USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

From TOTPs to Security Keys: Studying the Reality of Passwordless FIDO2 Authentication With PIN and Biometrics in a Corporate Environment

Leona Lassak, Nicklas Lindemann, and
Marvin Kowalewski, *Ruhr University Bochum*

https://www.usenix.org/conference/soups2025/presentation/lassak

This paper is included in the Proceedings of the
Twenty-First Symposium on Usable Privacy and Security.

August 11–12, 2025 • Seattle, WA, USA

ISBN 978-1-939133-51-9

Open access to the Proceedings of the
Twenty-First Symposium on Usable Privacy and Security
is sponsored by USENIX.

From TOTPs to Security Keys: Studying the Reality of Passwordless FIDO2 Authentication With PIN and Biometrics in a Corporate Environment

Leona Lassak
Ruhr University Bochum

Nicklas Lindemann
Ruhr University Bochum

Marvin Kowalewski
Ruhr University Bochum

Abstract

Phishing remains a major threat to companies. Many organizations use multi-factor authentication (MFA) methods like SMS or TOTPs which unfortunately still leave them vulnerable to attacks and even add cognitive, physical, and time strain for employees. Passwordless authentication with FIDO2 security keys could offer a promising alternative with strong phishing resistance and better usability, yet real-world adoption in corporate settings is underexplored. In a five-week field study at a mid-sized IT company, we compared security keys (PIN and biometrics) to passwords with TOTPs using authentication logs, surveys, and interviews with 34 employees. While biometric security keys reduced login times by nearly five seconds, PIN-based keys were not significantly faster. Despite this, and despite usability challenges such as hardware compatibility, employees were significantly more satisfied with both on-device authentication methods. Security perception remained unchanged, as employees already considered existing authentication secure. Critically, overall inconsistencies and complexities of authentication workflows were frequently criticized, suggesting that the authentication method itself may not always be the core issue and highlighting the need for organizations to analyze root causes of problems before adopting new authentication methods as quick fixes for fundamentally flawed infrastructures.

1 Introduction

Companies are a primary target of cyberattacks and their frequency steadily rises over the years [16]. Social engineering-based attacks, particularly phishing, pose one of the greatest threats to organizations [6, 14], often serving as an entry point for more severe attacks like ransomware [14]. While these attacks affect organizations of all sizes, small and medium-sized enterprises (SMEs) are especially vulnerable due to limited resources for implementing and maintaining robust IT infrastructures [4, 16, 19, 40].

Authentication forms a cornerstone of securing companies' infrastructures, assets, and valuable information. Yet, despite continuous efforts to strengthen the authentication landscape, current measures still fail to adequately defend against phishing attacks. Even modern two- or multi-factor authentication (2FA/MFA) methods, such as (time-based) one-time passwords (TOTPs), explicitly developed to counter phishing, have repeatedly been circumvented [7, 29, 42]. Additionally, these measures put strain on employees by increasing the complexity of the authentication process, negatively impacting employee satisfaction, and often leading to circumvention strategies that ultimately undermine the security benefits [38].

The FIDO Alliance's FIDO2 authentication standard (also known as *passkeys*) marks a significant advancement in the fight against phishing. FIDO2 enables public key-based phishing-resistant web authentication entirely without passwords ("passwordless"), using different authenticators, such as security keys and device-internal biometrics. Though recently synced multi-device credentials were introduced (storing private keys in the cloud), traditionally FIDO2 credentials are "device bound" (stored only on the creation device, e.g., a security key). Early studies with end users in controlled environments show an overall positive impression of both security keys [26] and biometrics-based FIDO2 [23]. However, the challenges and requirements companies face differ substantially from those of individual users, emphasizing the need to study FIDO2 adoption in organizational contexts explicitly. Farke et al. [13] conducted one of the first studies on security key usage in a small business with eight employees. However, their study was limited in size and only covered technical employees. Their findings highlighted issues such as increased authentication times due to necessary PIN entries, and overall

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.

infrequent usage of the security keys altogether. Building on this work, we aimed to investigate FIDO2 security key deployment in a larger and more diverse organizational setting. Our study was conducted in a real-world corporate environment at a medium-sized IT service provider, with an infrastructure reflecting modern multi-factor authentication practices. We systematically compare employees' experiences with and opinions about authentication using the standard password and TOTP to FIDO2 security keys using both PIN and biometrics for on-device authentication. More specifically, we explore the following research questions:

RQ1: How satisfied are employees with the different methods and what are major usability drawbacks?

RQ2: How secure do employees feel with different methods and are they aware of the security implications?

RQ3: What overall problems could companies encounter when introducing security keys?

Our findings showed that security keys significantly increase employee satisfaction, despite PIN-based keys offering little speed improvement compared to *PWD+OTP*. Biometric keys reduced login times by about five seconds. Despite technical issues like hardware compatibility, employees mostly preferred the new methods. Perceived security, however, remained relatively unchanged, as employees already considered the existing system secure. Critically, many challenges stemmed from inconsistent authentication workflows rather than the authentication method itself, highlighting the need to address structural issues before introducing new solutions.

2 Background & Related Work

Next, we provide background on multi-factor logins (MFA), Time-based One Time Passwords (TOTPs), and FIDO2.

2.1 Multi-Factor Authentication

Multi-factor authentication (MFA) is designed to strengthen security, particularly against phishing attacks, mitigating the risks associated with traditional single-factor authentication (1FA), where security depends solely on the confidentiality of a password. In organizations, regulations often mandate two- or multi-factor authentication to protect valuable infrastructures [11, 18]. Additional authentication factors come in various forms, including hardware tokens like smartcards, short-lived PINs sent via email or SMS, and cryptographic time-based one-time passwords (TOTPs).

Time-Based One-Time Passwords (TOTPs) TOTPs are cryptographically generated, time-bound credentials [28] which dynamically change at fixed intervals (usually every 30 seconds), thereby invalidating previously generated TOTPs. To generate TOTPs, the user's device and the authentication server exchange a secret key during enrollment. To compute the TOTP, the shared secret is then combined with a time-based counter, derived from the current time and the predefined time interval. The authentication server independently calculates the expected TOTP and verifies whether the submitted code matches its own generated value. In practice, TOTPs are typically generated in authenticator apps (e.g., Google or Microsoft Authenticator [27]) on personal devices like smartphones but can also be generated via other means such as dedicated hardware tokens, or password managers.

Although TOTPs as second factors harden the resilience against common phishing attacks, they are not entirely phishing-resistant [7, 29, 42]. The mechanism is still vulnerable to social engineering techniques such as spear-phishing, tricking employees into disclosing both their password and a valid TOTP [41]. Additionally, attackers can deploy automated Adversary-in-the-Middle (AitM) attacks [43]. By intercepting and relaying a compromised password and its corresponding TOTP within the valid time window attackers can establish a legitimate session for targeted accounts.

2.2 FIDO2

Developed by the FIDO Alliance, FIDO2 (Fast IDentity Online) is a W3C standard for passwordless web authentication, consisting of the *Client-to-Authenticator-Protocol* (CTAP2) and the *Web Authentication Protocol* (WebAuthn). CTAP2 defines the communication between the client platform (i.e., the web browser) and an authenticator (i.e., hardware security key). WebAuthn standardizes the communication between the client platform and a relying party (i.e., a website). FIDO2 is based on public key cryptography. On registration, authenticator and relying party exchange public keys, which the authenticator uses to sign challenges to authenticate the user. The signature is verified using the previously exchanged keys. Critically, contrary to passwords, FIDO2 does not rely on a *shared secret*, replacing the factor knowledge with the factor possession. The credentials are uniquely tied to the relying party, making them resistant to phishing, replay attacks, and server-side credential breaches.

To the authenticator, users authenticate using a PIN or biometric factors. There are two types of authenticators: *Platform authenticators* are integrated into devices and can be used with, e.g., Apple Face ID, Windows Hello, and Android. In this case, cryptographic keys are stored in the devices' trusted platform modules (TPM) or trusted execution environments (TEE). *Roaming authenticators* are platform-independent and can therefore be used across devices. The most common roaming authenticators are USB hardware tokens, or "security keys," such as Yubico's Yubikey [46] or Google's Titan Key [17]. Originally, FIDO2 credentials were "device-bound," meaning they were bound to the device they were created on and could not be extracted from it. With *Passkeys*, so-called "multi-device" or "synced" credentials were introduced, which are synchronized across devices via the cloud.

They primarily address concerns about fallback and usability issues with device-bound credentials [15]. As of now, FIDO2 is supported by all major browsers and operating systems including Apple, Microsoft, and Google [10].

2.3 Related Work

Next, we outline research on passwordless FIDO2 logins, especially in companies and user studies about security keys.

2.3.1 Passwordless FIDO2 in Companies

Farke et al. conducted one of the first employee-focused field studies on FIDO2 security keys in a small company, examining their potential to replace traditional passwords [13]. Over four weeks, eight employees could optionally sign in using their existing passwords or newly introduced security keys. Many participants abandoned the security keys during the study, as logging in with password managers proved significantly faster. The study also highlighted usability challenges, a lack of user awareness regarding security benefits, and technical limitations within the company's infrastructure.

Another five-week study by Farke et al. replaced password-based device logins with biometric Windows Hello in a small business with 13 employees [12]. Participants preferred Windows Hello for usability and speed. However, many opted for PINs instead of biometrics, mostly due their workplace setup (e.g., biometric hardware on the table was out of reach).

Kepkowski et al. assessed FIDO2 in workplaces with 118 professionals, revealing challenges with integrating FIDO2 in businesses due to complex authentication landscapes [21]. Key issues included a lack of know-how and tool sets, no standardized account recovery processes, high costs, and the absence of native integration for credential delegation.

Through interviews with CISOs, authentication managers, and FIDO2 experts, Lassak et al. [24] identified complexity and friction when integrating FIDO in existing deployments, technical issues like browser incompatibility and supporting legacy software, as well as poor security culture and regulatory requirements as additional hurdles to widespread deployment.

2.3.2 Passwordless FIDO2 with End Users

About 100 participants favored security keys in a lab study by Lyastani et al., who examined their potential to replace passwords for end users [26]. Still, users expressed concerns about losing account access if the key was lost and missed the option to use it on devices without USB ports. Authors concluded that concerns may hinder widespread adoption despite overall higher usability and acceptance than passwords.

Using smartphones as roaming authenticators, Owens et al. compared a prototype implementation to passwords with 97 participants [33]. The overall setup suffered from usability shortcomings beyond FIDO itself, yielding poor usability ratings. Nonetheless, participants recognized the security benefits but raised concerns about recovery and availability.

Early on, Oogami et al. investigated *biometrics*-based passwordless FIDO2 on ten participants' personal Yahoo! Japan accounts, finding issues with the user interface such as a fingerprint icon being mistaken for the fingerprint reader [31].

Lassak et al. studied misconceptions about biometric FIDO2 [23]. 42 online participants revealed their understanding of data storage, data protection, and mental models, generally perceiving it as more secure than password logins. Yet, 67% mistakenly believed their fingerprint was sent to the relying party. Educational notifications co-designed in subsequent focus groups, partially mitigated those misconceptions.

2.3.3 Security & Usability of Security Keys

The following summarizes the main findings from studies investigating security keys. The majority studied security keys for two-factor authentication [5, 8, 22, 34, 35], two for primary authentication [13, 26]. The studies compared the keys to passwords [13, 26, 34], SMS-based (T)OTPs [5, 22, 34], TOTPs on smartphones [22, 34], and other security keys [5, 22]. Five studies tested them in a lab environment [5, 9, 26, 34, 35], and another five did long-term field assessments between two and four weeks, mostly accompanied by manual diaries [5, 13, 22, 34, 35]. Four specifically studied the setup process [5, 9, 34, 35]. The remainder focused on everyday usage.

The initial impression of the keys was often positive, described by words like "easy," "usable," and "intuitive" [13, 26]. However, other studies, especially concerning the setup process, reported negative impressions as well [5, 9, 35]. Users often needed guidance during the setup phase. A common concern was the lack of easily accessible, specific setup instructions [5, 9], particularly for real-world applications where 2FA had to be activated before being able to use the keys [5].

Once users successfully completed the setup, they consistently highlighted the ① reduced cognitive workload compared to password-based logins as a key advantage [13, 26]. Additionally, they praised the ② faster login time compared to regular passwords [26], and other 2FA methods like SMS-based OTPs, and smartphone generated TOTPs [5, 34].

However, the keys also introduced new concerns, primarily related to the ③ physical effort required, as the key must always be available and thus carried by the user. Participants criticized its ④ small size [5, 35], which contributes to the risk of ⑤ loss or ⑥ breakage, raising fears of being locked out of an account when relying on security keys [5, 9, 12, 34, 35]. Additionally, users had problems due to ⑦ the limited number of or ⑧ hard-to-reach USB ports, and ⑨ the hardware incompatibility with mobile devices [9, 26, 35].

Throughout the studies participants, typically understood that the keys increase security somehow but rarely were able to explain why [5, 13, 35]. In the context of 2FA, participants typically attributed the security gain simply to the additional

factor not the key in particular (i.e., saying "extra layer of protection"). Barely anyone knew about their phishing-resistance.

Participants were split about using the keys in their personal lives. Many simply perceived no need for "*extra security*" [9, 22, 35]. Others argued with the fear of losing account access or were afraid someone else could access their account if the security key would not be protected further [26]. Some considered them well-suited for sensitive or high-value accounts (like banking or at work) [5, 13, 34, 35].

3 Methodology

In this section, we describe our surveys and interviews, demographic and recruitment information, and ethical considerations. The main goal of this work was to *measure* users' experiences with security keys in a real-world corporate environment compared to the previously used authentication with passwords and TOTPs (*PWD+OTP*). The study was conducted in a medium-sized IT service company in Germany with 34 employees between April and May 2024.

3.1 Study Concept

We introduced two main phases: 1) testing the traditional authentication (*PWD+OTP*) for one week, and 2) testing the security key-based authentication both with a PIN and biometrics-enabled security keys for two weeks respectively (four weeks in total). Figure 1 shows a high-level overview of the study procedure. Concretely, the following steps:

Recruitment & Kick-off. We recruited from multiple departments and interested employees were invited to a virtual kick-off meeting (cf. details in Section 3.5).

Phase 1. For one week, everyone continued using their regular login method, a combination of password and TOTP. At the end of the week, we sent a questionnaire instructing participants to answer within a few days and consequently scheduled individual interviews. This data forms the baseline for comparison with Phase 2 results.

Phase 2. After concluding Phase 1, all participants were asked to switch their login method to security keys. Note: Everyone had already received the key directly after consenting to participate which allowed a seamless and quick transition. To assist participants with the setup, we provided a written and illustrated step-by-step guide. In case of issues, participants were free to contact the researchers at any time for further assistance. For four weeks, participants then used the key for their regular authentication. We tested both PIN and fingerprint for on-device authentication. After two weeks, participants switched from PIN to biometrics, or vice versa, depending on the method they had started with (which was randomly assigned at the beginning of the study). Again, participants received short questionnaires, both after week two and four, to capture both authentication methods and were invited to a second interview. To respect participants' time and effort, we refrained from conducting two interviews for the security keys.

Conclusion. At the end of the last interview, we thanked everyone for their participation. Employees were free to choose whether or not to switch back to the password or continue using the security key. We also offered participants help with performing the rollback.

3.2 Testing Environment

The study was conducted in the company's production environment. All employees used notebooks provided by the company (MacOS or Windows 11) with their chosen browser. Employees were registered through the MFA software, which provides Single-Sign On (SSO) for integrated services. However, some services (e.g., customer-specific services) were not integrated with the software and thus had individual authentication processes. Per the company policy, all integrated services required multi-factor, except for the Intranet which only required a password. Remotely, employees connected to the network via VPN which could not be integrated with the MFA solution either and required its own login.

Original Setup All employee accounts were protected by two authentication factors: Password and TOTP. The one-time passwords were typically generated on the employee's smartphone (private or company phones). Very few used explicit hardware tokens to generate TOTPs (one participant in the study). While specific smartphone apps for TOTP generation were encouraged by the company, some employees opted for other means of token generation like KeePassXC [20], which adds the TOTP seed directly into the password manager and auto-fills the TOTP during logins. Employees could use password managers provided via the company software platform on their own terms, but they were not actively promoted. Saving passwords in the browser was explicitly prohibited.

Security Key Setup For the study, the company bought Yubico's *Yubikey Bio Series* [48], which allows both PIN and fingerprint authentication. With biometrics enabled, the key combines the presence check and authentication by requiring the user to tap the fingerprint sensor. The PIN is still in use as a fallback if the fingerprint is not recognized after three attempts. The key supports either USB-A or USB-C connectivity. The keys replaced *PWD+OTP* for the time of the study. Once participants had finished the local security key setup, administrators automatically switched them via the IAM (Identity and Access Management) solution at the beginning of Phase 2. Unfortunately, services that were not integrated with the MFA software did not support FIDO2 authentication yet so participants continued using password and TOTP even during Phase 2. However, most did not use any

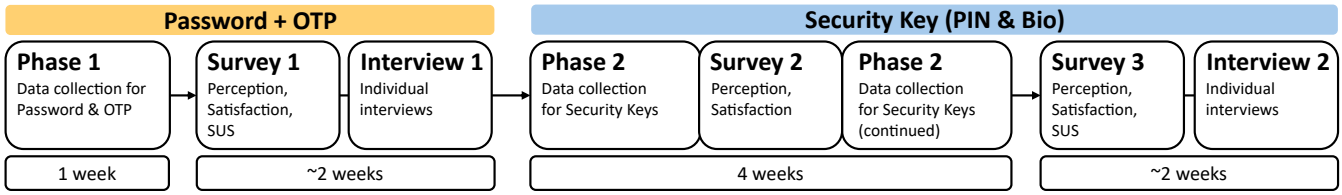

Figure 1: Overview of study timeline. Interviews were scheduled over two weeks to accommodate participants' availability.

of these services, as they were primarily department- or role-specific (e.g., Jira for developers, personnel file management for HR).

3.3 Questionnaires

To ensure comparability between ratings for *PWD+OTP* and security keys, we asked the same set of questions in all three surveys, only adjusting the wording slightly to match the respective login method. To minimize participants' time commitment, and because we gained deeper, qualitative insights through the interviews later on, most survey questions were closed-ended 5-point Likert scales. The full surveys are provided in Appendix A and covered the following topics:

Usability. We first asked participants about their overall satisfaction with the login process, login duration, and frequency of logins per day, as well as their estimates of login duration. Using an open-ended question, we inquired about potential problems participants may have encountered. To facilitate comparison across different authentication systems, we also incorporated the System Usability Scale (SUS) [3], a validated scale for measuring the perceived usability of technical systems.

Security. We first generally asked how secure participants felt using each mechanism and explicitly inquired about their perceptions of phishing resistance, as this is one of the main security advantages of security keys.

Demographics. Lastly, we collected participants' age, job title, and name, to link survey responses with interviews. The author who conducted the surveys and interviews worked at the company, so by nature these parts were not anonymous. However, all results were anonymized before being shared with team members outside the company which is further detailed in our Ethics section 3.6.

3.4 Interviews

We conducted interviews to substantiate survey answers and collect further qualitative insights. Hence, the interviews overall followed the same structure and covered similar topics as the survey but were semi-structured in nature depending on the topics participants primarily talked about. Interviews were limited to 30 minutes. Due to this time restriction we did not talk about every survey question with every participant. We began each interview by asking about the general experience with the respective login method, independent of what participants had answered in the survey to ensure an unbiased impression. All interviews were conducted in German and the conversations took place via Microsoft Teams. If participants agreed, the interviews were audio-recorded, and transcribed using *Whisper*, an AI language model running locally on the researchers' device [32]. These transcriptions were then manually corrected and subsequently coded. Quotes have been translated into English to the best of our ability. The full interview guides can be found in Appendix B.

3.5 Recruitment, Demographics, & Analysis

Recruitment Initially, participants were recruited via the company-wide IT-Board. The head of the IT department advertised the study during a meeting with other department and team leads, asking them to identify employees from their teams who may be interested in participating. This allowed us to easily reach especially non-technical departments, as we aimed to include a diverse range of backgrounds like economics, management, and human resources. For departments and teams where this recruitment strategy was unsuccessful, we approached the respective managers directly. We then invited interested employees to a virtual meeting where we provided information about the study (i.e., the study's purpose, duration, and procedure) and answered questions. The consent form was attached to the invitation, and participants were asked to sign it to confirm their participation. Subsequently, we sent out security keys to participants' work addresses.

Demographics 34 participants joined the study. About $\frac{3}{4}$ were male (26; 76%), roughly $\frac{1}{4}$ were female (8; 24%). No one identified as non-binary. Few participants were young adults 18 – 25 (3; 9%), the majority was 26 – 35 (11; 32%) or 36 – 45 (10; 29%) years old. Some were 46 – 55 (6; 18%) and older than 55 (4; 12%). The majority worked in engineering (20; 59%), eight in HR (24%), three in management (9%), and three in marketing (9%). The vast majority used macOS (29; 85%), while five participants used Windows 11 (15%). The surveys were completed by 34 (*PWD+OTP*), 26 (Security Key - *PIN*), and 31 (Security Key - *Bio*) participants respectively. 25 participants agreed to have their interviews recorded in Phase 1 (*PWD+OTP*) and 24 in Phase 2. The remainder was not documented and therefore is not part of the results.

Analysis Authentication logs were extracted from the company's MFA software and included user names, as well as timestamps and used methods of login events. These logs allowed us to derive login durations, frequencies, and (partially) failure rates. For FIDO, however, authentication failures are handled by the operating system and therefore do not appear in the MFA software. Each authentication event in the logs began when the participant entered their username and pressed enter, and ended when the authentication was successful.

For the open answers and interview results, we followed an open-coding process, adding codes to the codebook as they emerged. One researcher created the initial codebook, which was subsequently applied by two researchers independently.

3.6 Ethics

As our department did not have an institutional review board, we could not obtain official ethics approval. Instead, we strictly followed best practices of human subjects research such as defined in the Menlo Report as well as data protection guidelines including the EU's General Data Protection Regulation (GDPR). Before the study, we obtained participants' informed consent, informing them about the types and purposes of data collection, how the data is processed, and who gets access to it. Results were pseudonymized before being shared with company-external research team members. In agreement with their respective supervisors, the study was conducted during participants' working hours without additional compensation, which was clearly communicated before the study. Participants were free to withdraw from the study at any time without reason or penalty.

3.7 Limitations

Due to the complex authentication infrastructure in the company, testing the security keys only covered parts of employees' daily logins. We communicated this fact to participants in surveys and interviews and tried separating the feedback accordingly, but we acknowledge that it likely affected their opinion about security keys overall.

Any human subjects research including surveys and interviews can be affected by social desirability biases which can be amplified in the work context as participants might feel pressured to answer in the interest of their employer. To minimize this, we explained that participants' answers will not be shared with colleagues or supervisors, and that all data will be pseudonymized before analysis.

Interviews were scheduled for approximately 20 to 30 minutes to respect participants' time commitment. However, this time was not always sufficient to discuss all questions which may have caused us to miss some valuable insights. Not all participants were available for the entire four-week period due to vacations and sick days. Two participants mistakenly used security keys with biometrics the entire four weeks. Their data was consequently only used for the biometrics evaluations. Despite efforts, our sample skewed engineering-heavy so opinions of a broader sample may differ slightly.

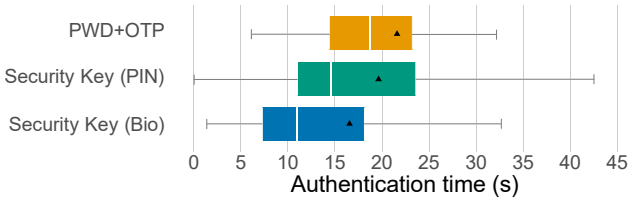

Figure 2: Login times without outliers by method.

Usability ratings, especially SUS scores, depend on many factors beyond the login method itself (e.g., study setup and environment). Therefore, ratings may differ substantially between studies and should only be interpreted within the study context. Lastly, the limited study duration likely did not cover challenging scenarios with possession-based credentials which only emerge after longer usage periods.

4 Results

The following presents our findings from authentication logs, surveys, and interviews. We first report login frequencies and durations for each mechanism, substantiating them with participants' ratings and open answers. Subsequently, we present participants' perceptions of security and phishing resistance.

4.1 Login Duration & Frequency

The authentication logs provide an objective view of login frequencies and durations. During Phase 1, we collected login events from 33 participants. For Phase 2, we analyzed login events from 32 participants (one participant dropped out after Phase 1). Table 1 provides an overview of the login events for all three authentication methods. In Phase 1 (*PWD+OTP*), which lasted only one week, we recorded a total of 255 successful login events. For Phase 2, the 4-week period where participants used security keys, we collected a total of 355 login events, 284 of which used security keys. 128 of those used the PIN, and 156 used biometrics. The remainder used *PWD+OTP* (i.e., due to late switches).

The average login with *PWD+OTP* took about $M = 21.6\,s$. Logins using security keys with PIN took on average $M = 19.6\,s$ and logins with biometrics took $M = 16.5\,s$. This is also shown in Figure 2. The measured differences were not statistically significant ($F(2,185) = 2.59, p = .078$).

Perception of Login Duration & Frequency In the surveys, we also asked participants to *estimate* the average login duration (cf. Figure 3). This is interesting because the perceived time reflects employees' satisfaction and sense of strain. A task may take the same amount of time objectively

Table 1: Login count and mean login duration by method.

Method	Count	Time
Password only	139	7.54 s
↪ OTP only	57	17.63 s
PWD+OTP	59	21.59 s
Security Key (PIN)	128	19.63 s
Security Key (Bio)	156	16.54 s

but feel more demanding, gradually depleting the limited compliance budget everyone has [1]. Participants estimated logins with *PWD+OTP* to take $M_{est} = 26.3\,s$ on average, which is about five seconds longer than the actual time authentications took ($M_{real} = 21.6\,s$). For logins using security keys with PINs, participants estimated $M_{est} = 14.6\,s$ and only $M_{est} = 11.6\,s$ with biometrics. This corresponds to almost half (*PIN*) and more than half (*Bio*) of the estimated time for *PWD+OTP* logins. Additionally, in both cases, the perceived duration was about five seconds *shorter* than the actual login time (*PIN:* $M_{real} = 19.6\,s$; *Bio:* $M_{real} = 16.5\,s$).

4.2 Satisfaction

In this section, we report participants' overall satisfaction with the authentication mechanisms, including SUS scores.

Overall Satisfaction Figure 4 shows that participants' overall satisfaction was lowest for *PWD+OTP*. The average rating was $M = 2.74$. For security keys overall, the average rating was $M = 3.63$, although biometrics-enabled keys were rated slightly higher ($M = 3.70$) than PIN-enabled keys ($M = 3.56$). Critically, the number of extremely dissatisfied and dissatisfied users reduced from 44% with *PWD+OTP* to about 20% with security keys. The few dissatisfied participants either experienced major technical issues with the security key itself or were unsatisfied with the overall authentication infrastructure, which we report more about in Section 4.3. The number of extremely satisfied or satisfied users increased from 21% (*PWD+OTP*) to 59% with security keys (PIN) and even up to 70% with security keys (Bio). According to Friedman rank sum's ($\chi^2(2) = 11.595, p = .003$) post-hoc analysis, the difference between biometrics and *PWD+OTP* ($p = .007$) is significant, while the differences between PIN and *PWD+OTP* ($p = .248$) and PIN and biometrics ($p = .566$) are not.

We also compared usability ratings by job type. There were no differences between technical and non-technical employees for *PWD+OTP* (Tech: $M = 2.75$, Non-Tech: $M = 2.71$) and security keys with PINs (Tech: $M = 3.59$, Non-Tech: $M = 3.50$), but ratings for security keys with biometrics were slightly higher among technical participants (Tech: $M = 3.80$, Non-Tech: $M = 3.50$).

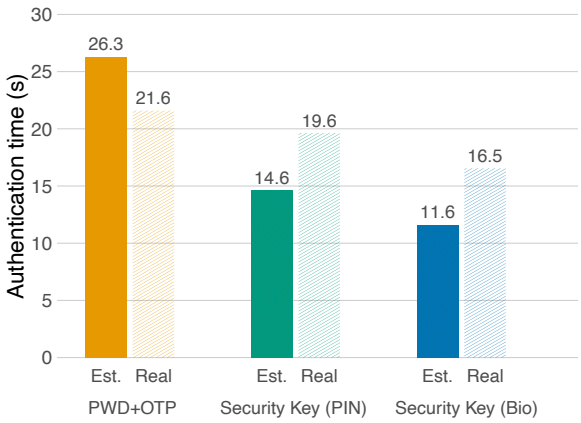

Figure 3: Estimated login times by method ("*Est.*"). Real login times for reference ("*Real*").

SUS Scores The System Usability Scale (SUS) allows for a standardized comparison of usability ratings. In our study, ratings for *PWD+OTP* ranged from 30 to 95 with a mean value of 60 ($SD = 15.70$). This rates *PWD+OTP* with the grade D (poor) [25]. Security keys were rated between a score of 43 and 100, with a mean score of 84 ($SD = 15.06$), corresponding to the grade A (excellent). This difference is statistically significant ($t(30) = -7.161, p < .001$). SUS scores were slightly lower for non-technical employees both with *PWD+OTP* (Tech: $M = 61.50$, Non-Tech: $M = 56.78$) and security keys (Tech: $M = 85.13$, Non-Tech: $M = 82.95$).

Satisfaction with Login Duration Looking only at participants' satisfaction with the login duration (cf. Figure 5), the difference between methods is even more pronounced. More than 60% of participants were dissatisfied or extremely dissatisfied with the duration of the login using *PWD+OTP*, with an average rating of $M = 2.47$. Contrary to that, with security keys, over 50% of the participants were satisfied or extremely satisfied with the login duration. Only 11% reported being dissatisfied with biometrics-enabled security keys ($M = 4.07$) and 18% with PIN-enabled keys ($M = 3.57$). These differences were also significant (Friedman rank sum: $\chi^2(2) = 27.071, p < .001$). Both PIN and Biometrics were ranked significantly higher than *PWD+OTP* (PIN: $p = .007$, Bio: $p < .001$) but were not significantly different from each other ($p = .483$). While job roles uniformly rated *PWD+OTP* (Tech: $M = 2.50$, Non-Tech: $M = 2.42$) and security keys with biometrics (Tech: $M = 3.68$, Non-Tech: $M = 3.55$), this time non-technical participants rated security keys with PINs noticeably lower (Tech: $M = 4.18$; Non-Tech: $M = 3.67$).

Future Use 15 participants intended to continue using security keys, especially with biometrics *"I'll definitely continue using it. And I'll use it with biometrics."* (P1). Two participants expressed this intention conditional on broader support

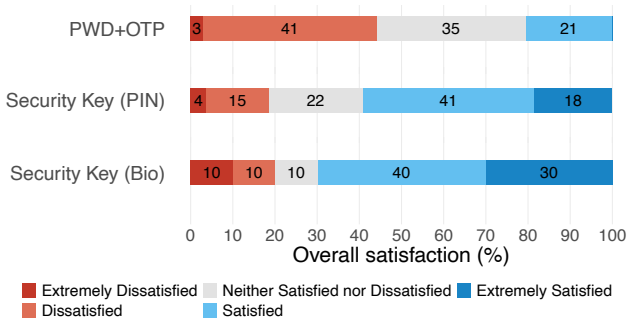

Figure 4: Overall satisfaction by method.

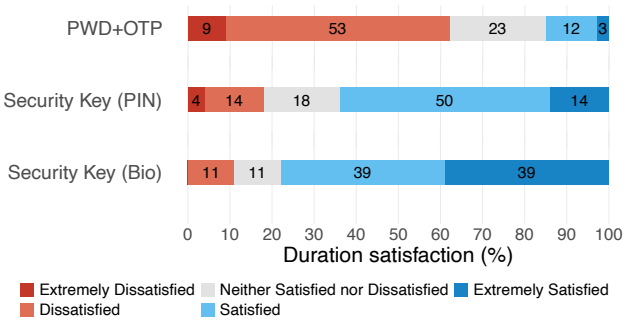

Figure 5: Satisfaction with login duration by method.

across all applications to avoid having to use multiple different login methods simultaneously *"if the security key would be universal for all applications, I could imagine [to use it]"* (P11), *"I would like to keep it if it completely replaces this password + OTP"* (P7).

4.3 Usability Drawbacks

Next, we report problems participants encountered and how they thought the login process could be improved. The codebooks are shown in Appendix C.1.

4.3.1 Password + TOTP

We identified four main usability drawbacks with *PWD+OTP*.

Smartphone Handling. The TOTP generation on the smartphone most frequently impacted the usability negatively ($n = 7$). Having to *"get out the authenticator every time"* (P5) especially when the smartphone is *"lying somewhere else"* (P5), was repeatedly mentioned as an annoyance. P18 summarized their dissatisfaction with *PWD+OTP* as *"It's about finding your cell phone, having your cell phone at the workplace, unlocking it – that's what it's all about."*

App Handling. Multiple participants ($n = 5$) also reported that they have stored many TOTPs in their authenticator app, which required them to scroll through a long list to find the correct token. P18 said they have to *"look up the OTP from a long list [...] This means that for my 30 logins, I first have to search for the [correct account]. That's what annoys me."*

Password Quantity & Complexity. Unsurprisingly, some participants ($n = 3$) criticized the need to remember multiple distinct passwords with high complexity requirements[1] that need to be used daily (*"So basically four or five passwords that aren't exactly short, which I somehow have to have ready at the same time."* (P25)). While some participants use local password managers to save their passwords, one reported that it helped them with password management but when *"the password is in KeePass*[2]*, then I'm out of luck because I have no way of accessing the passwords from my mobile devices"* (P55). Therefore, password managers that do not have a synchronization feature do not seem to remedy the password management problems sufficiently.

TOTP Setup Complicated. While not part of the study itself, multiple participants ($n = 3$) reported various problems with the process of adding a TOTP to their accounts. The setup was rated not intuitive (*"And yes, I also found the setup somehow not so intuitive"* (P81)) and complex (*"I found setting it up quite extensive"* (P97)). Some also reported problems with switching their TOTP generation to another smartphone.

4.3.2 Security Keys

Despite the overall higher satisfaction with security keys, participants encountered several usability issues.

Security Key Transportation. A total of $n = 10$ participants were concerned about the transportation of the security key between different work locations (i.e., home office and workplace). While smartphones were seen as devices that are rarely forgotten, security keys were considered more easily forgotten as they only serve the purpose of authentication at work. P7 reported that they *"forgot it once and then [they were] stuck and could no longer access the intranet."* P19 did not forget the key but noticed *"you always have to make sure that you carry it with you and don't forget it,"* and mentioned that they were *"looking for it for five minutes already before [they] found it."* Some participants attached the security key to their key ring at the expense of having the bulky key ring hanging from the USB port. Leaving the security key in the USB port was not considered a viable option due to the risk of breaking it during transportation. A few participants considered the security key poorly suited for when they have to move between different workplaces during the day.

Operating System Popups. FIDO2 authentication popups on the device are dictated by the operating system and cannot

[1] The company policy required a minimum of twelve characters, using at least three of the four character types (capital and lower case letters, numbers, symbols). Using parts of names or the company name was prohibited.

[2] *KeePass* is an open source password manager which stores passwords in an encrypted database locally on the user device. Synchronizing with other devices is not supported (natively). [20].

be influenced by the company. The popups ask the user which FIDO2 sign-in option to use. However, the interface does not offer setting a default, so users have to explicitly select the security key from the list each time they log in. Many ($n = 10$) did not understand why and were annoyed that multiple options were even offered (*"I just found it annoying that Windows [...] asks every time, do you want to use smartcard or FIDO, [...] every time, even though I don't have anything else in there."* (P17)). They also criticized that there was no default option (*"I don't know why Windows doesn't save the default method"* (P21)) and were annoyed by the popups making them select the same options repeatedly.

USB Slot Availability. Multiple users ($n = 6$) reported a shortage of suitable USB ports on their notebooks. Without using a docking station, only the device's built-in USB ports are available, typically used for headset, mouse, keyboard, or smartphone charging (*"I had to decide, okay, what do I connect to the last slot?"* (P7)). One participant argued that *"It's not that complicated, but you do have to organize it a bit, I would say,"* (P21) indicating this to be a fixable issue, but still adding a task not required with *PWD+OTP*.

USB Type of Security Key. The type of the USB connector was another annoyance ($n = 2$). While everyone found a way to handle the issue, many noted potential usability issues using USB-A security keys. Some changed from a Lenovo notebook to a MacBook and had no USB-A ports available without a docking station or USB hub. Some considered using the security key with their smartphone, which was impossible with only the USB-A key (*"But I couldn't do that with my iPhone because I have the A-key, not the C-key."* (P18)). Both scenarios can be mitigated by providing keys compatible with the company's common hardware setup. For instance, all modern company-issued laptops have at least one USB-C port or will be upgraded to devices with USB-C ports soon. However, this must be considered before deploying keys to larger groups of employees, particularly in a diverse hardware environment, and requires a proper company-wide strategy.

Desk Setup. Two participants struggled reaching the security key when plugged into the notebook or docking station which were positioned behind their displays. One solved the issue by connecting a USB hub to their notebook, the other suggested providing a USB extension cable together with the security key (*"So, if you add any kind of extension, then I'll keep it."* (P18)).

Poor Fingerprint Recognition. Eight participants struggled with the fingerprint recognition. While four reported sporadic non-recognition, more frequent than they are used to by their smartphone, one participant's sensor did not work most of the time. The majority, however, had no issues.

Fear of Breakage. In the literature, fear of breakage is often reported as a major concern [5, 26]. In our study, surprisingly few participants ($n = 3$) mentioned this aspect (*"I am always scared to break it"* (P62)), potentially because, unlike in lab studies, participants experienced its robustness in real-world conditions while using it over an extended period.

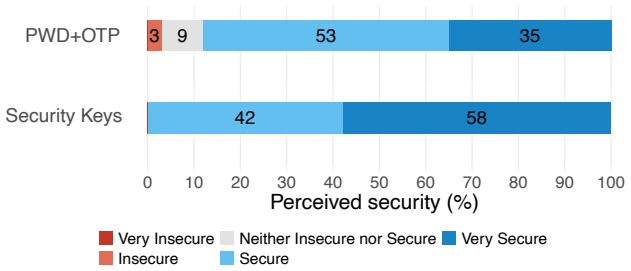

Figure 6: Ratings of perceived security across methods. Numbers on plots are in percentages.

4.3.3 Convoluted Authentication Infrastructure

Regardless of the authentication method, participants ($n = 12$) frequently criticized the need to log in multiple times a day due to the lack of single sign-on (SSO) integration across many services. *"I think it would be cool if you didn't have to do both, but could just go to the key instead,"* as P19 described the issue. For many services in the organization, integration would technically be feasible. Frequent login prompts can reduce users' attention to phishing cues and increase their susceptibility to MFA fatigue attacks [39, 49]. Therefore, expanding SSO adoption could not only improve usability and employee satisfaction but also help mitigate security risks.

4.4 Perception of Security

We also investigated participants' perceived security and how it differed between methods. Figure 6 shows the distribution of responses. Participants generally felt very secure with either of the methods. Only a single person indicated feeling insecure with *PWD+OTP*. Nonetheless, the ratings for security keys were still noticeably higher with 58% selecting "very secure" compared to only 29% for *PWD+OTP*. Below we describe participants' reasoning for their feelings and provide the codebooks in Appendix C.2.

4.4.1 Password + TOTP

Separate Secure Device. Many participants ($n = 10$) attributed the perceived security of *PWD+OTP* to having a second physical device (the smartphone), which is locked with a passphrase or pattern known only by the owner (*"This means that no one will probably be able to unlock the cell phone without your cooperation."* (P10)). Participants imagined a potential attacker would need physical access to the device to steal a TOTP (*"You would also have to have access to my company cell phone and know the code for it and then find the right app to retrieve [...] a current code there."* (P28)).

MFA in General. Seven participants ($n = 7$) felt secure due to the mere presence of a second, separate factor. They emphasized that the addition of a second factor improves security, with one noting that even if the password is compromised, it would *"not be useful"* (P44) without the second factor.

Trust in Decision Makers. Two participants felt secure because they trusted the IT department's decisions. P7 explained: that *"[it's the] trust in other people. I think [...] something will have been thought up to ensure that this is safe."* P1 said *"If I can't trust our people, then I no longer know who to trust"* regarding making educated choices for a secure authentication mechanisms.

TOTPs can be Phished. Two participants admitted fearing that they might enter the TOTP on a phishing site if they failed to recognize the website as such. They explained that they *"do not check the URL line every time"* (P21) and are also not aware of *"which domains belong to [company name]"* (P84).

Missing SSO & UI Inconsistencies. Adding to the usability concern surrounding inconsistent authentication infrastructures, this was also perceived as a security threat. One participant argued that *"the number of logins should be reduced"* because *"this also has something to do with susceptibility to phishing"* (P84). P22 pointed out that UI inconsistencies like differing login masks can increase the likelihood that users enter their credentials on phishing sites.

Software TOTP Location. Two rather tech-savvy participants pointed out that the security of the TOTP largely depends on how the seed is stored. P55 argued that *"If you now store the password and the second factor in the same place, then you only have one factor, so to speak"* and therefore criticized generating TOTPs in the password manager. P5 commented that many employees, especially students and apprentices, use private smartphones to generate TOTPs. They considered this the *"biggest security risk."* but were unable to explain why they perceived this to be a risk.

4.4.2 Security Keys

Password Threat Removed. Reflecting their main purpose, three participants noted that security keys eliminate passwords and thereby one fundamental security threat *"the password complexity is no point of attack anymore"* (P22).

Fingerprint Felt More Secure. One participant perceived that *"copying a fingerprint is a bit [...] more complicated and technically complex"* (P1). Another rated the fingerprint as more secure, a typical misconception with biometric authentication (*"because I would think that my PIN, which is always the same, could somehow theoretically be found out by someone"* (P19)). However, as the PIN is always available as the fallback, attackers can use it any time. Hence, biometrics are never "more secure," but just as secure as their fallback.

Dedicated Cryptographic Device. In contrast to multi-purpose devices like smartphones, one participant attributed the security of security keys to them being a *"special cryptographic device"* (P18).

Positive Media Coverage. Lastly, one participant who was personally interested in IT news, remembered positive articles about security keys and therefore felt safe using them (*"Now if you have Heise*[3] *articles saying that's totally great, if there are many voices saying that security keys are safe and usable, then I trust them, the mass media [...]"* (P20).

PIN is New Weakness. Five participants perceived the PIN which users choose for the security key as a new possible weak spot. P22 said that it *"only shifts the password problem of writing it down"* and that *"[people] can't remember a four-digit PIN and write them on pieces of paper and stick them on their cards or in their wallet."*

Fear of Theft & Loss. Only $n = 3$ participants feared theft or loss of the security key, which again is surprisingly few compared to related literature [5, 26]. Participants who had the concern argued that compared to smartphones, security keys are smaller and used less frequently and thus an attacker might *"pull the thing out in a thoughtless moment"* and the victim will *"only realize the next day that his key is gone"* (P17). Simply losing the security key without any malicious intent was also mentioned once.

4.4.3 Perception of Phishing Resistance

One of FIDO's core security benefits is phishing resistance, which we also explored. Nine participants correctly deemed *PWD+OTP* as susceptible to phishing. However, five of those simply did not associate the term phishing with authentication, believing phishing is just "clicking on a link." Therefore, they did not connect *PWD+OTP* with phishing prevention, thinking the topics are unrelated. Ten participants rated *PWD+OTP* as somewhat phishing-resistant. Some of those ($n = 4$) correctly understood the technical details of TOTPs, explaining that sophisticated attackers can forward stolen TOTPs via proxies, exploiting the valid time window, though arguing that this increases the complexity of attacks compared to only having passwords. Five incorrectly rated it as phishing-resistant due to the two-factor nature and the perceived "complexity" of exploiting the double authentication.

Six participants rated security keys as phishing-resistant, correctly understanding the technical details ($n = 5$) or highlighting that the attacker would need physical access to the key to use it. Eight participants did not believe security keys were phishing-resistant. Six of them assumed that if they were on a phishing website and complied with its requests, they would be just as vulnerable as with *PWD+OTP*. The remainder again did not associate phishing with authentication.

[3] Popular German technology news website (https://www.heise.de/).

5 Discussion

In the following sections, we discuss our findings.

5.1 Login Duration & Employee Satisfaction

While in other studies security key logins are typically faster than logins using other methods [5, 34], our study does not fully align with these findings. Participants were about five seconds faster when using security keys with biometrics, but barely faster when using security keys with PINs. This finding aligns with Farke et al., who found security keys to be substantially slower than passwords, particularly when they were auto-filled with password managers [13]. In most studies, security keys were investigated as second factors, and were compared to out-of-band 2FA mechanisms like SMS which may have higher latencies. Additionally, in some studies, security keys were used with only a "presence check" without the need to enter a PIN. While this can be considered sufficiently secure for 2FA, it would be highly undesirable for primary authentication, as in that case possession of the security key alone would grant account access [26, 35].

Measured vs. Perceived Usability. Despite the relatively small measurable time differences, employees were significantly more satisfied with security keys. While only one in five participants was extremely satisfied with *PWD+OTP*, 60% to 70% expressed the highest level of satisfaction when using security keys. The increased satisfaction likely correlates with the *perception* that authentication with security keys was faster than with passwords. This interpretation is also supported by the notable shift in satisfaction with the *login duration*: Only 15% were satisfied or very satisfied with the duration of *PWD+OTP*, compared to 50% with security keys. Considering that security keys were objectively not much faster, this highlights the importance of measuring the perception, even if it may not fully align with the reality. One might argue that perceived speed matters less than measured speed, however, research shows that employee satisfaction (which seems to correlate more with perceived than measured speed) is strongly linked to motivation and productivity [2, 37].

5.2 Addressing Usability Drawbacks

While some usability drawbacks are inherently linked to security keys, many can be mitigated through proper setup and planning by the company.

Device Transportation & Loss. Participants were mainly concerned with transporting and correctly storing the security keys. Keeping them on a key ring did not fully resolve these concerns, as it introduced new issues. Interestingly, unlike previous studies [5, 13, 26], fear of losing the key, which is closely related to transporting and storing it correctly, was rarely mentioned. This may be because *PWD+OTP* technically remained available throughout the testing period, though this was not explicitly pointed out to participants. Participants were however informed that the support hotline could quickly restore access if needed. From the company's perspective, fallback authentication and account recovery remain challenges. To fully unfold the security benefits of FIDO2, security keys need to be adopted completely and *PWD+OTP* must be disabled entirely. Recently, the FIDO standard rapidly advances towards broad support for (synced) platform authenticators (passkeys) [15] which might be able to mitigate risks of losing (device-bound) security keys and thereby accelerate both account recovery and deployments of new credentials. The company we studied was open to exploring passkey-based logins but emphasized the need for a provider that supports multiple platforms (i.e., MacOS, Windows, Linux, iOS). They highlighted that thorough testing is required before drawing conclusions about the suitability of any provider and noted the complexity of the authentication landscape making it hard to decide for or against any type of passkey (cf. Section 5.3). In any case, companies must establish a process for securely restoring access and minimizing downtime if a key is lost. Additionally, providing clear, well-structure guidance for employees is crucial to minimize uncertainty and promote secure practices and thereby prevent workarounds and reduce replacement needs.

Hardware Availability. Participants also struggled with limited USB slots. While there are security keys with connectors like NFC, universal adoption is unlikely since most notebooks support USB but not necessarily NFC. Limited USB slots will likely remain an issue across organizations and can only be mitigated by providing adequate hardware setups, such as docking stations or USB extensions. When introducing security keys, companies must ensure that all devices intended for authentication are compatible. In our case, USB-C was the most common shared connection type.

PIN Memorization. With biometrics-enabled security keys, users rarely need their PINs. Some participants quickly forgot the PIN after setting up biometrics, leading to security key resets and necessary account recovery assistance. This creates effort for employers and can cause frustration for employees. To mitigate this risk, companies should establish guidelines for proper PIN management, such as using a company-endorsed password manager.

OS Popups. Another annoyance were the repetitive FIDO2 OS popups. While keyboard shortcuts could technically offer a quick workaround, they are not a practical solution for most users. The FIDO standard supports disallowing entire authenticator types (e.g., platform authenticators) which consequently would prevent them from appearing as login options [44]. However, for this to work in practice, IAM software that administrators rely on must support this feature. Still, such system-wide deactivation, though possible in theory, is not always feasible in practice. For instance, it may conflict with local platform authentication methods like Windows Hello if they are enabled. Authentication providers should

allow administrators to specify whether roaming authenticators, platform authenticators, or both are permitted and ideally offer the option to set default authenticators.

5.3 Quick Fixes for Flawed Infrastructures?

The most frequent criticism was the lack of single sign-on (SSO) integration for many company services. While this problem already existed before the switch to security keys, it became more pronounced afterward. Previously, employees used the same authentication method (password and TOTP) just with different passwords across systems, whereas now they had to switch between *PWD+OTP* for non-integrated services and security keys for integrated services. This led to a vastly inconsistent user experience, with six participants explicitly mentioning wanting to switch back to passwords and TOTP after the study to maintain a consistent login experience, despite preferring the security keys overall. In some cases, the lack of FIDO2 support is unavoidable due to legacy software [21, 24]. Replacing such systems is often costly or infeasible, requiring alternative authentication methods. However, in the tested company, legacy services accounted for only a small portion of non-SSO systems. Companies need to minimize these exceptions and integrate them into risk assessments to balance security and cost. Proactively addressing SSO integration gaps is vital to ensuring a positive user experience and preventing frustration. Simply rolling out a new authentication mechanism, such as security keys, without addressing underlying inconsistencies in the authentication infrastructure is unlikely to be a sustainable solution.

5.4 Security

Unclear Security Benefits. The security ratings between the two login methods were relatively similar, primarily because *PWD+OTP* was already perceived as secure due to its two-factor nature. Still, participants felt equally or even more secure using security keys despite them *not* being a clearly separate second factor. The underlying phishing resistance of security keys is not obvious so it is unsurprising that participants did not realize their security benefits. Therefore, explicitly communicating these benefits in company-wide roll-outs is necessary to foster employees' understanding of changes to the login procedure and to help them correctly understand what attacks security keys protect from but also which attack vectors they still need to be careful about.

Concerns About PIN Complexity. Some participants raised concerns about short and weak PINs. FIDO shifts the attacker model from online threats to physical and local attackers, significantly reducing the overall attack surface. However, in corporate environments, targeted attacks are more likely than for average users, making concerns about the security of four-digit PINs valid. While security keys implement mitigations like rate limiting (i.e., resetting to factory settings after eight failed attempts [45]), this may not be sufficient for every use case. The security keys used in this study only support four-digit PINs without customizable complexity requirements. While employers can define organizational policies, some employees may still choose weak PINs nonetheless. Stronger security keys with more stringent PIN requirements could mitigate this risk but are often more expensive [47] and introduce additional complexity to the authentication landscape if not deployed uniformly to all employees. Ultimately, organizations must carefully weigh this risk against the security benefits of adopting security keys.

5.5 Future Work

Comparing to Ideal Password Setups. Passwords are a known-to-be-disliked authentication standard, so positive feedback for a new mechanism was expectable. Despite real-world constraints of existing environments, studying security keys compared to *best practice-based* password setups, e.g., using company-wide password managers, and following usable password creation rules [30] (complexity, length requirements) would be valuable to establish a fair comparison [36].

Synced Passkeys in Companies. With the FIDO standard evolving towards (synced) platform authenticators, future work could explore perceptions of security, usability benefits (e.g., easier transport, no USB-slot dependency), and potential privacy concerns with centralized syncing and cross-platform challenged in corporate settings.

Long-term Monitoring. Our study revealed several usability issues that can be addressed at the organizational level. Long-term studies with improved authentication setups could provide insights into the impact of these changes and surface issues with security keys that only emerge over time.

6 Conclusion

In this work, we evaluated the usability and perceived security of passwordless FIDO2 security keys in a corporate setting. Through surveys, interviews, and authentication logs, we compared security keys using PIN and biometrics with traditional passwords and TOTPs. Our findings revealed that biometric security keys significantly increased user satisfaction, with 70% of participants expressing approval compared to just 21% for password and TOTP. While FIDO2 keys seem promising for reducing login times, PIN-based keys were not notably faster. Usability challenges, including hardware compatibility and inconsistent authentication workflows, mostly seemed solvable through proper planning and preparation. We also highlighted the critical need for organizations to address underlying infrastructure problems before adopting new authentication methods. The results underline the potential of passwordless authentication with FIDO2 to improve security and user experience, provided that organizations first tackle root causes of authentication problems.

References

[1] Adam Beautement, M. Angela Sasse, and Mike Wonham. The Compliance Budget: Managing Security Behaviour in Organisations. In *New Security Paradigms Workshop*, NSPW '08, pages 47–58, Lake Tahoe, California, USA, September 2008. ACM.

[2] Clement Bellet, Jan-Emmanuel De Neve, and George Ward. Does Employee Happiness Have an Impact on Productivity? *Management Science*, 70(3):1656–1679, May 2023.

[3] John Brooke. SUS: A Quick and Dirty Usability Scale. *Usability Eval. Ind.*, 189, 1995.

[4] Alladean Chidukwani, Sebastian Zander, and Polychronis Koutsakis. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus, and Recommendations. *IEEE Access*, 10:85701–85719, August 2022.

[5] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 339–356, Santa Clara, California, USA, August 2019. USENIX.

[6] European Council. Top Cyber Threats in the EU. www.consilium.europa.eu/cyber-threats-eu, as of June 10, 2025.

[7] Cybersecurity and Infrastructure Security Agency (CISA). Implementing Phishing-Resistant MFA, 2023. www.cisa.gov/phishing-resistant-mfa, as of June 10, 2025.

[8] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The Tangled Web of Password Reuse. In *Symposium on Network and Distributed System Security*, NDSS '14, San Diego, California, USA, February 2014. ISOC.

[9] Sanchari Das, Andrew Dingman, and L. Jean 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*, FC '18, pages 160–179, Nieuwpoort, Curacao, February 2018. Springer.

[10] Alexis Deveria ("Fyrd") and Community. Support of the Web Authentication API on Mobile Devices, 2025. www.caniuse.com, as of June 10, 2025.

[11] The European Parliament and the Council of the European Union. Regulation (EU) 2015/1502 on Setting Out Minimum Technical Specifications and Procedures for Assurance Levels for Electronic Identification Means, 2015. www.eur-lex.europa.eu, as of June 10, 2025.

[12] Florian M. Farke, Leona Lassak, Jannis Pinter, and Markus Dürmuth. Exploring User Authentication with Windows Hello in a Small Business Environment. In *Symposium on Usable Privacy and Security*, SOUPS '22, pages 523–540, Boston, Massachusetts, USA, August 2022. USENIX.

[13] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In *Symposium on Usable Privacy and Security*, SOUPS '20, pages 19–35, Virtual Conference, August 2020. USENIX.

[14] Federal Bureau of Investigation (FBI) – Internet Crime Complaint Center. Internet Crime Report 2024, December 2024. www.ic3.gov/AnnualReport, as of June 10, 2025.

[15] FIDO Alliance. Apple, Google, and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins, 2022. www.fidoalliance.org, as of June 10, 2025.

[16] Bundesamt für Sicherheit in der Informationstechnik (BSI). The State of IT Security in Germany, November 2024. www.bsi.bund.de/Lagebericht, as of June 10, 2025.

[17] Google. Titan Security Key, 2025. www.google.com/titan-security-key, as of June 10, 2025.

[18] International Organization for Standardization. ISO/IEC 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements. Standard ISO/IEC TR 29110-1:2016, International Organization for Standardization, Geneva, Switzerland, 2022.

[19] Carlos Rombaldo Junior, Ingolf Becker, and Shane Johnson. Unaware, Unfunded, and Uneducated: A Systematic Review of SME Cybersecurity. *arXiv preprint arXiv:2309.17186*, 2023.

[20] KeePassXC. KeePassXC, 2025. www.keepassxc.org, as of June 10, 2025.

[21] Michal Kepkowski, Maciej Machulak, Ian Wood, and Dali Kaafar. Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study. In *IEEE Secure Development Conference*, SecDev '23, pages 37–48, Atlanta, Georgia, USA, October 2023. IEEE.

[22] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. In *Symposium on*

Network and Distributed System Security, NDSS '15, San Diego, California, USA, February 2015. ISOC.

[23] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *USENIX Security Symposium*, SSYM '21, pages 91–108, Virtual Conference, August 2021. USENIX.

[24] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In *USENIX Security Symposium*, SSYM '24, pages 7231–7248, Philadelphia, Pennsylvania, USA, August 2024. USENIX.

[25] James R. Lewis and Jeff Sauro. Item Benchmarks for the System Usability Scale. *Journal of Usability Studies*, 13(3):158–167, 2018.

[26] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy*, SP '20, pages 268–285, Virtual Conference, May 2020. IEEE.

[27] Microsoft. Download Microsoft Authenticator, 2024. www.microsoft.com/mobile-authenticator-app, as of June 10, 2025.

[28] David M'Raihi, Sven Machani, Marc Pei, and Mingliang Nystrom. TOTP: Time-Based One-Time Password Algorithm. RFC 6238, May 2011.

[29] Allan Muir, Kymani Brown, and Anteneh Girma. Reviewing the Effectiveness of Multi-Factor Authentication (MFA) Methods in Preventing Phishing Attacks. In *Proceedings of the Future Technologies Conference*, pages 597–607. Springer, November 2024.

[30] National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Lifecycle Management, June 2017. www.nist.gov/memorized-secret-verifiers, as of June 10, 2025.

[31] Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, and Tatsuru Higurashi. Poster: Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones. In *Symposium on Usable Privacy and Security*, SOUPS '20, Virtual Conference, August 2020. USENIX.

[32] OpenAI. Introducing Whisper, September 2022. www.openai.com/whisper, as of June 10, 2025.

[33] Kentrell Owens, Blase Ur, and Olabode Anise. A Framework for Evaluating the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Who Are You?! Adventures in Authentication Workshop*, WAY '20, pages 1–5, Virtual Conference, August 2020.

[34] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A Usability Study of Five Two-Factor Authentication Methods. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 357–370, Santa Clara, California, USA, August 2019. USENIX.

[35] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent E. Seamons. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *IEEE Symposium on Security and Privacy*, SP '18, pages 872–888, San Francisco, California, USA, May 2018. IEEE.

[36] Scott Ruoti, Brent Roberts, and Kent Seamons. Authentication Melee: A Usability Analysis of Seven Web Authentication Systems. In *The World Wide Web Conference*, WWW '15, pages 916–926, Florence, Italy, May 2015. ACM.

[37] Alam Sageer, Sameena Rafat, and Puja Agarwal. Identification of Variables Affecting Employee Satisfaction and Their Impact on the Organization. *Journal of Business and Management*, 5(1):32–39, 2012.

[38] M. Angela Sasse, Michelle Steves, Kat Krol, and Dana Chisnell. The Great Authentication Fatigue – And How to Overcome It. In *Cross-Cultural Design*, pages 228–239. Springer International Publishing, 2014.

[39] Peter Snyder, Michael K Reiter, and Chris Kanich. The Effect of Repeated Login Prompts on Phishing Susceptibility. In *Learning from Authoritative Security Experiment Results*, LASER '16, pages 13–19, San Jose, California, USA, 2016. USENIX.

[40] Assion K. Tetteh. Cybersecurity Needs for SMEs. *Issues in Information Systems*, 25(1):235–246, 2024.

[41] Kurt Thomas and Angelika Moscicki. New Research: How Effective Is Basic Account Hygiene at Preventing Hijacking, 2019. www.googleblog.com/account-hijacking, as of June 10, 2025.

[42] Zhi Wang, Xin Yang, Du Chen, Han Gao, Meiqi Tian, Yan Jia, and Wanpeng Li. Simple But Not Secure: An Empirical Security Analysis of Two-factor Authentication Systems. *arXiv preprint arXiv:2411.11551*, 2024.

[43] Alex Weinert. Defeating Adversary-In-The-Middle Phishing Attacks, 2024. www.microsoft.com/aitm-phishing-attack, as of June 10, 2025.

[44] World Wide Web Consortium. Web Authentication: An API for Accessing Public Key Credentials - Level 2, 2021. www.w3.org/webauthn-2, as of June 10, 2025.

[45] Yubico. Protocols and Applications, 2025. www.docs.yubico.com/protocols, as of June 10, 2025.

[46] Yubico. The YubiKey, 2025. www.yubico.com, as of June 10, 2025.

[47] Yubico. YubiKey 5 FIPS Series, 2025. www.yubico.com/yubikey-fips, as of June 10, 2025.

[48] Yubico. YubiKey Bio Series, 2025. www.yubico.com/yubikey-bio-series, as of June 10, 2025.

[49] Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. SoK: Human-Centered Phishing Susceptibility. *arXiv preprint arXiv:2202.07905*, 2022.

A Surveys

A.1 Survey 1 – PWD+OTP

C – Consent

[We only show an excerpt of the consent form due to space constraints.]

Purpose: This project is being conducted at [company] with the goal of evaluating the use of an alternative login method (security keys) and identifying potential barriers to company-wide adoption. During the evaluation period, all participants will be equipped with a security key, which will replace the login factors password and OTP. By analyzing log data and evaluating surveys and interviews, the usability and security of both login methods will be assessed [...]

Risks and Benefits: A temporary disruption of the login process at the time of transitioning to the new authentication method cannot be completely ruled out. Your participation in this study will help us to understand the usability and security of security keys in a corporate environment and enable an evaluation of their use at [company] [...]

G – General Questions

Thank you for participating in this survey. Unless otherwise stated, all questions refer exclusively to [company]'s MFA solution. Websites, both inside and outside [company], that do not use this MFA solution are not included.

Terminology *"Password + OTP"*: This refers to the entering a password followed by a one-time password (OTP). This is currently the standard login method used in the company.

G1 How often do you log in using MFA per day? (Estimate)
Answer: _____

G2 How satisfied are you with the frequency of login prompts per day?

Extremely dissatisfied	(1)	(2)	(3)	(4)	(5)	Extremely satisfied
	○	○	○	○	○	

G3 How easy or difficult do you consider the login process?

Extremely difficult	(1)	(2)	(3)	(4)	(5)	Extremely easy
	○	○	○	○	○	

G4 What changes would improve the login process?
Answer: _____

G5 Overall, how satisfied are you with the login process using Password + OTP?

Extremely dissatisfied	(1)	(2)	(3)	(4)	(5)	Extremely satisfied
	○	○	○	○	○	

G6 On average, how long does a login process typically take you? (In seconds, estimate)
Answer: _____

G7 How satisfied are you with the **duration** of the login process?

Extremely dissatisfied	(1)	(2)	(3)	(4)	(5)	Extremely satisfied
	○	○	○	○	○	

G8 Did you encounter any issues with the login during the test period?
○ Yes ○ No

G9 *[If **G8** yes]* What issues did you experience? (Brief bullet points)
Answer: _____

SUS **System Usability Scale (SUS) – 10 Questions**
The following questions help compare the use of Password + OTP with security keys later in the study. In this survey, "system" refers to the use of Password + OTP. *[Fully agree – Fully disagree]*

S – Security

S1 How safe do you feel using Password + OTP?

Very unsafe	(1)	(2)	(3)	(4)	(5)	Very safe
	○	○	○	○	○	

S2 Do you consider Password + OTP secure enough for the company?
○ Yes ○ No ○ Neutral: _____

S3 Are you familiar with the term "phishing?"
○ Term unknown ○ Term known, meaning unk. ○ Meaning known

S4 How secure do you consider Password + OTP as a combined login method?

Very insecure	(1)	(2)	(3)	(4)	(5)	Very secure
	○	○	○	○	○	

D – Demographics

D1 What is your name?
Answer: _____

D2 What is your gender?
○ Female ○ Male ○ Non-binary ○ Prefer not so say

D3 How old are you?
○ <18 years ○ 18 – 25 years ○ 26 – 35 years ○ 36 – 45 years
○ 46 – 55 years ○ >55 years ○ Prefer not so say

D4 What is your job title?
Answer: _____

A.2 Survey 2 & 3 – Security Keys

G – General Questions

Unless otherwise stated, all questions refer exclusively to the login process using a security key at [company]. Services and platforms that do not support security keys are not included.

Terminology *"Password + OTP"*: This refers to entering a password followed by a one-time password (OTP). This is currently the standard login method used in the company. *"Security Key"*: A security key, specifically the YubiKey Bio in this test phase, used for authentication during test phase 2.

[Note: Each questionnaire had a slightly changed wording based on the security key authentication method used, i.e., "Biometrics" or "PIN".]

G1 *[S2 & S3]* Which authentication method of the security key did you use most recently?
○ Biometrics (Fingerprint) ○ PIN

G2 *[S2 & S3]* Overall, how satisfied are you with using the security key with [Biometrics/PIN]?

Extremely dissatisfied	(1)	(2)	(3)	(4)	(5)	Extremely satisfied
	○	○	○	○	○	

G3 *[S2 only]* Has your login frequency changed after the transition from Password + OTP to the security key?
○ Yes ○ No

G4 *[S2 only]* *[If **G3** yes]* How often do you need to log in per day? (Estimate)
Answer: _____

G5 *[S3 only]* Has the duration of a login differed between the authentication methods (Biometrics or PIN) of the security key?
○ Yes ○ No

G6 *[S2 only]* Has the duration of a login changed due to the transition from Password + OTP to security key?
○ Yes ○ No

G7 *[S2 only]* On average, how long does a login process with the security key typically take you? (In seconds, estimate)
Answer: _____

G8 *[S3 only]* Which authentication method took longer?
○ Biometrics (Fingerprint) ○ PIN

G9 *[S3 only]* How large was this difference? (In seconds, estimate)
Answer: _____

G10 *[S2 & S3]* How satisfied are you with the **duration** of the login process using the security key with [Biometrics/PIN]?

Extremely dissatisfied	(1)	(2)	(3)	(4)	(5)	Extremely satisfied
	○	○	○	○	○	

G11 *[S2 only]* How satisfied are you with the **frequency** of the login process?

Extremely dissatisfied	(1)	(2)	(3)	(4)	(5)	Extremely satisfied
	○	○	○	○	○	

G12 *[S2 & S3]* How easy or difficult do you consider the login process using the security key with [Biometrics/PIN]?

Extremely difficult	(1)	(2)	(3)	(4)	(5)	Extremely easy
	○	○	○	○	○	

G13 *[S3 only]* What changes would improve the login process with the security key?
Answer: _____

G14 *[S2 & S3]* Did you encounter any issues while using the security key with [Biometrics/PIN]?
○ Yes ○ No

G15 *[S2 & S3]* *[If **G14** yes]* What issues did you experience? (Brief bullet points)
Answer: _____

SUS **System Usability Scale (SUS) – 10 Questions** *[S3 only]*

S – Security *[S3 only]*

S1 How safe do you feel using the security key?

Very unsafe	(1)	(2)	(3)	(4)	(5)	Very safe
	○	○	○	○	○	

S2 Which authentication method of the security key feels more secure?
○ Biometrics (Fingerprint) ○ PIN ○ Both methods feel the same

S3 Do you consider security keys secure enough for the company?
○ Yes ○ No ○ Neutral: _____

S4 How secure do you consider security keys as a login method?

Very insecure	(1)	(2)	(3)	(4)	(5)	Very secure
	○	○	○	○	○	

B Interview Guides

B.1 Interview Guide 1 – PWD+OTP

[Note: The first interview was conducted after testing "PWD+OTP".]

G – General Experiences

G1 How was your overall login experience during the test?

G2 Do you already have any thoughts about the test that you would like to share?

U – Usability

[Note: The reference for the following interview questions is the data collected from the first questionnaire.]

U1 Why are you (very) (dis)satisfied with the duration of the login?

U2 Why are you (very) (dis)satisfied with the frequency of logins?

U3 Why was the login process easy/difficult in your experience?

U4 [Optional] You indicated that [. . .] should be changed. Why do you think that?

U5 [Optional] You encountered [. . .] as an issue during the test period. Can you describe this in more detail?

U6 [Optional] Discussion of issues reported by others.

S – Security

S1 Why do you *feel* (very) (in)secure when using Password and OTP?

S2 Why do you consider password and OTP (not) secure enough for the company?

S3 Based on your understanding of phishing, do you think the combination of password and OTP protects against phishing?

S4 Why do you *consider* using password and OTP (very) (in)secure?

S5 Are there any additional evaluation criteria that you felt were missing in the survey or interview?

Wrap-Up

After the interview, we provided information about the following test period for "security key" testing.

B.2 Interview Guide 2 – Security Keys

[Note: The second interview was conducted after testing both security key authentication methods.]

G – General Experiences

G1 How was your overall login experience during the second test period?

G2 Do you already have any thoughts about the test that you would like to share?

U – Usability

U1 Why did (or didn't) the duration of a login process change?

U2 [Optional] Why are you (very) (dis)satisfied with the duration of the login?

U3 [Optional] Which login prompts were eliminated due to the switch to security keys?

U4 [Optional] Why are you (very) (dis)satisfied with the frequency of logins?

U5 You indicated that you are more satisfied with [Biometrics/PIN]. Why is that?

U6 Why was the login process easy/difficult in your experience?

U7 [Optional] You encountered [. . .] as an issue during the test period. Can you describe this in more detail?

U8 [Optional] Discussion of issues reported by other participants.

S – Security

S1 Why do you *feel* (very) (in)secure when using the security key?

S2 Why does [Biometrics/PIN] feel more secure to you?

S3 Why do you consider security keys (not) secure enough for the company?

S4 Do you think security keys protect against phishing?

S5 Why do you *consider* using security keys (very) (in)secure?

F – Future Use

F1 Would you like to continue using the security key after the test period?

F2 What should be prioritized to improve the use of security keys?

Wrap-Up

After the interview, we thanked participants for their participation and informed them that they are free to continue using the security keys or switch back to password and OTP with our help.

C Codebooks

C.1 Codebooks – Usability

Table 2: Usability drawbacks of PWD+OTP.

Code	Freq.	Description	Example
Smartphone handling	7	Having to use the smartphone for the second factor is annoying.	*It's about finding your cell phone, having your cell phone at the workplace, unlocking it, that's what it's all about.*
Password handling	4	The complexity and number of passwords is annoying to remember and handle.	*So basically four or five passwords that aren't exactly short, which I somehow have to have ready at the same time.*
Too many accounts	3	Users need to use multiple accounts on multiple services. Where to use which account might be unclear.	*Yeah, it's just annoying. It's annoying because we use different accounts.*
TOTP setup complicated	3	Setting up the TOTP generation on the smartphone is complicated.	*But I found the setup quite cumbersome.*

Table 3: Usability drawbacks of security keys.

Code	Freq.	Description	Example
Incomplete integration	12	Incomplete single sign-on integration leads to inconsistent authentication procedures and high numbers of daily logins.	*I think it would be cool if you didn't have to do both, but could just go to the key instead.*
Transportation and storage inconvenience	10	The security key is another device that must be transported and remembered.	*[...] you always have to make sure that you carry it with you and don't forget it.*
Recurring OS popups	10	The operating system asks participants to choose between FIDO2 sign-in options. Participants cannot choose a default option and have to click through the pop-ups in every authentication process.	*[...] what stood out to me negatively is the process of first having to confirm that you want to use the security key during each login.*
Inaccurate fingerprint recognition	8	Participants experienced unexpected behaviour of the fingerprint sensor. Fingerprint recognition was rated below average.	*My fingerprint isn't recognized as reliably as I'm used to with other fingerprint sensors.*
USB slot shortage	6	To use the security key for authentication, participants had to unplug other devices to free a USB slot for the security key or they reduced the number of USB devices to adapt to the situation.	*I had to decide, okay, what do I connect to the last slot?*
PIN memorization	5	The security key's PIN, set by the user, can be or was forgotten by participants.	*The initial problem was that between the first setup and the second use, I actually forgot the PIN, [...]*
Fear of breakage	3	The security key felt fragile and was bent when pressing on the sensor. Participants voiced concerns about the durability of the key.	*I am always scared to break it.*
USB type incompatibility	2	Participants had to use adapters or USB hubs to use a USB-A security key on USB-C slots or missed the possibility to use the key on other devices due to USB type incompatibility.	*But I couldn't do that with my iPhone because I have the A-Key, not the C-Key.*
Physical accessibility	2	The participants workplace setup does not allow easy access to USB peripherals because the notebook or docking station is placed behind displays or on the other side of the desk.	*In my setup, the docking station is behind the laptop, so it's kind of silly to plug the USB stick into the dock.*

C.2 Codebooks – Security

Table 4: Perceived security of *PWD+OTP*. The top part lists reasons for perceiving them as secure, the lower part as insecure.

Code	Freq.	Description	Example
Secure second device	10	Participants rate the smartphone as TOTP generators as secure, because the smartphone is locked.	*This means that no one will probably be able to unlock the cell phone without your cooperation.*
MFA security	7	2FA gives participants the feeling of security and is rated more secure than passwords only.	*I think the system with a second factor certainly provides a certain level of security.*
Trust in decision makers	2	Trust in the colleagues who plan and implement authentication.	*[It's the] trust in other people. I think [...] something will have been thought up to ensure that this is safe.*
Strong passwords	1	Randomly generated passwords from password managers not known to the user increase security.	*Uh, my password is also quite secure. It's stored only in my password manager. A random password.*
Phishing possible	2	Participants rate PWD+OTP less secure because of phishing susceptibility.	*Exactly, that susceptibility to phishing. Because a numeric code can be easily intercepted.*
TOTP location insecurity	3	The TOTP can be generated on insecure devices or at insecure virtual locations.	*If you store the password and the second factor in the same place, then you basically only have one factor, if you will.*
Inconsistent SSO/number of logins	1	The high number of daily logins and inconsistent SSO implementation increases the chance of successful phishing attacks.	*The number of login processes should rather be reduced. That also has something to do with susceptibility to phishing.*
Inconsistent UI	1	The UI of the authentication form differs due to inconsistent SSO. The IAM solution does not display the relying party's name.	*I mean, there are a few things I feel are missing from this method, like the standardization of masks and being able to see in the mask which resource I'm accessing.*
Hardware token display	1	Hardware TOTP generators display TOTPs visible for everyone.	*Yes, that's maybe less resistant than a software token because it's lying on my desk.*

Table 5: Perceived security of security keys. The top part lists reasons for perceiving them as secure, the lower part as insecure.

Code	Freq.	Description	Example
Fingerprint feels secure	3	Replication of fingerprints seems hard to participants. Biometric authentication is rated secure.	*For me, that means, what I understand by it, is that no one else can log in. So, no one who doesn't have my finger.*
Password removed as weakness	3	With security keys users cannot choose a weak password because it is not part of the authentication process.	*[...] because password complexity doesn't serve as an attack vector, so to speak. [...] That aspect is eliminated since you don't really have to remember anything anymore.*
Positive media coverage	1	Literature refers to security keys as secure, participants only read positively about security keys.	*If you follow relevant specialist literature, security keys are [...] new but still well-rated methods.*
Dedicated crypto device	1	The security key is built for one task, cryptography, the participant expects it performs well in that task.	*I just feel better because it's a special cryptographic device.*
PIN possible weakness	5	The security key's PIN can be weak, PIN may be written down.	*So if someone just uses a four-digit number, ideally something like their birth date, then you really only have the key left.*
Key easily lost/stolen	3	The security key can be lost because it is small. Theft may only be noticed late.	*The only security concern I think I would have with both is that you could lose the stick.*