No Password, No Problem?
A Large-Scale Field Study of Passkey Adoption and Usage

Tobias Reittinger
University of Regensburg
tobias.reittinger@ur.de

Günther Pernul
University of Regensburg
guenther.pernul@ur.de

***Abstract*—Passkeys were introduced to mitigate password-related security risks. However, passwords remain prevalent, and the usability of synchronization, one of the core benefits of passkeys, has not yet been studied. To address this gap, we conducted a large-scale field study examining passkey adoption and usage by partnering with an industrial healthcare service. In Phase 1 (n = 5,057), users chose between a passkey and a password with 2FA during registration. We reveal that (especially inexperienced) users struggle with passkey adoption but still perceive passkeys to offer superior usability and acceptance. Our survey results identified novel reasons why users decline passkeys, notably the habit of using passwords and lack of passkey experience, and pinpointed adoption barriers, including new misconceptions and manual passkey activation. In Phase 2 (n = 2,716), we monitored authentication behavior over six months and captured immediate feedback through surveys. We found that passkey usability and acceptance continued to increase, and success rates surpassed the declining metrics of passwords. Still, we uncovered new issues with cross-platform synchronization, passkey sharing, and interactions with password managers. Finally, we provide recommendations to streamline the adoption and usability of passkeys.**

1. Introduction

Although passwords are technically secure [48], they suffer from poor usability: Users are required to create passwords that are long and random [49], [79], compliant with complex policies [79], unique for each account [33], [68], and memorable for numerous accounts [31], [84]. Moreover, phishing campaigns, now amplified by generative AI [36], pose an escalating threat to password compromise [59]. Consequently, password-based authentication is one of the primary vectors for cyberattacks [60]. Multi-Factor Authentication (MFA) can mitigate these risks, but its adoption rates remain low [3], [15], and attackers often circumvent it through social engineering or sophisticated phishing [59], [60]. Despite these shortcomings, passwords continue to serve as the *de facto* standard for authentication [48], [75].

To address these issues, the Fast IDentity Online (FIDO) Alliance introduced FIDO2 passwordless authentication, which uses public-key cryptography to resist phishing and strengthen security compared to passwords [30], [50]. FIDO2 eliminates password creation and memorization [29] and inherently supports MFA via biometrics or a device passcode, but credentials remain tied to individual devices, limiting portability and recovery options [55], [65], [85]. To overcome these limitations, passkeys extend FIDO2 by offering credential synchronization across devices [25]. While synchronization introduces a tradeoff between security [45] and usability [51], passkeys deliver enhanced security and usability over password-based authentication [25]. However, password authentication still prevails [75]. We identified two research gaps in understanding passkey adoption and use: First, prior work has focused on lab experiments [53], [85] yet fails to capture real-world adoption barriers and longitudinal usage challenges. Second, although passkeys offer synchronization, this core feature has not yet been examined in a user study. We aim to close these gaps by answering the following research questions:

RQ1 *What concerns deter users from choosing passkeys, and what obstacles impede passkey adoption?*

RQ2 *Which challenges do users encounter with passkeys, including synchronization, in a multi-month period?*

We conducted a large-scale field study to examine passkey adoption (n = 5,057) and six-month usage (n = 2,716) by collaborating with a healthcare appointment platform (see Section 3.1). Thereby, we compared passkeys against passwords with two-factor authentication (2FA), collecting both authentication metrics and survey responses. Our contributions are as follows:

- We find that users are interested in passkeys but hesitate due to password habits and inexperience. Adoption success rates were lower than for passwords with 2FA, especially for novices, yet passkeys exhibited superior usability and acceptance. We also identify new barriers, including novel misconceptions and manual activation.
- With repeated logins, passkey success rates surpassed those of passwords with 2FA, while usability and acceptance continued to rise. We conducted the first user study assessing passkey synchronization, uncovering major cross-platform challenges, and also identifying issues with passkey sharing and password managers.
- We offer recommendations to enhance passkey adoption and usability, and publish the source code and statistical analysis to facilitate future work.

The paper is organized as follows. Section 2 reviews background and related work. Section 3 describes the methodology. Section 4 presents the results of passkey adoption. Section 5 reports passkey usage results. Section 6 discusses implications. Section 7 concludes the paper.

2. Background and Related Work

In this section, we describe the functionality of FIDO2 and passkeys and review related studies.

2.1. FIDO2

To mitigate the security risks of password-based authentication, the FIDO Alliance developed FIDO2, a successor to the initial Universal 2nd Factor (U2F) protocol [27], [40], [53]. By leveraging public-key cryptography [29], FIDO2 provides a secure, passwordless authentication supported by major operating systems (OSs) [66] and browsers [12], [58]. FIDO2 offers two modes:

- **Roaming Authentication:** This mode employs external hardware authenticators (e.g., security keys) that can be used across multiple devices via Client to Authenticator Protocol 2 (CTAP2), communicating securely over USB, Bluetooth, or NFC [26]. However, hardware-based tokens require an upfront purchase and can be lost or damaged [76], [85].
- **Platform Authentication:** In this mode, the authenticator is built into a user's device (e.g., smartphone, tablet, or PC) and leverages the W3C Web Authentication (WebAuthn) API for secure authentication [46]. Users verify their identity using **biometrics** (fingerprint or facial recognition, depending on device capability) or the device's **passcode** (PIN, pattern, or password) [46]. However, binding a credential to a single device can limit portability and complicate recovery if the device is lost [65], [85].

In sum, FIDO2 offers passwordless authentication that provides enhanced security compared to passwords [30], as credentials are inherently resistant to phishing attacks [50], but limited portability and recovery options [51], [65], [85].

2.2. Passkeys

Passkeys extend FIDO2's platform authentication by enabling credential synchronization across devices, addressing the limitations of device-specific storage [25]. Although synchronization introduces a security–usability trade-off [45], [51], it enhances portability and recovery options [25], [51].

- **Built-in Cloud Services:** Major vendors like Apple, Google, and Microsoft offer passkey synchronization via proprietary cloud services (e.g., iCloud Keychain, Google Password Manager, Windows Hello) [4], [7], [21]. However, this functionality is typically restricted to the same ecosystem.
- **Manual Device-to-Device Transfer:** Users can manually transfer passkeys cross-platform via a QR code or Bluetooth [30]. However, this requires physical proximity between devices, does not scale well for numerous devices, and may be less intuitive for users.
- **Third-Party Password Managers (PMs):** PMs, such as 1Password, Bitwarden, support cross-platform synchronization, and sharing [1], [8]. However, this functionality typically requires a premium subscription.

Most built-in cloud services and PMs allow users to share passkeys with others [1], [5], [8], [35]. Passkeys also inherently incorporate 2FA [46]: The first factor is the stored cryptographic key on the device (*something you have*). The second factor is either the user's biometrics (*something you are*) or the device's passcode (*something you know*). During passkey setup, users complete two steps, with their order and layout (one or two pages) varying by OS:

- **Storage Selection:** Users choose a passkey storage option: A built-in cloud service, PM, or another device. OSs offer either a default or require active selection.
- **Authentication:** Users authenticate locally with biometrics or the device's passcode to authorize passkey creation or authentication.

On subsequent logins, only the authentication step is required. Overall, passkeys offer a user experience (UX) distinct from FIDO2 security keys by enabling synchronization. Although passkeys deliver security and usability benefits over passwords [25], passwords remain the most common authentication method [75].

2.3. Related Work

Discussing related work, we first look at roaming authentication with security keys. Although these findings do not directly translate to passkeys, they offer insights into potential usability and acceptance challenges. Subsequently, we outline prior works on platform authentication and passkeys.

Roaming Authentication. Initially, security keys served as a second factor via the U2F protocol, a precursor to FIDO2. Das et al. [19], [20] evaluated U2F-based Yubico Security Keys (YubiKeys), demonstrating how clearer setup instructions and the removal of confusing demo features improved usability. However, acceptance remained low due to users' fears of losing access and uncertainty about the technology's benefits. Building on these observations, Reynolds et al. [74] compared setup and long-term usage. They found that while participants initially struggled with configuring their accounts, those who succeeded found YubiKeys both convenient and secure for everyday use. In a related study, Ciolino et al. [13] contrasted security keys with SMS-based one-time passwords (OTPs), reporting longer setup times and interface complexities for security keys. These factors led many users to prefer SMS OTPs. Subsequently, FIDO2 introduced passwordless logins, allowing security keys to function as a first factor [27], [40]. Lyastani et al. [55] found FIDO2 with a YubiKey more usable and acceptable than passwords, though concerns about device loss, trust, and hardware limitations persisted. Farke et al. [23] further explored a four-week deployment of FIDO2 keys in

a small software company. Although employees appreciated the enhanced security and simplicity, many reverted to passwords due to fear of key loss and slower authentication. Collectively, these studies highlight the importance of intuitive setup, clear benefit communication, and user-friendly designs in enhancing adoption rates.

Platform Authentication. In addition to roaming authentication with security keys, FIDO2 supports platform authentication via WebAuthn, allowing users to utilize their own devices, such as smartphones, as authenticators. Oogami et al. [64] highlighted usability barriers to WebAuthn fingerprint authentication on Android devices, noting that many users tapped the on-screen fingerprint icon instead of the physical sensor. Building on these findings, Lassak et al. [53] investigated common misconceptions about FIDO2 biometric WebAuthn. They found that clarifying how and where biometric data are stored significantly improved user perceptions and willingness to adopt biometric WebAuthn over passwords. Similarly, Owens et al. [65] compared smartphone-based FIDO2 authenticators to passwords, observing that, despite enhanced security, participants were deterred by complex setup processes, slow authentication, and limited recovery options. In a quantitative study, Nawrath [63] found platform authentication yielded higher success rates on mobile devices. However, compatibility challenges and concerns about data privacy remained. Würsching et al. [85] later compared platform authentication (using Apple Touch ID) with roaming authentication (using a YubiKey). Their findings showed that platform authentication was rated more favorably for user acceptance. Still, many users expressed concerns about account recovery and multi-device access, specifically noting the inconvenience of carrying an external key for roaming authentication. Overall, these studies demonstrate the potential of FIDO2 passwordless authentication yet emphasize the need to address setup complexities, clarify biometric data handling, and ensure device compatibility.

Passkeys. Subsequently, passkeys evolved from these developments, offering multi-device synchronization [30]. Lassak et al. [54] surveyed organizational hurdles to deploying passkeys, identifying the lack of standardized fallback options, technical constraints, and user resistance to change as key barriers. Security studies map emerging risks: Daffalla et al. [18] introduced a framework for analyzing interpersonal threats and identified abuse vectors across major services. Islam et al. [45] revealed vulnerabilities in cloud-based passkey synchronization and proposed a novel framework to detect the unauthorized use of leaked passkeys. Further, Büttner and Gruschka [10] categorize passkey access levels and show that synced passkeys, while enhancing recoverability, centralize security risk in the provider. Additionally, multiple industry case studies discuss how organizations benefit from passkeys' enhanced UX [16], [37], [38], [61], [77].

Our Differentiation To Prior Work. We distinguish our work from previous studies in content and methodology. While most prior studies centered on roaming authenticators (e.g., security keys) or single-device platform authentication, we investigate passkeys and their unexplored multi-device synchronization features. Given the continued prevalence of passwords [75], we also examine why users might resist or abandon passkeys and identify adoption barriers. Moreover, while earlier research relied on lab experiments and diary studies, our industrial collaboration (Section 3.1) enables continuous monitoring of real-world authentication use and immediate user feedback. To the best of our knowledge, we present the first large-scale field study of passkey adoption and usage, offering actionable insights to improve the adoption and usability.

3. Methodology

From October 2024 to May 2025, we conducted an exploratory user study in two phases (adoption and usage) employing a mixed-methods approach.

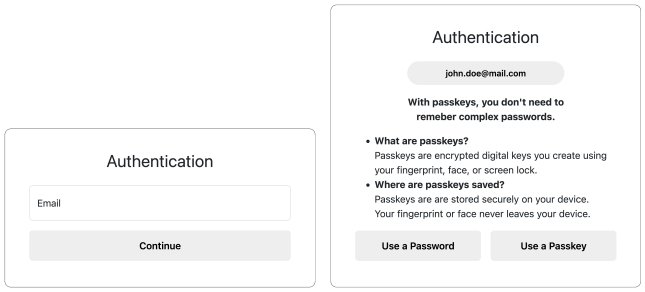
3.1. Study Design

Below, we outline the implementation, study groups, and the design of both between-group phases.

Implementation. We partnered with a European healthcare appointment platform, hereafter referred to as the **platform**, that recently added passkeys. The passkey implementation is available on GitHub. Passkeys are stored on participants' devices via platform authenticators and serve as the primary authentication method. Roaming authenticators (e.g., security keys) were disabled to isolate passkey use. We layered study instructions, measurements, and surveys atop the existing platform infrastructure.

Study Groups. In this study, we compared two user groups based on their self-selected authentication method (Figure 1). Participants who chose passkeys were assigned to **Group K**, which inherently requires 2FA. They can select either biometrics or the device's passcode as the second factor (Section 2.2). In contrast, participants opting for passwords formed **Group W**, which combines a password with 2FA. For Group W, we adopted a common password policy requiring at least eight characters in accordance with NIST recommendations [39]. Passwords also had to include characters from a minimum of two character classes (e.g., uppercase, lowercase, numeric, or special symbols), as seen in practice by services such as PayPal [67]. The second factor for Group W was an SMS-based OTP valid for ten minutes, chosen both for its prevalence in the industry [2], [34], [44], [56] and because the platform already supports it. Consequently, both groups employ forms of MFA commonly seen in real-world applications [55], [62].

Phase 1: Passkey Adoption. Phase 1 aimed to uncover the key motivators and challenges associated with passkey adoption in a realistic setting. In line with current industry practices (e.g., Apple [43], Google [34], Uber [44]), participants first entered their email address (see Figure 1a) and were then offered the choice to create a new account using either a passkey or a password (see Figure 1b). This step divided all participants into two groups: those who chose a passkey (Group K) and those who selected



(a) 1. Enter email (b) 2. Choose authentication

Figure 1: Authentication choice, following recommendations of the FIDO Alliance [28] and Lassak et al. [53].

TABLE 1: Participants during the study by authentication method: Group K (passkey) vs. Group W (password + 2FA).

Study	Step of Study	Group K	Group W	Σ
Phase 1	Authentication Choice	2,950	2,107	5,057
	Successful Adoption	1,664	1,924	3,588
Phase 2	At least one auth. attempt	1,295	1,421	2,716

a password (Group W). In accordance with the FIDO Alliance UX guidelines [28], we provided general information about passkeys and incorporated insights from Lassak et al. [53] addressing common misconceptions about biometrics. Although this information may have influenced decisions, it aligns with the guidance typically provided by vendors during passkey setup (e.g., Adobe [2], Amazon [42], Google [34]). To mitigate potential bias, we randomized the order of the sign-up buttons. All interactions with the authentication methods were monitored, and participants were allowed to cancel their setup at any point, thereby replicating a genuine user experience. After completing or canceling the setup process, participants were directed to a survey designed to capture their reasons for their choice, any difficulties they encountered, and relevant demographic details. Participants who did not successfully adopt their chosen method were surveyed about their reasons for discontinuation, but were subsequently excluded from Phase 2 to prevent bias. Only those who successfully adopted their chosen authentication method advanced to Phase 2.

Phase 2: Passkey Usage. Phase 2 aimed to investigate the experience and potential usability challenges of passkeys during long-term usage and compare their UX to that of 2FA-based passwords as a baseline. We monitored the authentication behavior of participants who successfully adopted their chosen method in Phase 1 for six months, starting from each participant's adoption date. At each login, participants entered their email addresses and were then presented with their previously selected authentication method. Because passkey telemetry does not report storage location, second factor, or synchronization type, we used a brief post-authentication survey after each attempt to capture these attributes and participants' experiences accurately. To ensure robust data collection, only participants who made at least one authentication attempt during the study period were included. Participants retained their initially chosen authentication method throughout the study, aligning with industry practice [47], to prevent password fallback during multi-device use and thereby preserve observable synchronization events. Switching the authentication method was available after completion or upon withdrawal. Further, participants could register multiple passkeys and synchronize them via built-in cloud services, device-to-device transfers, or PMs. For **account recovery**, both groups received a six-digit SMS OTP (valid for 10 minutes) and then registered a new passkey (Group K) or set a new password (Group W). A follow-up survey captured their recovery experiences. OTPs are commonly used for recovery, either via SMS (e.g., Adobe [2], Amazon [42]) or email (e.g., FIDO's passkey prototype [28]). SMS-based OTP recovery is vulnerable to phishing [51], but widely used with passwords in practice [2], [34], [44], and prior research has suggested exploring its use for passkeys [65], [85].

3.2. Recruitment and Participants

Participants were new users signing up for the healthcare production platform. Users with passkey-compatible devices were invited to create a new account. We outlined the study objectives, data collection procedures, expected duration, and incentives (see Section 3.5). Table 1 lists participant numbers during the study.

In Phase 1, 5,057 participants completed the authentication choice, 3,588 successfully adopted it and advanced to Phase 2, and 2,716 made at least one authentication attempt. Attrition was similar (31.8% in Group K and 29.5% in Group W), reflecting typical patterns observed in platform usage and longitudinal research [65]. Participants are from diverse demographics, as detailed in Appendix B.

3.3. Data Collection

We collected measured and self-reported data in both phases. Survey questionnaires are listed in Appendix A and the characteristics of quoted participants in Appendix D.

Phase 1: Passkey Adoption Data. During registration, we monitored participants' interactions with the authentication methods. We distinguished between the initial authentication choice (passkey or password) and the subsequent adoption outcome. This dual-phase data collection enabled us to quantitatively assess both the decision to adopt passkeys and the barriers encountered during adoption.

Additionally, participants provided qualitative feedback via a free-text survey available in both English and German. To control for accidental selections, we asked whether their choice was intentional. They also explained their reasons for choosing or not choosing passkeys, described any difficulties encountered during adoption, and clarified their reasons for canceling the adoption. Additionally, the survey collected background information, including computer science (CS) background, prior use of passkeys and OTPs, scores on the

Affinity for Technology Scale (ATI) [32], privacy concerns (PC) [52], and demographic details. Background data were only collected in Phase 1, as Phase 2 participants are a subset of this sample. On average, the survey took 5 minutes to complete (Mdn = 4 min).

After adoption, participants were asked to complete the usage survey of Phase 2 to investigate the influence on authentication choice or adoption success.

Phase 2: Passkey Usage. During the six-month usage period, we recorded several metrics to assess how participants, those who made at least one authentication attempt, interacted with the authentication methods. We tracked:

- Number of authentication attempts
- Duration of each authentication attempt
- Number and duration of recovery attempts
- Contextual data, such as device type, operating system (OS), and a unique device identifier

After each login attempt, we displayed participants a survey to report their authentication experiences, such as issues encountered and reasons for failures [55], [65]. Since a passkey implementation only reports success or failure, we asked participants of Group K for additional details in the survey, including the used second factor, if and how the passkey was synced from another device, and any associated challenges. Both groups then completed the System Usability Scale (SUS) [9] and the Acceptance Scale [55], [82]. The survey took 4 minutes on average (Mdn = 4 min).

3.4. Data Analysis

For qualitative analysis of free-text survey responses, we employed a flexible coding approach [22]. One researcher conducted the initial coding, which a second researcher co-interpreted. Discrepancies were resolved through joint discussions. The codebook is described in Appendix C, and code frequencies are stated in the results (Sections 4 and 5).

In the quantitative analysis, ordinal variables were analyzed with the Wilcoxon-Mann-Whitney test [57], as the Shapiro-Wilk test [78] indicated non-normality. Nominal variables used Pearson's chi-square test [69] with Cramér's V for effect size [17]. We fit a multivariable logistic regression to estimate adjusted odds ratios while controlling for covariates. Significance was set at $p < 0.001$ for all tests. Medians are reported to minimize outlier effects.

To assess authentication performance, we define an **authentication session** as any sequence of attempts within a ten-minute window. This session-based metric is adapted from earlier research on FIDO2 [65] and reflects real-world behavior in which users may enter multiple credentials in quick succession. A session is considered **successful** if a participant completes the initial adoption process (Phase 1), logs in without invoking account recovery (Phase 2), and registers a new passkey or password (account recovery in Phase 2). Conversely, a session is categorized as **unsuccessful** if the participant cancels the procedure, fails to complete authentication, or allows the session to time out.

Session duration is measured as the elapsed time from the click on one of the authentication options (Phase 1), the click on the "Login" button (Phase 2), and the click on the "Forgot Password" button through to the last interaction of the final attempt in that session. Attempts that are initiated within an existing session window are attributed to that session. Any attempt starting ten minutes or more after the session's start will begin a new session. We flagged outliers with >3 failed sessions in 24h, identifying one outlier (five failures) and no evidence of scripted abuse.

In Phase 2, we classify a synchronization as **platform-specific** when a passkey is synchronized within a vendor ecosystem (e.g., from iOS to macOS or Android to Android) and as **cross-platform** when it spans heterogeneous ecosystems (e.g., from iOS to Windows, or Android to iOS).

3.5. Ethical Considerations

Before conducting the study, the ethics committee of the German Association for Experimental Economic Research e.V. approved our study, and we received an Institutional Review Board (IRB) certificate, which is available online.[1]

User Study. Before the study, we displayed a GDPR-compliant privacy policy. Participation was voluntary, and we limited personal information to demographics. To reduce bias, users were told the study concerned authentication without additional details. Participants were briefed on objectives, data collection, and their right to withdraw at any time, either via a button in the settings tab or, if logged out, via a link in the invitation email, and provided informed consent. Upon completion or withdrawal, they received a debriefing. All surveys ran on a self-hosted LimeSurvey[2] instance to ensure data privacy. To minimize burden from the retained-authentication requirement, we (i) clearly communicated the request, (ii) confirmed with the platform vendor that no participants contacted support about study-related restrictions, and (iii) appointments remained bookable through traditional channels. To encourage participation, we ran a raffle for a €100 gift card. When enrollment exceeded expectations, we added 100 €5 gift cards post-study to increase the number of winners. In retrospect, a raffle that scales proportionally with enrollment would be preferable, as it lets participants know their odds in advance and maintains fairness regardless of final sample size.

Impact on Access to Healthcare. The study did not affect participants' access to healthcare services. Although the platform offers a convenient interface for booking doctor appointments, users can still schedule appointments via traditional methods (e.g., phone or email). The platform also provides public access to doctor information without registration. The passkey feature was thoroughly tested before implementation to ensure no adverse impact on platform access. No participants reported issues with the passkey implementation, aside from the obstacles inherent to passkeys, which are unrelated to the implementation itself.

1. IRB certificate: https://gfew.de/en-ethik/PFMLTKKY
2. https://github.com/LimeSurvey/LimeSurvey

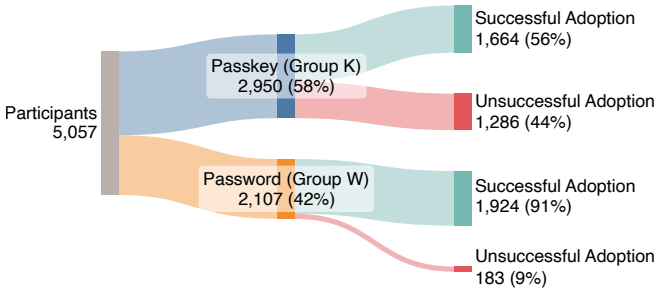


Figure 2: Flow diagram illustrating participants' authentication choices and adoption outcomes.

TABLE 2: Authentication choices and adoption outcomes of participants, segmented by prior passkey experience (Exp.) and no passkey experience (No Exp.).

Category	Exp.	No Exp.	Total
Total Participants	2,396	2,661	5,057
Passkey (Group K)	1,721 (72%)	1,229 (46%)	2,950 (58%)
Successful Adop.	1,235 (72%)	429 (35%)	1,664 (56%)
Unsuccessful Adop.	486 (28%)	800 (65%)	1,286 (44%)
Password (Group W)	675 (28%)	1,432 (54%)	2,107 (42%)
Successful Adop.	613 (91%)	1,311 (92%)	1,924 (91%)
Unsuccessful Adop.	62 (9%)	121 (8%)	183 (9%)

3.6. Pilot Study

Before conducting the main user study, we performed a pilot study (n = 13). The pilot study, which included both Phase 1 and Phase 2 procedures, aimed to detect technical difficulties and identify ambiguities in the survey questions. Based on the feedback, minor adjustments were made to improve the clarity of the questionnaire. As a result of these revisions, pilot data were excluded from analysis.

4. Results: Passkey Adoption (Phase 1)

This section details the findings of Phase 1 on passkey adoption. We begin by presenting the quantitative metrics, followed by qualitative insights into the factors driving adoption decisions and the obstacles encountered during the adoption of both passkey and password with 2FA.

Because prior passkey experience emerged as the strongest predictor of both choice and adoption success across two logistic regression models (see Sections 4.1.4 and 4.1.5), we stratify results by prior experience.

4.1. Passkey Adoption Metrics

This section details our findings on quantitative adoption metrics. Nearly all participants, 4,972 out of 5,057 (98%), indicated that their choice of authentication method was intentional, and all participants reported password experience.

TABLE 3: Adoption outcomes and median duration of authentication sessions of Group K, differentiated by OS.

Category	Mobile		Desktop	
	Android	iOS	macOS	Windows
Group K	1,554	844	191	361
Successful	896 (58%)	539 (64%)	76 (40%)	153 (42%)
Unsuccessful	658 (42%)	305 (36%)	115 (60%)	208 (58%)
Duration	12.9 s	6.2 s	20.4 s	19.2 s

4.1.1. Authentication Choices. Figure 2 shows 58% (2,950 of 5,057) of participants opted for passkeys, whereas 42% (2,107 of 5,057) selected passwords. These findings **indicate a promising level of interest in passkeys.**

4.1.2. Adoption Outcomes. In Group K, 56% (1,664 of 2,950) of participants who attempted passkey adoption achieved successful authentication, compared to 91% (1,924 of 2,107) of participants in Group W using passwords with SMS-based 2FA. Moreover, successful adopters required an average of 1.38 attempts in Group K versus 1.10 attempts in Group W. These findings **suggest that passkey adoption imposes greater friction than passwords with 2FA**.

4.1.3. Durations. The median duration of authentication sessions was 12.6 s for Group K and 52.9 s for Group W. Within Group W, the median time to create and enter a password was 24.8 s, while SMS-based 2FA took a median of 28.1 s. The results **indicate that passkey authentication is faster than passwords and passwords with 2FA**.

Table 3 shows that median authentication times for Group K varied across OSs, Android (12.9 s), iOS (6.2 s), macOS (20.4 s), and Windows (19.2 s), **indicating faster passkey adoption on mobile platforms than on desktops**.

4.1.4. Factors Influencing Authentication Choices. We evaluated the association between a range of variables and participants' authentication choices (see Table 9 in Appendix B). A chi-square test [69] on demographics, CS background, and OS, along with a Wilcoxon–Mann–Whitney test [57] on ATI, indicated no significant influence on the authentication choice.

A Wilcoxon-Mann-Whitney test [57] showed PC scores differed significantly between Group K (Mdn = 5.5) and Group W (Mdn = 5), $U = 2,567,618.0$, $p < .001$, with a small effect size $r = .15$ [14], **indicating participants with higher privacy concerns chose passkeys more frequently**.

Overall, 47% (2,396 of 5,057) of participants reported prior passkey experience, and 53% (2,661 of 5,057) didn't. In detail, 72% (1,721 of 2,396) of participants with prior passkey experience chose passkeys, compared to only 46% (1,229 of 2,661) among those without such experience, as displayed in Table 2. A chi-square test [69] revealed a significant association between prior passkey experience and authentication selection, $\chi^2(1, N = 5,057) = 341.08$, $p < .001$, with a moderate effect size ($V = .26$) [14], **suggesting that participants familiar with passkeys are more likely to select them for authentication**.

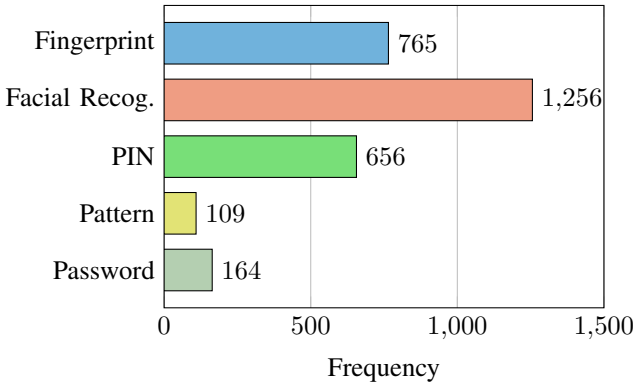


Figure 3: Frequencies of passkey second factors in Phase 1.

A binomial logistic regression substantiated these patterns with a significant model fit, $\chi^2(24) = 608.62$, $p < .001$; Nagelkerke $R^2 = .153$; accuracy = 65.7%. Controlling for demographics and OS, predictors of choosing passkeys were **prior experience** (OR = 2.93, 95% CI $[2.59, 3.30]$, $p < .001$), **privacy concerns** (OR = 1.42, $[1.35, 1.51]$, $p < .001$), **acceptance** (OR = 1.27, $[1.19, 1.36]$, $p < .001$), and **SUS** (OR = 1.01, $[1.007, 1.013]$, $p < .001$). Full coefficients and odds ratios are reported on GitHub.

4.1.5. Factors Influencing Passkey Adoption Outcome. We examined the association between various factors and the successful adoption of passkeys, with detailed results listed in Table 9 in Appendix B. A chi-square test [69] on demographics and CS background along with a Wilcoxon–Mann–Whitney test [57] on ATI and PC indicated no significant influence on passkey adoption success.

Prior passkey experience was significantly associated with successful adoption, $\chi^2(1, N = 2{,}950) = 396.04$, $p < .001$, with a moderate effect size ($V = .37$) [14]. Table 2 shows 72% (1,235 of 1,721) of experienced participants had successful adoptions, versus 35% (429 of 1,229) of inexperienced ones, **indicating that prior passkey experience increases the likelihood of successful adoption**.

Additionally, a chi-square test [69] suggested that the OS significantly influenced passkey adoption outcomes, $\chi^2(3, N = 2{,}950) = 70.39$, $p < .001$, with a small effect size ($V = .15$) [14]. Table 3 details that participants using mobile devices (smartphones and tablets) achieved higher success rates, 58% on Android and 64% on iOS, compared to 40% on macOS and 42% on Windows. These results **indicate that passkey adoption is more successful on mobile devices than on desktop ones**.

The secondary passkey factor significantly influenced outcomes, $\chi^2(4) = 68.71$, $p < .001$, with a small effect ($V = .15$). Figure 3 shows Phase 1 distributions: There were 765 authentications with a fingerprint (60% success rate), 1,256 with facial recognition (62%), 656 with a PIN (45%), 109 with pattern (58%), and 164 with password (42%). The results **suggest that biometric methods are most commonly employed, and biometrics and patterns offer higher passkey adoption rates than PINs and passwords.**

TABLE 4: Survey results on motivating factors influencing the decision to adopt passkeys in Group K, split by prior passkey experience (Exp.) and no prior experience (No Exp).

Motivating Factors	**Exp.** $n = 1{,}721$	**No Exp.** $n = 1{,}229$	**Total** $n = 2{,}950$
No memorization required	33%	54%	42%
Fast authentication	51%	22%	39%
Enhanced security	29%	38%	33%
No password creation	5%	10%	7%
Multifactor ease	6%	1%	4%
No password resets	2%	1%	2%
Other	1%	1%	1%

Note. Numbers are in-group percentages; multiple factors possible. n denotes the number of users in the corresponding group.

Finally, passkey storage location was significantly associated with adoption success, $\chi^2(3, N = 2{,}950) = 21.05$, $p < .001$, with a small effect size ($V = .08$) [14]. Of the 2,950 participants, 1,628 stored passkeys in the built-in cloud service (57% success rate), 244 in a PM (43%), 39 on another device (54%), and 1,039 were unsure of their storage location (58%). These results **suggest built-in cloud storage is the most frequently chosen option, whereas PM-based storage is linked to lower success rates**.

A binomial logistic regression supported these patterns. The model fit was significant $\chi^2(31) = 2332.15$, $p < .001$; Nagelkerke $R^2 = .733$; accuracy = 86.9%. Controlling for all other variables, significant predictors of successful passkey adoption were **prior experience** (OR = 4.51, 95% CI $[3.52, 5.79]$, $p < .001$), **acceptance** (OR = 4.21, $[3.58, 4.95]$, $p < .001$), and **SUS** (OR = 1.116, $[1.105, 1.127]$, $p < .001$). Full coefficients and odds ratios are outlined on GitHub.

4.1.6. Usability and Acceptance. Wilcoxon-Mann-Whitney test [57] showed SUS scores differed significantly between Group K (Mdn = 75) and Group W (Mdn = 67.5), $U = 2{,}640{,}040.5$, $p < .001$, $r = .13$, **indicating passkeys have higher usability than passwords with 2FA**.

Similarly, the acceptance scores differed significantly between Group K (Mdn = 1.11) and Group W (Mdn = 0.67), $U = 2{,}508{,}831.0$, $p < .001$, $r = .17$, **indicating passkeys have higher acceptance than passwords with 2FA**.

4.2. Factors Influencing Decision to Adopt Passkeys

This section outlines the factors influencing the decision to adopt passkeys, detailing motivating factors and concerns.

4.2.1. Motivating Factors. Table 4 summarizes the survey findings on why Group K chose passkeys. Chi-square test [69] revealed motivating factors varied significantly according to participants' prior passkey experience, $\chi^2(6) = 316.91$, $p < .001$, $V = .29$, indicating a moderate effect [14].

- *No Memorization.* Passkeys eliminate the need to remember complex passwords. This reason was cited by 42% overall (33% exp., 54% no exp.).

TABLE 5: Survey results on concerns influencing the decision against passkey adoption in Group W, split by prior passkey experience (Exp.) and no prior experience (No Exp).

Concerns	**Exp.** n = 675	**No Exp.** n = 1,432	**Total** n = 2,107
Habit of using passwords	44%	48%	47%
Lack of exp. or knowledge	32%	36%	35%
Lack of perceived benefit	18%	26%	23%
Passkey misconceptions	2%	12%	8%
Account recovery concerns	5%	6%	6%
Multiple client concerns	6%	5%	5%
Past negative experiences	13%	0%	4%
Deferred passkey adoption	1%	3%	2%
Security & privacy concerns	2%	1%	2%
Other	1%	1%	1%

Note. Numbers are in-group percentages; multiple concerns possible. n denotes the number of users in the corresponding group.

TABLE 6: Survey results on barriers to passkey adoption among unsuccessful Group K participants, split by prior passkey experience (Exp.) and no experience (No Exp).

Barriers	**Exp.** n = 486	**No Exp.** n = 800	**Total** n = 1,286
Passkey misconceptions	19%	28%	25%
Passcode misconceptions	18%	26%	23%
Manual passkey activation	15%	18%	17%
Perceived complexity	10%	12%	11%
Account recovery concerns	10%	8%	9%
Multiple client concerns	9%	8%	8%
Password manager issues	9%	6%	7%
Biometric misconceptions	5%	8%	7%
Technical difficulties	3%	3%	3%
Other	2%	1%	1%

Note. Numbers are in-group percentages; multiple barriers possible. n denotes the number of users in the corresponding group.

- *Fast Authentication.* Passkeys enable fast authentication, written by 39% overall (51% exp., 22% no exp.):

> *"[...] It is a lot quicker than typing out a password as I am able to use my Face ID for this."* (P8, Group K)

- *Enhanced Security.* Passkeys offer enhanced security, named by 33% overall (29% exp., 38% no exp.).
- *No Password Creation and Policy.* By removing the need to create and manage passwords, this factor was selected by 7% overall (5% exp., 10% no exp.).
- *Multifactor Ease.* Passkeys offer convenient MFA (e.g., biometrics), cited by 4% (6% exp., 1% no exp.).
- *No Password Resets.* Avoiding frequent password resets were noted by 2% overall (2% exp., 1% no exp.).
- *Other.* Includes misclicks or ambiguous answers.

4.2.2. Concerns. Table 5 details why Group W opted against passkeys. Chi-square test [69] revealed that concerns varied significantly by prior passkey experience $\chi^2(9) = 265.79$, $p < .001$, $V = .31$, indicating a moderate effect [14].

- *Habit of Using Passwords.* A reliance on familiar passwords was noted by 47% overall (44% exp., 48% no exp.), making it feel easier than switching to passkeys.
- *Lack of Experience or Knowledge.* No passkey exp. or knowledge was cited by 35% (32% exp., 36% no exp.).
- *Lack of Perceived Benefit.* Twenty-three percent overall (18% exp., 26% no exp.) did not perceive a clear advantage in adopting passkeys over passwords.
- *Passkey Misconceptions.* Incorrect passkey assumptions were reported by 8% (2% exp., 12% no exp.), e.g.:

> *"I don't own a physical passkey."* (P3, Group W)

- *Account Recovery Concerns.* Worries about regaining access if a device is lost or damaged were cited by 6% overall (5% exp., 6% no exp.). One respondent noted:

> *"I am terrible at losing or breaking my phone. If I use a passkey, it is a nightmare to log into apps on a new phone. [...]"* (P15, Group W)

- *Multiple Clients.* Doubts about seamless use across devices were cited by 5% (6% exp., 5% no exp.).
- *Past Negative Experiences.* Some participants recalled previous difficulties and therefore refrained from passkeys (4% overall; 13% exp., 0% no exp.), as noted:

> *"I have had trouble with passkeys on a few websites. I didn't want to go through that hassle."* (P1, Group W)

- *Deferred Adoption.* Two percent overall (1% exp., 3% no exp.) delayed the adoption by initially registering with a password and adding a passkey later:

> *"I like to sign up with passwords first and passkeys second. Don't trust them enough."* (P5, Group W)

- *Security and Privacy Concerns.* Few participants (2% overall; 2% exp., 1% no exp.) felt that passwords offered better security. A participant wrote the following remark, overlooking that most smartphones also support alphanumeric passcodes, and passkeys additionally require physical access to the device to be exploited.

> *"I felt more secure using a password because it offers more possible combinations than a passkey PIN does."* (P12, Group W)

- *Other.* Covers misclicks or ambiguous answers.

4.3. Barriers to Successful Passkey Adoption

Table 6 lists barriers for Group K participants who attempted but didn't complete passkey adoption. Chi-square

test [69] showed a significant association between passkey experience and barriers, $\chi^2(9) = 27.70$, $p < .001$, $V = .14$.

- *Passkey Misconceptions.* Misunderstandings about passkeys occurred in 25% of participants (19% exp. and 28% no exp.), primarily due to expecting password-like behavior or confusion about the process:

> *"I kept clicking [on] passkey, but it kept popping up my Face ID."* (P16, Group K)

- *Passcode Misconceptions.* The need to enter the device passcode (PIN, pattern, or password) was misinterpreted as a security risk by 23% (18% exp. and 26% no exp.), fearing it granted the platform excessive access:

> *"I had to enter my device PIN, which I found very suspicious! [...]"* (P7, Group K)

- *Manual Passkey Activation.* Several OSs require manually activating passkeys, e.g., enabling iCloud Keychain on iOS/macOS, or Windows Hello on Windows. 17% (15% exp., 18% no exp.) noted this barrier due to technical difficulty or reluctance to change settings:

> *"It was going to make me change the settings on my PC. I didn't want to do that. [...]"* (P2, Group K)

- *Perceived Complexity.* Overall, 11% (10% exp., 12% no exp.) felt the setup process was overly complicated:

> *"Too many boxes came up, and I didn't understand what was being asked of me."* (P14, Group K)

- *Account Recovery Concerns.* 9% (10% exp., 8% no exp.) feared losing access if their device was lost.
- *Multiple Clients.* 8% (9% exp., 8% no exp.) expressed concern about cross-device passkey use.
- *Password Manager Integration.* 7% (9% exp., 6% no exp.) reported PM integration issues, including no Android browser support [41], needing to adjust settings or install extensions, and failed passkey insertion:

> *"I couldn't save it in my password manager, and I want to have all my accounts there."* (P6, Group K)

- *Biometric Misconceptions.* Although our description of passkeys incorporated prior work [53] to address biometric misconceptions, 7% of participants still voiced these concerns (5% exp., 8% no exp.):

> *"I got nervous about the app storing my fingerprint, even though it said it would store on my device only. Because I do not trust the app yet."* (P11, Group K)

- *Technical Difficulties.* All devices supported passkeys, yet technical errors were reported by 3% overall.
- *Other.* Encompasses misclicks and ambiguous answers.

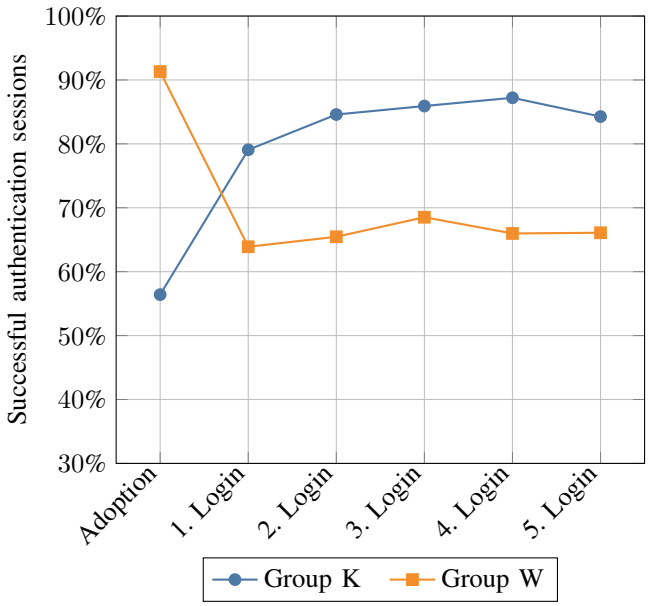


Figure 4: Successful authentication rates of both groups during adoption (Phase 1) and five subsequent logins (Phase 2).

4.4. Barriers to Password with 2FA Adoption

Among 183 participants of Group W who began but didn't finish authentication, 163 (89%) had SMS-OTP problems (e.g., not receiving or finding the message, entering a wrong code, or confusion), 13 (7%) faced password-policy issues, 5 (3%) timed out, and 2 (1%) gave unclear reasons.

5. Results: Passkey Usage (Phase 2)

In this section, we present the findings from Phase 2 on passkey adoption and compare them to Group W, which serves as the baseline to interpret the results. We examine usage telemetry, challenges, synchronizations, and recovery.

5.1. Longitudinal Usage Telemetry

Table 7 presents usage telemetry from the first five login attempts per participant in Phase 2 alongside Phase 1 results, illustrating longitudinal trends from initial passkey enrollment through sustained use. It also reports sample sizes for both measured metrics and self-reported surveys (86% overall completion; 75% in Phase 2). To maintain representative participant numbers, we limited the analysis to up to five login sessions per participant. Nevertheless, of the 6,233 attempted authentication sessions recorded in Phase 2, 6,172 (99%) are included in our analysis.

5.1.1. Success Rates. Figure 4 shows the success rates during participants' first five login attempts. During the adoption phase (Phase 1), Group W had a higher success rate than Group K (91% vs. 56%). At the first login in

TABLE 7: Longitudinal comparison of Groups K and W across initial adoption (Phase 1) and five subsequent login sessions per participant (Phase 2). For each session, authentication metrics include total attempts, successful attempts (with success rate), and median duration. Survey outcomes include completion rates, median SUS scores, and median acceptance ratings.

			Phase 1	Phase 2				
	Category	**Group**	**Adoption**	**1. Login**	**2. Login**	**3. Login**	**4. Login**	**5. Login**
Sessions Measured	**Attempts**	Group K	2,950	1,295	727	490	344	89
		Group W	2,107	1,421	909	432	291	174
	Successful	Group K	1,664 (56%)	1,024 (79%)	615 (85%)	421 (86%)	300 (87%)	75 (84%)
		Group W	1,924 (91%)	908 (64%)	595 (65%)	296 (69%)	192 (66%)	115 (66%)
	Duration	Group K	12.6 s	9.2 s	8.9 s	9.4 s	9.6 s	8.5 s
		Group W	52.9 s	59.1 s	57.3 s	60.0 s	58.3 s	58.5 s
Surveys Self-Reported	**Completed**	Group K	2,950 (100%)	1,012 (78%)	533 (73%)	341 (70%)	232 (67%)	68 (76%)
		Group W	2,107 (100%)	1,088 (77%)	708 (78%)	325 (75%)	214 (74%)	134 (77%)
	SUS	Group K	75.00	81.25	80.00	82.50	85.00	82.50
		Group W	67.50	60.00	57.50	55.00	57.50	55.50
	Acceptance	Group K	1.11	1.33	1.44	1.56	1.50	1.56
		Group W	0.67	0.56	0.67	0.89	0.72	0.67

Phase 2, this trend reversed: Group K jumped to 79% (a 23-point gain), while Group W fell to 64% (a 27-point drop). In subsequent logins, Group K's success rose to 84-87%, whereas Group W plateaued at 65-69%. In total, during Phase 2, Group K recorded 2,945 login attempts, of which 2,435 (83%) succeeded and 510 (17%) failed. By comparison, Group W made 3,227 attempts, yielding 2,106 (65%) successes and 1,121 (35%) failures. On average, Group K required 1.17 attempts per successful login, compared with 1.44 attempts for Group W. These results **indicate that, after initial setup, passkeys deliver higher and more consistent success rates than passwords with 2FA**.

5.1.2. Durations. Median authentication durations for Group K decreased from 12.6 s at initial adoption to between 8.5 s and 9.6 s during subsequent logins. In contrast, Group W's median time rose from 52.9 s at setup to between 57.3 and 60.0 s across login sessions. The accelerating speed of passkey logins likely reflects both a streamlined process since users no longer choose a storage location and growing familiarity with the authentication flow. By comparison, password logins probably remained slow due to repeated entry attempts. These results **demonstrate that passkey authentication continues to speed up over time, whereas password-based login becomes progressively slower**.

5.1.3. Usability and Acceptance. Self-reports align with the measured trends. In Phase 1, Group K had higher median SUS scores (75 vs. 67.5) and acceptance (1.11 vs. 0.67) than Group W. At the first login in Phase 2, Group K's SUS rose to 81.25 and acceptance to 1.33, while Group W's SUS fell to 60 and acceptance to 0.56. Over subsequent logins, Group K sustained SUS scores of 80-85 and acceptance ratings of 1.33-1.56, whereas Group W's SUS declined to 55-57.5 and acceptance plateaued at 0.56-0.89. These results **indicate that passkeys improve in perceived usability and acceptance over time and maintain those gains, whereas passwords with 2FA show stagnation or decline**.

5.2. Encountered Challenges

We now present the challenges participants experienced when using passkeys, as reported in the survey.

5.2.1. Reasons for Unsuccessful Logins. Participants in Group K recorded a total of 510 unsuccessful login attempts, yielding 394 completed surveys. The reported causes are:

Unsuccessful Synchronization. The most common issue, cited by 77% of participants, was unsuccessful passkey synchronization. Specific issues are detailed in Section 5.3.

Device Dependency. Eighteen percent of participants encountered problems due to device dependency. Typical scenarios included lost, broken, or stolen devices. A few participants also lost access after performing a device reset.

Technical Difficulties. Four percent of participants noted encountering technical errors during the login process.

Other. A small fraction (1%) provided unclear reasons.

5.2.2. Passkey Sharing. In 170 login attempts, participants noted three hurdles when trying to share passkeys with others (e.g., family members). First, not all storage solutions support user-to-user sharing. For example, Windows Hello synchronized passkeys across a user's Windows devices but offered no mechanism to share them with other users, leaving a PM as the only option for passkey sharing on Windows. Second, even when a storage location did support sharing, participants were often unaware of this capability or mistakenly searched for the option in the app or device settings. Third, among those who did discover the sharing feature, the workflow was perceived as complex: For iCloud, users must create a "Shared Group" in the "Passwords" app, add existing contacts from their address book, and then assign passkeys to that group. Several participants also noted that the app's name, "Passwords", is misleading given its role in also managing passkeys. These insights **suggest that platform constraints, poor discoverability, and complex procedures hinder users' ability to share passkeys**.

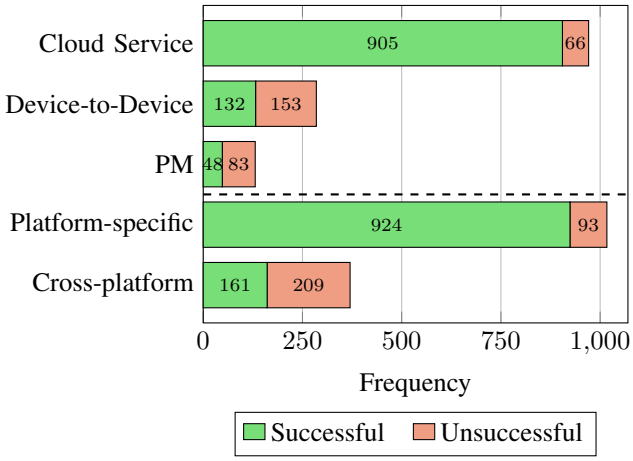


Figure 5: Frequencies and success rates of passkey synchronizations by method (cloud service, device-to-device, and PM) and scope (platform-specific vs. cross-platform).

5.2.3. Immutable Storage Location. In 84 attempts, participants noted a key limitation: once created, a passkey's storage location cannot be changed. If the initial storage lacks sharing or cross-platform synchronizations, users cannot transfer it (e.g., to a PM), without undergoing account recovery to generate a new passkey. As some OSs set a default storage location (e.g., iCloud Keychain on Apple devices), users seldom consider this choice and are unaware of its long-term implications. As one participant noted:

> *"It's trapped in the [iCloud] keychain[.] I can't move it to Bitwarden and sync it to Windows."* (P4, Group K)

This **suggests users may lack accurate mental models of passkeys and expect them to work like passwords.**

5.2.4. Non-uniform Authentication UI. In 67 attempts, participants reported inconsistent authentication interfaces across OSs. On Android, participants were prompted to select a storage location actively, while iOS presented a default choice that could be passively accepted or manually changed. Terminology varied as well, e.g., labels such as "master key" appeared instead of "passkey". These discrepancies caused confusion and fostered uncertainty about whether a passkey had been created and where it was stored, **suggesting that UI and terminology inconsistencies impede users from forming mental models of passkeys**.

5.2.5. Perceived Loss of Control. In 32 attempts, participants expressed concerns about losing control of their credentials, unsure where passkeys were stored, how to delete or share them, or how to transfer them for future logins. These uncertainties **suggest that users may not have yet formed reliable mental models of passkey functionality**.

5.3. Synchronization of Passkeys

1,387 login attempts involved synchronization. Figure 5 shows frequencies and success rates by method and scope. The most prevalent synchronization method was via built-in cloud services, with 971 attempts (905 successful and 66 unsuccessful), resulting in a 93% success rate. Manual device-to-device transfers accounted for 285 attempts (132 succeeded and 153 failed), for a 46% success rate. PM-based synchronization was used 131 times (48 successful, 83 unsuccessful) for a 36% success rate. The results **indicate that cloud-based synchronization is reliable and widely adopted in practice, while manual transfers and PM-based methods pose substantial difficulties for users**.

When grouped by scope, platform-specific synchronizations comprised 1,017 attempts (924 successful, 93 unsuccessful), resulting in a 91% success rate. In contrast, cross-platform synchronizations succeeded in only 161 out of 370 attempts (44% success), **suggesting that platform-specific passkey synchronization is robust in practice, whereas cross-platform synchronization remains problematic**.

We examine the particular challenges as follows.

5.3.1. Built-in Cloud Services. Some participants noted that they first had to enable synchronization via the built-in cloud service. Many were unaware of this step and struggled to find the corresponding option. One participant described:

> *"Took me ages to realize I needed to enable synchronization first."* (P10, Group K)

Moreover, even when synchronization was enabled and participants were signed in to the same account on both devices, the service occasionally failed to sync. Although most attempts succeeded, these results **suggest that the primary barrier to using built-in cloud services is the initial activation of synchronization**.

5.3.2. Manual Device-to-Device Transfer. There are two manual transfer options. The first involved scanning a QR code with the device currently holding the passkey, typically a mobile device. Some participants reported believing they did not have a QR code scanner installed, despite most camera apps offering built-in scanning. One participant noted:

> *"I can't scan this [QR] code[.] I don't have a scanner installed."* (P13, Group K)

A few participants scanned the QR code but noted that nothing happened, preventing synchronization.

The second option used Bluetooth. Multiple users reported that transfers failed despite Bluetooth being enabled.

These findings **indicate that manual passkey transfer is perceived as overly complex and error-prone**.

5.3.3. Third-Party Password Managers. Participants face several challenges when leveraging PMs for passkey synchronization. Android 15, the latest release, currently lacks support for creating or inserting passkeys in browsers [41], which prevented participants from saving or auto-filling their credentials. Further, after installing a PM on their device, participants had to manually enable its passkey functionality in the system settings on mobile devices and install browser

extensions for desktop devices, a step many overlooked. Most OSs also lack the option to designate a PM as the default storage location for passkeys. Even when enabled, inserting passkeys from PMs sometimes failed, forcing users to resort to manual transfer or recovery:

> *"I have the passkey in Dashlane, it's on my phone, but I can't insert it [...]"* (P9, Group K)

Participants also had to install the PM's browser extension on desktop devices to use passkeys in a web browser.

In summary, these insights **indicate that synchronizing passkeys via a PM imposes technical constraints and involves overly complex configuration steps**.

5.4. Account Recovery

This section presents the account recovery results, including success rates, durations, and qualitative feedback.

5.4.1. Success Rates. In Group K, participants experienced 510 unsuccessful login sessions and initiated account recovery in 416 cases (82%), of which 377 recoveries succeeded (91%). In Group W, there were 1,121 failed attempts and 908 recovery initiations (81%), yielding 836 successful recoveries (92%). The results **suggest that success rates are similar for passkey and password recovery**.

5.4.2. Duration. The median durations of account recovery were 62.5 s for Group K and 72.0 s for Group W, **indicating that passkey recovery is faster than recovery with passwords and 2FA**.

5.4.3. Reasons for Unsuccessful Recoveries. In Group K, 39 account-recovery attempts failed, and 30 participants completed the follow-up survey. Of those, 29 (97%) reported SMS-OTP issues, failing to receive or locate the message, entering an incorrect code, or being unsure how to proceed, while one response was ambiguous. In Group W, 72 recovery attempts were unsuccessful, with 52 survey completions: 49 (94%) cited SMS-OTP problems and three timed out.

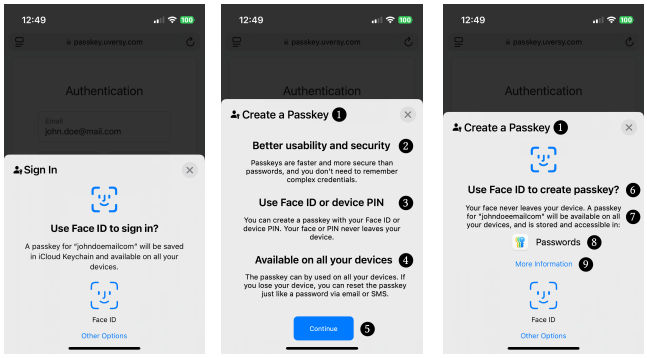
6. Discussion

We discuss the implications of our results and, alongside each topic, outline recommendations for future work.

6.1. Strategies to Accelerating Passkey Adoption

Our results show that passkeys deliver higher usability and faster authentication than passwords with 2FA, contrary to prior findings [65], [70]. We observe higher acceptance yet substantially lower adoption. Together, these findings suggest that passkeys can enhance UX while also revealing critical adoption barriers. We outline strategies to support users' choice of passkeys and overcome adoption hurdles.

Passkey Choice. We confirm prior findings [85], showing that users value the security and simplicity of passwordless authentication and the lack of memorization, yet



(a) Original UI (b) Step for No Exp. (c) Updated UI

Figure 6: Comparing the exemplary original iOS UI (a) with proposed enhancements: A informational overlay for inexperienced users (b) and an updated adoption UI (c).

they hesitate to choose passkeys because of concerns about cross-device use, technical failures, and recovery. Our study contributes novel insights by identifying concerns that appear more decisive for adoption, including entrenched password habits, limited passkey experience, and low perceived benefit. We also found that participants with prior passkey experience adopted passkeys far more often than novices.

We propose two recommendations. First, we advocate the use of digital nudges, which are interventions that preserve users' choices without materially altering incentives [73], [81]. Nudges have been shown to promote cybersecurity behavior change [6], [71], [72]. Beyond the information-salience nudges [80] already emphasized in current UX guidelines [28], we suggest:

- Offer passkeys as the default authentication method for users with passkey experience, while retaining a clear password fallback. Experience can be inferred locally, via an OS-level flag set after the user's first adoption on the device, or by the vendor, via prior passkey registrations tied to the user's account. Consider applying this nudge to sensitive accounts (e.g., online banking).
- Provide social proof by showing numerous users chose passkeys, encouraging them to follow the crowd [80].
- Increase the effort required to select passwords by adding a confirmation step, e.g., "Are you sure you want to use a password?" [11].

Second, we suggest emphasizing passkeys' benefits. Unlike prior work [65], our data show that passkeys are adopted much faster than passwords, yet few inexperienced users were aware of this. We propose augmenting the information text in the UX guidelines [28], such as: "Passkeys are faster and more secure than passwords, and you don't need to remember complex credentials." Future work should test the impact of the nudges and messages on passkey adoption.

Passkey Adoption. Passkey adoption faces usability challenges, leading to lower success rates than passwords with 2FA. We confirm biometric misconceptions from prior work [53] and uncovered novel ones: Many users interpreted the required passcode entry (PIN, pattern, or password)

as a security vulnerability, frequently resulting in adoption cancellations, particularly among first-time passkey users.

To address these issues, we propose revising the passkey adoption UI, as exemplified by the iOS UI in Figure 6. Most of the reported problems persist across OSs, so our recommendations generalize broadly. Since users without prior passkey experience had substantially lower success rates, we recommend adding an informational overlay on the first attempt (Figure 6b), also educating users when the service itself provides no passkey guidance. The OS can detect whether a user has previously created a passkey and display this screen accordingly. To tackle misconceptions, the overlay explicitly informs users that they are creating a passkey ❶, succinctly highlights its benefits ❷, and reassures them that their biometrics [53] and passcode never leave their device ❸. Concerns regarding multi-client use and account recovery are addressed ❹ before the user can proceed with the passkey adoption process ❺. We also propose updating the default passkey adoption interface (Figure 6c), which could appear initially in subsequent authentications. In this revised UI, users are informed that they are creating a passkey via Face ID ❻ and reminded that their biometrics and passcode never leave their device ❼. As most users were unaware of where passkeys are stored, and some feared less control, we explicitly state the storage location and how users can access their passkeys ❽. An option to reopen the informational overlay at any time ❾ ensures that users can revisit the guidance as needed. Consistent with prior work [53], [64], we urge OS vendors to adopt a standardized authentication UI with uniform terminology.

Beyond the UI, we newly identified that participants experienced friction when system settings had to be modified during passkey adoption. On iOS and macOS, users must enable iCloud Keychain, and Windows requires activation of Windows Hello. To use passkeys with a PM, mobile OSs require manual activation, and desktop OSs demand browser-extension installation. Thereby, users are seldom made aware of these prerequisites. To streamline adoption, we recommend either automatically enabling all necessary passkey-related settings or prompting users with a one-click option upon OS update or PM installation (or update). By preempting the required settings changes in advance, effort and confusion during the adoption process could be reduced. We further encourage Google to offer an API for PM support within its Chrome browser on Android [41].

Our results confirm that mobile devices and biometric second factors are associated with higher adoption rates [63], [65]. To extend these benefits to desktops, OS vendors should continue expanding biometric capabilities through hardware (e.g., Touch ID on macOS) and software (e.g., facial recognition in Windows Hello) and offer biometrics as the default second factor. Future work should empirically test our recommendations' impact on passkey adoption.

6.2. Addressing Challenges of Passkey Usage

Our longitudinal analysis found that passkey success rates and usability increased over time while authentication times decreased, aligning with prior research [65]. Further, we newly show that passkeys achieved markedly higher success rates after first usage than passwords, suggesting users adapt quickly to them. Still, we identified novel challenges, particularly involving passkey sharing and synchronization.

Dedicated Passkey Management App. We uncovered that passkeys are primarily stored in built-in cloud services, but users can't easily locate or manage them, leading to a loss of control. Since passkey management is often buried deep within settings, making it difficult to discover, we propose OSs to offer a standalone management app. While iOS and macOS include a "Passwords" app, its name conceals passkey functionality, and it lacks essential features. The app should streamline sharing by including a "Share" button for each passkey and support storage migration, enabling moving passkeys from cloud storage to a PM. Users should be introduced to this app during passkey adoption (Figure 6c).

Passkey Synchronization. We gained novel insights into the usability of passkey synchronization, identifying it as the primary cause of failed logins:

Built-in Cloud Services: Some OSs require users to enable passkey synchronization manually. We recommend enabling synchronization by default and, for users who haven't activated it, prompting after the first passkey creation with a one-click activation option. Because most users rely on built-in cloud services tied to a single ecosystem, vendor lock-in [24] is exacerbated, and platform switching is impeded. Future work could explore cross-cloud synchronization (e.g., adding a Windows Hello account to iCloud Keychain), and the FIDO Alliance should standardize such a system.

Manual Device-to-Device Transfer: Primarily used for cross-platform sync, it proved too complex and error-prone for most users. We recommend adding interactive guidance (e.g., a short animation or video) in the passkey login UI.

Third-Party Password Managers: PM challenges from adoption also persisted in use. Further, OSs should prompt users, during PM installation or update, to choose a default passkey storage, a feature currently offered only on iOS. Furthermore, PM vendors should validate that their implementations correctly insert passkeys during login.

Account Recovery. Unlike security keys, which lack scalable recovery and can lock users out if the sole key is lost [55], passkeys can be backed up via device synchronization [30]. Yet, our results uncover that synchronization, especially cross-platform, does not always succeed. While registering multiple passkeys on different devices would be ideal for security, it imposes major usability burdens [51]. Thus, prior work advocated exploring an OTP-based recovery option to enable users to register a new passkey [65], [85], which we implemented via SMS. Compared to password recovery, this approach achieves similar success rates with faster recovery times, suggesting a reasonable balance between security and usability for most services.

6.3. Limitations

Recruitment. Recruitment was not fully random, as participants needed to use our industry partner's platform, but demographics approximated the general population. Since all users were European, results may not generalize beyond this region; future work could replicate the study in other regions. **Field Study.** We traded experimental control for authentic behavior and real-world challenges. Data sensitivity of the healthcare context may have affected authentication choices. Attrition was similar, 31.8% in Group K and 29.5% in Group W, matching typical longitudinal research [65]. **Group Assignment.** Allowing users to self-select their authentication method reflects real choices but may introduce bias. The brief informational text, based on FIDO UX guidelines [28] and Lassak et al. [53], and the limitation on switching authentication methods may have introduced bias, but both mirror industry practice [34], [42], [44], [47]. **Self Reporting.** Our survey relies on self-reports, which may be imprecise, so we asked for immediate feedback after each authentication. **Design of Control Group.** The control group used passwords with at least eight characters from two classes (Section 3.1) and 2FA, which may have affected comparisons but reflects common practice [39], [56], [67]. **Retention.** The initially selected authentication method was retained during the study, which does not represent real-world conditions. Future work should permit method switching. **Autofill.** Password autofill was allowed but not tracked, which could impact authentication durations of Group W. We suggest future work to document password autofill use.

7. Conclusion

This paper presents a large-scale field study on the adoption and usage of passkeys. Although initial passkey adoption had lower success rates than passwords with 2FA, we showed that passkeys offer superior usability and acceptance. With repeated logins, they outperformed passwords with 2FA in success rates while usability and acceptance continued to grow. We found new adoption barriers, such as novel misconceptions and manual passkey activation, as well as key usage challenges, including cross-platform synchronization, passkey sharing, and interactions with password managers. Accordingly, we offer actionable recommendations to streamline passkey adoption and usability.

Availability

To facilitate future research, we made our study's implementation open-source[3], enabling researchers to replicate our study and capture key metrics. Although we are unable to share raw data due to a data protection agreement between the platform vendor and its users, all statistical analyses performed with SPSS and the codebook have been published.

3. Open-source code: https://github.com/PasskeyStudy/Availability

Declaration of Generative AI Technologies in the Writing Process

During the preparation of this work, the authors used DeepL, Grammarly, and ChatGPT (Version 4o) in order to improve the language and readability. After using the tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.[4]

Acknowledgments

We thank Magdalena Glas, Thomas Baumer, the reviewers, and our shepherd for their constructive feedback.

References

[1] 1Password. What are passkeys?, 2024. Accessed: 02/11/25. URL: https://1password.com/product/passkeys.

[2] Adobe. Login and security, 2025. Accessed: 02/11/25. URL: https://account.adobe.com/security.

[3] Elham Al Qahtani, Lipsarani Sahoo, Yousra Javed, and Mohamed Shehab. "why would someone hack me out of thousands of students": Video presenter's impact on motivating users to adopt 2fa. In *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, pages 139–150, 2022.

[4] Apple, Inc. About the security of passkeys, 2022. Accessed: 02/11/25. URL: https://support.apple.com/en-us/102195.

[5] Apple, Inc. Share passwords or passkeys with people you trust on iphone, 2025. Accessed: 02/11/25. URL: https://support.apple.com/en-gb/guide/iphone/iphe6b2b7043/ios.

[6] Thomas Baumer, Tobias Reittinger, Sascha Kern, and Günther Pernul. Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 239–258, Philadelphia, PA, August 2024. USENIX Association. URL: https://www.usenix.org/conference/soups2024/presentation/baumer.

[7] Arnar Birgisson. Security of passkeys in the google password manager, 2022. Accessed: 02/11/25. URL: https://security.googleblog.com/2022/10/SecurityofPasskeysintheGooglePasswordManager.html.

[8] Bitwarden. Innovating in passwordless, 2024. Accessed: 02/11/25. URL: https://bitwarden.com/passwordless-passkeys/.

[9] John Brooke et al. Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.

[10] Andre Büttner and Nils Gruschka. Device-bound vs. synced credentials: A comparative evaluation of passkey authentication. In *Proceedings of the 11th International Conference on Information Systems Security and Privacy - Volume 2: ICISSP*, pages 651–659. INSTICC, SciTePress, 2025. doi:10.5220/0013380600003899.

[11] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–15, 2019.

[12] Dhiman Chakraborty and Sven Bugiel. simfido: Fido2 user authentication with simtpm. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 2569–2571, New York, NY, USA, 2019. Association for Computing Machinery.

4. For transparency, we publish AI Usage Cards documenting our use of generative AI [83]: https://ai.uversy.com/passkeys

[13] 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 *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 339–356, Santa Clara, CA, August 2019. USENIX Association.

[14] Jacob Cohen. *Statistical power analysis for the behavioral sciences*. routledge, 2013.

[15] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "it's not actually that horrible" exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2018.

[16] Silvia Convento, Court Jacinic, and Becca Shareff. Making authentication faster than ever: passkeys vs. passwords, 2023. Accessed: 02/11/25. URL: https://security.googleblog.com/2023/05/making-authentication-faster-than-ever.html.

[17] Harald Cramér. *Mathematical Methods of Statistics*. Princeton University Press, 1946.

[18] Alaa Daffalla, Arkaprabha Bhattacharya, Jacob Wilder, Rahul Chatterjee, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. A framework for abusability analysis: The case of passkeys in interpersonal threat models. In *Proceedings of the 34th USENIX Security Symposium*. USENIX Association, 2025.

[19] 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: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers 22*, pages 160–179. Springer, 2018.

[20] Sanchari Das, Gianpaolo Russo, Andrew C Dingman, Jayati Dev, Olivia Kenny, and L Jean Camp. A qualitative study on usability and acceptability of yubico security key. In *Proceedings of the 7th workshop on socio-technical aspects in security and trust*, pages 28–39, 2017.

[21] Vincent Delitz. Windows 11's upcoming passkey (windows hello) features, 2024. Accessed: 02/11/25. URL: https://www.microsoft.com/en-us/security/blog/2024/05/02/microsoft-introduces-passkeys-for-consumer-accounts/.

[22] Nicole M Deterding and Mary C Waters. Flexible coding of in-depth interviews: A twenty-first-century approach. *Sociological methods & research*, 50(2):708–739, 2021.

[23] 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 *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 19–35, 2020.

[24] Joseph Farrell and Paul Klemperer. Coordination and lock-in: Competition with switching costs and network effects. *Handbook of industrial organization*, 3:1967–2072, 2007.

[25] FIDO Alliance. Apple, google and microsoft commit to expanded support for fido standard to accelerate availability of passwordless sign-ins, 2022. Accessed: 02/11/25. URL: https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/.

[26] FIDO Alliance. Client to authenticator protocol (ctap), 2022. Accessed: 02/11/25. URL: https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html.

[27] FIDO Alliance. Sc magazine: Finding fido: What fast identity online is, and how it works, 2022. Accessed: 02/11/25. URL: https://fidoalliance.org/sc-magazine-finding-fido-what-fast-identity-online-is-and-how-it-works/.

[28] FIDO Alliance. Fido alliance ux guidelines for passkey creation and sign-ins, 2023. Accessed: 02/11/25. URL: https://fidoalliance.org/wp-content/uploads/2023/05/FIDO-Alliance-UX-Guidelines-for-Passkey-Creation-and-Sign-ins.pdf.

[29] FIDO Alliance. Fido authentication, 2023. Accessed: 02/11/25. URL: https://fidoalliance.org/fido2/.

[30] FIDO Alliance. Passkeys, 2024. Accessed: 02/11/25. URL: https://fidoalliance.org/passkeys/.

[31] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, page 657–666, New York, NY, USA, 2007. Association for Computing Machinery. doi:10.1145/1242572.1242661.

[32] Thomas Franke, Christiane Attig, and Daniel Wessel. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ati) scale. *International Journal of Human–Computer Interaction*, 35(6):456–467, 2019.

[33] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. " what was that site doing with my facebook password?" designing password-reuse notifications. In *Proceedings of the 2018 acm sigsac conference on computer and communications security*, pages 1549–1566, 2018.

[34] Google. The easiest and most secure way to sign in to your google account, 2025. Accessed: 02/11/25. URL: https://www.google.com/account/about/passkeys/.

[35] Google. Save, manage & protect your passwords, 2025. Accessed: 02/11/25. URL: https://support.google.com/accounts/answer/6208650.

[36] Google Cloud. Cybersecurity forecast 2024, 2024. Accessed: 02/11/25. URL: https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf.

[37] Google LLC. Mercari's passkey authentication speeds up sign-in 3.9 times, 2023. Accessed: 02/11/25. URL: https://developers.google.com/identity/passkeys/case-studies/mercari.

[38] Google LLC. Password manager dashlane sees 70% increase in conversion rate for signing-in with passkeys compared to passwords, 2023. Accessed: 02/11/25. URL: https://developers.google.com/identity/passkeys/case-studies/dashlane.

[39] Paul Grassi, James Fenton, Elaine Newton, Ray Perlner, Andrew Regenscheid, William Burr, Justin Richer, Naomi Lefkovitz, Jamie Danker, Yee-Yin Choong, Kristen Greene, and Mary Theofanos. Digital identity guidelines: Authentication and lifecycle management. Special Publication 800-63B, National Institute of Standards and Technology, Gaithersburg, 2020. URL: https://doi.org/10.6028/NIST.SP.800-63b.

[40] Eric Grosse and Mayank Upadhyay. Authentication at scale. *IEEE Security & Privacy*, 11(1):15–22, 2013.

[41] Travis Hogan. Save and sign in to android apps with passkeys using 1password, 2024. Accessed: 02/11/25. URL: https://blog.1password.com/save-use-passkeys-android/.

[42] Amazon.com Inc. Passkey, 2025. Accessed: 02/11/25. URL: https://www.amazon.com/ax/claim/webauthn/enroll.

[43] Apple Inc. Sign in with apple account, 2025. Accessed: 02/11/25. URL: https://www.icloud.com/.

[44] Uber Technologies Inc. Passkeys, 2025. Accessed: 02/11/25. URL: https://account.uber.com/passkeys.

[45] Mazharul Islam, Sunpreet S. Arora, Rahul Chatterjee, and Ke Coby Wang. Detecting compromise of passkey storage on the cloud. In *Proceedings of the 34th USENIX Security Symposium*. USENIX Association, 2025.

[46] Michael B. Jones, Akshay Kumar, and Emil Lundberg. Web authentication: An api for accessing public key credentials level 3, 2023. Accessed: 02/11/25. URL: https://www.w3.org/TR/webauthn-3/.

[47] KAYAK. Sign in or create an account, 2025. Accessed: 02/11/25. URL: https://www.kayak.com/login.

[48] Jan H. Klemmer, Marco Gutfleisch, Christian Stransky, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. "make them change it every week!": A qualitative exploration of online developer advice on usable and secure authentication. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 2740–2754, New York, NY, USA, 2023. Association for Computing Machinery.

[49] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the sigchi conference on human factors in computing systems*, pages 2595–2604, 2011.

[50] Dhruv Kuchhal, Muhammad Saad, Adam Oest, and Frank Li. Evaluating the security posture of real-world fido2 deployments. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 2381–2395, New York, NY, USA, 2023. Association for Computing Machinery.

[51] Johannes Kunke, Stephan Wiefling, Markus Ullmann, and Luigi Lo Iacono. Evaluation of account recovery strategies with fido2-based passwordless authentication. *arXiv preprint arXiv:2105.12477*, 2021.

[52] Markus Langer, Cornelius J König, and Andromachi Fitili. Information as a double-edged sword: The role of computer experience and information on applicant reactions towards novel technologies for personnel selection. *Computers in Human Behavior*, 81:19–30, 2018.

[53] 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 *30th USENIX Security Symposium (USENIX Security 21)*, pages 91–108, 2021.

[54] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. Why aren't we using passkeys? obstacles companies face deploying fido2 passwordless authentication. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 7231–7248, Philadelphia, PA, August 2024. USENIX Association. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/lassak.

[55] 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 *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285. IEEE, 2020.

[56] Siqi Ma, Runhan Feng, Juanru Li, Yang Liu, Surya Nepal, Diethelm, Elisa Bertino, Robert H Deng, Zhuo Ma, and Sanjay Jha. An empirical study of sms one-time password authentication in android apps. In *Proceedings of the 35th annual computer security applications conference*, pages 339–354, 2019.

[57] Henry B Mann and Donald R Whitney. On a test of whether one of two random variables is stochastically larger than the other. *The annals of mathematical statistics*, pages 50–60, 1947.

[58] mdn web docs. Web authentication api, 2024. Accessed: 02/11/25. URL: https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API#browser_compatibility.

[59] Microsoft. Microsoft digital defense report 2023, 2023. Accessed: 02/11/25. URL: https://www.microsoft.com/de-de/security/security-insider/microsoft-digital-defense-report-2023.

[60] Microsoft. Microsoft digital defense report 2024, 2024. Accessed: 02/11/25. URL: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024.

[61] Milica Mihajlija and Yumeji Hattori. How yahoo! japan increased passkeys adoption to 11% and reduced sms otp costs, 2023. Accessed: 02/11/25. URL: https://web.dev/case-studies/yahoo-japan-passkeys?hl=en.

[62] Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin, and Jean-Pierre Seifert. Sms-based one-time passwords: Attacks and defense: (short paper). In *Detection of Intrusions and Malware, and Vulnerability Assessment: 10th International Conference, DIMVA 2013, Berlin, Germany, July 18-19, 2013. Proceedings 10*, pages 150–159. Springer, 2013.

[63] Florian Nawrath. Quantitative analysis of fido2 client support. *Proc. WAY*, 2021.

[64] Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, and Tatsuru Higurashi. Observation study on usability challenges for fingerprint authentication using webauthn-enabled android smartphones. *Age*, 20:29, 2020.

[65] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. User perceptions of the usability and security of smartphones as {FIDO2} roaming authenticators. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 57–76, 2021.

[66] passkeys.dev. Device support, 2024. Accessed: 02/11/25. URL: https://passkeys.dev/device-support/.

[67] PayPal. Password security, 2025. Accessed: 01/29/25. URL: https://www.paypal.com/bb/webapps/mpp/security/secure-passwords.

[68] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310, 2017.

[69] Karl Pearson. X. on the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 50(302):157–175, 1900.

[70] Sangeeta Ranjit and Scott Bingham. Convincing a billion users to love passkeys: Ux design insights from microsoft to boost adoption and security, 2024. Accessed: 08/14/25. URL: https://www.microsoft.com/en-us/security/blog/2024/12/12/convincing-a-billion-users-to-love-passkeys-ux-design-insights-from-microsoft-to-boost-adoption-and-security/.

[71] Tobias Reittinger, Magdalena Glas, Sarah Aminzada, and Günther Pernul. Employee motivation in organizational cybersecurity: Matching theory and reality. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 3–16. Springer, 2024.

[72] Tobias Reittinger, Magdalena Glas, Sarah Aminzada, and Günther Pernul. Motivational factors in cybersecurity: linking theory to organizational practice. *Information & Computer Security*, 2025.

[73] Tobias Reittinger and Günther Pernul. A taxonomy of positive incentives to motivate cybersecurity behaviors. In *Proceedings of the 58th HI International Conference on System Sciences (HICSS-58)*, 2025.

[74] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. A tale of two studies: The best and worst of yubikey usability. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 872–888. IEEE, 2018.

[75] Ryan Schin. Despite increasing cybersecurity attacks, people still believe antiquated username and passwords are strong enough. Accessed: 02/11/25. URL: https://www.yubico.com/press-releases/despite-increasing-cybersecurity-attacks-people-still-believe-antiquated-username-and-passwords-are-strong-enough/.

[76] Fabian Schwarz, Khue Do, Gunnar Heide, Lucjan Hanzlik, and Christian Rossow. Feido: Recoverable fido2 tokens using electronic ids. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, page 2581–2594, New York, NY, USA, 2022. Association for Computing Machinery.

[77] Kateryna Semenova. How kayak reduced sign in time by 50% and improved security with passkeys, 2023. Accessed: 02/11/25. URL: https://developers.googleblog.com/2023/10/how-kayak-reduced-sign-in-time-and-improved-security-with-passkeys.html.

[78] Samuel Sanford Shapiro and Martin B Wilk. An analysis of variance test for normality (complete samples). *Biometrika*, 52(3-4):591–611, 1965.

[79] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, 18(4):1–34, 2016.

[80] Cass R Sunstein. The council of psychological advisers. *Annual Review of Psychology*, 67(1):713–737, 2016.

[81] Cass R Sunstein. Misconceptions about nudges. *Available at SSRN 3033101*, 2017.

[82] Jinke D Van Der Laan, Adriaan Heino, and Dick De Waard. A simple procedure for the assessment of acceptance of advanced transport telematics. *Transportation Research Part C: Emerging Technologies*, 5(1):1–10, 1997.

[83] Jan Philip Wahle, Terry Ruas, Saif M Mohammad, Norman Meuschke, and Bela Gipp. Ai usage cards: Responsibly reporting ai-generated content. In *2023 ACM/IEEE Joint Conference on Digital Libraries (JCDL)*, pages 282–284. IEEE, 2023.

[84] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 175–188, 2016.

[85] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. Fido2 the rescue? platform vs. roaming authentication on smartphones. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023.

Appendix A. Survey Questionnaires

We present the survey questionnaires of both phases. Following [85], we displayed non-descriptive section names to participants (e.g., "Category A").

A.1. Phase 1

Motivating Factors. *Participants who chose passkeys (Group K) were asked the following questions.* (1) You selected a passkey as your authentication method. Did you choose this option intentionally? [*Yes / No*] (2) Why did you choose a passkey? [*Free text answer*] (3) Did you encounter any difficulties during the setup of the passkey? [*Free text answer*]

Barriers. *Participants who chose passkeys (Group K) and canceled the adoption were asked the following question.* (1) Why did you cancel the passkey setup process? [*Free text answer*]

Concerns. *Participants who chose passwords (Group W) were asked the following questions.* (1) You selected a password as your authentication method. Did you choose this option intentionally? [*Yes / No*] (2) Why did you not choose a passkey? [*Free text answer*] (3) Did you encounter any difficulties during the setup process? [*Free text answer*]

Computer Science Background and Prior Experience. (1) Do you have a background in computer science? [*Yes / No*] (2) How often have you used passwords before this study? [*0 times / 1-3 times / ≥3 times*] (3) Passkeys are a new authentication method. How often have you used passkeys before this study? [*0 times / 1-3 times / ≥3 times*] (4) SMS OTPs are one-time passwords (often six-digit codes) sent via text message to verify your identity. How often have you used an SMS OTP before this study? [*0 times / 1-3 times / ≥3 times*]

Affinity for Technology Interaction (ATI). In the following, we will ask you about your interaction with technical systems. The term "technical systems" refers to apps and other software applications, as well as entire digital devices (e.g., mobile phone, computer, TV, car navigation). Please indicate the degree to which you agree/disagree with the following statements.

[*Six options from "Completly disagree" to "Completly agree"*] (1) I like to occupy myself in greater detail with technical systems. (2) I like testing the functions of new technical systems. (3) I predominantly deal with technical systems because I have to. (4) When I have a new technical system in front of me, I try it out intensively. (5) I enjoy spending time becoming acquainted with a new technical system. (6) It is enough for me that a technical system works; I don't care how or why. (7) I try to understand how a technical system exactly works. (8) It is enough for me to know the basic functions of a technical system. (9) I try to make full use of the capabilities of a technical system.

Privacy Concerns. How much do you agree or disagree with the following statements? [*Seven options from "Strongly disagree" to "Strongly agree"*] (1) I am concerned that companies are collecting too much personal information about me. (2) I am concerned about my privacy. (3) To me, it is important to keep my privacy intact. (4) Novel technologies are threatening privacy increasingly.

Demographics. (1) What is your gender? [*Female / Male / Other / No answer*] (2) How old are you? [*18-19 / 20-29 / 30-39 / 40-49 / 50-59 / 60-69 / 70-79 / ≥80*] (3) What is your highest education? [*Still in school / Middle school / High school / Bachelor / Master / Doctorate / Other*]

A.2. Phase 2

Problems. (1) Did you encounter any problems with the [respective authentication method] during the login? [*No problems / Few problems / Some problems / Many problems*] (2) Please describe the problems you encountered with the [respective authentication method] during the login briefly. [*Free text answer*] (3) Your login attempt with the passkey was unsuccessful. What was the reason for that? [*Free text answer*]

Passkey Authentication Details. (1) Where did you store the passkey? [*Built-in Cloud service (e.g., iCloud Keychain, Google Password Manager, Windows Hello) / Third-Party Password Manager (e.g., 1Password, Bitwarden, Dashlane) / Another device / I don't know*] (2) Which second factor did you use for the passkey authentication? [*Fingerprint / Facial*

Recognition / PIN (e.g., six digits) / Pattern (gesture-based) / Password (e.g., letters, numbers, symbols)] (3) Did you experience any issues with your second factor authentication? If so, please briefly describe them. [*Free text answer*] (4) Have you synchronized your passkey or attempted to do so? If yes, please indicate whether the process was successful. [*Not synchronized / Built-in Cloud Service (e.g., iCloud Keychain, Google Password Manager, Windows Hello) / Manual Device-to-Device Transfer via QR code / Manual Device-to-Device Transfer via Bluetooth / Third-Party Password Manager (e.g., 1Password, Bitwarden)*] [*Successful / Unsuccessful*] (5) Did you experience any issues with the passkey synchronization? If so, please briefly describe them. [*Free text answer*]

Appendix B. Participants' variables

We list the variables of Phase 1 participants in Table 9.
System Usability Scale (SUS). The word "system" refers to [respective authentication method] you just used to log in. How much do you agree or disagree with the following statements? [*Five options from "Strongly disagree" to "Strongly agree"*] (1) I think that I would like to use this system frequently. (2) I found the system unnecessarily complex. (3) I thought the system was easy to use. (4) I think that I would need the support of a technical person to be able to use this system. (5) I found the various functions in this system were well integrated. (6) I thought there was too much inconsistency in this system. (7) I would imagine that most people would learn to use this system very quickly. (8) I found the system very awkward to use. (9) I felt very confident using the system. (10) I needed to learn a lot of things before I could get going with this system.
Acceptance Scale. Please evaluate [respective authentication method] by selecting the one option that best represents your assessment for each row of adjectives. [*Five options between these pairs: Useless vs. Useful; Unpleasant vs. Pleasant; Bad vs. Good; Annoying vs. Nice; Superfluous vs. Effective; Irritating vs. Likeable; Worthless vs. Assisting; Undesirable vs. Desirable; Sleep-inducing vs. Raising alertness*]
Account Recovery. (1) Did you encounter any problems during account recovery? [*No problems / Few problems / Some problems / Many problems*] (2) Please describe the problems you encountered during account recovery briefly. [*Free text answer*] (3) Your account recovery was unsuccessful. What was the reason for that? [*Free text answer*]

Appendix C. Survey Codebook

The codebook of the open-ended survey questions is available in the GitHub repository[3] We considered codes from previous studies on platform authentication with FIDO2 [53], [54], [55], [64], [85].

TABLE 8: Survey participants' characteristics.

Phase 1				Phase 2			
ID	**Group**	**Gender**	**Age**	**ID**	**Group**	**Gender**	**Age**
P1	Group W	M	45	P13	Group K	F	69
P2	Group K	M	41	P14	Group K	F	32
P3	Group W	F	44	P15	Group W	M	27
P4	Group K	M	34	P16	Group K	F	32
P5	Group W	F	36				
P6	Group K	M	32				
P7	Group K	F	37				
P8	Group K	F	55				
P9	Group K	M	54				
P10	Group K	M	34				
P11	Group K	M	54				
P12	Group W	M	59				

Note. For anonymity reasons and better readability, we reset ID numbers to consecutively start at one.

Appendix D. Quoted Survey Participants' Characteristics

We characterize participants with quotes in Table 8.

TABLE 9: Variables of participants in Phase 1, and their associations with passkey choice and adoption.

Category	Variable	Passkey Choice				Passkey Adoption Outcome (Group K)			
		Group K $n = 2,950$	**Group W** $n = 2,107$	**Statistic**	**ES**	**Successful** $n = 1,664$	**Unsuccessful** $n = 1,286$	**Statistic**	**ES**
Gender	Female	1493 (50.6%)	1057 (50.2%)	$\chi^2(2) = 0.57$, $p = .753$	.01	826 (49.6%)	667 (51.9%)	$\chi^2(2) = 5.48$, $p = .064$	.04
	Male	1454 (49.3%)	1049 (49.8%)			838 (50.4%)	616 (47.9%)		
	Other	3 (0.1%)	1 (0%)			0 (0%)	3 (0.2%)		
	No answer	0 (0%)	0 (0%)			0 (0%)	0 (0%)		
Age	18-19	59 (2.0%)	50 (2.4%)	$\chi^2(7) = 3.60$, $p = .825$	.03	34 (2.0%)	25 (1.9%)	$\chi^2(7) = 4.82$, $p = .682$	.04
	20-29	467 (15.8%)	329 (15.6%)			268 (16.1%)	199 (15.5%)		
	30-39	637 (21.6%)	464 (22.0%)			352 (21.2%)	285 (22.2%)		
	40-49	621 (21.1%)	429 (20.4%)			352 (21.2%)	269 (20.9%)		
	50-59	562 (19.1%)	385 (18.3%)			301 (18.1%)	261 (20.3%)		
	60-69	424 (14.4%)	330 (15.7%)			254 (15.3%)	170 (13.2%)		
	70-79	154 (5.2%)	100 (4.7%)			87 (5.2%)	67 (5.2%)		
	80+	26 (0.9%)	20 (0.9%)			16 (1.0%)	10 (0.8%)		
Education	Still in school	72 (2.4%)	39 (1.9%)	$\chi^2(6) = 3.64$, $p = .725$	.03	42 (2.5%)	30 (2.3%)	$\chi^2(6) = 12.27$, $p = .056$	.06
	Middle school	1203 (40.8%)	863 (41.0%)			657 (39.5%)	546 (42.5%)		
	High school	934 (31.7%)	646 (30.7%)			522 (31.4%)	412 (32.0%)		
	Bachelor	242 (8.2%)	183 (8.7%)			148 (8.9%)	94 (7.3%)		
	Master	127 (4.3%)	101 (4.8%)			70 (4.2%)	57 (4.4%)		
	Doctorate	59 (2.0%)	41 (1.9%)			44 (2.6%)	15 (1.2%)		
	Other	313 (10.6%)	234 (11.1%)			181 (10.9%)	132 (10.3%)		
ATI		3.78	3.78	$U = 2,992,336.5$, $p = .024$	.03	3.78	3.89	$U = 1,048,786.0$, $p = .356$	.02
PC		5.50	5.00	$U = 2,567,618.0$, $\mathbf{p < .001}$	.15	5.50	5.25	$U = 1,050,959.5$, $p = .405$	.02
CS bkgd.	Yes	279 (9.5%)	181 (8.6%)	$\chi^2(1) = 1.12$, $p = .290$	.01	177 (10.6%)	102 (7.9%)	$\chi^2(1) = 6.20$, $p = .013$	.05
	No	2671 (90.5%)	1926 (91.4%)			1487 (89.4%)	1184 (92.1%)		
Prior exp.	Yes	1721 (58.3%)	675 (32.0%)	$\chi^2(1) = 341.08$, $\mathbf{p < .001}$	.26	1235 (74.2%)	486 (37.8%)	$\chi^2(1) = 396.04$, $\mathbf{p < .001}$	.37
	No	1229 (41.7%)	1432 (68.0%)			429 (25.8%)	800 (62.2%)		
OS	Android	1554 (52.7%)	1124 (53.3%)	$\chi^2(3) = 7.46$, $p = .059$	.04	896 (53.8%)	658 (51.2%)	$\chi^2(3) = 70.39$, $\mathbf{p < .001}$	.15
	iOS	844 (28.6%)	541 (25.7%)			539 (32.4%)	305 (23.7%)		
	macOS	191 (6.5%)	160 (7.6%)			76 (4.6%)	115 (8.9%)		
	Windows	361 (12.2%)	282 (13.4%)			153 (9.2%)	208 (16.2%)		
Storage	Build-in Cloud	-	-			933 (56.1%)	695 (54.0%)	$\chi^2(3) = 21.05$, $\mathbf{p < .001}$	.08
	PM	-	-			104 (6.3%)	140 (10.9%)		
	Another device	-	-			21 (1.3%)	18 (1.4%)		
	I don't know	-	-			606 (36.4%)	433 (33.7%)		
2FA	Fingerprint	-	-			457 (27.5%)	308 (24.0%)	$\chi^2(4) = 68.71$, $\mathbf{p < .001}$	.15
	Facial Recog.	-	-			780 (46.9%)	476 (37.0%)		
	PIN	-	-			295 (17.7%)	361 (28.1%)		
	Pattern	-	-			63 (3.8%)	46 (3.6%)		
	Password	-	-			69 (4.1%)	95 (7.4%)		
SUS		75.0	67.5	$U = 2,640,040.5$, $\mathbf{p < .001}$	.13	82.5	55.0	$U = 255,974.5$, $\mathbf{p < .001}$	.66
Acceptance		1.11	0.67	$U = 2,508,831.0$, $\mathbf{p < .001}$	.17	1.56	0.56	$U = 461,774.0$, $\mathbf{p < .001}$	.49

Note. Depending on the variable, we display **frequencies (with in-group percentages) or the median** (to minimize outlier effects). n = Number of participants; ES = Effect Size; ATI = Affinity for Technology Interaction; PC = Privacy Concerns; CS bkgd. = Computer science background; Prior exp. = Prior passkey experience; OS = Operating system; PM = Third-party password manager; 2FA = Passkey second factor; Facial Recog. = Facial Recognition; SUS = System Usability Scale. - = not applicable; The statistic is either Pearson's chi-square test [69] or the Wilcoxon-Mann-Whitney test [57], and the effect size (ES) is either Cramér's V [17] for the chi-square test [69] or the rank-biserial correlation coefficient r for the Wilcoxon-Mann-Whitney test [57]. **Significance level of $\mathbf{p < 0.001}$**, highlighted in bold font.

E. Meta-Review

The following meta-review was prepared by the program committee for the 2026 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

E.1. Summary

The paper presents a large-scale field study of passkey adoption by partnering with a European healthcare service. Participants were users of this platform and, after agreeing to join the study, had the option to secure their account with 1) a passkey or 2) a password with 2FA (SMS 2FA). The study had two phases: first, a large-scale survey (n=5,057) about why participants chose a particular option, followed by six months of monitoring of authentication behavior (n=2,716) with in-situ surveys. The authors identified several reasons for adoption or refusal of passkeys, as well as barriers during usage (e.g., synchronization between devices). The authors concluded with recommendations on how to improve the passkey ecosystem.

E.2. Scientific Contributions

- Independent Confirmation of Important Results with Limited Prior Research
- Provides a Valuable Step Forward in an Established Field

E.3. Reasons for Acceptance

1) The paper provides independent confirmation of important results with limited prior research. The results of this large-scale field study add to the field by confirming issues and benefits of passkeys ”in the wild.”
2) The paper provides a valuable step forward in an established field. It contributes new insights into the passkey ecosystem involving several stakeholders (e.g., synchronization across platforms or within a platform), adding to the growing literature on passkeys/FIDO2.