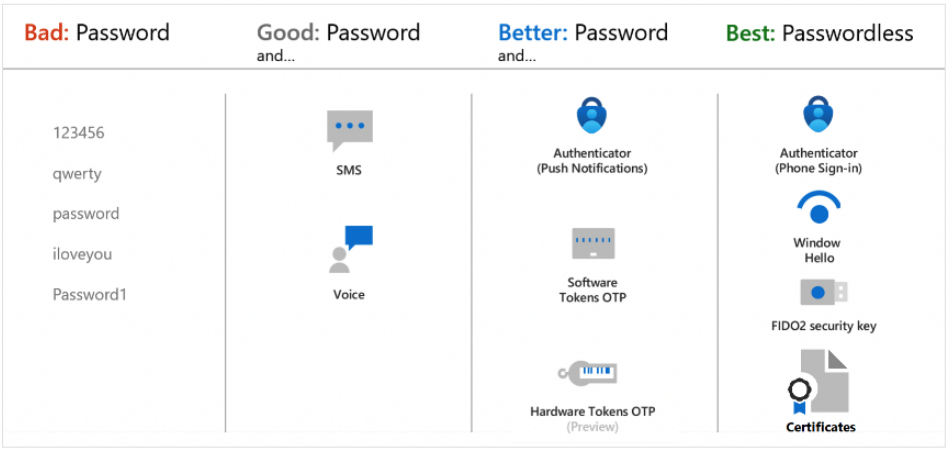


Figure 2.4: Ranked authentication methods by [Mic23]. Passwords are bad, passwords in combination with other factors are better, and passwordless is the best.

2.4 Usability and Human Computer Interaction

Human–Computer Interaction (HCI) focuses on the interaction between humans and computer systems. The design of interfaces is important, and how the user and computer system work together. HCI is a multidisciplinary field involving computer science, cognitive and behavioral science, and industrial design [ISO10]. See Figure 2.5 for other related fields.

Various factors must be considered when developing new systems, products, or services to ensure a successful system [Nie20]. A system that appears excellent from a technical standpoint may not necessarily be optimal for its users. Therefore, human-centered design is an approach that aims to create interactive systems that are both usable and useful. This is achieved by prioritizing the users and their needs while combining knowledge and techniques from human factors and usability [ISO10].

Understanding the user is of the highest importance. The system should be designed for a specific user group, considering their limitations, capabilities, knowledge, experience, education, habits, preferences, and more. Additionally, there may be multiple user groups with various needs, each requiring detailed consideration. The use context can vary among the user groups, and user requirements may conflict with those of other groups or stakeholders, making it challenging to satisfy everyone (ISO 9241-210:2010) [ISO10].

ISO 9241 aims to guide the development of usable systems to those responsible for managing hardware and software design and re-design processes [ISO10]. It offers requirements and recommendations for identifying and planning effective human-centered design practices. This approach has several benefits, such as improved productivity, performance, user satisfaction, and security [Nie12; ISO10].

Figure 2.5: Related fields to Human-Computer Interaction [CSBM17].

2.4.1 User Experience

User Experience (UX) and HCI are related. While HCI focuses on designing computer systems and their interfaces, user experience design focuses on creating positive user experiences, for example, when interacting with authentication systems. However, there are several ways to define User Experience. Previous work [LRH+09] has conducted a survey to gather 275 different researchers' views on UX due to difficulties

in agreement on what user experience actually is and embraces. It is a fast-growing field without a clear definition and, therefore, not a common understanding of the term. A frequent agreement from the paper was that UX is context-dependent, dynamic, and subjective, focusing more on individual aspects rather than social ones [LRH+09]. ISO defines UX as *"A person's perceptions and responses resulting from the use and/or anticipated use of a product, system or service"* [ISO10].

ISO adds three notes to this definition [ISO10]:

> **Note 1:** The user experience surrounds users' emotions, beliefs, preferences, perceptions, and behaviors before, during, and after system use.
>
> **Note 2:** User experience is influenced by brand image, presentation, functionality, attitudes, and the use context.
>
> **Note 3:** When considering users' personal goals, usability can include senses and emotional aspects typically associated with user experience.

2.4.2 Usability

Usability is a sub-discipline of user experience design. Usability measures how easily users interact with a system within a specific context, and it is possible to measure usability [Soe20]. It is often used in UX design processes as it contributes to a better user experience [Soe20].

ISO's definition of usability is the *"Extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction"*. This definition also includes a notable point regarding usability that should be considered while considering the combination of specific users, goals, and context of use [ISO10].

When analyzing the usability of a system, it is necessary to define certain attributes. However, these attributes vary across different sources. For instance, the Norman Nielsen Group, a leader in the field of UX, explains usability using five components: learnability, efficiency, memorability, errors, and satisfaction. Other sources include different attributes such as effectiveness, comprehensibility, engagement, simplicity, and ease of learning [ZA05].

Usability testing is used to evaluate the usability of a system. One or more observers observe participants perform specified tasks in a test environment similar to the real environment to use the system. The goal is to identify obstacles to usability and put together recommendations to help developers to develop usable systems. It involves various steps such as discovering a problem, planning the test, defining tasks, questions, or surveys, test roles, designing the laboratory with useful equipment, planning participant requirements, and performing pilot testing, before actually conducting the test [Lew12].

Chapter 3
FIDO Passwordless Authentication

This chapter presents relevant background information for the thesis, covering FIDO authentication and related work. The chapter is organized into three main sections, each contributing to understanding contexts within FIDO authentication. Section 3.1 explains the FIDO (Fast Identity Online) framework and the FIDO2 standard, highlighting their value in modern authentication. Section 3.2 provides an overview of the current state of FIDO2's adoption and usage. Finally, Section 3.3 presents a review of related work on the field, specifically focusing on usable security, thereby establishing a broader context of the research. The following chapter also includes an identification of the relevant background material carried out in the project preceding this thesis [Øse22].

Together, Chapters 2 and 3 provide a solid foundation of knowledge on authentication, the risks associated with password-based authentication, and the advantages of FIDO's passwordless authentication while also exploring human factors relevant to users interacting with authentication systems.

3.1 Fast Identity Online (FIDO)

Fast Identity Online (FIDO) authentication is a set of open standards for passwordless authentication [FA23c]. FIDO authentication is based on public-key cryptography as described in Section 2.3.3, making FIDO authentication a secure authentication method resistant to phishing and replay attacks. The authentication standards are developed by the FIDO Alliance and enable authentication to both a device and online services. The online services can be accessed from a browser or as an application, in mobile and desktop environments. Several authentication methods are supported by the FIDO Alliance, enabling FIDO authentication. Examples are various forms of biometric recognition, security key, and a smartphone used for cross-device authentication. However, fingerprint recognition and security key are

the methods we focus on in this thesis. One of the benefits of FIDO authentication is the range of devices and methods available to use for authentication, such as security keys, smartphones, and computers [FA23b].

3.1.1 The FIDO Alliance

The *FIDO Alliance*, an open industry association with a mission to reduce the reliance on passwords in authentication standards, developed FIDO authentication. The FIDO Alliance was formed in 2012 by several leading organizations and individuals [FA21b]. Hundreds of global tech leaders have worked together to push toward the organization's mission which is to change the nature of authentication with secure, open standards. The standards are more secure than passwords and SMS One-time Passwords (OTPs), and easier to use [FA22c]. The tech leaders work with enterprises, payments, telecom, government, and healthcare. Some organization members of the alliance are Amazon, Apple, Google, and Microsoft. These members influence the deployment of FIDO and establish best practices for deploying FIDO authentication. Furthermore, the members raise awareness of the Alliance's mission and FIDO specifications [FA21b].

The FIDO Alliance carried out three measures to fulfill its mission. Firstly, they developed technical specifications that are not dependent on passwords. As a result, FIDO Alliance has published three sets of specifications ensuring measures towards their mission. These specifications are Universal Authentication Framework (UAF), Universal Second Factor (U2F), and FIDO2.

FIDO U2F, also called CTAP1, supports a robust second factor to user login, where the first factor is a password. The second factor accepts a compliant FIDO security key [FA22e]. FIDO UAF supports a passwordless experience by allowing users to register their devices to an online service by selecting a local authentication mechanism. Local authentication mechanisms include swiping a finger, looking at the camera, speaking into a mic, and entering a PIN code [FA20]. The local authentication mechanism stored is further used to authenticate, and then passwords are no longer required for the specific device. In addition, FIDO UAF supports a combination of multiple local authentication mechanisms, such as a fingerprint combined with a PIN code. This ensures a higher degree of security [FA22e]. FIDO U2F and FIDO UAF will not be the focus of this research study. However, FIDO's newest specification, FIDO2, a standard ensuring passwordless sign-in across devices and platforms on online services and applications, is built on the U2F and UAF standards and will be discussed in Section 3.1.3.

The second measure carried out towards the Alliance's mission is the certification programs to ensure successful worldwide adoption of the mentioned specifications. The purpose of the certification programs is to enable implementations to be identified as officially FIDO certified and ensure interoperability between the implementations of FIDO [FA22b]. In other words, interoperability among FIDO products is critical for the widespread adoption of FIDO authentication. Multiple companies within several markets have taken advantage of the certification programs. Huawei, Yubico, and Google are some of the companies in the FIDO-certified ecosystem today [FA22b]. Third and last measure, FIDO Alliance submits its technical specifications to organizations to be standardized formally. This aims to ensure that FIDO standards are being recognized and adopted worldwide. Furthermore, when the specifications are standardized formally, FIDO becomes more adopted by others, increasing consistency and interoperability between FIDO products.

3.1.2 FIDO Registration and Login Process

FIDO protocols use public key cryptography as described in Section 2.3.3 [FA17]. In order to describe the functionality of public key cryptography in FIDO, which enhances authentication security, we separate it into the registration and login phase.

Figure 3.1 illustrates the registration phase of the FIDO protocol. First, the user must choose a type of FIDO authenticator which matches the online service's policies. This could be a security key or a smartphone with fingerprint sensor, like in this case. Second, the user approves that the authenticator can be used by unlocking the phone using fingerprint. Third, the user's device generates a private-public key pair. The key pair is unique for the user's device, account, and online service. Lastly, the online service receives the public key and can now connect to the user's account [FA17].

Figure 3.2 illustrates the login phase. First, when a user tries to log into a service, the online service sends a challenge to the user. Then the user has to sign in with the registered device for the corresponding service. The second step is for the user to answer this challenge by using the same FIDO authenticator used in the registration phase, in this case unlocking the phone. The challenge answer is replied by the device and not the user itself. The device will further choose the correct key to the corresponding service and create a response to the challenge sent by the service. Lastly, the device sends the challenge in return to the service, with the answer. The public key stored by the online service is then used to verify the device's answer, authenticate the user, and ensure login [FA17].

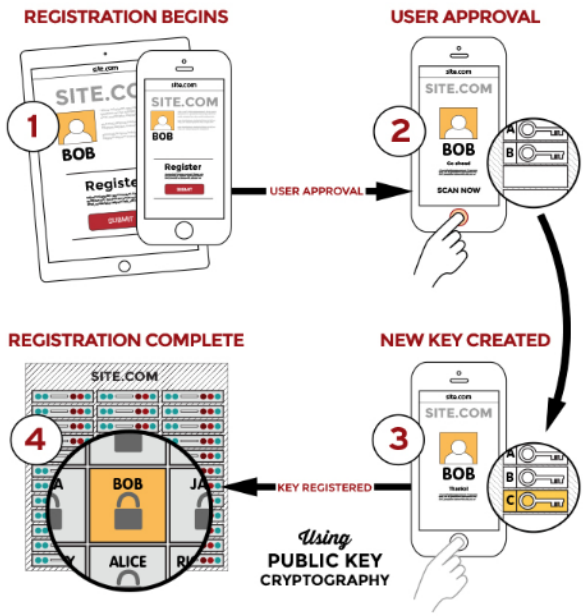


Figure 3.1: Illustration provided to demonstrate the registration process in FIDO, which utilizes public key cryptography [FA17].

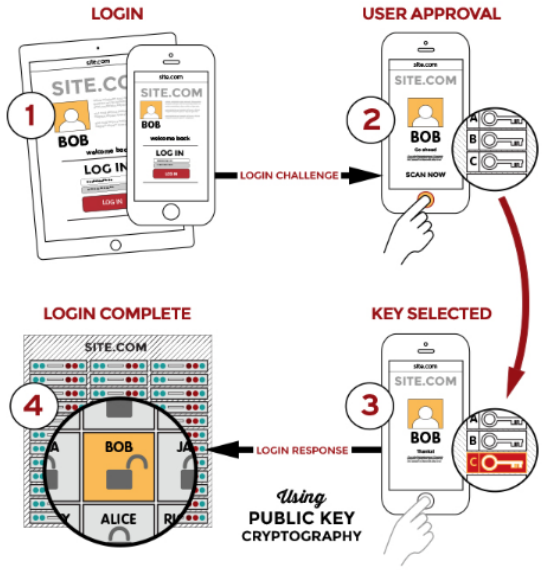


Figure 3.2: Illustration provided to demonstrate the login process in FIDO, which utilizes public key cryptography [FA17].

FIDO's Unique Credentials

When using FIDO, the cryptographic keys, also known as login credentials, are unique for each online service or device [FA22d]. This prevents users from being tracked across different websites. Moreover, the private key remains stored on the user's device and is never shared with the online service. It is important to note that when using a fingerprint credential or other biometric methods integrated into the device, the same device used during the setup process must always be used for authentication. This requirement originates from the fact that the private key is locally stored and inaccessible from other devices. These characteristic enhances the security of FIDO authentication.

User Experience Guidelines Documentation

The Executive Director and Chief Marketing Officer of FIDO Alliance, Andrew Shikiar, wrote a blogpost describing FIDO authentication as simpler and stronger than passwords [FA21a]. However, Shikiar describes a need to get users more habituated to the user experience. Service providers implementing FIDO authentication on their websites have no similar user interface guidelines to follow. Therefore the user interface for implementing FIDO authentication varies for each web service, and thereby the user experience varies.

FIDO's Board of Directors created the FIDO UX Task Force (UXTF) with the purpose of developing the best UX practices for FIDO implementations [FA21b]. Product leaders from Apple, eBay, Google, and Microsoft, among others, participated as volunteers for this project with the purpose of ensuring authentication without passwords is more usable.

The FIDO Desktop Authenticator UX Guidelines were published in June 2021 and are designed to help the ones responsible for implementing the interface or user experience of FIDO desktop authentication for a browser-based website [FA21b]. The guidelines aim to accelerate decision-making when implementing FIDO authentication and specify what information and controls should be given to the user.

Passkeys

Passkey is a term the FIDO Alliance uses for multi-device FIDO credentials [FA23b]. The term was introduced by Apple in 2021 and is a relatively new concept [Yub22a]. Passkeys enable users to access their FIDO sign-in credentials on multiple devices, including new ones, without the need to enroll each device separately for every

account. The credentials are synced into the cloud to enable this function. For example, if a user has a fingerprint credential on an iPhone, the fingerprint can also be utilized on a Mac connected to the same iCloud account, synced via the cloud. This is possible due to the private key being stored in the user's iCloud, allowing other authorized Apple devices to access it [Yub22b]. However, it is important to note that the biometric data is still stored locally on the device. Only the private key is stored in the cloud.

Another advantage of passkeys is that if users lose their device, they cannot access any accounts without that specific device. However, with passkeys, they are synced into the cloud, functioning like a backup passkey [Yub22a]. This ensures that even if the device is lost, the user can still access their accounts. All passwordless credentials are not multi-device FIDO credentials or synced into the cloud. Therefore, the term "passkey" will not be used in this thesis to avoid confusion.

3.1.3 FIDO2: The Standard for Online Service Authentication

As preceded in the project preceding this thesis, to standardize FIDO authentication for the entire Web platform, FIDO Alliance partnered with *The World Wide Web Consortium (W3C)*, an international organization working to develop web standards for online services and applications [FA22d; Øse22]. Together they created a passwordless login standard, the *FIDO2 Standard*, which ensures consistent, secure, and user-friendly logins across devices and platforms [FA22a]. The authentication can be done in both desktop and mobile environments, without the need of traditional credentials like passwords or usernames. The FIDO2 Standard consists of W3C's Web Authentication specification, *WebAuthn*, and FIDO's Client to Authenticator Protocol 2 (*CTAP2*)[Øse22]. FIDO Alliance classifies their authenticators into two types, known as platform authenticators and roaming authenticators [Yub]. We will now look into the components of FIDO2; the authenticator types, WebAuthn, and CTAP2 before looking into how FIDO2 works illustrated in Figure 3.3.

Platform Authenticators

An authenticator that is integrated and built into a device and only works on that device is called a platform authenticator [Yub]. It is also called an internal authenticator, and cannot be disconnected from the device. Common examples are biometric authentication methods such as Touch ID on macOS and iOS, Windows Hello on Windows 10, and fingerprint and face recognition on Android [Yub]. Biometric data is always stored locally on the device in the form of a mathematical representation. On Apple devices, this storage location is referred to as the "Secure Enclave" [App21].

Typically, a platform authenticator has a biometric sensor, but it can also support other types of inputs, such as PIN. These authenticators often offer alternative authentication methods, allowing users to enter a PIN in case biometrics is not preferred or cannot be used [Yub].

Roaming Authenticators

Roaming authenticators, also called external or cross-platform authenticators, are portable authenticators that can be used to authenticate across multiple devices [Yub]. Examples of roaming authenticators are hardware security keys and smartphones. To authenticate through a roaming authenticator, it needs to be connected to the device through USB, NFC, or Bluetooth. In addition, these authenticators often offer a type of user verification, for example, the use of a PIN [Yub].

Web Authentication (WebAuthn)

WebAuthn, short for Web Authentication, is a browser-based API that allows web services to simplify and secure user authentication by using registered devices (phones, laptops, etc.) as factors [Yub21b]. It is a relatively new global standard, finalized by FIDO and W3C and officially recognized as a W3C web standard in March 2019 [FA22d]. To enable this secure authentication, browsers, platforms, and websites must support WebAuthn. More about which browsers, platforms, and websites support to WebAuthn today in Section 3.2.3. The WebAuthn standard supports platform authenticators and roaming authenticators. This means web services and applications supporting WebAuthn can offer their users strong authentication with authenticators, such as security keys or biometric readers, on supported platforms and browsers [Yub21b].

Client to Authenticator Protocol 2 (CTAP2)

CTAP2, the Client to Authenticator Protocol 2, is a protocol that enables the communication between a roaming authenticator and another client or platform [Yub21a]. This could, for example, be between a security key and a browser or an operating system. The CTAP2 communication goes over USB, NFC, or Bluetooth communication mediums. The protocol is developed by the FIDO Alliance [Yub21a].

How FIDO2 works

An explanation of how FIDO2 works was given in the project preceding this thesis, and is illustrated in Figure 3.3. It consists of the two core components WebAuthn and CTAP2. They both are required to achieve FIDO's passwordless login on online services. To summarize the figure, WebAuthn allows websites to add FIDO-based authentication, and CTAP2 enables a roaming authenticator to work with desktops or browsers that support WebAuthn. A relying party, for example, a FIDO server, verifies the authentication. To use FIDO2 authentication, you need a platform that has a platform authenticator or supports roaming authenticators. The roaming authenticator communicates with the client, a platform or browser, over CTAP2, while the client communicates with the relying party through WebAuthn [Yub; Øse22].

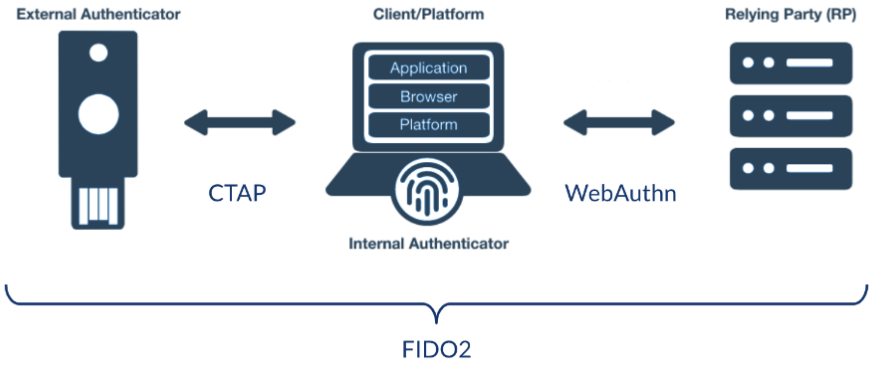


Figure 3.3: Overview of how FIDO2 works. FIDO2 consists of CTAP and WebAuthn [Yub21b].

3.2 Current Situation around FIDO2

To use FIDO2's passwordless authentication, there are several components that have to be compatible and support the FIDO2 standard. The web service, browser, and platform must support FIDO specifications and WebAuthn, and the user needs to have a roaming or platform authenticator. This section presents different services supporting FIDO2, compatible browsers and platforms, and the estimated number of users using FIDO2 authentication today.

3.2.1 FIDO2 as Single-Factor versus Two-Factor Authentication

FIDO2 can be used as single-factor or two-factor authentication. When FIDO2 is used as the first and only factor (SFA), the password is swapped with the passwordless authentication method, and the login process becomes *passwordless*. However, using FIDO2 in 2FA does not make the login experience passwordless. This is because the process still includes a password as the first factor.

3.2.2 Services Offering FIDO2 Authentication

Many big services provide FIDO2 authentication today. Some examples are known companies like Facebook, Twitter, YouTube, Github, PayPal, and Amazon. See Figure 3.4 for more examples [FA23a]. A study from 2020 saw that there were at that time no high-profile websites that had implemented FIDO2 as single-factor authentication, only as two-factor authentication [AWAC20]. Today, still the majority of services offer FIDO2 authentication only as two-factor authentication. However, even though providing FIDO2 as SFA may increase the adoption of FIDO2, the study investigated potential factors of why there is slow adoption of FIDO2 and indicated that supporting single-factor would not be enough to make widespread adoption of passwordless authentication [AWAC20].

Figure 3.4: Examples of services supporting FIDO2 implementation are Samsung, Google, Microsoft, MasterCard, 1Password and Apple [FA23a].

Services offering FIDO2 as Single-Factor Authentication

In this thesis, we are interested in passwordless authentication, but only a few services implement FIDO2 as SFA, making the login passwordless. Microsoft, eBay, Yahoo! Japan, and the travel fare engine Kayak are examples. In addition, there are some foreign companies and banks providing this, but cannot be accessed from Norway. New from May 3rd, 2023, was that Google also started to provide FIDO2 as SFA [Goo23a].

3.2.3 Compatible Platforms and Browsers

In order to authenticate through FIDO2, not only the web service needs to support FIDO2 and WebAuthn. Also, the user must ensure they have a compatible browser and platform supporting WebAuthn, and a platform supporting CTAP2 if a roaming authenticator is used. Platforms supporting platform authenticators (for example biometrics) are Android 7+, iOS 14.5+, Windows 10, macOS Catalina, and macOS Big Sur [Aut23]. Roaming authenticators (for example security keys) are supported by the same Operating Systems (OSs) as mentioned above, and Linux as well. Known browsers supporting WebAuthn are Chrome, Safari, Firefox, and Edge. However, the type of OS determines which of the listed browsers it is compatible with. Figure 3.5 shows an example of which browser is compatible with which OS on a platform authenticator [Aut23].

	Android 7+	iOS 14.5+	Windows 10 *(with Windows Hello)*	macOS Catalina	macOS Big Sur	Desktop Linux
Chrome	Yes	Yes	Yes	Yes	Yes	-
Safari	N/A	Yes	N/A	No	Yes	N/A
Firefox	No	Yes	Yes	No	No	-
Brave	No	Yes	Yes	Yes	Yes	-
Edge	No	Yes	Yes	Yes	Yes	-
Internet Explorer	N/A	N/A	No	N/A	N/A	N/A

Figure 3.5: Compatibility of OS's and browsers with platform authenticators in FIDO2 authentication [Aut23].

On “https://webauthn.me/browser-support”, a user can check whether their current device, or more specifically the OS, and browser they enter the web page with, supports WebAuthn and if their device is compatible with platform authenticators and/or roaming authenticators [Aut23].

3.2.4 Quantifying User Adoption of FIDO2 Authentication

There are limited statistics available on the current adoption rate of FIDO2 authentication. Despite this, we know most services providing FIDO2 authentication provide it as the second factor. We can then investigate how many people use 2FA. This is also difficult to answer without exact numbers and highly reliable sources. Considering Facebook as an example, a known social media platform, in 2021, 1.5 million users used 2FA [McC22]. This is not much compared to 3.5 billion active accounts in the same year [Dea23]. At Google, less than 10% have enabled 2FA [Fly23]. Considering that the users using 2FA have several options for the second factor, the chance they use FIDO2 authentication methods and not more common methods like email codes, OTP, authenticator applications, or sms-codes is not the best.

Regarding the type of FIDO2 authenticator, it is interesting how many people have a FIDO2-compatible authenticator. According to Cisco Duo’s 2022 Trusted Access Report, over 80% of today’s smartphones enable biometrics, making many potential users [Duo23]. Moreover, over 22 million Yubikeys are sold, which is the most common security key [Yub23e].

Many individuals today own compatible authenticators, making them potential users of FIDO2 authentication. However, the current adoption of FIDO2 authentication remains limited, presenting a notable opportunity for large companies to increase its usage among their user base.

3.3 Related Work on FIDO Passwordless Authentication

Various usability aspects on digital authentication have been studied in previous related work.

Security Keys Related work from Das et al. [DDC18] performed a usability study of the FIDO security key in 2018. The study aimed to identify difficulties with the Yubico security key that might be barriers to adoption. One of the barriers found was the misconception between biometrics and the circular touch sensor on the YubiKey. Moreover, the study was separated into two phases. After the first

phase, recommendations were given to Yubico, and the second phase conducted consisted of new implementations based on the given recommendations. The two-phase experimental study revealed a significant increase in usability in the second phase but not any corresponding increase in acceptability. Furthermore, M. Farke et al. [FLS+20] explored FIDO2 security keys for primary authentication on a web application in a small firm. The primary concern found during this research was losing access to the account through a defect or loss of the security key, especially if it was the only way to authenticate. Therefore account recovery was considered an obstacle to adoption.

Smartphones Owens et al. [OAKU21] studied how users percept the usability and security of smartphones as the FIDO2 roaming authenticator. This research can be seen together with M. Farke's research indicating account recovery as a primary concern. Owens' research indicated account recovery and availability as their primary concern among the participant group. The smartphones were compared with the security key, which can be stolen or lost. Moreover, the smartphone may run out of battery. Multiple authenticators are therefore recommended for FIDO2 to avoid being locked out of the account. Security keys, on the other hand, do not run out of battery. Furthermore, passwords were found to be more usable than smartphones due to difficulties in the setup process.

A research study by Würsching et al. [WPHH23] compared the platform and roaming authenticator on smartphone. Apple Touch ID was used as the platform authenticator, and a Yubico YubiKey was used as the roaming authenticator. From a usability perspective, results found that both platform and roaming authenticators on smartphones had similarly high level of usability. However, platform authenticators had a higher acceptance. Account recovery was also indicated in this study as a usability barrier. Moreover, to adopt FIDO2 on their smartphone, results revealed that the adoption was dependent of specific account types. Accounts used often was not found beneficial for roaming authenticator due to the physical effort of inserting the security key for every sign-in. Nevertheless, the study indicated differences in how users prioritize usability, security and availability for account types.

Business Use Case Another study by Farke et al. [FLPD22] conducted a qualitative study of Windows Hello and its usability and perceived security. A small business was recruited for the study. Windows Hello was found as convenient to use. However, PIN was preferred instead of biometrics due to their hardware support and setup of their workplace. For instance, no biometric hardware were available, or the biometric hardware was placed far away from being recognized with biometrics.

General User Interface Issues Related work from Oogami et al. [OGY+20] was carried out in the project preceding this thesis. Oogami et al. investigated how users feel using WebAuth as an authentication standard. Their focus was on a fingerprint on an Android phone. By carrying out their observation study, their results showed that users were familiar with unlocking their smartphones with a fingerprint and without any mistakes. However, only some people managed to set up the WebAuthn registration successfully. In this observational study, the participants were told to tap the fingerprint "sensor" in order to finish the registration, but results showed that several did not know what a sensor was. The failed participants tapped the fingerprint-like icon on the screen. One of the reasons for the misunderstanding was due to the dialogue box explaining how to register further. The research concluded a possibility that the registration procedure and how it was explained have a significant impact on the usability.

Misconceptions A study by Lassak et al. [LHGU21] studied the use of biometrics within FIDO2 and WebAuthn. To consider the identified security misconceptions, the most identified misconception was regarding how the biometrics were stored. There were 48% of the participants who believed that biometric data was stored in the online service's database. To further consider the identified usability misconceptions, the most severe misconception was that the participants thought they could sign in to the website with a different device. Lassak's study indicates a misunderstanding among people about the functionality of WebAuthn. In order to authenticate with WebAuthn, a user needs to register for each device.

Chapter 4
Research Methods

This chapter outlines the research methods used in our study to investigate the user experience of FIDO2. First, Section 4.1 presents the research goal, then Section 4.2 describes the overall research strategy for conducting the research study. We have selected factors and metrics in Section 4.3, which serve as the root for our research methods when investigating the user experience. To explore the factors and metrics, we designed a usability test described in Section 4.4, and a follow-up interview described in Section 4.5. Section 4.6 presents the participant group consisting of ten participants. Furthermore, Section 4.7 present ethical considerations concerning the test procedure, while Section 4.8 presents the test environment, including the room, software, and hardware equipment used. Section 4.9 presents our iterative pilot testing performed to collect reliable and precise findings during the research methods. Finally, we present the research's limitations in Section 4.10.

4.1 Research Goal

Our goal was to identify obstacles that could prevent the widespread adoption of FIDO2. Microsoft and eBay's websites were used to test FIDO2 as SFA. We used Microsoft and eBay's specific web interfaces as two examples of how passwordless authentication can be used and visualized. The FIDO2 authentication methods used were fingerprint and security key. Ten participants conducted a set of tasks individually on each of the websites. The tasks were related to setup and sign-in of passwordless authentication methods, specifically security key and fingerprint. We aimed to investigate user experience through usability factors such as ease of use, effectiveness, trustfulness, and user satisfaction. To collect quantitative and qualitative data, we used a mixed-method approach to perform a usability test and a follow-up interview. Our research provided a comprehensive understanding of the obstacles from a user experience perspective.

4.2 Research Strategy

A literature review has been conducted to study findings in other studies closely related to our research and to identify various factors that influence the user experience of passwordless authentication on online services. A study by Lassak et. al [LHGU21] studied the misconceptions of WebAuthn using biometrics, where they studied biometrics on mobile devices. However, in their future work, they stated the importance of studying biometrics within apps compared to a website context.

The research paper by Lyastani et al. performed a comparative usability study of FIDO2 passwordless authentication as single-factor authentication [LSN+20]. The study aimed to understand users' perceptions, acceptance, and concerns about passwordless authentication, with a security key as the authentication method. Regarding usability, Lyastani et al. found that FIDO2 was considered more usable than passwords. However, the fear of losing the security key caused concerns in adoption due to account recovery. The literature review involved identifying relevant papers by using keywords like *Authentication, FIDO, FIDO2, W3C, WebAuthn, passwordless, password, usable security, user experience, and usability.* By conducting a litterature review, we understood the field better and could define an interesting research question for our research [Sny19].

Figure 4.1 illustrates an overview of our research process. First, we did a literature review before we were able to define a research question. Then we selected and designed our research methods. After recruiting participants and running pilot testing, we continued with the actual usability test and follow-up interview. Finally, we could analyze and discuss the results.

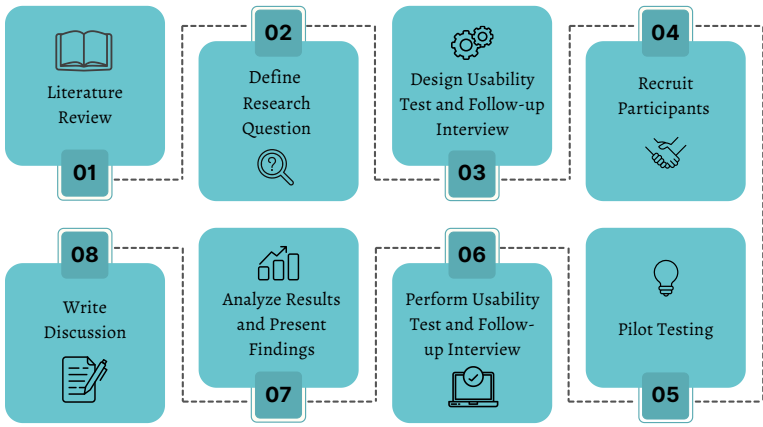


Figure 4.1: Overview of the research process followed through this research study.

Overview of Research Design - Mixed Methods

We have based our research design on a framework illustrated in John W. Cresswell's book "Research Design" [Cre09], which is given in Figure 4.2. To answer our research question and objectives, a mixed methods approach was conducted. To reason for why we chose the mixed methods approach, we will base the reasoning on the given figure.

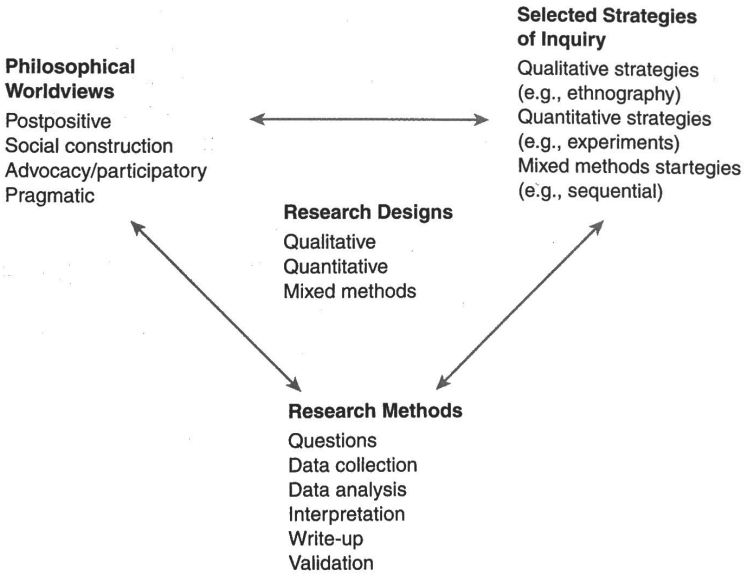


Figure 4.2: A Framework for Research Design: The Interconnection of Worldviews, Strategies of Inquiry, and Research Methods [Cre09].

The first element of the framework, to consider the **philosophical worldviews**, the motivation for choosing mixed methods was through pragmatists' worldview, which does not focus specifically on the methods, but instead emphasizes the research problem and uses all approaches available to understand the problem. In addition, the pragmatists do not look at the world as one unit. The similarity with the mixed methods approach is the focus on collecting data from several approaches, rather than only a qualitative or quantitative approach [Cre09].

Secondly, the type of mixed methods approach was chosen. This is the **strategy of inquiry**. We chose a concurrent mixed method approach, that are procedures where the quantitative and qualitative data are merged to provide a comprehensive analysis of the research problem. Both forms of data are collected simultaneously [Cre09].

The third element of the framework is the **research methods**. We have designed a usability test with a follow-up interview, and these methods are selected to contribute to answering the research question. We collected both quantitative and qualitative data through observations, participants' thoughts, and questions. The observations were performed with schemes and charts to record and quantify specific observations, enabling us to collect quantitative data. Participants' thoughts and questions we asked provided valuable qualitative data for our analysis. The follow-up interview allowed the participants to comment on their experience after task completion, ensuring a more valid study of our objective observations.

4.3 Selecting Usability Factors and Metrics

In order to collect data during the usability test and the follow-up interview, we needed to define some measurements. To do so, we selected usability factors and metrics that contributed to explore what obstacles exist to the widespread adoption of FIDO2. These measurements scope our research and play a significant role in understanding existing obstacles associated with the transition from password-based authentication to passwordless authentication.

First, we recognized the importance of defining the relevant factors before choosing the specific metrics associated with the factors. This process involved studying multiple usability test papers that explored various factors and metrics [Fin10; ZA05; II22; TRH+12] It became clear that no mandatory factors or metrics must be studied in a usability test. Instead, selecting factors and metrics depended on the specific research goals. This notion was supported by the findings of the paper titled "Usability Measurement and Metrics: A consolidated model" [SDKP06].

Section 4.3.1 and 4.3.2 introduces the selected factors and metrics for the usability study, and discuss how these factors contributed to collecting data. The usability factors and metrics found were suitable for studying the user experience and implementations of FIDO2.

4.3.1 Usability Factors

The authors of the well-used paper "Usability Measurement and Metrics: A consolidated model" investigated other usability test papers and identified ten common factors often used in usability testing [SDKP06]. Then, they recommended selecting a subset of factors from their consolidated model that aligns with the goals of the usability study.

Considering the research study mentioned above, we carefully evaluated the factors outlined in the paper. As a result, we selected four factors we believed would contribute to answering our research question and gaining valuable insights throughout the usability study and follow-up interview.

The following factors were chosen:

Effectiveness refers to users' ability to complete tasks. Effectiveness can be measured by the completion rate, which means comparing the performance with reaching a required end state [ZA05]. When measuring whether a user has completed a task in the usability test, it is assumed that no assistance is provided during the tasks. In our usability test, we want to measure if the participant can set up and sign in with FIDO2 without help.

Ease of Use refers to how straightforward it is to complete a task. The intuitiveness of the interface of the services is important. Ease of use includes clear instructions and information preventing users from making obvious mistakes or less efficient path choices. The level of simplicity and efficiency will be taken into account.

Trustfulness refers to if the user trusts the solution. In our research, the solution refers to FIDO2 authentication. The users' perceptions of security are important, and previous authentication experiences may influence this. In addition, the level of trust in the equipment used to perform passwordless authentication will be studied. Trust is essential because users must be confident in the technology's ability to protect their sensitive information to adopt it.

User Satisfaction reflects the users' attitude toward the system. We wanted to study participants' attitudes toward passwordless authentication in our usability test. It includes the experience of setting up and signing in passwordless, the perceptions of simplicity and efficiency, and whether the satisfaction aligns with their expectations and preferences [ZA05]. By analyzing user satisfaction, we gained valuable insights into their overall experience.

We did consider other factors which could be relevant and useful. For instance, we saw the factor *efficiency* as relevant to our research study. However, efficiency focuses on time, and we saw the success rate within effectiveness as more important. To adopt FIDO2, we found it more relevant whether the participant actually managed to complete the setup and sign-in than the amount of time they spent on the setup and sign-in. Effectiveness was chosen over efficiency due to a better focus on addressing the overall user experience and identifying obstacles of FIDO2.

4.3.2 Usability Metrics

After selecting the four factors, the next step was to decide how we wanted to measure the factors, which involved selecting relevant metrics contributing to answering the research question. As mentioned in Section 4.3.1, we considered factors other than the ones we chose, and the same was for the metrics. Time spent on each task was a metric considered, but we concluded this was not our primary focus in order to answer the research question. We saw, for instance, the time it took as less important than figuring out whether the participants navigated correctly.

For this study, three quantitative metrics were considered and described below:

Critical Error was measured to assess the factor effectiveness. A critical error leads to the task not being completed, or solved incorrectly. In our study a critical error was the user being unable to set up a passwordless authentication method correctly or unable to sign in with security key or fingerprint. By measuring critical errors as part of the effectiveness, we could identify major issues that must be addressed to improve the passwordless setup and sign-in process. Addressing these issues will help more users understand how to use passwordless authentication, and perhaps adopt it on a larger scale. If the participant successfully completes the task, there were zero critical errors, which was the optimal result for an acceptable service.

Non-Critical Error measured ease of use. A non-critical error did not prevent the participant from completing the task but resulted in solving the task less efficiently. Examples of non-critical errors in this research included clicking at incorrect page redirects, navigating in loops between the same pages, or clicking unnecessary buttons like “Cancel”.

Eye Movement measured ease of use. We measured eye movement as a metric to gain insights into participants’ reading patterns on the services’ websites. By understanding what participants read and what they skipped, we could assess the intuitiveness and effectiveness of the websites. Different types of eye movements provided indications of whether participants easily found relevant information or if they had to search around the page. We also considered the visibility of clear instructions for passwordless authentication and the presentation of important information to ensure participants were well-informed.

Together, these three quantitative metrics indicated the level of difficulty of the services’ websites, regarding navigation and information, which is a crucial point in adopting passwordless authentication [OGY+20; LSN+20].

Overview of Usability Factors, Metrics and Tools

Figure 4.3 summarizes our chosen usability factors and metrics. In addition, the figure illustrates a row with what we have named "Tools", such as flowcharts, observation schemes, think-aloud protocol, and interview. The flowcharts are used to asses critical and non-critical errors, and then also effectiveness and ease of use. Observation schemes are used for measuring eye movement and ease of use. To measure trustfulness and user satisfaction we employ follow-up interviews, while the think-aloud protocol is used to measure user satisfaction. These tools are used to measure our four factors and will be explained in more detail in Section 4.4.2, 4.4.3, 4.4.4, and 4.5.

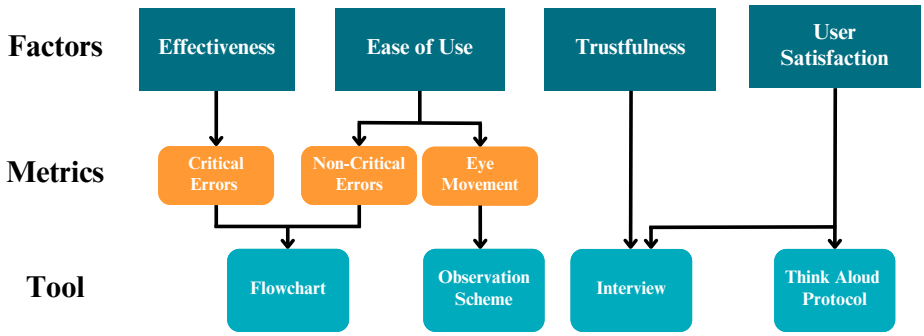


Figure 4.3: Relation between factors, metrics, and tools showing how we assess the usability factors and metrics through their respective tools used during the research study.

4.4 Usability Test

This section explains the usability test. Section 4.4.1 provides the task descriptions given to the participants in the usability test. Section 4.4.2 and 4.4.3 explain how flowcharts and observation schemes were utilized to collect data during the usability test. Lastly, Section 4.4.4 describes how the think-aloud protocol contributed to collect data while the participants solved the tasks.

4.4.1 Tasks

Four tasks were given to the participants and performed on both websites, Microsoft and eBay. Half of the participants started with Microsoft, and the other half started with eBay. We did this in order to study whether the results depended on the starting service. Participants were asked to perform the tasks given in Appendix A on artificial accounts created specifically for the study. We created a story to include some creativity and hopefully give motivation to solve the tasks. However, the tasks are provided in this section without the story:

> **Task 1:** Set up one passwordless method (i.e., security key or fingerprint) and then remove the password, *if possible*.
>
> **Task 2:** Sign in using the passwordless method you just registered.
>
> **Task 3:** Set up the other missing passwordless method you did not set up in the initial task.
>
> **Task 4:** Sign in using the second passwordless method you just registered.

To consider an example, Participant 1 (P1) started to perform the four tasks on Microsoft. Firstly, P1 registered fingerprint as the passwordless method in the first task and removed the password. Then P1 signed into Microsoft using the fingerprint just registered. In the third task, P1 registered the security key as the passwordless method, and in task four, P1 signed into Microsoft using the security key. After finishing all four tasks on Microsoft, P1 navigated on to eBay's website and performed the same four tasks. After finishing the four tasks on both Microsoft og eBay, P1 was done with all tasks for the usability test.

In the first task, the participant could choose between either setting up a security key or a fingerprint. This approach was intentionally designed to explore what they preferred to try first.

A passwordless account does not have any possibility to sign in with passwords because the password is removed completely and replaced with other passwordless authentication methods. Setting up a passwordless account is only possible on Microsoft, not eBay. The password can be removed and replaced with the Microsoft Authenticator app on Microsoft. On the other hand, eBay does not offer to remove the password, but the possibility to add other passwordless authentication methods in addition to the password. Therefore, when logging into eBay, the user can choose between using the password *or* the passwordless method to sign in. Furthermore, this explains the reason for having written *if possible* in the initial task.

The tasks were designed based on a study of each online service. Furthermore, the tasks included exactly the same processes a user would encounter when adopting passwordless authentication themselves, which means setting up a passwordless method and signing in with it. This created a realistic and relevant environment for the participants. However, it is worth noticing that the steps within each process may vary in some degree due to different user interfaces for each service.

4.4.2 Counting Errors With the Use of Flowcharts

A graphical overview of the steps in the tasks was created using flowcharts. Flowcharts were a valuable tool for collecting data in our usability test, as they provided a simple and visual way of illustrating each task's steps. This research employed the shapes and arrows illustrated in Figure 4.4 to design flowcharts. The start state describes the specific website where the task began, and the end state describes the goal of each task. Actions describe clicks or other activities in the process, and arrows indicate the direction of the process and the connection between actions.

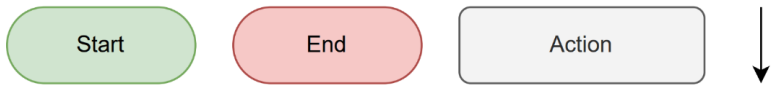


Figure 4.4: Overview of shapes and arrows used in the flowcharts for this study.

Flowcharts have been utilized in this study as a tool to analyze critical and non-critical errors in setting up FIDO2 and signing in with FIDO2 on Microsoft and eBay. Four flowcharts have been created, two for Microsoft and two for eBay. For each web service, one flowchart illustrates the steps to set up FIDO2, and the other demonstrates the steps to sign in using FIDO2. These are the two processes described in Chapter 1. As previously mentioned, the primary focus has been the setup and sign-in of the security key and fingerprint. Despite the online services offering other

passwordless authentication options, we only visualized the steps necessary for our primary focus. Each flowchart illustrates the most efficient path from start to end.

Figure 4.5 shows the flowchart illustrating the setup of FIDO2 on Microsoft. From the flowchart, we can see the necessary steps to remove password, register fingerprint, and register security key as passwordless authentication method. On the right-hand side of the flowchart, we can see a division into three defined milestones:

Milestone 1 consider the steps needed to locate security settings.

Milestone 2 is divided into two parts. *Part a)* illustrates the steps for finding where to set up the security key and fingerprint. *Part b)* demonstrates the steps for finding where to set up a passwordless account. When performing a task, the participant was free to choose between the order of the two parts.

Milestone 3 is also divided into two parts due to being a continuation of Milestone 2. If the participant starts with *Part 2a)*, then the participant continued on *Part 3a)*. Then the participant returned to *Part 2b)* and then continued on to *Part 3b)*. *Part a)* is to set up a security key and fingerprint correctly, and *Part b)* involves turning on passwordless account successfully, i.e. remove the password successfully. Both parts needed to be conducted to mark the task as successfully completed.

Figure 4.6 shows the flowchart illustrating the sign-in with FIDO2 on Microsoft. The flowchart shows the necessary steps to sign in with a fingerprint and security key. Additionally, milestones are added:

Milestone 4 illustrates the steps to find where to sign in with a security key and fingerprint.

Milestone 5 illustrates the steps to successfully sign into Microsoft's website with a security key and fingerprint.

The tasks were divided into milestones to understand where in the tasks obstacles occur. Furthermore, to identify the obstacles to FIDO2, it was helpful to have performed a detailed study of all steps to understand the functionality of FIDO2. In general, provided by both services, the user has to find security settings (*Milestone 1*), find where to set up passwordless authentication methods (*Milestone 2*), set them up correctly (*Milestone 3*), find where to sign in passwordless (*Milestone 4*) and sign in successfully with passwordless (*Milestone 5*).

The aim was to identify challenges or coherences in each milestone rather than examining every detail offered on Microsoft and eBay's websites. Specifically, the study aimed to explore whether the difficulties with transitioning from password-based authentication to passwordless authentication lie, for instance, in locating security settings or setting up a passwordless authentication method correctly.

The flowcharts illustrating eBay's setup and sign-in process are seen in Figure 4.7 and 4.8. Moreover, the flowcharts include the same milestones described for Microsoft; except no milestone for password removal due to eBay not offering this option today.

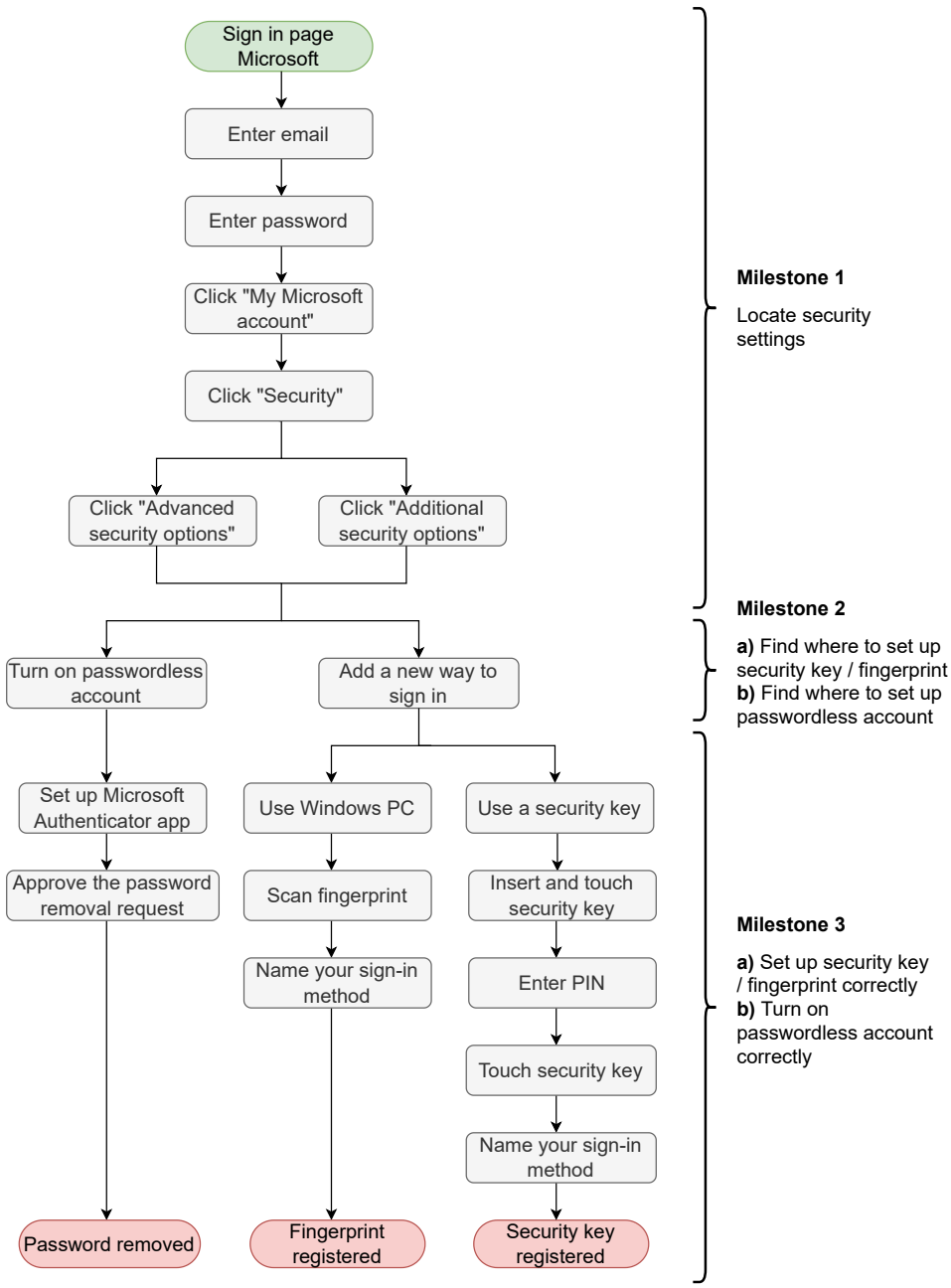


Figure 4.5: Flowchart illustrating the **setup** of security key and fingerprint, and password removal on **Microsoft**. The flowchart is separated into different milestones to study the path from start to end in more detail.

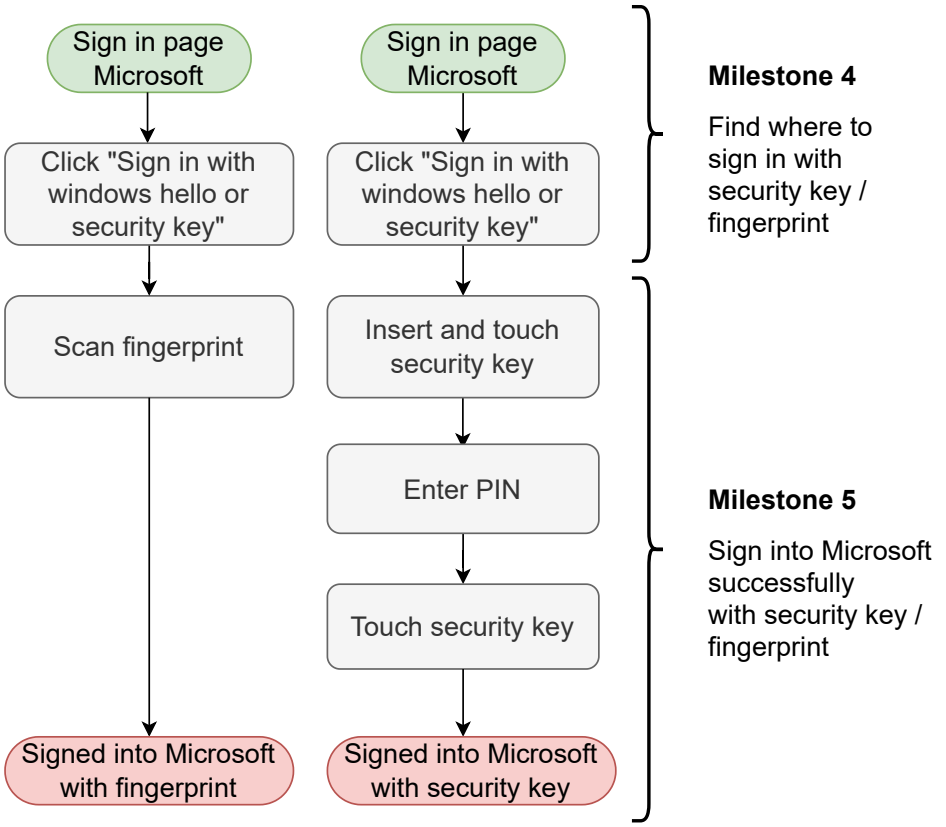


Figure 4.6: Flowchart illustrating the **sign-in** of security key and fingerprint on **Microsoft**. The flowchart is separated into different milestones to study the path from start to end in more detail.

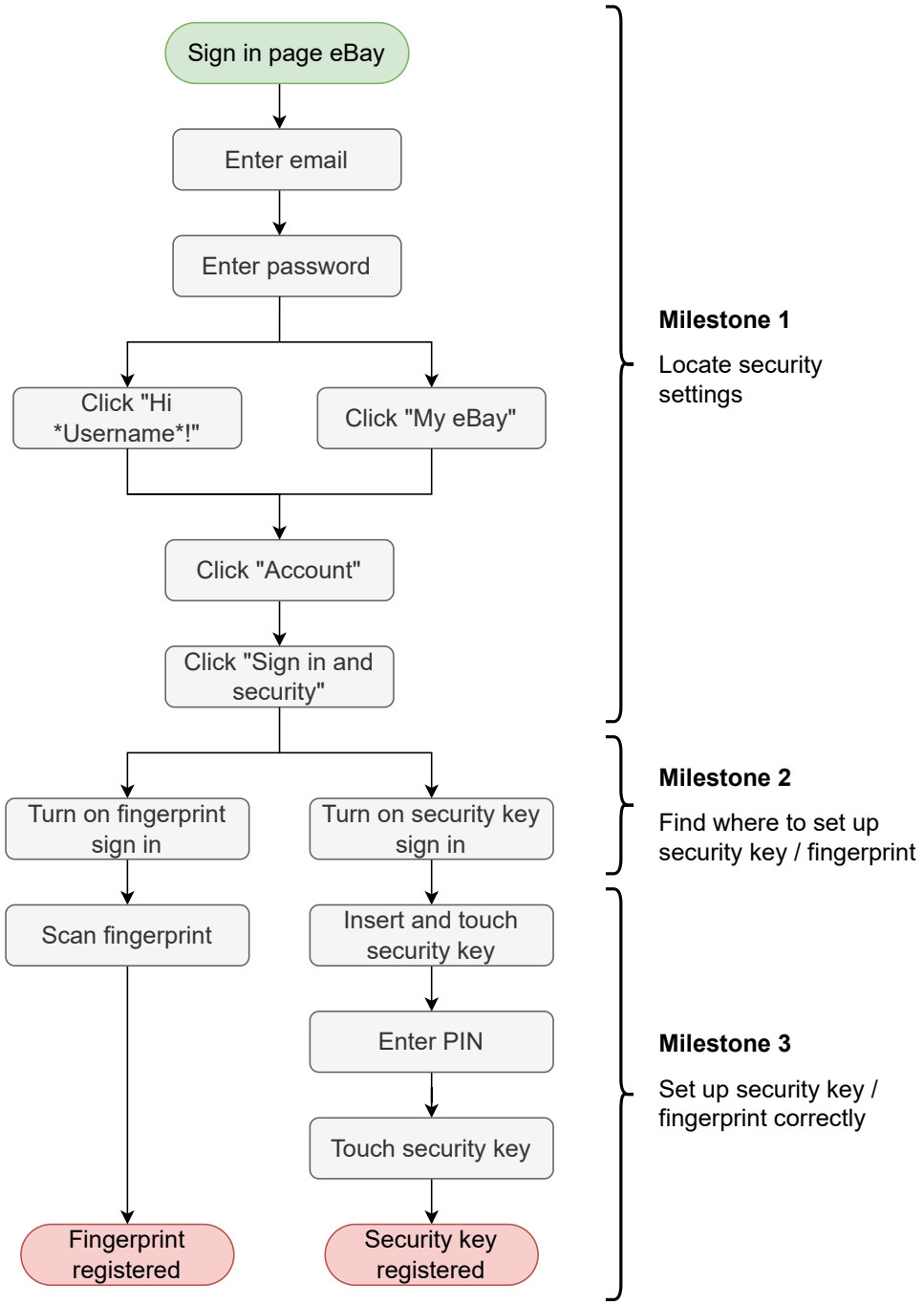


Figure 4.7: Flowchart illustrating the **setup** of security key and fingerprint on **eBay**. The flowchart is separated into different milestones to study the path from start to end in more detail.

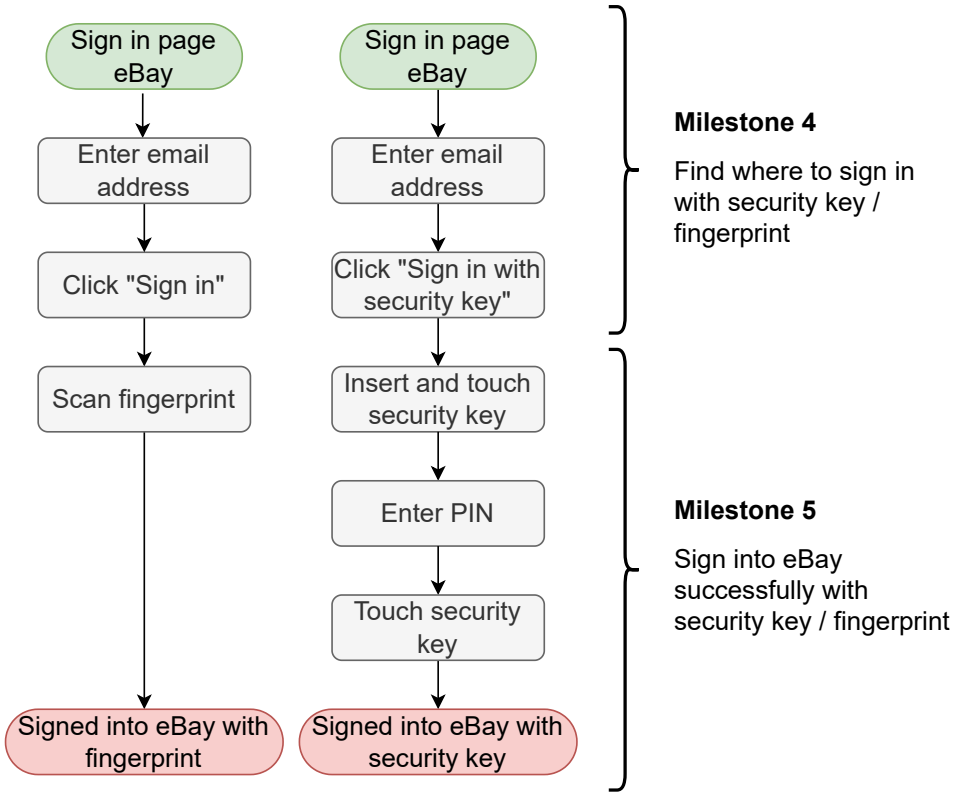


Figure 4.8: Flowchart illustrating the **sign-in** of security key and fingerprint on **eBay**. The flowchart is separated into different milestones to study the path from start to end in more detail.

Measurement of Errors in Practice

Participants had no access to the flowcharts. The flowcharts were printed out beforehand, so the observer had it visually in front. Since we were two observers, one of the observers sat to the right of the participant with the flowchart printed and followed the steps outlined in the flowcharts while the participants solved the tasks. The purpose of following the flowcharts as observers were to count the number of critical and non-critical errors during the tasks were solved for each participant. The number of errors was further used to address the quantitative results.

Critical errors described in Section 4.3.2, were found by observing the participant fail, give up, or solve the task incorrectly. We counted the total number of critical errors per participant for each task. This was done by marking a line next to the milestone on the Flowchart to gain insight into where the critical error occurred in the task. Successful task completion was also counted as a quantitative result.

The non-critical errors were also counted by marking a line next to the milestone when the participant performed an action that caused the task to be solved less efficiently. We summed up the total number of non-critical errors for each milestone per participant to understand the crossroads at which the non-critical errors occurred.

As observers, we consequently observed the participant's path choice and compared it to the flowchart. If the participant solved a task without errors, we checked milestones and tasks to be solved successfully. This way of observing and marking the errors, as described above, gave quantitative results. Studying errors as a metric gave insight into identifying where usability challenges, or at what milestones, occur for FIDO2 authentication.

4.4.3 Observing Eye-Movement

Observing eye movements can provide valuable insights into how people interact with web pages. There are several metrics that can be studied to find relations between eye movement patterns and usability problems [EW07]. Some examples of things that can be studied are scanning behavior versus reading behavior, long fixations, not looking at elements of the page, interaction like clicking at references in text and images. This can give insight into behavior, interests, and confusions [EW07]. Eye tracking technology is commonly used for this purpose and can be customized software and hardware used to visualize which part of the screen the user looked at and for how long. Because of limited resources in this project, manual eye observation was performed. However, there are some limitations related to manual eye movement observation, which will be discussed in Section 4.10.

Choosing the Specific Eye Movement behaviors

When measuring eye movements manually, it's important to have a clear observation scheme in place. This means defining what specific aspects of eye movements we would look for and how we would note them. In our case, we chose to focus on whether the eye was scanning the web page and searching for relevant areas to focus on (*Visual scanning*), if the eyes were reading something carefully (*Focused reading*), or if they did not read much, but only the headings and outlined text (*Heading attention*).

The three behaviors observed during the test:

Visual Scanning: This behavior refers to the participant's difficulty locating and focusing their gaze on the appropriate area of a website. Participants may face pages with multiple elements, such as menus, images, and text, which could make it difficult to determine where to look. Additionally, on some websites, the text may be too small, driving it challenging to identify the correct area to focus on or find the relevant content. As a result, the participant's gaze may shift frequently across the screen, and they might even move their head around to look at different parts of the page.

Heading Attention: This behavior is when the participant quickly processes outstanding, eye-catching text. This text is typically in larger fonts, bolded, or outlined. Participants may focus primarily on the headings and ignore other text on the page. This behavior is typically when the content is lengthy or complex, and the headings are sufficient to navigate the website or understand the content at a high level. The participants may skip smaller text that seems unimportant or redundant based on their understanding of the headings, which may lead to a less comprehensive understanding of the material.

Focused Reading: This behavior refers to reading all text, including the smaller text, in a careful manner. Participants may read the material in detail to understand better the content or explanations provided. This behavior is typical when the participant wants to obtain explicit information or when the smaller text provides the necessary context for understanding the headings. Participants who show high levels of focused reading may spend more time reading and may reread sections of the text to ensure comprehension.

We chose these behaviors to see whether the participant read specific instructions and information. For example, finding out if it would be crucial to read the benefits of passwordless accounts to understand why it is important or how to set up and use the authentication methods. We would then be able to see better if the interfaces are intuitive or if there is a need to read instructions carefully. Also, we were interested to see if it was easy to find the settings or if it was confusing with too much information and possible buttons to click on.

Measurement of Eye-Movement in Practice

To facilitate the study of eye movements, the second observer, not observing the flowcharts, sat directly across from the participant during the tasks. Further, a computer displayed the participant's screen, which allowed us to analyze the relationship between eye movement and specific task elements. By simultaneously observing clicks and eye movements, we could determine whether the participant was reading the information and instructions carefully or simply clicking through the pages quickly without reading.

An observation scheme was used to document the observations and can be found in Appendix B. The scheme identified which part of the task (milestone) the participant was doing, and check-off boxes to indicate which of the three eye behaviors they did throughout the milestone. We established clear categorizations for eye behavior during observation. When the eyes were flickering and moving around the screen quickly, this would be categorized as "Visual scanning." If the eyes paused at various spots on the screen for a brief period, we categorized it as "Heading attention." Finally, if the eyes stayed calm or did clear back-and-forth movements focused on a specific spot, we categorized it as "Focused reading." These three behaviors had clear and different eye movements and could be separated by the observer. This way of observing was also manageable to do manually and gave quantitative results.

4.4.4 Exploring Thoughts Through a Think-Aloud Protocol

During the usability test, the participants were instructed to *think-aloud*. This means verbalizing their thoughts while solving the tasks. Using the Think-aloud protocol during usability tests is common and recommended [Lew12]. It can provide valuable qualitative data that complements quantitative data collected during the test. By listening to everything the participants expressed, we gathered valuable information about their experience with passwordless authentication, including any problems they encountered with the use of the authentication technology. The think-aloud protocol was used to study the user satisfaction factor. Although comparing results

from different participants may pose a challenge due to the open-ended verbalization of thoughts, analyzing phrases they express could provide a valuable understanding of their experiences with passwordless authentication.

The usability test was voice recorded in order to document everything the participant said during the test. Analysis of this recording allowed us to focus on the participants' errors and eye movements while they were present, and what they said after they had left. The think-aloud protocol allowed us to understand better how users interacted with the authentication and identify areas for improvement. Moreover, the expressed phrases can be valuable when compared to the quantitative metrics we measure.

4.5 Follow-up Interview

The follow-up interview took place after the participants completed the tasks. The pre-created interview aimed to understand the participants' thoughts and experiences better. If anything was unclear after observing the participants and listening to their thoughts throughout the usability test, we could provide more questions we still wondered during the interview. We performed a semi-structured interview and used an interview guide when asking questions. In total, we had prepared 10 questions in the interview guide. However, the number of questions given to each participant varied based on their level of engagement, previous responses, and the details of their answers. This advantage of semi-structured interviews allowed us to achieve more in-depth answers by asking follow-up and additional questions and understanding the participants' thoughts better.

The questions focused on the participant's experiences with the setup and sign-in processes, their opinions on the two authentication methods, their perceptions of the security, and suggestions for improvement. In the beginning, we had big and open questions, letting the participant talk freely. Some other questions were more specific. Each question in the interview guide was related to one or several research factors defined in Section 4.3.1. The interview guide can be found in Appendix C.

The follow-up interview was also voice recorded, which was beneficial if we missed some valuable answers during the questions asked.

4.6 Participant Group

4.6.1 The Number of Participants

According to the graph in Figure 4.9, almost all usability problems are expected to be identified with 15 participants. However, Jakob Nielsen, a usability researcher and one of the developers of the graph, recommends using a smaller number of participants, around 5, for each usability test [Nie00]. This is because over 85% of the problems are likely to be discovered with this number, see Figure 4.9. Using only a few participants works especially well when usability tests are performed on a product. Then, the test can be repeated multiple times in an iterative process, where improvements based on the results from the previous test are corrected in the new version of the product [Nie00].

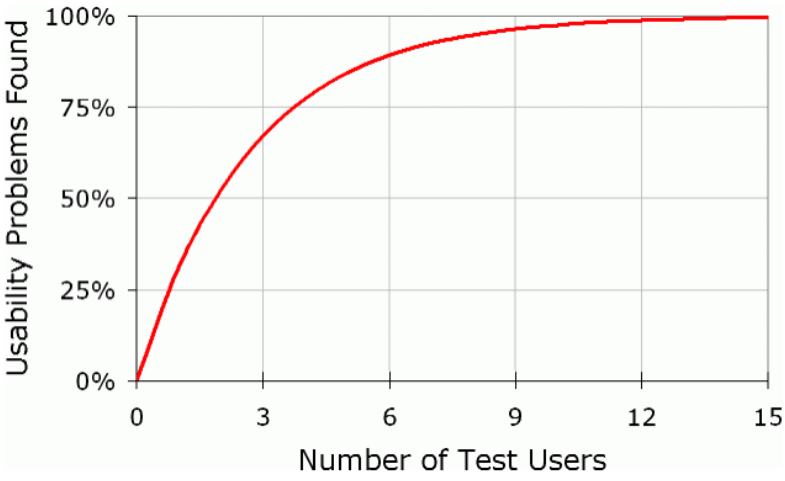


Figure 4.9: Graph from previous research showing the number of participants used in usability testing [Nie00].

However, as we only planned to run the usability test once, we decided to test more than five participants to identify as many problems as possible. The goal of the research was to understand which obstacles users find using FIDO's passwordless authentication method, and testing a larger number of participants could help us achieve this goal. Ten participants should identify around 95% of the problems, which is more than five participants would identify. However, choosing more than ten participants would not give any significantly better result than ten according to Figure 4.9. Therefore, we chose the usability test to be conducted on ten participants.

4.6.2 Demographics

Participants in a usability test should be chosen among potential end-users of FIDO's passwordless authentication methods. This group is big and diverse, and it would be optimal to test different groups of end-users who have different experiences and behave differently with technology [Nie00]. However, as the resources for this project were limited, we focused on only one type of end-users.

The participants for this usability test are aged 23-28, all Norwegian, and pursuing a master's degree in Communication Technology and Digital Security at the Norwegian University of Science and Technology (NTNU). As the participants are technology students interested in security, the participants have the potential to be the next adopters of FIDO's passwordless authentication. We will study whether this group of potential end-users finds passwordless authentication challenging or not, and if so, which obstacles hinder their adoption of it. The participants were recruited on campus through snowball sampling.

Both the term 'FIDO' and the security key are very likely unknown to the participants. However, everyone has used a biometric factor to unlock their phone or computer. The participant group was evenly split between women and men, with a 50/50 gender ratio. This ensures that the usability test results will reflect the experiences and feedback of both genders. However, it is important to highlight that our participant group was not representative of all end-users as the end-users are a diverse group [Lew12].

4.7 Ethical Considerations

During the usability test, ethical considerations were taken into account to ensure participant permission and data privacy. First, before starting the usability test, the participants were required to read and sign a consent form to indicate that they agreed with the study terms. The consent form has been validated by Sikt, "*The Norwegian Agency for Shared Services in Education and Research*" and can be found in Appendix D. Key aspects of the consent form were that both screen and voice recordings would be recorded during the test (no video recording of the participant). The purpose of the recordings was explained to the user; to document everything that the participant said during the test, and associate it to the correct task they performed.

Furthermore, another important aspect of the consent form was related to fingerprint authentication. In order to use fingerprint as authentication, their fingerprint had to be configured on the computer used for the test. The consent form also highlighted that participants had the freedom to stop the test or disagree with the terms at any time. In such cases, all information related to the participant would be deleted immediately, to respect their privacy.

Before the participants left the test room, they were able to observe the deletion of their fingerprint from the computer, ensuring their biometric data was removed. Once the participant left, the sound and screen recording was processed and then deleted in order to store personal information as short as possible.

We wanted to provide participants with understandable information about all aspects of the study, ensuring transparency and clarity. We described all data collected, the reasons behind the data collection, and when the data was going to be deleted. Additionally, we ensured that participants understood the purpose of the test.

4.8 Test Environment

This section provides information on how the test was performed, the setup of software and hardware in order to execute the test tasks, in addition to an overview of the test room.

4.8.1 Test Procedure

The participants received detailed information about the usability test and follow-up interview procedures shown in Appendix E. The functionality and use of the two passwordless authentication methods, fingerprint and security key, were explained in detail, such as where the fingerprint sensor was located, how the security key should be inserted and touched, etc. The intention was *not* to let participants figure out by themselves how the passwordless methods functioned. Next, the participant was given one task at a time, with the following task provided after finishing the previous one. This procedure aimed to keep the participant's attention on a single task. The tasks were presented on a sheet of paper. Participants were instructed to indicate when they assumed they had completed the task or if they wanted to give up. Throughout the tasks, we did not interrupt or influence the participants, and the participants were not allowed to receive help. Finally, after the usability test, participants were asked the follow-up questions.

4.8.2 Test Environment Software

Selecting Online Services for the Test

To evaluate the user experience of FIDO2 authentication, two real online services implementing this functionality were used. The choice of services was based on specific requirements:

1. Widely known services: The selected services needed to be popular and widely recognized to ensure participants could relate to and realistically use them.
2. Single-factor authentication with a FIDO2 passwordless method: To eliminate the use of passwords during the test, services offering passwordless single-factor authentication were selected.
3. Multiple services for comparison: Including more than one service allowed for comparing results across different services.

While selecting services for the usability test, we started by reviewing the possible options of services offering FIDO2 single-factor authentication, as presented in Section 3.2.2. At the time of selection, only two services, namely eBay and Microsoft, provided passwordless single-factor authentication and were recognized and known among many people. For clarification, Google introduced their FIDO2 SFA feature on May 3, 2023, after the usability tests were completed [Goo23a]. In addition, we encountered a few non-Norwegian banks that offered passwordless single-factor authentication. However, they were not chosen due to practical constraints and the inability to test these services. Both eBay and Microsoft met all the requirements, which qualified them as the most suitable for the usability test.

In advance of the test, an artificial account was created at both services, ready to be used during the usability test.

Additional Software

Additional software was necessary to conduct the usability test. It was necessary to have a browser and platform that supported WebAuthn, along with an external authenticator, such as a security key. We utilized a Google Chrome browser on a macOS Catalina platform. The video conferencing platform, Zoom, was used to record sound and the screen. Zoom is a widely used program that NTNU has relied upon during the pandemic, and is therefore considered a safe software program by the institution.

4.8.3 Hardware Components

The user experience of FIDO2 authentication can be explored on several devices as long as the device supports biometric sensors and roaming authenticators, as we planned to test both of these authentication methods. However, to compare the results easier, all participants performed the test on the same device. In addition, to avoid complicating our observation, the test was only performed on desktop operating systems rather than tablets or smartphones due to the small screen size. Previous research have studied FIDO2 on smartphones [OAKU21; WPHH23]. We selected a MacBook Pro with a fingerprint sensor as the computer for this research because it was our only compatible option for testing both FIDO2 authentication methods.

In addition, a security key was used in the usability test as it is a common FIDO2 authenticator. A YubiKey 5Ci was used as the security key because it was compatible with the Mac's input ports. The final hardware component was an iPhone XR displaying the Microsoft Authenticator app.

4.8.4 Overview of the Test Room

The test room was equipped with a large table and three chairs: one for the participant and two for us as observers. One of us sat directly opposite the participant, with a screen displaying the participant's computer screen and observing the eye movement behaviors. The other observer sat beside the participant, focusing on counting the number of errors during the tasks. This seating arrangement was designed to ensure that both of us had a clear view of the screen and could closely track the progress of each participant.

Figure 4.10 shows an illustration of how it looked when we conducted the usability test and follow-up interview. As Figure 4.10 described, the participants had three sheets of paper in front of them during the usability test. One sheet of paper provided pictures of the security key and how to use it. In other words, pictures describing how to insert, touch, and release the security key. The second sheet of paper contained all the necessary credentials for the pre-created artificial accounts. The credentials were usernames, passwords, and PIN codes. The last sheet of paper provided the task descriptions, where the participant could only see one task at a time.

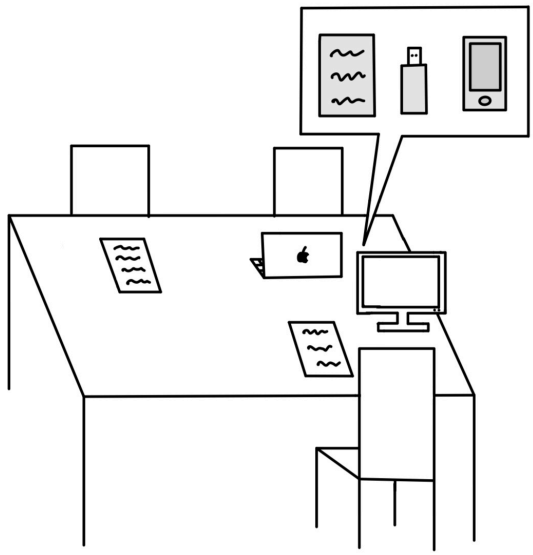


Figure 4.10: Illustration showing the test room. Two observers with each their sheets of paper, one positioned in front of a screen, while the other alongside the participant. The participant was placed in front of the laptop with three sheets of paper, security key, and phone.

4.9 Pilot Testing

It is recommended to run pilot tests before carrying out a usability test [Lew12]. A pilot test involves running a test that simulates the actual usability test to discover weaknesses in the methodology and ensure the design meets our requirements. Areas that can be evaluated include whether sufficient time has been allocated for each test, whether the task description is clear, and whether the metrics being observed are interesting and observed equally by the observers. Pilot testing should be continued until the test design of the usability test has become stable [Lew12].

We ran eight pilot tests with representative test-participants who shared the same demographics as the ten participants in the actual usability test. They completed the usability test and the follow-up interview. However, we made improvements based on observations and their feedback. Each pilot test was reviewed to identify areas needing improvement, such as when participants did something unintended or required adjusted instructions. Some of our improvements were as follows:

Clarifying Terminology Initially, we asked participants if they were familiar with passwordless authentication without specifying that we meant FIDO2, which is for online service authentication. As a result, we received affirmative responses related to device unlocking rather than online services. To address this misunderstanding, we clarified the context in all questions by explicitly mentioning *passwordless authentication on online services*.

Flowchart Design: An Iterative Improvement Initially, the flowcharts were created in great detail, covering every possible step in the processes of setup and sign-in, such as timeouts and further loops. However, this resulted in overly complicated, user-unfriendly flowcharts to follow for us during the usability test.

Therefore, we revised the flowcharts to be less detailed, focusing only on the essential steps of the processes, which we defined as milestones. The pilot testing helped to simplify the flowcharts for better user comprehension. Nevertheless, starting with detailed flowcharts for each service provided a clear understanding of each service, which we found to be useful and important to be able to follow the participants executing the tasks.

Strengthening Observer Roles Practicing the role of observers significantly enhanced our ability to carry out our tasks effectively. Initially, as two observers, we faced challenges in defining our roles. However, through practice, we clarified responsibilities and how to document our findings and communicate with the participants. Running the pilot tests enabled us to approach the usability test with a clear focus, knowing precisely what actions to take, what to say, and what to observe.

Enhancing Question Precision The first pilot tests indicated that the follow-up questions were not precise and needed improvement. We understood this due to repetitions in the answers and participants not answering the intended queries. As a result, the follow-up interview questions were revised several times to ensure clarity and avoid repetition.

4.10 Limitations

The limitations related to our study are mainly seen in the context of the research method performed. We have defined three main limitations: *small and homogeneous participant group*, *manual eye tracking* and *bias in interview responses*.

Participant Group

We recruited ten participants for the usability test and follow-up interview, which is an acceptable sample size within usability testing. However, it is important to note that due to the small number of participants, each individual has a significant influence on the results presented in this thesis.

Another limitation we acknowledge is the homogeneity of the participant group. The participants not only share similar age, educational, and knowledge backgrounds but also happen to be our friends as they are enrolled in the same study program. This homogeneity may limit the diversity of perspectives and experiences. Despite the limitations, we got valuable insights and observed both similarities and differences in participants' user experience of FIDO2 on online services.

Manual Eye Tracking

Typically, eye movements are tracked using specialized combined software and hardware equipment. This was not available for us, so we performed manual eye tracking, which has its limitations. However, we have tried our best to be as objective as possible when performing eye tracking. We categorized different types of eye movements to guide our observations and followed a pre-created observation scheme with these categorizations to ensure all participants' eye movements were equally evaluated.

Bias in Interview Responses

During the interviews, there is a possibility that participants' responses were influenced by biases. Due to their awareness that the project was a master's thesis, they may have been influenced to believe that passwordless authentication is superior to traditional password-based authentication. We focused on providing an objective introduction to mitigate this. Also, questions asked in the interview were carefully designed and tested in pilot tests to prevent any potential influence on the participants' responses.

Chapter 5
Results

This chapter presents the findings obtained from the usability test, with the follow-up interview conducted immediately afterward. The findings mainly focus on user experience related to the setup and sign-in processes using FIDO2. The usability test and the interviews complement each other, and by triangulation, we overcome weaknesses in using one method with the strengths of the other.

Section 5.1.1 and 5.1.2 present the numbers of non-critical and critical errors identified while participants completed the tasks associated with each milestone of the passwordless authentication setup and sign-in. The tasks and the milestones for both Microsoft's and eBay's setup and sign-in process were presented in the flowcharts in Section 4.4.2. We identified obstacles encountered during the setup and sign-in process by analyzing where the errors most frequently occurred. We also present the participants' eye movement behaviors observed in Section 5.1.3 while they were performing the tasks. We gained insight into what the participants searched for, read, and ignored. When relevant, we also present the simultaneous think-aloud protocol results that in some cases, deepened our understanding of our observations. Microsoft and eBay provided different user interfaces for the transition from password-based to passwordless authentication, and the analysis of error and eye movement revealed obstacles from a user experience perspective.

Section 5.2 presents findings from the follow-up interview. These findings are organized into four topics: experiences of passwordless authentication setup and sign-in in Section 5.2.1, awareness of passwordless authentication in Section 5.2.2, users' perceptions of passwordless authentication in Section 5.2.3, and future adoption of passwordless authentication in Section 5.2.4. The qualitative data collected through the think-aloud protocol supplements the interview answers where relevant.

5.1 Usability Test Findings

This section presents observations observed during the usability test where the ten participants sat up passwordless authentication, namely security key and fingerprint, at eBay and Microsoft, and later signed in. The participants started with either Microsoft (group A) or eBay (group B) and they selected themselves whether to set up fingerprint or security key first.

The non-critical and critical errors were identified through pre-created flowcharts and eye movement observations through pre-created observation schemes. This section proceeds in a chronological order that aligns with the sequence of milestones.

5.1.1 Identified Critical Errors

Our results revealed no critical errors, as all participants successfully completed the tasks without giving up or solving them incorrectly. We measured the critical error rate in either success or unsuccess regarding if they managed to complete all tasks or not. In other words, the success rate was ten out of ten since all participants managed all tasks. From now on, we only presents non-critical errors.

5.1.2 Identified Non-critical Errors

Non-critical errors were identified among all participants, indicating that all participants faced some degree of difficulty and did not choose the most efficient path. In order to identify the non-critical errors, results related to each milestone described in Section 4.4.2 will be presented. The amounts of non-critical errors were mostly found in locating the correct security settings and setting up the passwordless authentication method correctly the first time, especially the security key.

Milestone 1: Locate Security Settings

To study the results found in milestone 1, Table 5.1 and Table 5.2 summarizes the number of non-critical errors per participant on Microsoft and eBay. The tables reveal that participants made more non-critical errors on Microsoft than on eBay. It is important to note that Group A completed the tasks on Microsoft first, while Group B completed the tasks on eBay first. However, we can see their starting point did not influence, Microsoft was still the webpage with the most non-critical

errors. There were not many non-critical errors, but the errors still proved a degree of difficulty at Microsoft due to non-critical errors indicating unnecessary steps.

Table 5.1: Number of non-critical errors per participant on Microsoft when locating security settings.

Microsoft									
Find security settings									
Group A					Group B				
P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
7	2	2	3	3	0	0	2	1	0

Table 5.2: Number of non-critical errors per participant on eBay when locating security settings.

eBay									
Find security settings									
Group A					Group B				
P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
0	0	0	0	1	0	0	0	0	0

The most common non-critical error in locating security settings was clicking "change password." However, this option only allowed the participant to create a new password and had nothing to do with passwordless authentication. After clicking this option, the participants quickly expressed through the think-aloud protocol that this was not what the task asked about, and thereby returned and tried another way. One participant created a new password and expressed confidence in creating a new one before having the opportunity to go passwordless. Regardless of which service, in total, there were seven out of ten participants who tried clicking the "change password" option. Yet, this happened the most on Microsoft.

Milestone 2 and 3: Remove Password from Account

All participants successfully removed their password and replaced it with the Microsoft Authenticator app. We observed the process of removing the password on Microsoft was experienced as straightforward and easy to follow the given instructions.

Figure 5.1 illustrates the interface for where to remove the password. A user must click "Turn on" passwordless account, marked with a red circle, to remove the password and replace it with the app. Furthermore, below "Turn on," Microsoft provides a link for additional help where the users can learn more about removing

their password. There were a few participants who entered this link and expressed the need to understand the procedure of removing password.

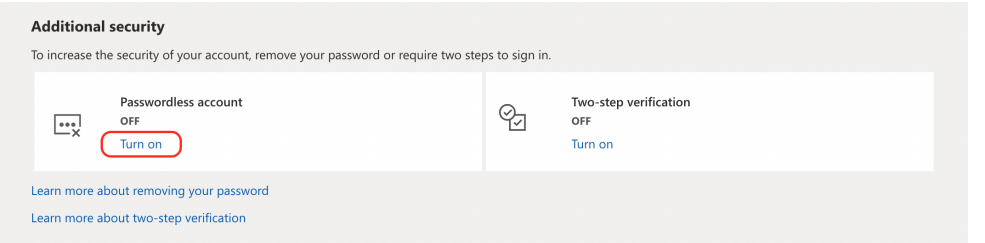


Figure 5.1: Snapshot from Microsoft's security settings interface showing where to remove the password and set up a passwordless account instead.

Milestone 2 and 3: Set Up Passwordless Authentication Methods

The following titles in italics format provide findings for the general setup process, both finding where to set up a passwordless method and setting it up correctly. We provide findings where results on Microsoft and eBay are separated, the order of tested services varies, and differences in setup of the security key and fingerprint.

Studying Microsoft and eBay Separately

The bar charts in Figure 5.2 and Figure 5.3 summarizes the average number of non-critical errors per participant for the setup process on both Microsoft and eBay. These averages are not based on which service the participant started with or which passwordless authentication method they chose first. "Method 1" from the bar chart describes the first chosen method in the tasks, whether a security key or fingerprint, and "Method 2" is the passwordless method not chosen initially. Furthermore, finding where to set up the method was described as one milestone, and setting it up correctly was another milestone, which is the reasoning for the descriptions and division on the x-axis. The purpose of these bar charts is to illustrate the differences in non-critical errors for the two services during the setup process.

For both Microsoft and eBay, we observed a decrease in the average number of non-critical errors in finding where to set up the first method and where to set up the second one. However, eBay had a significantly lower error rate compared to Microsoft. Moreover, we observed an increase in the average number of non-critical errors from setting up the first method correctly to setting up the second method correctly on both services.

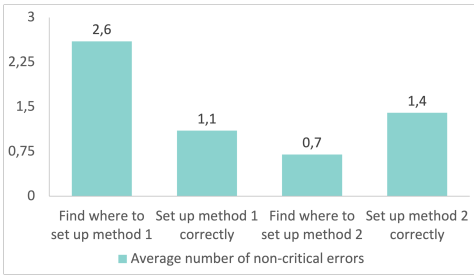


Figure 5.2: Identified non-critical errors during **setup** tasks on **Microsoft**.

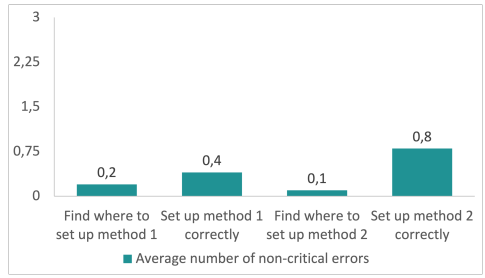


Figure 5.3: Identified non-critical errors during **setup** tasks on **eBay**.

Order of Tested Services

Figure 5.4 presents the average number of non-critical errors per participant on the first service tested during the usability test without distinguishing between Microsoft and eBay. Moreover, the bar chart does not consider the order of chosen authentication methods. The reason for not organizing the results based on Microsoft and eBay, like above, but rather on the first and second services tested by the participants, was to determine if there was a difference in non-critical errors between first and second service. This approach allowed us to focus more on the general patterns of non-critical errors between two arbitrary services, making the study less specific to Microsoft and eBay and more relevant in a broader context. Figure 5.5 presents similar results but for the second service tested instead.

The figures illustrate a decrease from finding where to set up the first method to set up the second one. Similarly, an increase in setting the two methods up correctly. The second online service tested has a smaller average number of non-critical errors than the first one tested for the usability test.

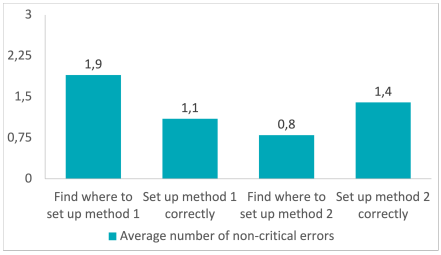


Figure 5.4: Identified non-critical errors during the setup tasks on **first service**.

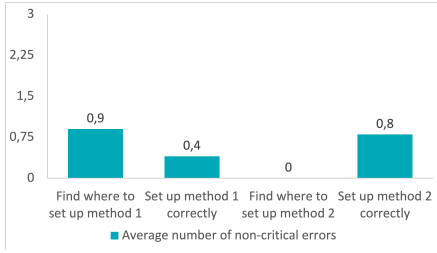


Figure 5.5: Identified non-critical errors during the setup tasks on **second service**.

Differences in Errors for the Security Key and Fingerprint

Table 5.3 presents the total number of non-critical errors for setting up the security key and the fingerprint correctly on Microsoft and eBay, respectively. The numbers are based on total number of non-critical errors for all participants. The results revealed more errors for the correct setup of the security key than the fingerprint, regardless of the service. However, the table shows more non-critical errors for the passwordless authentication methods on Microsoft than eBay.

Table 5.3: Number of non-critical errors for security key and fingerprint setup on Microsoft and eBay.

Service	**Number of Non-Critical Errors**	
	Security Key	**Fingerprint**
Microsoft	18	7
eBay	10	2

Regarding the setup of the security key, the most common non-critical error was related to the physical device's use, specifically when to insert the security key, when to touch it, and how to touch it. On the other hand, for setting up the fingerprint, non-critical errors were related to participants misunderstanding the fingerprint icon. We observed some participants attempted to scan their fingerprint whenever they saw a fingerprint icon, whereas the service required users to click a "continue" button before scanning their fingerprints. Similar to the security key, participants inserted the key before clicking "continue".

Milestone 4 and 5: Sign In with Passwordless Authentication Method

The interface displayed in Figure 5.6 demonstrates how users can sign into Microsoft. Users can sign in using a passwordless authentication method by clicking "Sign in with Windows Hello or a security key which is illustrated with a red circle." However, nine out of ten participants unnecessarily entered their email and clicked "next" instead of selecting the passwordless option directly, which was a common non-critical error among the participants signing into Microsoft.

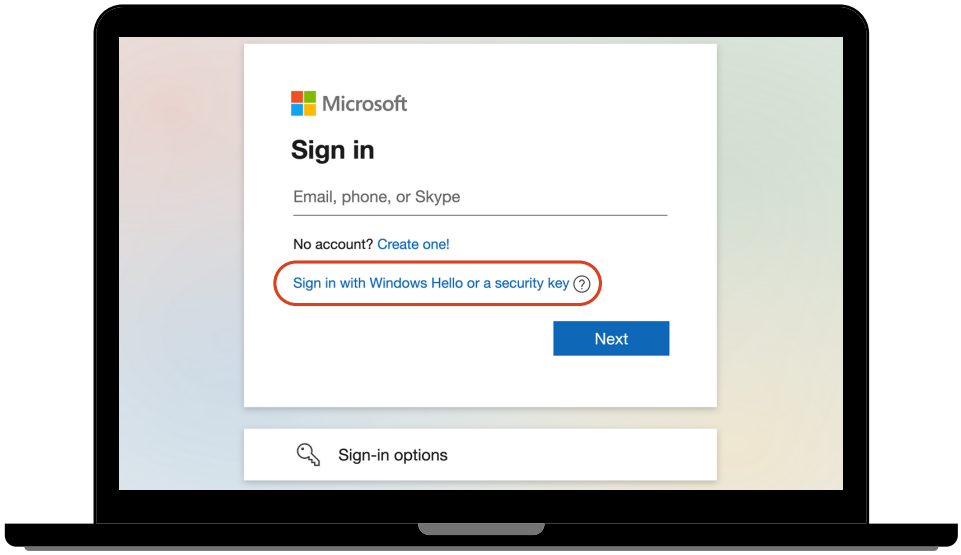


Figure 5.6: Interface for signing into **Microsoft**. We can see both email sign-in and passwordless sign-in marked with a red circle.

Figure 5.7 eBay's sign-in interface. In contrast to Microsoft, eBay requires users to enter their email before signing in with a passwordless authentication method. All participants managed to find where to sign in passwordless by entering their email and clicking "next" without any doubts. After clicking "next", the passwordless method sat up was shown as the default method to sign in with.

"I liked that after registering my fingerprint on eBay, it understood I wanted to sign in with it, so it was the default login method even though it was possible to sign in using the password." -P8

Figure 5.8 and Figure 5.9 summarizes the average number of non-critical errors per participant for signing in to Microsoft and eBay, respectively. The bar charts

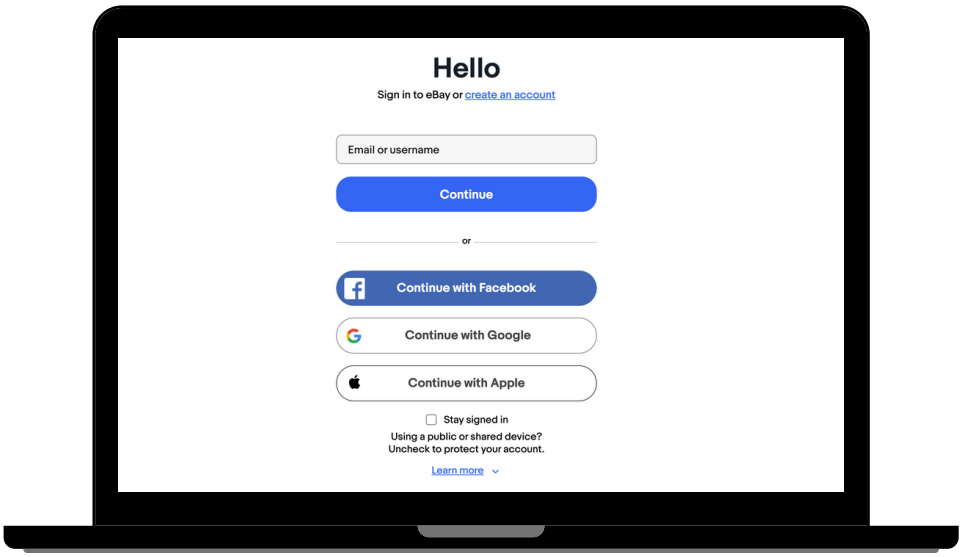


Figure 5.7: Interface for signing into **eBay**. We do not see any possibilities for directly passwordless sign-in.

show significantly fewer errors in the sign-in process compared to setting up the passwordless account on Microsoft and eBay, described in Section 5.1.2. The sign-in process on Microsoft showed a decrease in non-critical errors from finding where to sign in and to sign in successfully. Also, the result shows that the second time finding where to sign in and actually signing in was performed with fewer errors. However, eBay had a lower non-critical error rate throughout the sign-in process among the participants.

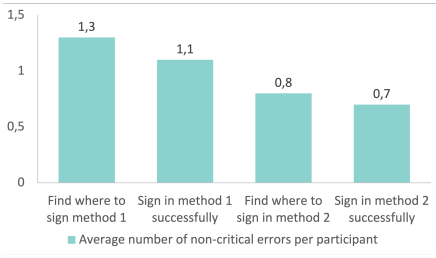


Figure 5.8: Identified non-critical errors during **sign-in** tasks on **Microsoft**.

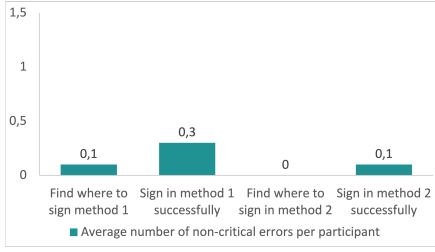


Figure 5.9: Identified non-critical errors during **sign-in** tasks on **eBay**.

5.1.3 Analyzing Eye Movements

Observing the eye movement behavior during the usability test gave insight into where the participants read written text and how they interacted with the user interfaces. Also, we got a better insight into how intuitive the user interfaces were. The observations focused on eye movement behaviors such as *visual scanning*, *heading attention*, and *focused reading*, explained in Section 4.4.3. The results are presented in an order that aligns with the sequence of milestones, looking into the eye movement behaviors encountered at each stage.

Locating Security Settings

Figure 5.10 shows the different eye behaviors we observed during locating security settings. Most participants did a *visual scanning* behavior, searching for a suitable area to focus on while locating the settings. Only a few could locate the settings solely by looking at headings. There were multiple buttons, text, menus, and figures to look at on both services' home pages. This resulted in eyes, and even the head at some participants, moving back and forth on the page. After they had found a place to fix their eyes, several participants continued to read more carefully. We could see from the eye behaviors that locating the settings was slightly more complicated on eBay than on Microsoft. This was confirmed by the think-aloud protocol, where several participants expressed their confusion about eBay having their account menu on the opposite side of the page than what they were used to.

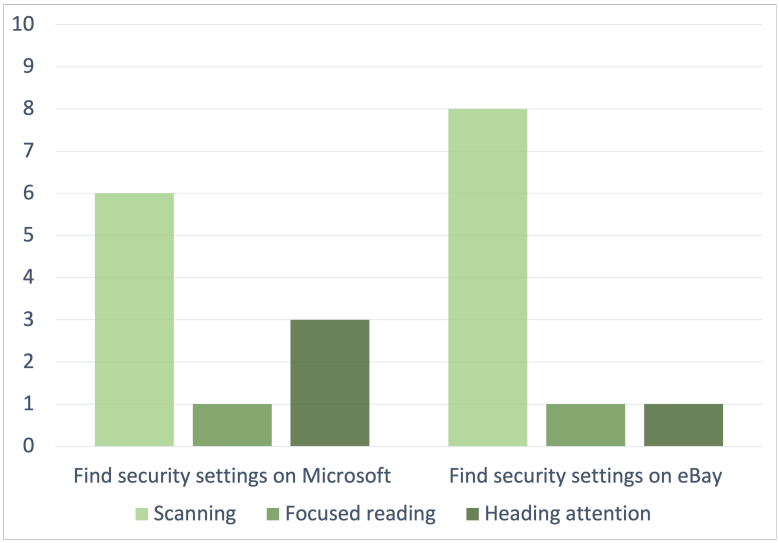


Figure 5.10: Eye behavior (scanning, focused reading, or heading attention) observations while locating the security settings. The y-axis represents the number of participants, and the x-axis represents each behavior for each milestone.

Removing the Password

When setting up the passwordless account at Microsoft, users could easily find where to turn it on by only reading headings after locating the correct security settings page. After clicking "Turn on," see Figure 5.1, the turn-on process involved several pop-ups, and a few users read carefully to ensure they got all the important steps and information. However, the tendency was the more pop-ups they saw, the less carefully they read, and the majority skipped reading and just clicked "Next" on these pop-ups. The information on these pop-ups was related to the advantages of a passwordless account and how to replace the password with the Microsoft Authenticator App.

Finding the Location to Set Up Fingerprint and Security Key

At the security settings, the participants had to locate where on the page to configure the fingerprint and security key. This process involved mostly focused reading, see Figure 5.11. Through the think-aloud protocol, the participants said they did not know what they were looking for; hence they had to read. On Microsoft, we observed that many participants did not know where to start reading as they scrolled up and down with their eyes in the beginning. The security page differed a lot between the two services. The two main differences were 1) the word choices: eBay uses

"Fingerprint," while Microsoft uses "Windows Hello," and 2) eBay has all security settings on one page, while on Microsoft, the user has to click on "add a new way to sign in" before they could see the authentication options. However, after finding the first option of either a security key or fingerprint, finding the second option did not need much more effort than heading attention as they were placed close to each other.

Figure 5.11 shows the eye behavior observed while locating the exact settings on the security page to set up passwordless authentication methods. The bar chart is based on finding where to set up "method 1," and "method 2," on the first and second service, without knowing which service was tested first.

This result does not focus on a specific service's interface but rather on finding out whether it becomes easier to locate the setup location after doing it on a previous service. The findings gave an interesting result, revealing that locating the security settings was not easier on the second service. In fact, it proved to be more challenging, requiring extensive eye searching to identify the correct area for reading and locating the setup location. This can be seen in Figure 5.11 in the third stage, where most participants had to scan visually and got confused, whereas this was not needed that much the first time, in stage one.

Setting up Security Key and Fingerprint

During the setup of the two authentication methods, the participants were split into two groups regarding their eye behavior. One group read carefully to understand how to configure them correctly, while the other only read headings and outlined text. Previous findings revealed that participants tended to read less when facing plenty of pop-ups, which was confirmed. Setting up both authentication methods contained several steps and pop-ups, especially the security key, and participants focused more on illustrations than reading the text. Setting up fingerprint was mainly accomplished by heading attention, except some people needed focused reading to understand exactly when to touch the fingerprint sensor. Figure 5.12 is an example of ignored text while setting up the security key. A pop-up with important information regarding the need to touch the key was written at the end of the second line. This information was positioned so that only a few participants read it. Some participants expressed through think-aloud that they did not read the pop-up initially. Instead, they mistakenly believed that the service was processing the key and that they simply had to wait. After waiting, they eventually realized the need to read the message and understood that they had to physically touch the key.

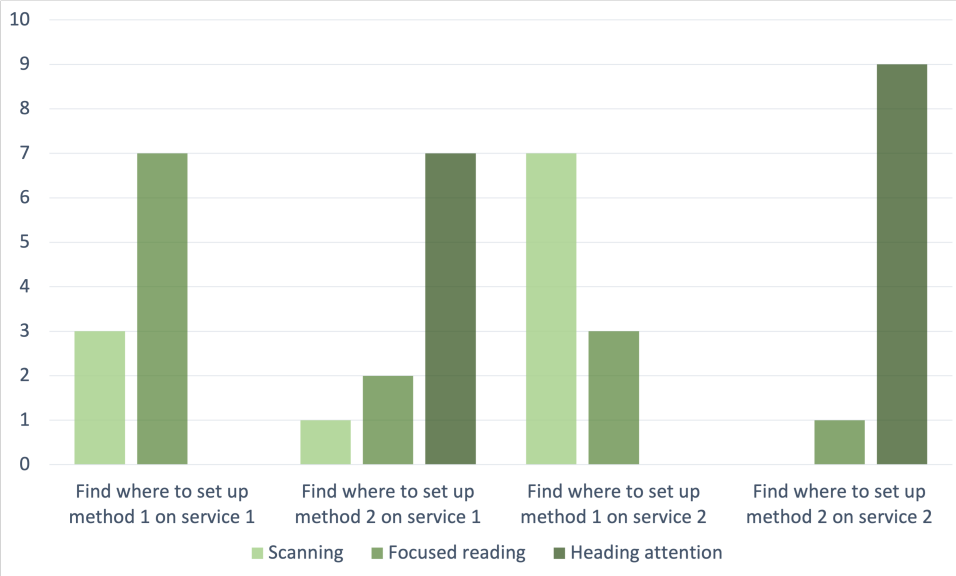


Figure 5.11: Eye behavior (scanning, focused reading or heading attention) observations while locating where to set up passwordless authentication methods. The y-axis represents the number of participants, and the x-axis represents each behaviour for each milestone, described as stages in the text.

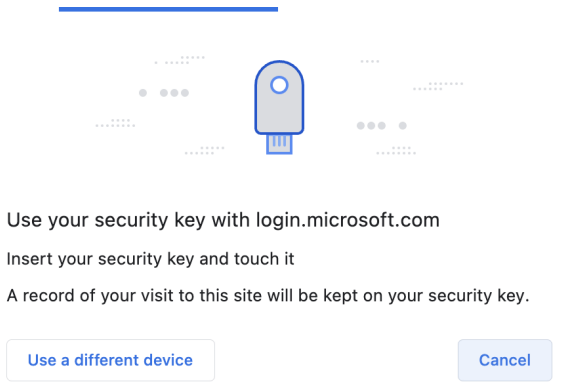


Figure 5.12: Interface showing the instructions when setting up the security key. The instructions guide the user to insert the security key and touch it, and there is a loading blue bar at the top of the figure.

"I did not read I should touch the key, so I waited for a long time until I finally started to read the instructions." -P2

Signing In

Finally, signing in passwordless was a straightforward task at eBay, as all participants could complete the task with only heading attention. The headings and outlined text were enough to guide them correctly. In contrast, the sign-in process at Microsoft involved more text, with only one outlined heading stating "Sign in," see Figure 5.13. Some users read the smaller text carefully to locate passwordless sign-in, while others did not read and missed the passwordless sign-in option before they understood they had clicked wrong. Another result was that the steps of signing in with a passwordless method were exactly the same as configuring it, resulting in participants remembering the pop-ups and not needing to read them again.

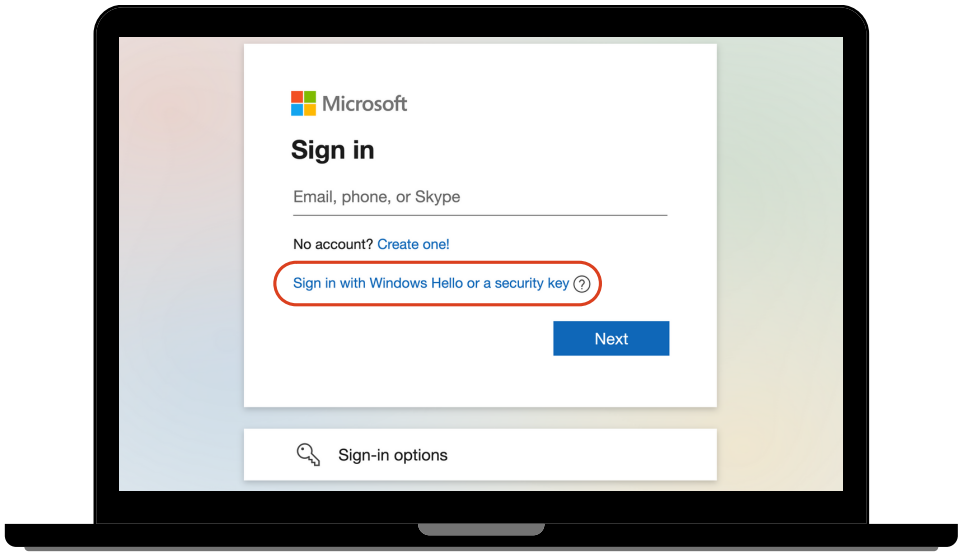


Figure 5.13: Interface for signing into Microsoft.

Observations Unrelated to the Milestones

In general, the participants read more on Microsoft than on eBay, regardless of whether they visited Microsoft first or not. There were also more text and options on all webpages at Microsoft. It is also important to mention that some participants tended not to read anything carefully throughout the test, only focusing on headings and outlined text. On the other hand, other participants tended to read everything very carefully and focused. One tendency was to read carefully at the beginning of

each task, but after a while ended up only reading headings and skipping text in small text size before they completed the task. In other words, they changed eye behavior while solving a task. The other tendency was to begin not reading much, but after a while, not finding what they looked after, they had to read everything more carefully. If the participant changed behavior during the task, the first eye behavior they did was selected in the observation scheme. This influences the results and graphs and was the reason for our focus on tendencies rather than the exact number of participants that did scanning, focused reading, or heading attention at each task.

The eye-tracking data revealed various challenges met by participants while setting up and signing in with different authentication methods, highlighting areas for improvement in both services. The two main challenges observed through the eye movement observations were locating the security settings page and locating where on that page to set up passwordless authentication methods, especially on the second service. Also, a main finding was that many participants skipped reading all the text provided on the websites, even though it could be important information they skipped. All over, the participants had a tendency to read less further throughout the task description. For example, we could see on both services, that the last time they signed in, they knew where to click, and there was no need to read carefully.

5.2 Follow-up Interview Findings

This section presents the participants' answers during the follow-up interview. The semi-structured approach of the interview allowed for variations in the specific questions asked, while ensuring that all participants were addressed on the same thematic areas of queries. The structure of this section is divided into four themes aiming to provide a systematic presentation of the participants' answers. First, Section 5.2.1 presents experiences and thoughts on the usability of the two authentication methods and the interface for setup and sign-in. Then, Section 5.2.2 provides participants' awareness of passwordless authentication. Section 5.2.3 summarize participants' responses regarding their perception of security and trust. And finally, Section 5.2.4 presents participants' considerations and perspectives on the future adoption of FIDO2 authentication on desktop platforms.

5.2.1 Experiences Related to Usability and the Interface

Most of the participants expressed satisfaction with solving the tasks and enjoyed the opportunity to try something new. Multiple participants found the beginning of the usability test more challenging because it was complicated to locate the security settings and find where to set up a new authentication method. However, they said the remaining part of the test was manageable afterward. Furthermore, they expressed that adding and setting up additional methods became more straightforward after configuring the first new method.

Some participants found eBay's website to be easier due to the presentation of the text being less overwhelming than on Microsoft's site. They mentioned that the text on Microsoft was small and looked indistinguishable at first sight, which required more reading to locate the correct place to click. Others reported that they guessed where to click instead of reading everything. Additionally, most participants mentioned that they were unfamiliar with both websites, and this was their first time navigating them.

The Passwordless Setup Experience

The participants echoed many of our observations during the usability test, especially in the setup and sign-in phase. Consequently, the following two sections about setup and sign-in may contain repetitive information from the earlier error and eye tracking analysis. To avoid redundancy, we will present the findings in a concise list format. This section regards the *setup* experience:

- **Expectations before tasks regarding setup:** Most participants believed the security settings would be a logical place to begin after reading the task descriptions, which they could confirm was correct after the test.
- **Difficulty in finding where to set up a passwordless method:** This was more difficult than actually setting it up. Two participants reported that they could not find the option to "add a new way to sign in" on Microsoft until they carefully read through all the information provided on the website. Other findings were:
- **Security key setup:** On one hand, both websites provided a figure of a security key which helped participants feel confident that they were in the right place to configure it. However, some participants faced challenges with the security key, especially the uncertainty about when to insert the key and

when to touch it. For example, some participants were confused about whether "having the key ready" meant inserting it.

- **Clear instructions and intuitive websites:** Almost all participants found that the setup process itself had clear instructions and was straightforward, especially when setting up the fingerprint. Several participants mentioned that eBay provided a better experience as it had clear and concise instructions to "Turn on fingerprint" and "Turn on security key." In contrast, Microsoft had only the option to "add a new way to sign in" before displaying methods like fingerprint and security key.
- **The need for Microsoft Authenticator app:** To replace the password, some participants were negative to an extra requirement and extra steps in the process.

Overall, many participants found it easier to set up authentication methods after the first time as they became more familiar with the process.

The Passwordless Sign-in Experience

Overall, participants expressed satisfaction and reported a positive experience with the passwordless *sign-in* process. The following list presents the main findings related to the passwordless sign-in process during the follow-up interview:

- **Fast and easy process:** This was due to pop-ups and the information provided. One participant commented that it was as fast as using a password manager, while another found it even faster than entering a password as long as they remembered to touch the key.
- **Challenges with the security key:** Participants expressed irritation with inserting and removing the key, and entering the PIN code.
- **Confused about default sign-in method on Microsoft:** One participant experienced confusion after entering their email on Microsoft because the default sign-in method on Microsoft was set to the Microsoft Authenticator app.
- **Positive to sign-in with fingerprint:** Participants liked that the fingerprint was the default login method once registered on eBay, reducing the need for an extra step to click on fingerprint sign-in. Using fingerprints also relieved some participants as they no longer needed to concentrate while entering complex passwords. Generally, with fingerprint sign-in, they valued that they did not need to remember anything.

Comparison of Fingerprint and Security Key Regarding the Usability

9/10 participants preferred fingerprint authentication over security key due to user-friendliness. They found it the fastest and most practical option, as they did not have to remember anything, and their fingerprint was always with them. However, two participants mentioned that they had experienced issues with their fingerprints not being recognized on their phones. One said they did not know why, while the other said they used to climb, resulting in sore fingertips.

On the other hand, participants found several drawbacks with the physical security key. Some participants found it irritating and a barrier to carry around, and they often forgot to touch the key when inserted into the device. Also, they had to remember and enter the PIN code, which they mentioned as a drawback. One benefit of the security key mentioned by participants was its convenience when switching between devices, such as an office computer and a personal computer. A summary of expressed advantages and disadvantages are seen in Table 5.4.

Table 5.4: Usability advantages and disadvantages of fingerprint and security key.

Fingerprint	
Advantages	**Disadvantages**
- Fastest method - No need to remember bringing something - No need to remember PIN	- Sensor may not recognize fingerprint
Security key	
Advantages	**Disadvantages**
- Convenient when switching between devices	- Need to carry the key - Need to remember PIN - Need to enter PIN for every use - Need to touch the key - Need to configure backup keys

Thoughts about Buying the Key Regarding the cost of the security key, we asked about the participants' willingness to pay for it. Most participants expressed a maximum of 100-500 NOK, with one participant willing to pay up to 1000 NOK. However, when informed about the correct price of the keys (around 500 NOK for the cheapest option of YubiKey), and Yubico's recommendation of multiple backup keys, they all found it too expensive and impractical. While some saw the importance of having backup keys, they felt that the cost outweighed the benefits, especially

considering the potential for losing them. Participants who already had a computer with fingerprint sensor saw no need to buy additional security keys when they could use their computer for passwordless authentication for free.

Participants without fingerprint sensors on their computers started comparing the keys' cost to buying a slightly more expensive computer with a built-in fingerprint sensor. A few preferred spending money on the built-in fingerprint sensor instead of buying the security keys as they found the fingertouch more practical. A few others said they would rather stay with traditional passwords than invest in passwordless authentication methods. To summarize, none of the participants wanted to buy the key. The ten participants, keeping in mind they were students, thought the security key's cost was too expensive when weighed against its level of user-friendliness.

5.2.2 Awareness of Passwordless Authentication

Knowledge About Passwordless Authentication in General

Participants were asked whether they had heard about passwordless authentication. All participants answered positively. The majority of participants were familiar with fingerprint authentication for unlocking computer devices and facial recognition on smartphones. However, their knowledge of these methods was primarily limited to device unlocking. Some participants mentioned the use of facial recognition for accessing specific phone applications such as Vipps, bank accounts, and the Microsoft Authenticator app. On the other hand, not all participants were familiar with security keys. Half of the participants had heard of security keys through courses at the university or companies that uses them, but they had little knowledge of their functionality or usage and had never used them before. The remaining participants had no prior knowledge or experience with security keys.

Knowledge about Passwordless Authentication on Online Services

Participants were asked whether they were aware of passwordless authentication methods like security keys or fingerprints for accessing *online services*. The findings, summed up in Figure 5.14, indicated that eight out of ten participants were not aware of this possibility, with only two participants reporting prior knowledge.

The first participant with prior knowledge had heard about major companies such as Apple, Amazon, and Facebook working on developing passwordless authentication technology. However, they were unsure about the current availability on these

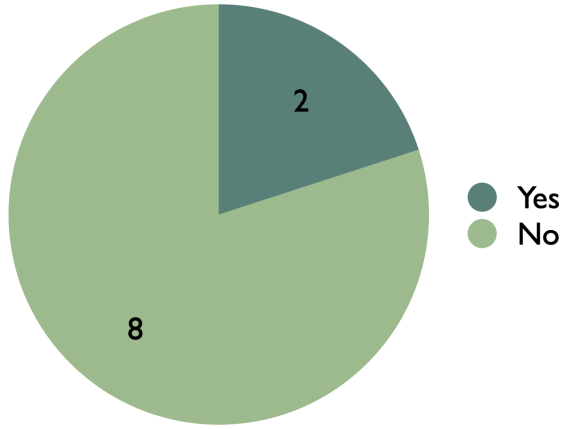


Figure 5.14: Number of participants with knowledge of passwordless authentication methods on online services.

services and whether other online services offer it. The other participant who answered affirmatively had recently seen passwordless authentication alternatives on Github. On Github, they were given the option to add a security key or fingerprint as a *secondary* authentication factor. The participant had chosen to use the fingerprint as the second factor. However, they clarified that they had not come across or used a passwordless authentication method as the only factor for accessing any online service. In summary, out of the two participants who had prior knowledge, only one of them had actually experienced using a passwordless authentication method on an online service.

It is worth noting that one participant expressed surprise and enthusiasm, stating, "I was surprised that passwordless sign-in at websites was possible. Very cool!" This reaction highlights the eagerness and positive perception of passwordless authentication among participants.

5.2.3 Perceptions of Security and Trust

Perceptions of Fingerprint and Security Key Regarding the Security

Asking about the participants' perceptions of the security of passwordless authentication compared to password-based authentication, we discovered that they had a solid understanding of password security, likely gained through their academic studies. They highlighted common password vulnerabilities and acknowledged that passwords could be a weak form of authentication. Although they expressed being unsure of how passwordless authentication security works regarding cryptography and how the data is stored, they speculated that it was likely to be more secure than passwords.

Regarding the security of the fingerprint authentication method, opinions were mixed. In total, nine out of ten participants trusted fingerprint as an authentication method. Some pointed out that fingerprints are unique and individual and, therefore, almost impossible to hack. In addition, some justified the opinion that attempting brute force attacks on fingerprints would be ineffective since they all differ. Others mentioned that the fingerprint could not be stolen the same way as a physical key and are, hence very safe. Another reason they trusted fingerprint authentication was based on their use of fingerprint sign-in on their smartphone for many years without any security issues. Despite this, some participants did not fully trust fingerprints as an authentication method as they were afraid they would not gain access to their account if their finger was wet, dirty, or sore after climbing. Another participant worried that using a fingerprint sensor could leave identifiable marks on the sensor, which could be exploited to recreate their fingerprint later. This concern came from experiences with touch screen devices, where the participant had observed their fingerprint remained on the screen. Regarding the security key, participants' thoughts were also divided. In total, four out of ten participants trusted this authentication method. While some valued the extra security provided by an additional independent authentication device and a PIN, the majority expressed concerns about their potential to be lost or stolen. The concern was even more significant if the security key got lost with information like their name or job so that a malicious person could find their usernames or emails and access their accounts. Others mentioned concerns about the PIN being easily guessed. One commented that through university, they had learned that they should never trust a USB device and, therefore, not trust the key.

Figure 5.15 illustrates how many of the participants trusted fingerprints, and how many trusted the security key in a Venn diagram. Eight participants trusted fingerprint and four trusted the security key, whereas two trusted both authentication methods.

Figure 5.15: Number of participants who trusted fingerprint and security key.

We also obtained answers on general passwordless security, which includes aspects beyond just security key and fingerprint methods. Two participants said they felt passwordless SFA is less secure compared to any 2FA. This perception came from prior knowledge about combining multiple factors, like in 2FA, which was seen as the safest authentication method. Also, one participant was concerned about using passwordless authentication on smaller or "shady" websites, unsure if the websites could steal the credentials or store them poorly. They considered the potential risks of using the same, identical passwordless credential, such as a fingerprint or security key, across multiple web services. The main concern was the possibility that if an unauthorized person were to gain access to these credentials, they would eventually be able to benefit from them and sign into all other platforms used with passwordless authentication.

To summarize, all participants expressed greater trust in passwordless authentication over passwords in terms of security. A few considered the security level equivalent to creating a complex password for each account. Two participants trusted both the security key and the fingerprint, as SFA, and others only one of the methods. In contrast, one expressed a more casual attitude towards security, placing greater importance on using 2FA rather than focusing on the security of each authentication method.

Perceptions of Suitable Account Types for Passwordless Authentication

The majority of participants stated that passwordless authentication was best suited for critical accounts requiring an extra security layer. However, the definition of "critical accounts" varied significantly among participants. For example, while some mentioned social media due to the high amount of personal information, others referred to personal and business email accounts, bank accounts, and work or university accounts. However, one participant would not use it for any accounts with sensitive information as they were not yet comfortable with new authentication methods and needed to learn more about it first.

A few participants believed that passwordless authentication fitted best to accounts where they sign in often, not because of the security benefits but because of the ease of use. Another participant noted that they would not use it for streaming sites because it was common to share accounts, and everyone sharing the account needed to sign in, making passwordless authentication impractical. Finally, some participants expressed passwordless authentication as suitable for all accounts since using fewer passwords enhanced the security.

Table 5.5 lists preferences for what type of accounts should be passwordless, based on a given reasoning.

Table 5.5: Reasons for using passwordless authentication on different account types.

Type of account	Reasoning
Any accounts	Fewer passwords → better security
Any accounts *with* personal information	Feels safer to protect information with passwordless authentication
Any accounts *without* personal information	Not comfortable using passwordless authentication to protect important information yet (new technology)
Accounts they sign into often	Due to ease of use and not security
Not streaming accounts	Want to share the account with family/friends, a very secure method gets impractical

5.2.4 Adoption of Passwordless Authentication on Online Services

What Remains Before the Participants Start Using Passwordless Authentication on Online Services?

Some participants highlighted the adoption of new technologies as a barrier in itself. This perception came from dealing with unfamiliar concepts and the belief of a challenging setup process. Additionally, even if they knew that the setup was not difficult, the time investment required for transitioning to passwordless authentication presented another obstacle. However, a few participants expressed after performing the usability test, they found the process easier than first thought and lowered their barrier to do it themselves later. Anyway, they said that without this exposure, they had stayed skeptical.

A few participants expressed that they required some encouragement to actively transition to passwordless security settings. They stated the navigation to the security settings and discovered passwordless authentication methods as something you only do if you knew what to look for. One suggestion for improvement was to have a pop-up window appearing after login, directing users to the setup page of passwordless authentication. They said it would eliminate the problem of finding it on their own. Another suggestion from the participants was to allow users to create new accounts only by registering passwordless authentication methods, eliminating the need to change authentication methods later on. In addition, one said this would also eliminate the barrier of just doing it, as there is no need to change.

Participants highlighted the need for more information about passwordless authentication methods. For example, one participant noted that they already had an account at Microsoft but had no idea that passwordless authentication was an option.

One participant said they had recently done an authentication check, with passwords and 2FA, on all services they used and could not remember any security key option except for GitHub offering it. The participant had looked up the term to understand what it was and found it interesting. If more services provided this option, they would be more likely to use a security key as they switch between two computers, one of which does not provide fingerprint authentication. Two other participants mentioned that more devices supporting biometric scans would encourage their use.

Perceived Value in Using Passwordless Authentication

All participants recommended passwordless authentication on online services to friends. However, some participants only recommended fingerprint authentication due to its lower cost and perceived ease of use compared to the security key. The main reasons for recommending passwordless authentication were its perceived security and convenience in terms of faster sign-in.

On the other side, one participant mentioned that the limited availability of websites supporting passwordless authentication and the need for a compatible device or security keys could sometimes be why not recommending it. Additionally, another pointed out the importance of informing their friends to have a strong PIN on their phone, when using phone-based biometric authentication, as passwordless sign-in with a phone only increases the security when the PIN is strong too.

Regarding recommending it to their parents, the majority expressed they would recommend it due to the better level of security. Many mentioned that their parents struggled with creating and storing passwords well. One participant said their parents were afraid of being hacked and thought they would prefer using passwordless authentication. Moreover, many said they would set up passwordless authentication for their parents as they are not very technical. However, others thought their parents had enough technical knowledge to set it up themselves.

Some participants acknowledged that their parents might be skeptical about new technology and unwilling to adopt passwordless authentication. Others mentioned that their parents already used biometric authentication to unlock their phones, making biometric sign-in a more natural fit for them. A few participants highlighted the potential downsides of using a security key when getting older, such as the risk of losing the small key and learning to use a completely new device. In summary, several expressed biometric authentication as the best choice for their parents.

Chapter 6
Discussion

This chapter presents a discussion of our results from Chapter 5, and how they contribute to answering our defined research question.

In Chapter 4 we identified the four factors *Effectiveness*, *Ease of Use*, *Trustfulness*, and *User Satisfaction* to be essential for widespread adoption of FIDO2. In our usability test, our observations of errors and eye movements, contributed mainly to our understanding of the two first factors, while, the interviews shed light on all four factors. These factors will not be studied separately because they are deeply connected. A discussion of how the factors impact the adoption of FIDO2 is provided in Section 6.1.

Based on our results, we identified four main obstacles to the widespread adoption of FIDO2. From a user experience perspective, the identified obstacles are *Missing Awareness of Passwordless Authentication Possibilities on Online Services*, *Poor Interfaces for Setup and Sign-in*, *Suboptimal transition to passwordless authentication* and *Misconceptions and Knowledge Gaps of Passwordless Security*. These obstacles will be discussed step by step from Section 6.2 to Section 6.5. Furthermore, Section 6.6 provides recommendations for service providers implementing FIDO2 on their online websites.

6.1 How the Factors Impact Adoption

From the usability test and follow-up interview, it became clear that the impact of the factors was not isolated; rather, the participants' user experience was influenced by the effect of all factors. For instance, if the process was found less intuitive and less user-friendly, their trust in passwordless authentication decreased. A user interface providing clear instructions has most likely contributed to effectiveness, due to all participants completing the tasks with no critical errors. Furthermore, this

may impact user satisfaction due to the participant indicating being satisfied with the solved tasks directly after the usability test.

Studying the factors in relation to each other has been valuable in identifying the obstacles. All factors impact overall user satisfaction, and we see this as an important factor to consider when increasing the adoption of FIDO2. If the user is not satisfied with the process for passwordless authentication, it is challenging to adopt it. Even though users do not follow the most efficient path during the processes or do not read the important information, it is more important to consider whether the users are satisfied with the process. Our participant group expressed being satisfied, despite our observations on errors and reading behavior, indicating the potential for more efficient setup and sign-in processes.

6.2 Awareness of Passwordless Authentication

While several web services already support sign-in with FIDO2, either as SFA or 2FA, users often remain unaware of this possibility. As we saw in Section 5.2.2, eight out of ten participants were unaware of passwordless authentication on online services. Enabling 2FA can lead users to the security settings page, where they can discover the option of passwordless authentication. However, this process relies heavily on the user's initiative to discover this alternative. Users who are not particularly interested in security are unlikely to stumble across this option randomly and may remain unaware if the same promotion strategy continues. To make the adoption of FIDO2 a reality, it is crucial for web services to proactively educate their users' about the existence and benefits of passwordless authentication.

In addition, several participants had a platform authenticator without knowing it could be used as an authentication method on online services. Several participants in this study reported using biometrics, such as fingerprint or facial recognition, to unlock their smartphones or computers. However, they were unaware that these same authentication methods could be utilized for sign-in on online services as our findings indicated in Section 5.2.2. However, we think that users having a security key are most likely aware of its usage as a passwordless authentication method. Hence they do not need extra information about its authentication possibilities in the same ways as with platform authenticators.

Surprisingly few participants were aware of passwordless authentication on online services, even though they pursued a master's degree in Communication Technology and Digital Security. The participants mentioned their awareness of password disadvantages. However, they were unaware of the benefits of passwordless authentication.

The responsibility of raising awareness should not rest on the users. Web services, platform authenticator providers, and other stakeholders should collaborate to give users comprehensive information about passwordless authentication and its advantages. Educational campaigns, interactive tutorials, and intuitive user interfaces can play a significant role in spreading knowledge and encouraging users to explore passwordless options.

The Term "Passwordless Authentication"

The choice of terminology may impact the adoption of passwordless authentication. While *passwordless authentication* is a generic and inclusive term that contains various methods, including patterns, biometrics, security keys, and apps, the term may not immediately remind users of all possible options. Using more specific terms can provide users with a clearer understanding of the authentication methods they can use. For example, today, we see platform authenticators use their own passwordless technology brand name instead of the term *passwordless authentication*. Windows calls its biometric authentication methods Windows Hello, while Apple calls it Touch ID and Face ID. By highlighting these terms, users are more likely to associate passwordless authentication with the convenient biometric methods they are already familiar with. In addition, these users already have what they need to go passwordless, which makes it a more effortless way to quit passwords. However, this only applies to authentication methods the users already have and are familiar with. A security key or YubiKey needs to find other approaches to expand its use and contribute to the FIDO2 adoption.

6.3 Poor Interfaces for Setup and Sign-in

As described in the background material, well-designed web interfaces are important to ensure users have a positive user experience when interacting with authentication systems.

6.3.1 Word Choice Obstacles to Setup Interface

Results revealed that the design of the user interfaces was not optimal during the setup and sign-in process. Options for passwordless authentication, such as a security key or fingerprint, were often hidden under "advanced security options" and presented in small text, making it difficult for participants to discover the options. To set up passwordless authentication methods on Microsoft's website, users had to click

"add a new way to sign in or verify," marked with a red circle in Figure 6.1. Several participants had to scroll up and down the page to find where to set up a security key or fingerprint, as described in Section 5.2.1. As described in Section 5.1.3, participants expressed their confusion about what to look for, which may be the reason for the scrolling on the page. This may have been due to Microsoft having several options available on the security page, and there was no clear text saying "fingerprint" or "security key." One participant commented on this:

"When I wanted to add a new way to sign in, I expected to find the words security key and fingerprint at Microsoft, but I couldn't." -P7

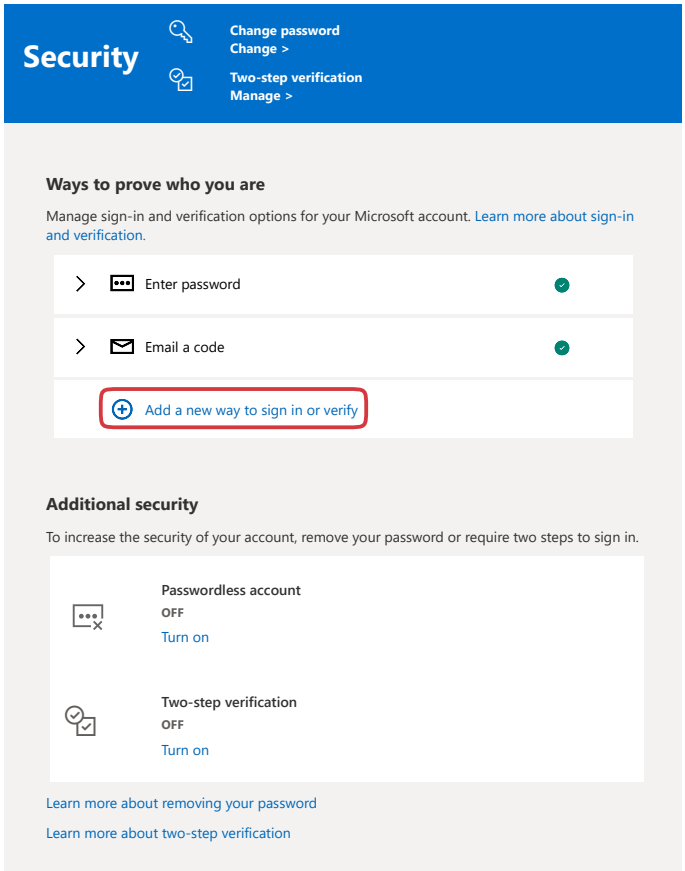


Figure 6.1: Microsoft's interface for advanced security settings not displaying fingerprint and security key options.

On the other hand, it was easier for participants to find where to set up passwordless authentication on eBay's website because they explicitly used the words "fingerprint" and "security key" on one security page. eBay's interface for providing the passwordless authentication method can be seen in Figure 6.2. This Figure is a snapshot from a longer list when entering the security page. The purpose of the figure is to show how eBay visualizes its options. Comparing these interfaces, eBay allows users to add a passwordless method faster than Microsoft, requiring fewer steps and resulting in fewer non-critical errors, as shown in Figure 5.3 and Figure 5.2.

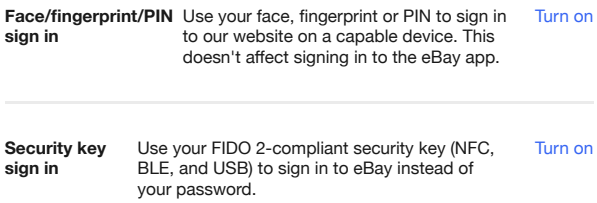


Figure 6.2: eBay's interface for security settings displaying fingerprint and security key options.

We see that the choice of words provided by the websites impacts the user experience of passwordless authentication. Participants expressed confusion about Microsoft not providing passwordless options in larger text, and we also see that this resulted in a higher average of non-critical errors on Microsoft than on eBay when finding where to set up the first method. These results were given in Section 5.1.2, where we can read 2.6 average non-critical errors for Microsoft and 0.2 average non-critical errors on eBay. The choice of words may have had the largest impact due to this difference. Therefore, to ensure ease of use and user satisfaction for the end-user, we see the importance of clear and descriptive text as early in the process as possible, so the user does not need to search around the webpage and perform several unnecessary steps. This only leads to a confused and frustrated end-user, not providing any confidence or satisfaction to the user.

Figure 6.3 shows the interface after clicking "Add a new way to sign in or verify," where the user is given several additional options to sign in other than a password. As described in the results, several participants pointed out, both during think-aloud and in the follow-up interview, the confusion about the option: "Use your Windows PC," when the usability test was performed on a Mac. On the one hand, through the eye movement study, some participants only read the bold headings and therefore did not read the text below where "fingerprint" was described. This led to some participants clicking "Show more options," or exiting the pop-up window. These non-critical errors could have been because of lack of confidence in their chosen

path, possibly due to confusing word choice. On the other hand, some participants read more carefully and pointed out the confusion but clicked the Windows option anyways, possibly because they did not find other potentially correct alternatives.

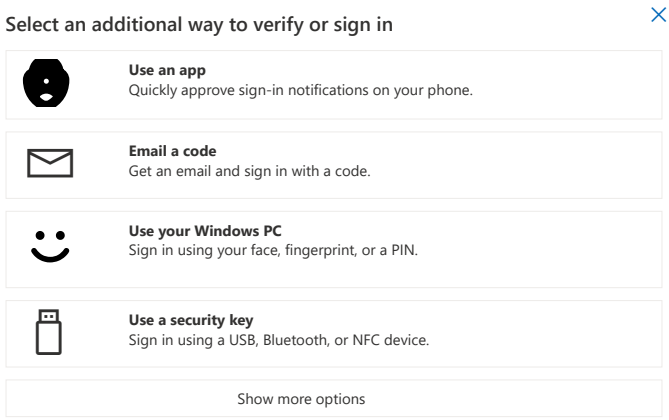


Figure 6.3: Microsoft's pop-up window for selecting new ways to sign in.

Since the passwordless authentication methods security key and fingerprint were provided in the same pop-up window on Microsoft, this may have led to a decrease in non-critical errors on average when setting up the second authentication method, as we saw in the bar chart given in Figure 5.4. When a participant had found the first method, the other method was available at the same location; see Figure 6.3. Studying Figure 5.4 and Figure 5.5 in more detail, we observed an increase in non-critical errors from setting up the first method to setting up the second method correctly. The increase may have been due to completely different setup processes for fingerprint and security key. Due to this, we could say that one method might not necessarily be easier than the other due to different setups and different instructions. Microsoft and eBay are two online services providing different strategies for the instructions to set up the security key correctly. The interface on Microsoft can be seen in Figure 6.4 and for eBay in Figure 6.5.

The different interfaces differ mostly in the amount of text given as instructions. Microsoft provides more detailed instructions than eBay. From Table 5.3, we observe a lower average for eBay than Microsoft in non-critical errors for setting up the security key correctly. This may indicate that the more text provided as instructions is not necessarily easier to understand. When the participants saw the text given in Figure 6.4, most participants read carefully and focused. However, results revealed that this might not have any effect due to the challenges in understanding when to insert the key and when to touch its sensor. When a participant saw the descriptions in Figure 6.4 and Figure 6.5, the participant inserted the key and touched it, but

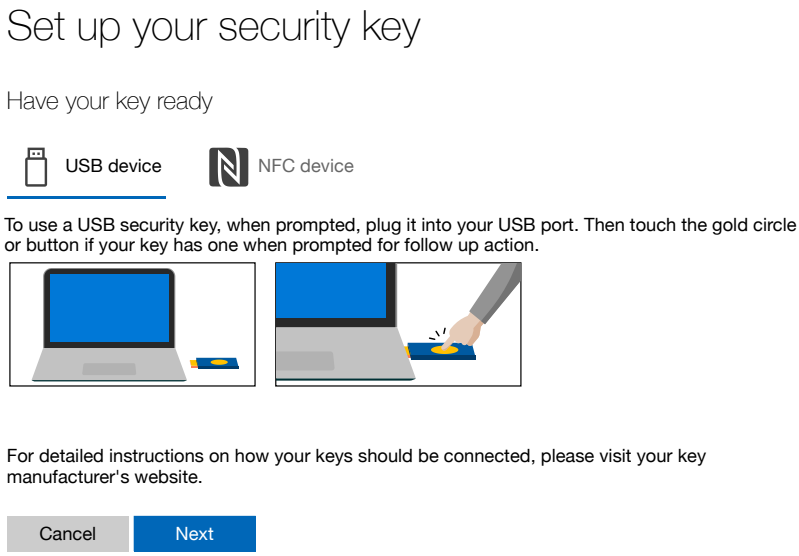


Figure 6.4: Microsoft's instructions for security key setup.

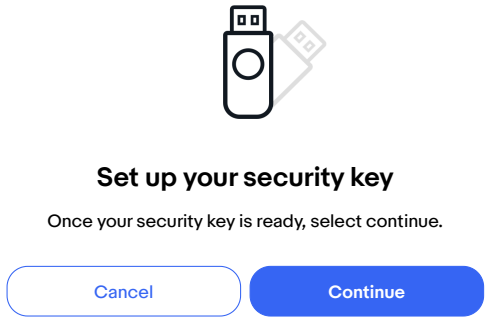


Figure 6.5: eBay's instructions for setup of security key.

the websites needed the user to click "Continue" or "Next" before inserting it. This was seen as a typical non-critical error among the participants. In addition, the key illustrated by both eBay and Microsoft looks different than the one used in the usability test. The illustration has the sensor on top of the key, but the one we used for the usability test had the sensor on both sides of the key. This might have been confusing for the participants.

6.3.2 Obstacles to Sign-in Interface

The interface for the sign-in process was generally understandable. However, results from the non-critical errors and eye movement showed that participants did not read the text in a small size on Microsoft displaying passwordless sign-in, which further caused a less efficient path for signing into the account. Nine out of ten participants entered their email and did not notice the option in a red circle in Figure 6.6. Moreover, during the second time signing in, some participants entered their email again, indicating that they did not notice the passwordless option available for them. On eBay, all users were required to enter their email addresses initially, even when signing in passwordless. We can say that the passwordless sign-in option is not visible enough on Microsoft due to these analyzed results. Comparing the different interfaces confirms that there is no universal interface for FIDO2 authentication. If a user started the usability test on eBay's website, and further moved on to Microsoft, we observed tendencies to scan with the eyes when signing in passwordless, indicating confusion. Since eBay had email as a requirement, it seemed like the participants expected Microsoft to have the same requirement. By studying Figure 5.8 and Figure 5.9, we see a significantly lower error rate for eBay, which may indicate the users were satisfied with following the habit of entering their email first.

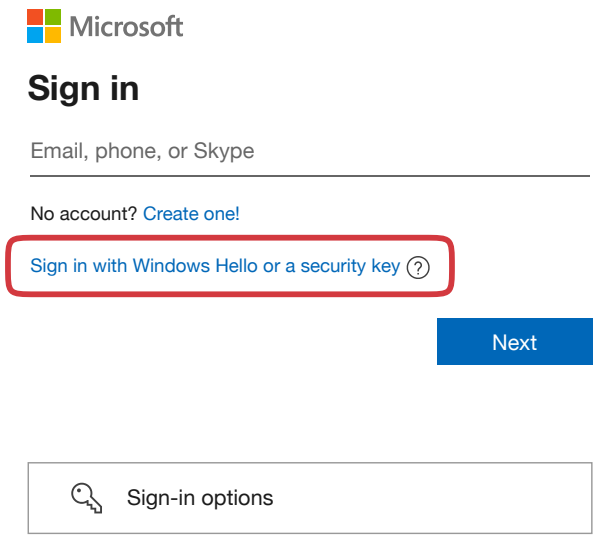


Figure 6.6: Sign-in interface on Microsoft.

In the process of setup and sign-in of fingerprint, Figure 6.7 shows how the fingerprint authentication interface looked on a Mac. Participants expressed being confused regarding the button displaying "Use Password." If the participant was unfamiliar with Apple's interface and unaware that they should scan their fingerprint on the sensor when getting this pop-up, they clicked the button instead, which was a typical non-critical error. From related work in Section 3.3, we have seen that the fingerprint icon is confusing for the user. A user does not always understand where and when the user should scan their fingerprint in the process for setup and sign-in.

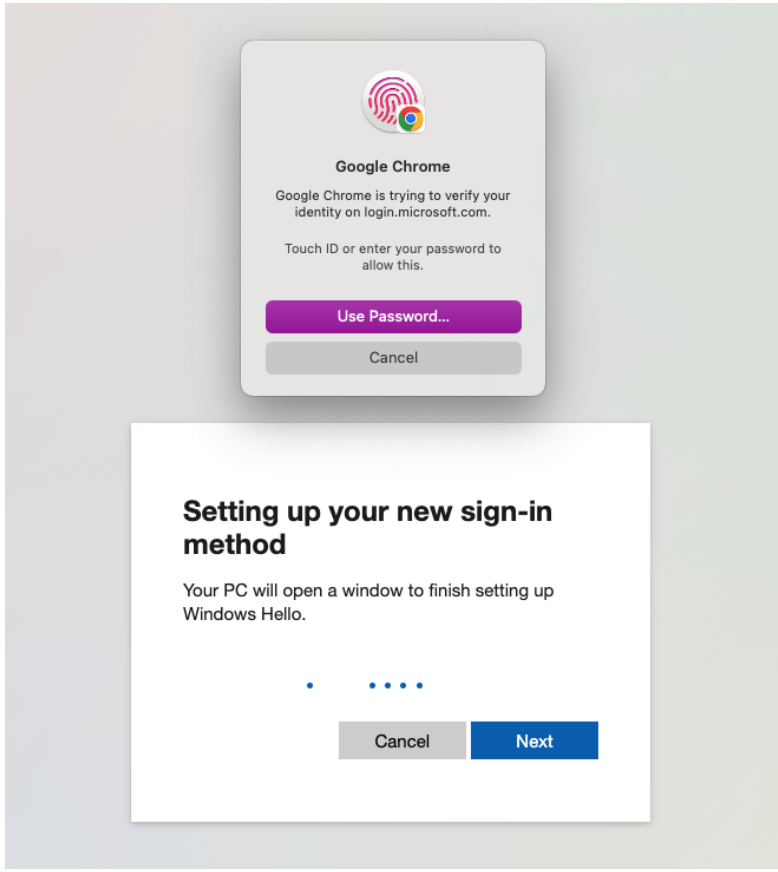


Figure 6.7: Fingerprint pop-up on a Mac, with information from Microsoft in the background. The user can scan their fingerprint when this window pops up, click "Use Password" or click "Cancel."

Furthermore, it is worth noting that all participants, except one, were new to the processes for setup and sign-in with FIDO2. Despite no experience, results revealed that the processes became easier throughout the usability test due to repetitive tasks. We observed fewer non-critical errors and less reading from the bar charts studying

setup and sign-in on the first online service compared to the second online service, as shown in Figure 5.4 and Figure 5.5. The bar charts for the sign-in process are not included because they show the same pattern as the setup process. Therefore, we can see that the participants are learning by doing and being more efficient the more they perform the same tasks on the same interface. One participant also expressed in the interview the following statement, confirming this:

"It became easier and easier throughout the tasks." -P4

We observed how participants become familiar with a specific interface and expect a similar interface when encountering new online services, and we found this intriguing. However, the reality is that user interfaces differ, which makes them less user-friendly. Users typically have multiple accounts, so consistency within the websites' interfaces might be beneficial to ensure more users adopt FIDO2. All over, we have observed the importance of a convenient interface that ensures a positive user experience for end-users.

6.4 Suboptimal Transition to Passwordless Authentication

The transition from password-based authentication needs to be simplified to ensure end-user adoption. We describe the transition as the process of manually changing security settings. If the users are satisfied and find the transition user-friendly, the adoption might have been more efficient. It is an obstacle for the users if they need to figure out the possibility on their own, compared to having the possibility given directly to them through a pop-up notification. Authentication should be effortless and user-friendly, and if it is more time-consuming than satisfying, the user experience is negatively affected.

Simplifying the Transition with Informative Pop-Ups

We will discuss one participant's suggestion for a more user-friendly transition solution from Section 5.2.4. The participant suggested having a pop-up window appear when logging into an online service, which redirected the user to set up passwordless authentication. When we created an artificial account for the usability test on eBay and signed into the account for the first time, the pop-up shown in Figure 6.8 was seen.

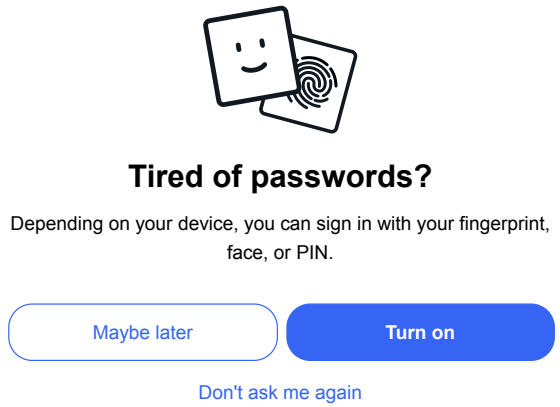


Figure 6.8: Pop-up when logging into eBay encouraging the user to turn on a fingerprint, face, or PIN.

Figure 6.8 shows how eBay informs and makes it visible to users that they offer passwordless authentication. When we designed the usability test, we knew that eBay offered this pop-up window. However, we clicked "Don't ask me again" for the artificial account. We are aware that this is a positive action toward informing users of FIDO2 on online services. However, for this research study, we wanted to study the path from the websites' homepages to security settings, as this is the most common way to turn on passwordless on most services, making the test more general rather than eBay-specific. Microsoft does not provide any pop-ups to ensure faster setup of passwordless authentication. Providing pop-ups ensures the transition becomes easier and reduces the barrier for the end user. In other words, it simplifies the transition from password-based to passwordless authentication.

6.5 Misconceptions and Knowledge Gaps of Passwordless Security

Trustfulness is crucial for users' acceptance and adoption of passwordless authentication methods. Therefore, it is important to understand their perception of security in passwordless authentication. If they perceive passwordless authentication as insecure, they may wait or avoid adopting these methods, hindering the widespread adoption and taking advantage of the benefits they receive by applying it. In addition, identifying users' knowledge gaps and misconceptions about the security of passwordless authentication allows for targeted education. Addressing user's concerns and

providing precise information can reduce unnecessary concerns, potential risks, and vulnerabilities associated with passwordless authentication. One important part of giving relevant and precise information is to ensure users drive informed decisions while choosing to use or not use passwordless authentication. This section highlights misconceptions and knowledge gaps we identified through our research, with the intention of using these insights for future educational work.

Passwordless Authentication in General

In general, participants expressed awareness of insecurities associated with *passwords* as an authentication method. Especially they pointed out that passwords can be cracked and acknowledged the existence of relatively easy methods to achieve this. This knowledge could be something they have learned through their education or personal experiences, but most importantly, they are aware of it. However, their knowledge about *passwordless* authentication was limited, especially regarding its security aspects. While they were familiar with biometric authentication methods, mainly through their use on phones and devices, they had not considered other application areas beyond unlocking devices. Moreover, their understanding of the security behind passwordless authentication was lacking, and was also something the participants pointed out and was aware of. For example, one participant said the following about passwordless authentication:

> *"I do not know the cryptography behind it, or how the data is stored. But I think it is safe."* -P1

Despite their limited knowledge, the participants perceived passwordless authentication as more secure than traditional passwords. Their belief was justified by the vulnerabilities of passwords. This argument emerged as the most frequently used justification for the perceived benefits of passwordless authentication. Notably, they did not mention other benefits of passwordless authentication, like phishing or keylogger resistance. On Microsoft, a pop-up like Figure 6.9 highlighted the advantages of quitting passwords, including that passwordless methods are resistant to phishing attacks. Although all participants received a pop-up and had the opportunity to read it, none of them recalled or mentioned the advantages written in the pop-up during the interview. Further, this supports the finding that participants did not pay close attention to pop-up windows.

Figure 6.9: Pop-up information about setting up a passwordless account on Microsoft, including the advantages of it.

In summary, the participants were positive against passwordless authentication. However, many were also aware of their limited understanding of how the security mechanisms actually worked. In the following section, we will look into each of the two authentication methods. A tendency we saw, was that their responses were often characterized by assumptions and personal thoughts rather than knowledge.

Perceptions of Security in Fingerprint Authentication

When we asked if they trusted fingerprint, eight out of ten participants answered a clear "Yes," which is good news regarding a potential adoption. However, our observations revealed some noteworthy aspects we will highlight. While we experienced a lot of positive engagement around fingerprint, participants' justifications for their trust appeared to be limited and unjustified. Surprisingly, only two participants considered any potential issues with fingerprint authentication. In contrast, all participants saw several potential issues regarding the security key.

Several participants expressed trust in fingerprint authentication based on their familiarity with using it to unlock their phones. They seemed to lean on the fact that after years of using fingerprint unlocking, they had grown a habit of using it and did not question its security. It is worth considering whether the perception is influenced by their trust in their phone providers. They might believe that if Apple includes fingerprint authentication on their devices, it must be secure.

The most common argument for why they trusted fingerprint authentication was because their fingerprint is unique, and it led them to think the uniqueness made it impossible for anyone else to access their accounts. By this, we saw, for example, a lack of awareness regarding fingerprint sensor limitations. None of the participants mentioned the varying quality and preciseness of sensors, which affects the actual uniqueness of fingerprints when used for authentication on services or devices. For example, Apple reports a 1 in 50 000 chance of successfully accessing a device using Touch ID [App17].

There were a few concerns regarding fingerprint authentication, described in Section 5.2.3. First, one was concerned about where the fingerprint was stored, and if the online services stored their fingerprint data. The same result was also found by Lassak et al. [LHGU21], and they managed to decrease the misconception rate through targeted notifications. However, they addressed that notifications were insufficient to solve this misconception for all users. During this part of the interview, we saw another misconception about how the fingerprint was stored. Some believed it was stored like a photo, which we know from Section 3.1.3 is incorrect. Another concern was the fingerprint leaving identifiable marks on the physical sensor, which could later be exploited to recreate their fingerprint. Lastly, they were afraid of not being recognized by the sensor and not being able to access their own accounts. The concerns may have contributed to not trusting fingerprint as authentication method. However, only two in our participant group thought about these concerns.

Perception of Security in Security Key Authentication

Half of our participants had never heard of the security key before and were unaware of the security behind it. Some pointed out that the PIN for the security key had the same functionality as a password and could be cracked. Even with an eight-digit long PIN, they were skeptical about whether it was safe enough. They expressed that relying only on the PIN for account protection made them skeptical about the overall security, especially considering the big perceived likelihood of losing the key.

We observed several knowledge gaps among participants. For example, they were unaware of signing in using an alternative authentication method and deactivating a lost key. Additionally, there was a misconception regarding a malicious person would have knowledge of the key's associated accounts. These misconceptions may have influenced their perceptions of the overall security of the security key. However, participants expressed worries about leaving the key unattended at the university or workplace, as they believed their colleagues could guess typical accounts used with the key. In the end, the risk of losing the security key was a big issue and the reason they did not trust it.

We experienced that many were negative to the key after finishing the usability test due to misunderstandings of how they used it correctly and efficiently. It was the first time trying the key for everyone, and not all had the best experiences understanding its use. This may have also affected their trust, as we saw that ease of use and trustfulness are connected and influence each other. Also, the security key's cost was unacceptable for all participants. However, it is worth remembering that all participants were students, a demographic often associated with limited financial resources. All over, the participants' perceptions of security keys indicate poor news for future adoption.

To summarize the participants' perceptions of trust, we saw that trustfulness in passwordless authentication methods was influenced by familiarity with the authentication method. It is important to recognize the significance of user familiarity and comfort when developing user interfaces to improve trust and acceptance of passwordless authentication. Due to a lack of knowledge, several misconceptions lead to the user not trusting the authentication methods. These misconceptions could be recognized and used to improve user satisfaction and trustfulness, as Lassak et al. [LHGU21] did with some misconceptions.

6.6 Recommendations

The recommendations are meant for the ones implementing FIDO2 into their online services. We are aware of the recommendations not being a quick fix. However, the purpose of providing recommendations is to understand what could gradually be done in order to ensure the adoption of FIDO2 over time. Based on our findings and our discussions, we have provided the following recommendations, which we see as the most important to consider:

Better User Interface for Setup and Sign-in: Despite all participants managing to complete the tasks, the user interface is not optimal for the widespread adoption of FIDO2. A user interface improvement is necessary to ensure an intuitive and straightforward path for setting up and signing in with FIDO2. Microsoft provides step-by-step guides and information boxes for the user to understand how to set up FIDO2 on their website, which is an action toward user adoption. Seen from a different perspective, too much information provided could potentially lead to an overload of information, which further could lead users to not read any of the text provided. Service providers should provide consistency in the setup of passwordless authentication in order to make it easier for the end-user to adopt several services. In addition, we see the choice of words as a crucial part of ensuring the user feels satisfied with the process.

Informing Users of Passwordless Authentication Possibilities: There is a need to inform users of their authentication options. Placing this information and options cannot be done inside advanced security settings or written in small text, as this is not user-friendly and difficult for users to find. In addition, there is a need to inform users about their compatible devices for passwordless authentication on online services.

Targeted Education: By providing targeted education to users, misconceptions and unclear aspects may be resolved, leaving users more positive against passwordless authentication. This applies to both the use and the security of the different methods. In addition, users may make decisions based on knowledge and not only assumptions, which we have seen are common. Education should be given on the services' websites or by providers of platforms and roaming authenticators, to ensure users notice the information.

Focus On Adopting Platform Authenticators: Based on our results, participants were not willing to spend money on a security key. None of them were willing to use a security key over fingerprint, when needing to pay for the key. Therefore, at least for individuals with limited budgets, such as students, a security key may be difficult to adopt. Due to this, it may be beneficial to prioritize the focus on platform authenticators for future adoption actions. Additionally, platform authenticators are more familiar to our participant group, as several participants already owned smartphones and computers with biometric sensors. Instead of purchasing an additional device, they preferred using the device they already had.

Chapter 7
Conclusion and Future Work

Section 7.1 presents a conclusion to our defined research question and associated research objectives. Section 7.2 provides suggestions for future work based on our findings.

7.1 Conclusion

As more online services and platforms adopt FIDO2, such as Google's recent announcement of its support for passwordless login in May 2023, it is valuable to identify user experience obstacles that hinder the widespread adoption of FIDO2.

By conducting a usability test and follow-up interview on two services that offered FIDO2 authentication, we found that participants were positive towards passwordless authentication. However, the main obstacle was the missing awareness of passwordless authentication on online services. Consequently, implementations of FIDO2 on web services lack sufficient visibility, which hinders its adoption on a larger scale.

Furthermore, the study revealed insightful findings regarding the research objectives. A conclusion to each of the four objectives is given below.

RO1: Effectiveness Firstly, studying the effectiveness factor proved a full success rate, and all participants managed to complete the tasks. This indicated manageable processes for students with a technology background.

RO2: Ease of Use The processes were found to be relatively straightforward by the participants, which gave insight into the degree of ease of use. However, user-friendliness and intuitiveness were still not found to be optimal due to some identified obstacles. For example, there were tendencies to confusion about when to insert and touch the security key, indicating insufficient descrip-

tions. Additionally, locating the security settings was found challenging due to inconsistency in websites' interfaces. For example, we saw Microsoft and eBay providing different paths to reach the settings.

RO3: Trustfulness To emphasize trustfulness, participants in general trusted passwordless authentication over password-based authentication. Without any knowledge about how the two authentication methods work regarding security, they trusted the fingerprint more than the security key. This was due to familiarity with biometric sign-in on smartphones for years, and they were used to think that biometrics were secure. They expressed concerns about losing the security key and saw it as not sufficiently secure to resist malicious people. We saw that their perceptions of the two methods' security did not match the actual security, leading to less trust in the security key.

RO4: User Satisfaction To consider user satisfaction, the participants expressed overall satisfaction after completing all tasks successfully. The satisfaction was due to positive attitudes towards passwordless sign-in because it felt fast and secure. Regarding user-friendliness, the participants highlighted fingerprint as the most convenient method. This was due to no need for carrying an extra device, and there were fewer steps in the authentication process than the security key. Manually switching to passwordless authentication inside the security settings on all web services was seen as an obstacle. Participants owned multiple accounts, making it time-consuming to enable passwordless authentication on all services without a universal interface.

These four research objectives have contributed to answer our research question:

RQ: *What obstacles related to user experience hinder the widespread adoption of FIDO2 passwordless authentication?*

All participants successfully completed the setup and sign-in process with FIDO2, despite some struggles. This indicates that it is possible for users to adopt FIDO2 authentication. However, the user interface for setup and sign-in was not found optimal, and the transition from password-based to passwordless authentication was not seen as sufficiently simplified to achieve widespread adoption. The perception of security was not considered an obstacle to the widespread adoption of FIDO2 because participants trusted the fingerprint. Moreover, many of the participants already owned a device with a fingerprint authenticator, and therefore the participants were willing to adopt it on online services. However, the main obstacle was the participants' lack of awareness of passwordless authentication on online services. In order to adopt FIDO2, people must be aware of it; therefore, the missing awareness remains a significant barrier to its widespread adoption. Based on the findings, and the answer

to the research question and objectives, suggestions for future research are given in the following section.

7.2 Future Work

This section provides five suggestions for further research based on our findings and experiences during the research study.

Investigating Diverse Participant Groups

We studied a participant group of ten technology students pursuing the same master's degree as ourselves. However, it would be valuable to expand the recruitment phase and include people from diverse demographic backgrounds, such as variations in age, gender, and education. Typically, the younger generation typically has higher technology levels compared to the older generation because they grew up in a digital world, making it easier for them to understand new technology. We see the older generations as an interesting participant group that could potentially provide other findings. Additionally, a broader range of perceptions, experiences, and user satisfaction with FIDO2 could have been found by investigating different participant groups. Moreover, the diversity could provide a more comprehensive understanding of the obstacles hindering the widespread adoption of FIDO2.

Investigating New Implementations and Updates of FIDO2

Web services' implementations of FIDO2 keep improving, and new web services' implement FIDO2 as a new way to authenticate. We explored Microsoft and eBay, and saw during the research study that Microsoft suddenly updated its user interface for FIDO2 implementation, more specifically, the text descriptions given in the sign-in interface. Furthermore, Google's FIDO2 SFA implementations should be investigated, particularly Google Workspace and Google Cloud Platform, as they recently announced support on June 5th, 2023. Additionally, other services implementing FIDO2 should be investigated for obstacles hindering adoption, and the ones already supporting FIDO2 should still be investigated when new updates are brought to their websites. It would have been interesting to see whether the improvements we identified in would lead toward a more positive direction in adopting FIDO2.

Exploring User Experience on Other Passwordless Methods

Our study focused on two passwordless authentication methods that support FIDO2 authentication, namely fingerprint and security key. Other passwordless authentication methods that support FIDO2 should be explored. Facial recognition or cross-device authentication are some examples. A complete understanding of the possible passwordless authentication methods could give an idea of the users' preferences in the choice of authentication method. Additionally, gain more insight into the benefits and challenges of each method.

Comparing User Experience on Smartphones and Desktops

We performed the usability test on a desktop environment. However, it would have been interesting to perform the same research on smartphones to investigate if the user experience differs from desktop environments and if users are more used to FIDO2 authentication on the smartphone. Perhaps more people use or are willing to use FIDO2 on smartphones in comparison to desktops, highlighting the importance of understanding user preferences across different platforms.

Long-Term Study on a Single Participant Group

A follow-up study with the same participants over a period of time could offer valuable insights. It would be interesting to ask the participants in a subsequent interview whether they adopted FIDO2 or not after becoming aware of the possibilities. Furthermore, it would have been interesting to explore whether participants' attitudes changed after several weeks or months compared to the 45 minutes we had with each participant. Future work should consider conducting a long-term study on a single participant group to observe if raising the awareness of FIDO2 contributes to increased adoption.

References

[App17] Apple, *About Touch ID advanced security technology*, https://support.apple.com/en-us/HT204587, as of Sunday 18th June, 2023, Sep. 2017.

[App21] Apple, Secure Enclave, May 2021. [Online]. Available: https://support.apple.com/no-no/guide/security/sec59b0b31ff/web (last visited: Jun. 18, 2023).

[Aut23] Auth0, Browser support, 2023. [Online]. Available: https://webauthn.me/browser-support (last visited: Jun. 10, 2023).

[AWAC20] F. Alqubaisi, A. S. Wazan, *et al.*, «Should We Rush to Implement Password-Less Single Factor FIDO2 Based Authentication?», URC '20, pp. 1–6, Apr. 2020.

[BRAM09] D. Bhattacharyya, R. Ranjan, *et al.*, «Biometric authentication: A review», *International Journal of u- and e- Service, Science and Technology*, vol. 2, Sep. 2009.

[Cre09] J. W. Creswell, «Research design: Qualitative, quantitative, and mixed methods approaches.», in Sage, 2009.

[CSBM17] B. Chakraborty, D. Sarma, *et al.*, «A review of constraints on vision-based gesture recognition for human-computer interaction», *IET Computer Vision*, vol. 12, Nov. 2017.

[CT19] R. Chowhan and R. Tanwar, «Password-less authentication: Methods for user verification and identification to login securely over remote sites», in Jan. 2019, pp. 190–212.

[DDC18] S. Das, A. Dingman, and L. J. Camp, «Why Johnny Doesn't Use Two Factor: A Two-Phase Usability Study of the FIDO U2F Security Key», in *Financial Cryptography and Data Security*, ser. FC '18, Nieuwpoort, Curacao: Springer, Feb. 2018, pp. 160–179.

[Dea23] B. Dean, Facebook Demographic Statistics: How Many People Use Facebook in 2023?, Mar. 2023. [Online]. Available: https://backlinko.com/facebook-users (last visited: Jun. 10, 2023).

[Dep12] P. Depot, Brute-force attacks, 2012. [Online]. Available: https://www.password-depot.de/en/know-how/brute-force-attacks.htm (last visited: Feb. 9, 2023).

[Duo23] C. Duo, The 2022 Duo Trusted Access Report, 2023. [Online]. Available: https://duo.com/resources/ebooks/the-2022-duo-trusted-access-report#anchor (last visited: Jun. 1, 2023).

[EW07] C. Ehmke and S. Wilson, «Identifying web usability problems from eyetracking data», *Paper presented at British HCI conference 2007*, Sep. 2007.

[FA17] F. Alliance, How FIDO Works, Jan. 2017. [Online]. Available: https://fidoalliance.org/how-fido-works/ (last visited: Feb. 1, 2023).

[FA20] F. Alliance, FIDO UAF Architectural Overview, Oct. 2020. [Online]. Available: https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html (last visited: Jun. 9, 2023).

[FA21a] F. Alliance, World's Largest Tech Companies Drive FIDO Alliance's New User Experience Guidelines, Jun. 2021. [Online]. Available: https://fidoalliance.org/fido-alliances-new-user-experience-guidelines/ (last visited: Mar. 13, 2023).

[FA21b] F. U. T. F. Members, FIDO Alliance: FIDO Desktop Authenticator UX Guidelines, Jun. 2021. [Online]. Available: https://fidoalliance.org/ux-guidelines/ux-guidelines-desktop-authenticators/ (last visited: Mar. 13, 2023).

[FA22a] F. Alliance, Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins, https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/, as of Sunday 18th June, 2023, May 2022.

[FA22b] F. Alliance, Certification Overview, Apr. 2022. [Online]. Available: https://fidoalliance.org/certification/ (last visited: Mar. 14, 2023).

[FA22c] F. Alliance, Changing the Nature of Authentication, Dec. 2022. [Online]. Available: https://fidoalliance.org/overview/ (last visited: Mar. 10, 2023).

[FA22d] F. Alliance, FIDO2: Web Authentication (WebAuthn), Feb. 2022. [Online]. Available: https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/ (last visited: Jun. 14, 2022).

[FA22e] F. Alliance, User Authentication Specifications Overview, Dec. 2022. [Online]. Available: https://fidoalliance.org/specifications/ (last visited: Mar. 14, 2023).

[FA23a] F. Alliance, FIDO Members, Jan. 2023. [Online]. Available: https://fidoalliance.org/members/ (last visited: Jun. 10, 2023).

[FA23b] F. Alliance, Passkeys, Feb. 2023. [Online]. Available: https://fidoalliance.org/passkeys/ (last visited: Feb. 9, 2023).

[FA23c] F. Alliance, What is FIDO?, Jan. 2023. [Online]. Available: https://fidoalliance.org/what-is-fido/ (last visited: Mar. 14, 2022).

[FHV14] D. Florêncio, C. Herley, and P. C. Van Oorschot, «Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts», in *USENIX Security Symposium*, ser. SSYM '14, San Diego, California, USA: USENIX, Aug. 2014, pp. 575–590.

[Fin10] K. Finstad, «The usability metric for user experience», *Interacting with computers*, vol. 22, no. 5, pp. 323–327, 2010.

[FLP16] M. Farik, N. Lal, and S. Prasad, «A review of authentication methods», *International Journal of Scientific & Technology Research*, vol. 5, pp. 246–249, Nov. 2016.

[FLPD22] F. M. Farke, L. Lassak, *et al.*, «Exploring User Authentication with Windows Hello in a Small Business Environment», in *Symposium on Usable Privacy and Security*, ser. SOUPS '22, Boston, Massachusetts, USA: USENIX, Aug. 2022, pp. 523–540.

[FLS+20] F. M. Farke, L. Lorenz, *et al.*, «"You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company», in *Symposium on Usable Privacy and Security*, ser. SOUPS '20, Virtual Conference: USENIX, Aug. 2020, pp. 19–35.

[Fly23] J. Flynn, 17 Essential Multi-Factor Authentication (MFA) Statistics [2023], Feb. 2023. [Online]. Available: https://www.zippia.com/advice/mfa-statistics/ (last visited: Jun. 10, 2023).

[GGF17] P. Grassi, M. Garcia, and J. Fenton, *Digital identity guidelines*, en, Jun. 2017. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63-3.

[Goo23a] A. Birgisson and D. Smetters, So long passwords, thanks for all the phish, Mar. 2023. [Online]. Available: https://security.googleblog.com/2023/05/so-long-passwords-thanks-for-all-phish.html (last visited: Mar. 20, 2023).

[Goo23b] Google, Titan Security Key, 2023. [Online]. Available: https://cloud.google.com/titan-security-key (last visited: Mar. 14, 2023).

[HA15] M. Hassaballah and S. Aly, «Face recognition: Challenges, achievements and future directions», *IET Computer Vision*, vol. 9, no. 4, pp. 614–626, 2015. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-cvi.2014.0084.

[Hel02] M. E. Hellman, «An overview of public key cryptography», *IEEE Communications Magazine*, vol. 40, no. 5, pp. 42–49, 2002.

[Hon12] J. Hong, «The state of phishing attacks», *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, 2012.

[II22] T. Issa and P. Isaias, «Usability and human–computer interaction (hci)», in *Sustainable Design: HCI, Usability and Environmental Concerns*. London: Springer London, 2022, pp. 23–40. [Online]. Available: https://doi.org/10.1007/978-1-4471-7513-1_2.

[ISO10] ISO, ISO 9241-210:2010(en) Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems, 2010. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-1:v1:en (last visited: Jun. 1, 2023).

[Jen22] B. K. Jena, What is Phishing Attack? Definition, Types and How to Prevent it, Feb. 2022. [Online]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-phishing-attack (last visited: Jun. 5, 2023).

[KL17] H. Kim and E. A. Lee, «Authentication and authorization for the internet of things», *IT Professional*, vol. 19, no. 5, pp. 27–33, 2017.

[KMJ18] T. Kakarala, A. Mairaj, and A. Javaid, «A real-world password cracking demonstration using open source tools for instructional use», pp. 0387–0391, May 2018.

[KZ10] H. Z. U. Khan and H. Zahid, «Comparative study of authentication techniques», *International Journal of Video & Image Processing and Network Security (IJVIPNS)*, vol. 10, no. 04, pp. 09–13, 2010.

[Lew12] J. Lewis, «Chapter 46: Usability testing», in Mar. 2012, pp. 1267–1312.

[LHAS14] Z. Li, W. He, *et al.*, «The Emperor's New Password Manager: Security Analysis of Web-based Password Managers», in *USENIX Security Symposium*, ser. SSYM '14, San Diego, California, USA: USENIX, Aug. 2014, pp. 465–479.

[LHGU21] L. Lassak, A. Hildebrandt, *et al.*, «"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn», in *USENIX Security Symposium*, ser. SSYM '21, Virtual Conference: USENIX, Aug. 2021, pp. 91–108.

[Lor20] N. Lord, Uncovering Password Habits: Are Users' Password Security Habits Improving?, Sep. 2020. [Online]. Available: https://www.digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic.

[LRH+09] L.-C. Law, V. Roto, *et al.*, «Understanding, scoping and defining user experience: A survey approach», Apr. 2009, pp. 719–728.

[LSN+20] S. G. Lyastani, M. Schilling, *et al.*, «Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication», in *IEEE Symposium on Security and Privacy*, ser. SP '20, Virtual Conference: IEEE, May 2020, pp. 268–285.

[McC22] C. McCart, Two-factor authentication statistics 2020-2022, Jul. 2022. [Online]. Available: https://www.comparitech.com/studies/data-breaches-studies/two-factor-authentication-statistics/ (last visited: Jun. 10, 2023).

[Mic23] Microsoft, What authentication and verification methods are available in Azure Active Directory?, Aug. 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods (last visited: Feb. 2, 2023).

[Nie00] J. Nielsen, «Why you only need to test with 5 users», Mar. 2000. [Online]. Available: https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/.

[Nie12] J. Nielsen, «Usability 101: Introduction to usability», Jan. 2012. [Online]. Available: https://www.nngroup.com/articles/usability-101-introduction-to-usability/.

[Nie20] J. Nielsen, «10 usability heuristics for user interface design», Nov. 2020. [Online]. Available: https://www.nngroup.com/articles/ten-usability-heuristics/.

[NIS22] NIST, NIST General Information, Mar. 2022. [Online]. Available: https://www.nist.gov/director/pao/nist-general-information.

[NIST] B.4 Authenticators and Verifiers. [Online]. Available: https://pages.nist.gov/800-63-3-Implementation-Resources/63B/Authenticators/ (last visited: Feb. 2, 2023).

[NM16] A. Nath and T. Mondal, «Issues and challenges in two factor authentication algorithms», *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, vol. 6, pp. 318–327, Jan. 2016.

[OAKU21] K. Owens, O. Anise, *et al.*, «User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators», in *Symposium on Usable Privacy and Security*, ser. SOUPS '21, Virtual Conference: USENIX, Aug. 2021, pp. 57–76.

[OGY+20] W. Oogami, H. Gomi, *et al.*, «Poster: Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones», in *Symposium on Usable Privacy and Security*, ser. SOUPS '20, Virtual Conference: USENIX, Aug. 2020.

[Okt23] Okta, Public Key Encryption: What Is Public Cryptography?, 2023. [Online]. Available: https://www.okta.com/identity-101/public-key-encryption/ (last visited: Mar. 15, 2023).

[PCKT19] A. Q. M. S. U. Pathan, A. Chakraborty, *et al.*, «Fingerprint authentication security: An improved 2-step authentication method with flexibility», *International Journal of Scientific and Engineering Research*, vol. 10, pp. 438–442, Jan. 2019.

[PMA22] M. Papathanasaki, L. Maglaras, and N. Ayres, «Modern authentication methods: A comprehensive survey», *AI, Computer Science and Robotics Technology*, Jun. 2022. [Online]. Available: https://doi.org/10.5772/acrt.08.

[PNP+16] P. Poornachandran, M. Nithun, *et al.*, «Password reuse behavior: How massive online data breaches impacts personal data in web», in *Innovations in Computer Science and Engineering: Proceedings of the Third ICICSE, 2015*, Springer, 2016, pp. 199–210.

[PSPP22] V. Parmar, H. A. Sanghvi, *et al.*, «A comprehensive study on passwordless authentication», pp. 1266–1275, 2022.

[PTN+17] S. Pearman, J. Thomas, *et al.*, «Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat», in *ACM Conference on Computer and Communications Security*, ser. CCS '17, Dallas, Texas, USA: ACM, Oct. 2017, pp. 295–310.

[PZB+19] S. Pearman, S. A. Zhang, *et al.*, «Why People (Don't) Use Password Managers Effectively», in *Symposium on Usable Privacy and Security*, ser. SOUPS '19, Santa Clara, California, USA: USENIX, Aug. 2019, pp. 319–338.

[SC09] S. Sagiroglu and G. Canbek, «Keyloggers: Increasing threats to computer security and privacy», *IEEE technology and society magazine*, vol. 28, no. 3, pp. 10–17, 2009.

[SDKP06] A. Seffah, M. Donyaee, *et al.*, «Usability measurement and metrics: A consolidated model», *Software Quality Journal*, vol. 14, pp. 159–178, Jun. 2006.

[SKD+16] R. Shay, S. Komanduri, *et al.*, «Designing Password Policies for Strength and Usability», *ACM Transactions on Information and System Security*, vol. 18, no. 4, 13:1–13:34, May 2016.

[Sny19] H. Snyder, «Literature review as a research methodology: An overview and guidelines», *Journal of Business Research*, vol. 104, pp. 333–339, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0148296319304564.

[Soe20] M. Soegaard, «Usability: A part of the user experience», Jul. 2020. [Online]. Available: https://www.interaction-design.org/literature/article/usability-a-part-of-the-user-experience.

[Sum22] N. Summers, Do you really need to change your password every 90 days?, Feb. 2022. [Online]. Available: https://blog.1password.com/should-you-change-passwords-every-90-days/ (last visited: Mar. 8, 2023).

[Tho23] P. Thorsheim, PasswordsCon 2023 Bergen, https://passwordscon.org/passwordscon-2023-bergen/, as of Sunday 18th June, 2023, May 2023.

[TRH+12] A. N. Tuch, S. P. Roth, *et al.*, «Is beautiful really usable? toward understanding the relation between usability, aesthetics, and affect in hci», *Computers in Human Behavior*, vol. 28, no. 5, pp. 1596–1607, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563212000908.

[USE23] USENIX, Symposium on Usable Privacy and Security 2023: Call for Posters, https://www.usenix.org/conference/soups2023/call-for-posters, as of Sunday 18th June, 2023, May 2023.

[W3C19] W3C, W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins, https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.en, as of Sunday 18th June, 2023, Mar. 2019.

[WAMG09] M. Weir, S. Aggarwal, *et al.*, «Password Cracking Using Probabilistic Context-Free Grammars», in *IEEE Symposium on Security and Privacy*, ser. SP '09, Oakland, California, USA: IEEE, May 2009, pp. 391–405.

[WPHH23] L. Würsching, F. Putz, *et al.*, «FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones», in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '23, Hamburg, Germany: ACM, Apr. 2023, 68:1–68:16.

[WS19] N. Woods and M. Siponen, «Improving password memorability, while not inconveniencing the user», *International Journal of Human-Computer Studies*, vol. 128, pp. 61–71, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1071581919300102.

[YM19] M. Yıldırım and I. Mackie, «Encouraging users to improve password security and memorability», *International Journal of Information Security*, vol. 18, Dec. 2019.

[Yub] Yubico, Platform and Roaming Authenticators. [Online]. Available: https://developers.yubico.com/Developer_Program/WebAuthn_Starter_Kit/Platform_and_Roaming_Authenticators.html (last visited: Feb. 3, 2023).

[Yub20] Y. Support, Can I duplicate or clone a YubiKey?, Sep. 2020. [Online]. Available: https://support.yubico.com/hc/en-us/articles/360016614880-Can-I-duplicate-or-clone-a-YubiKey- (last visited: Mar. 14, 2023).

[Yub21a] Yubico, What is CTAP?, Mar. 2021. [Online]. Available: https://www.yubico.com/resources/glossary/ctap/ (last visited: Jun. 9, 2023).

[Yub21b] Yubico, What is WebAuthn?, Nov. 2021. [Online]. Available: https://www.yubico.com/authentication-standards/webauthn/ (last visited: Jun. 9, 2023).

[Yub22a] C. Harrell, A Yubico FAQ about passkeys, May 2022. [Online]. Available: https://www.yubico.com/blog/a-yubico-faq-about-passkeys/ (last visited: Jun. 18, 2023).

[Yub22b] Yubico, What is a passkey?, Nov. 2022. [Online]. Available: https://www.yubico.com/resources/glossary/what-is-a-passkey/ (last visited: Jun. 15, 2023).

[Yub23a] Yubico, About us, Jun. 2023. [Online]. Available: https://www.yubico.com/about/about-us/ (last visited: Mar. 14, 2023).

[Yub23b] Yubico, Get started with YubiKey 5 Series, Jun. 2023. [Online]. Available: https://www.yubico.com/no/setup/yubikey-5-series/ (last visited: Mar. 14, 2023).

[Yub23c] Yubico, Google defends against account takeovers and reduces IT costs, 2023. [Online]. Available: https://www.yubico.com/resources/reference-customers/google/ (last visited: Mar. 16, 2023).

[Yub23d] Yubico, How the Yubikey works, Apr. 2023. [Online]. Available: https://www.yubico.com/why-yubico/how-the-yubikey-works/ (last visited: Mar. 14, 2023).

[Yub23e] Yubico, Press room, May 2023. [Online]. Available: https://www.yubico.com/press/ (last visited: Jun. 1, 2023).

[Yub23f] Yubico, Spare YubiKeys, Apr. 2023. [Online]. Available: https://www.yubico.com/products/spare/ (last visited: Mar. 14, 2023).

[ZA05] D. Zhang and B. Adipat, «Challenges, methodologies, and issues in the usability testing of mobile applications», *International Journal of Human–Computer Interaction*, vol. 18, no. 3, pp. 293–308, 2005. [Online]. Available: https://doi.org/10.1207/s15327590ijhc1803_3.

[Øse22] M. Øseth, «The future of passwords», Department of Information Security, Communication Technology, NTNU – Norwegian University of Science, and Technology, Project report in TTM4502, Dec. 2022.

Appendix

A Task Sheet Given to the Participants

Task Descriptions

Your name is John/Jane Doe, and you work for Digital Innovations. Your boss Sarah wants you to test some passwordless authentication features at Microsoft and eBay. The first tasks will be related to Microsoft/eBay, and you will get further instructions when you move on to eBay/Microsoft.

Task 1
Your first task is to set up a passwordless authentication method. You have the option to set up either a security key or fingerprint as the passwordless authentication method. Remove your password from your account, **if possible**.

Task 2
Next, Sarah wants you to sign in using the passwordless authentication method you just registered. For example, if you registered a security key, use it to sign in, and if you registered your fingerprint, use this as the sign-in method.

Task 3
Sarah wants you to set up the other passwordless authentication method you did not set up in the initial task. For example, if a security key was registered, set up a fingerprint in this task, and conversely.

Task 4
Finally, Sarah wants you to sign in using the passwordless authentication method you just registered.

Appendix B
Observation Scheme for Eye Tracking

The following two pages provide the observation schemes used under eye movement observations. One scheme is for Microsoft, and another is for eBay.

Microsoft

Participant ____

		Visual Scanning	Heading Attention	Focused Reading	Notes
Task 1	**Milestone 1** Locate security settings				
	Milestone 2b Find where to set up passwordless account				
	Milestone 3b Turn on passwordless account correctly				
	Milestone 2a - setup Find where to set up authentication method 1 security key / fingerprint				
	Milestone 3a - setup Set up authentication method 1 correctly				
Task 2	**Milestone 4 - sign in** Find where to sign in with authentication method 1				
	Milestone 5 - sign in Sign into Microsoft successfully with authentication method 1				
Task 3	**Milestone 2a - setup** Find where to set up authentication method 2 security key / fingerprint				
	Milestone 3a - setup Set up authentication method correctly				
Task 4	**Milestone 4 - sign in** Find where to sign in with authentication method 2				
	Milestone 5 - sign in Sign into Microsoft successfully with authentication method 2				

Observation Scheme for Eye Movement Observation

eBay

Participant ____

		Visual Scanning	Heading Attention	Focused Reading	Notes
Task 1	**Milestone 1** Locate security settings				
	Milestone 2 - setup Find where to set up authentication method 1 security key / fingerprint				
	Milestone 3 - setup Set up authentication method 1 correctly				
Task 2	**Milestone 4 - sign in** Find where to sign in with authentication method 1				
	Milestone 5 - sign in Sign into eBay successfully with authentication method 1				
Task 3	**Milestone 2 - setup** Find where to set up authentication method 2 security key / fingerprint				
	Milestone 3 - setup Set up authentication method correctly				
Task 4	**Milestone 4 - sign in** Find where to sign in with authentication method 2				
	Milestone 5 - sign in Sign into eBay successfully with authentication method 2				

Appendix C
Interview Guide

The following page provides the interview guide used during follow-up interviews. The questions were in Norwegian, but the answers were translated into English.

Interview Guide:

Participant number: _____

1) Hvordan synes du det gikk?

2) Har du hørt om passordløs autentisering før? Hvis ja, i hvilke forbindelser?

3) Visste du at det var mulig å logge inn på nettbaserte tjenester med passordløs autentisering, med andre ord helt uten passord? Hvis ja, i hvilke forbindelser?

4) Beskriv din opplevelse av å sette opp passordløs autentisering.

5) Beskriv din opplevelse av å logge inn med passordløs autentisering.

6) Sammenlign de to passordløse autentiseringsmetodene. Hvilken metode likte du best, og hvorfor?
    a) Security keyen må kjøpes av deg som bruker, hvor mye ville du vært villig til å betale for den?

7) Hvilke typer kontoer mener du passer best for passordløs autentisering, og hvorfor tror du disse kontoene er godt egnet for dette?

8) Hva er din opplevelse av sikkerhet og trygghet ved passordløs autentisering sammenlignet med passord-basert autentisering?

9) Har du noen tanker om hvordan passordløs autentisering kunne vært annerledes, som ville gjort det sannsynlig at du tok det i bruk?

10) Vil du anbefale passordløs autentisering til:
    a) En venn på din alder? Hvorfor/Hvorfor ikke?
    b) Dine foreldre?Hvorfor/Hvorfor ikke?

Kommentarer?

Appendix D
Consent Form

The following three pages provide the consent form approved by SIKT.

Samtykkeskjema

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å få innsyn i brukeropplevelsen ved passordløs autentisering. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Formålet med prosjektet er å undersøke brukeropplevelse av passordløs autentisering ved nettbaserte tjenester gjennom en brukertest og et intervju i etterkant. Prosjektet er utført i forbindelse med vår masteroppgave ved NTNU. Forskningsspørsmålet vi analyserer er hvilke hindringer i brukeropplevelse som påvirker utbredelsen av passordløs autentisering. Hovedhensikten med brukertesten er å samle inn brukeropplevelser tilknyttet bruk av passordløse autentiseringsmetoder.

Hvem er ansvarlig for forskningsprosjektet?
Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU Trondheim - kontakt@iik.ntnu.no
Veileder ansvarlig for prosjektet - Maria Bartnes maria.bartnes@sintef.no

Hvorfor får du spørsmål om å delta?
Vi ønsker å teste brukeropplevelsen ved passordløs autentisering på ti studenter ved studieprogrammet Kommunikasjonsteknologi og digital sikkerhet. Derfor er du, som student ved dette studieprogrammet, spurt om å delta.

Hva innebærer det for deg å delta?
Hvis du velger å delta i prosjektet, innebærer det at du løser et sett med oppgaver på en tildelt Mac og svarer på spørsmål i etterkant. I oppgaveløsningen vil du bruke fingeravtrykket ditt som en metode for å autentisere deg. Du vil bli spurt om å tenke høyt under oppgaveløsningen. Det vil ta deg ca. 45 minutter å delta. Spørsmålene i etterkant tar for seg dine erfaringer du gjorde underveis i brukertesten og dine meninger om passordløs autentisering.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Dersom du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Dersom du velger å trekke ditt samtykke vil all innsamlet data om deg slettes. Informasjon innsamlet og lagret vil kun være tilgjengelig for oss som er ansvarlig for prosjektet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Vi navngir deg med et deltakernummer, og ikke ved navn. Dette sørger for at du ikke vil bli gjenkjent i masteroppgaven. Opplysninger som samles inn:

- **Lyd- og skjermopptak** - Skjermopptaket inkluderer ikke bilde eller video av deg, men et opptak av skjermen og lyd. Vi bruker lyd- og skjermopptaket for å kunne notere ned hva du sier underveis i brukertesten, og koble det til hvor i oppgaveløsningen du var. Bruk av eventuelle sitater vil bli videre etterspurt og avtalt med deg som deltaker.
- **Fingeravtrykk** - For å gjennomføre testen må ditt fingeravtrykk registreres på Macen som brukes i gjennomføringen. Fingeravtrykket lagres da kryptert lokalt i Secure Enclave på Macen. Fingeravtrykket lagres ikke som et bilde, men som en matematisk representasjon. Det er ikke mulig å regenerere fingeravtrykket fra dataene som er lagret. Dine data slettes fra Macen umiddelbart etter testen er gjennomført og overføres aldri ut av maskinen som brukes. Fingeravtrykket vil bli brukt til å autentisere deg ved to nettbaserte tjenester: Microsoft og eBay.

Tiltak for å sikre at ingen uvedkommende får tilgang til personopplysninger:
- Vi oppbevarer dataen kortest mulig ved å behandle og slette lyd- og skjermopptak samme dag.
- Vi sletter fingeravtrykket umiddelbart etter testen, både fra Macen som brukertesten blir gjennomført på og som autentiseringsmetode på begge tjenestene, slik at deltakeren ser at det blir gjort.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke. Sikt – Kunnskapssektorens tjenesteleverandør, har vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Studenter ansvarlig for prosjekt: Ingunn Furuberg, ingunnlf@stud.ntnu.no og Marie Øseth, marioset@stud.ntnu.no
- Veileder ansvarlig for prosjektet: Maria Bartnes, maria.bartnes@sintef.no

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via e-post: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

Prosjektansvarlig (Forsker/veileder)

Studenter

_____ _____

Samtykkeerklæring

☐ Jeg har mottatt og forstått informasjon om prosjektet, og har fått anledning til å stille spørsmål. Jeg samtykker til å delta i brukertest og gjennomføre et intervju i etterkant.

_____

(Signert av prosjektdeltaker, dato)

Appendix E

Information Sheet for the Usability Test

The following page provides the information given to the participant after the consent form signature but before the start of the usability test.

Information Sheet

Ting som skal demonstreres - **Markert i grønt**

Velkommen til brukertest hvor vi skal se nærmere på passordløs autentisering! Denne brukertesten består av et sett oppgaver, etterfulgt av noen spørsmål som skal besvares. Vi skal teste brukeropplevelsen med passordløs autentisering, og ikke deg.

Vi begge vil være tilstede og ta notater underveis i brukertesten, så ikke bry deg om at vi sitter her. I tillegg vil _____ være ansvarlig for å gjennomgå informasjonen før brukertesten, veilede deg mellom oppgavene og stille spørsmål i etterkant.

(Consent form er signert, og vi kan da sette opp fingeravtrykket på macen, og starte lyd og skjerm-opptak)

Før vi begynner så vil vi forklare hva du har tilgang til av utstyr underveis i brukertesten:

- *Mac*
- *Mobil - Mer spesifikt kun Microsoft Authenticator inne på telefonen.*
- *Security key - Dette er en security key. Den kan brukes til passordløs autentisering. Den har en **USB-C inngang** på den ene siden, og en **lightning inngang** på andre siden. Lightning inngangen trenger du ikke bry deg om. Macen støtter **USB-C inngang på venstresiden**. Det finnes en berøringssensor på security keyen. **Denne brukes ved å berøre begge gulltappene samtidig**.*
- *Fingerprint - Fingerprint finner du **her**. Det kan brukes til passordløs autentisering. Den brukes ved å **berøre knappen** med fingeren du registrerte i starten.*

Følgende informasjon har du tilgjengelig dersom du skulle få behov. Dette er informasjon tilknyttet din fiktive konto på både Microsoft og eBay, to tjenester du kommer til å teste passordløs autentisering på. Vi har opprettet kontoene for deg på forhånd:

- *Brukernavn til tjenesten (Microsoft og eBay):*
- *Passord til tjenesten (Microsoft og eBay):*
- *PIN-kode security key:*
- *Passord til Mac:*
- *Microsoft Authenticator PIN-kode:*

Til slutt har vi følgende informasjon til deg:

- *Du vil i denne brukertesten få gitt noen oppgaver. Vi ber om at når du er ferdig med en oppgave, så sier du "Ferdig" til oss.*
- *Du kan trekke deg når som helst fra brukertesten*
- *Vi ønsker at du tenker høyt når du løser oppgavene. Fortell gjerne hva du ser på, tenker og føler mens du utfører oppgavene.*
- *Du vil ikke ha muligheten til å søke på Google, eller be oss om hjelp underveis i testen.*

Før vi starter testen, har du noen spørsmål?

Appendix F
Lightning Talk at PasswordsCon 2023

We presented our master thesis at PasswordsCon in Bergen 15th of May 2023. The password conference lasted for two days. Figure F.1 shows a picture of us when we presented our master thesis at the conference. On PasswordsCon's webpage [Tho23], all speakers are listed with uploaded presentation slides, including ours.

Figure F.1: Presentation at PasswordsCon 2023.

Appendix G

Poster submission accepted to the SOUPS 2023

The following page provides a poster we submitted to Symposium on Usable Privacy and Security (SOUPS) 2023, in response to their Call for Posters [USE23]. We submitted the poster on May 25th, 2023, and it was accepted for the SOUPS 2023 poster session on June 8th, 2023. We are excited to have the opportunity to present our poster at SOUPS 2023 conference, which will take place in Anaheim, CA, USA, in August 2023.

From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2

Ingunn Furuberg, Marie Øseth, Maria Bartnes, and Lillian Røstad

NTNU
Norwegian University of Science and Technology

1 MOTIVATION

Previous work [1] indicates that FIDO2-based passwordless authentication is more usable and secure

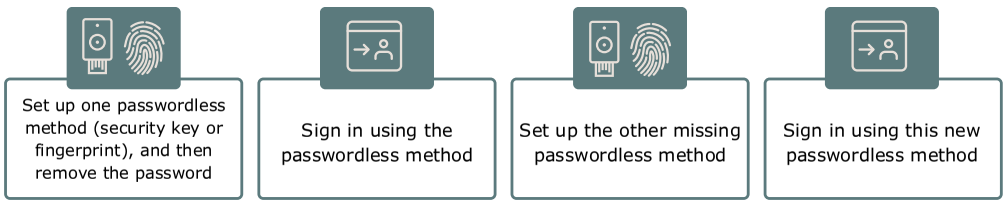
Apple, Google, and Microsoft recently committed to the protocol by expanding their support through passkeys

Research Question:
What obstacles related to user experience hinder the widespread adoption of FIDO2?

2 METHOD

Usability study with a follow-up interview.
Four **tasks** being performed on two online services:

ebay
Microsoft



Usability Factors

- Ease of Use
- Effectiveness
- Trustfulness
- User Satisfaction

3 RESULTS

Awareness:
2/10 participant had knowledge of the possibility of passwordless authentication on the Web

Perceptions:
Found it trustworthy. Perceptions varied, depending on whether the participants were already using passwordless authentication

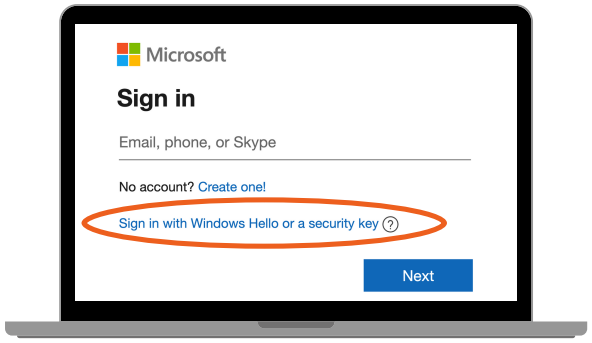
Interface:
Missing out on important information which makes setup and sign-in processes less efficient and experience less user-friendly

4 DISCUSSION

Lack of Information:
Due to a lack of information from services, users were unaware of passwordless authentication options

Poor Interface for Setup/Sign-in:
Small text and unclear instructions made the processes less user-friendly

Simplifying the Transition:
Process to change security settings manually was seen as a barrier



[1] S. Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel.
Is FIDO2 the Kingslayer of User Authentication?
A Comparative Usability Study of FIDO2 Passwordless Authentication.
In IEEE Symposium on Security and Privacy, May 2020.
[2] Microsoft Corporation, microsoft.com
[3] eBay Inc., ebay.com

NTNU
Norwegian University of
Science and Technology