FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones

Leon Würsching*
Technical University of Darmstadt
Darmstadt, Germany
lwuersching@seemoo.tu-darmstadt.de

Florentin Putz*
Technical University of Darmstadt
Darmstadt, Germany
fputz@seemoo.tu-darmstadt.de

Steffen Haesler
Technical University of Darmstadt
Darmstadt, Germany
haesler@peasec.tu-darmstadt.de

Matthias Hollick
Technical University of Darmstadt
Darmstadt, Germany
mhollick@seemoo.tu-darmstadt.de

ABSTRACT

Modern smartphones support FIDO2 passwordless authentication using either external security keys or internal biometric authentication, but it is unclear whether users appreciate and accept these new forms of web authentication for their own accounts. We present the first lab study (N=87) comparing platform and roaming authentication on smartphones, determining the practical strengths and weaknesses of FIDO2 as perceived by users in a mobile scenario. Most participants were willing to adopt passwordless authentication during our in-person user study, but closer analysis shows that participants prioritize usability, security, and availability differently depending on the account type. We identify remaining adoption barriers that prevent FIDO2 from succeeding password authentication, such as missing support for contemporary usage patterns, including account delegation and usage on multiple clients.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in HCI*; **Laboratory experiments**; *Empirical studies in ubiquitous and mobile computing*; • **Security and privacy** → **Usability in security and privacy**.

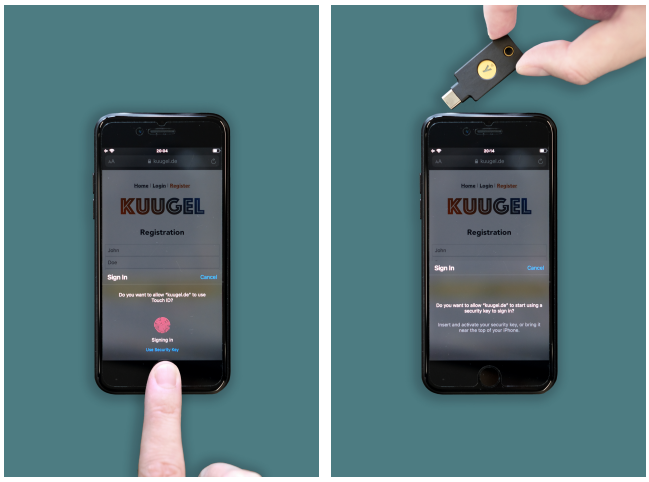
KEYWORDS

Usability, Security, Passwordless, User Authentication, Biometrics, Accounts

ACM Reference Format:
Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. 2023. FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3544548.3580993

*Both authors contributed equally to this research.

CHI '23, April 23–28, 2023, Hamburg, Germany



(a) Group P: Apple Touch ID **(b) Group R: Yubico Yubikey**

Figure 1: The different user interactions with the smartphone during the experiment. Group P used Apple Touch ID as a platform authenticator and Group R used a Yubico YubiKey as a roaming authenticator.

1 INTRODUCTION

Authentication is one of the central building blocks for securing the Internet. Since the 1970s, web services have conventionally relied on text-based passwords as the de-facto standard for user authentication. Secure passwords, however, are hard to memorize [72], password reuse enables severe attacks [38], and password-based authentication is prone to phishing [22]. Despite stronger security guarantees, all previous approaches in the *"quest to replace passwords"* failed to get widespread adoption, mainly because of their inferior deployability and usability [11].

To address the first entry barrier – *deployability* – more than 250 technology companies and browser vendors [29] have founded the Fast IDentity Online Alliance (FIDO), jointly designing the FIDO2 standards for passwordless authentication [30]. As a result, all major web browsers are now FIDO2-ready [46], as they support the corresponding W3C Web Authentication (WebAuthn) standard [69]. FIDO2 mandates public-key cryptography to provide user authentication based on authenticators containing the user's private

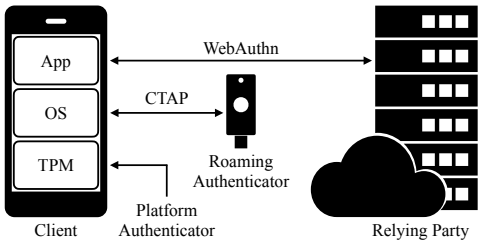


Figure 2: The parties and protocols involved in FIDO2 authentication scenarios. On the client side, *"App"* and *"OS"* are abbreviations for the application accessing the relying party and the client's operating system, respectively.

key [28]. Unlike passwords, FIDO2 authentication is resistant to phishing, keylogging, replay attacks, and server breaches [41].

As more and more websites support FIDO2 authentication, it becomes essential to study the second entry barrier – *usability* – to find out how users react to this paradigm shift from knowledge-based factors to possession-based and biometrics-based factors. There are two variants of FIDO2 authentication with fundamentally different user interactions:

For *roaming authentication*, the private keys are stored on an external roaming authenticator, e.g., a YubiKey [76], which connects to the client device via Universal Serial Bus (USB), near-field communication (NFC), or Bluetooth Low Energy (BLE). A recent usability study within the desktop environment by Lyastani et al. [44] suggests that users accept and prefer roaming authentication as an alternative to passwords. Many participants, however, were concerned about carrying a security key with them physically and potentially losing it. Despite the prevalence of FIDO2 support in recent iPhones and Android devices [2, 27], **smartphones have not been studied as FIDO2 clients for roaming authentication yet**, but only as roaming authenticators themselves [51, 57].

The second variant of FIDO2, *platform authentication*, mitigates these availability concerns, as the smartphone's integrated trusted platform module (TPM) stores the private keys, protected by an additional local authentication using the smartphone's unlock mechanism, e.g., Apple Touch ID [7]. However, platform authentication raises new usability concerns about the fundamentally different mental model. Users need to grasp a more complex authentication method combining a private key stored on the smartphone's TPM that is further protected by biometrics-based local authentication. Platform authentication on smartphones has received little attention so far. Oogami et al. [50] studied how to improve compatible websites' user experience, and Lassak et al. [43] developed smartphone notifications addressing platform authentication misconceptions. However, **the research community lacks an understanding of whether users understand, accept, and trust passwordless platform authentication as an alternative to roaming authentication and passwords**.

In this work, we try to bridge this knowledge gap by reporting, to the best of our knowledge, the first large-scale lab study comparing FIDO2 platform authentication and roaming authentication on smartphones. We recruited 87 participants, randomly assigned them to one of two groups, and had them perform a series of practical web authentication tasks on an Apple iPhone. The first group used platform authentication with Apple Touch ID for the web (Figure 1a), while the second group used roaming authentication with an NFC-based YubiKey (Figure 1b). The participants reflected on their experience in a survey, which featured a combination of quantitative questions using standardized metrics and qualitative open-ended text questions. This paper presents our work as follows:

- As our main contribution, we conduct the **first large-scale lab study that compares FIDO2 platform and roaming authentication on smartphones** (Section 4).
- We show that platform and roaming authentication have excellent usability on smartphones, but lay users generally prefer platform authentication (Section 5).
- From our questionnaire's qualitative categories, we identify the strengths and weaknesses of FIDO2 on smartphones (Section 6). Based on our participants' feedback, we investigate how to address the weaknesses of passwordless authentication and discuss account-specific adoption decisions and usage patterns (Section 7).
- We provide a replication package with our evaluation scripts and the pseudonymized dataset [71] collected in our study, consisting of 22 variables for each of our 87 participants. We also release our mockup website's source code [70] to facilitate future work.

Our questionnaire encouraged participants to reflect on their everyday authentication use cases and whether they would be willing to use FIDO2 for their own accounts. While most of our participants were generally willing to adopt passwordless authentication, account-specific adoption barriers remain for both roaming and platform authentication, which we discuss in detail.

2 BACKGROUND AND RELATED WORK

This section explains how the FIDO2 standards enable passwordless authentication on smartphones. Section 2.1 describes relevant parts of the standards. Then, we explain roaming authentication (Section 2.2) and platform authentication (Section 2.3), including summaries of related studies of FIDO2. We also consider authentication-related studies outside the FIDO2 cosmos (Section 2.4).

2.1 FIDO2

The FIDO2 standards provide strong and passwordless authentication for the Internet. All major web browsers support them [46], and an increasing number of online services offer FIDO2 authentication both in one-factor authentication (1FA) and multi-factor authentication (MFA) scenarios [29]. FIDO2 consists of two standards, WebAuthn [69] and Client to Authenticator Protocol (CTAP) [28], which specify the communication between relying party, the client, and the authenticator (Figure 2). Together they form a challenge-response protocol, confirming the user's identity to the relying party by verifying the user's possession of the authenticator that manages their public key credentials.

In our study, WebAuthn handles the communication between a smartphone (client device) and a website (relying party). However, FIDO2 is flexible and also supports local authentication scenarios, e.g., a user unlocking a Windows computer via Windows Hello

[47]. On the client-side, WebAuthn expects an authenticator with access to the secret key corresponding to the public key stored at the relying party. FIDO2 supports two types of authenticators:

2.2 Roaming Authentication

A roaming authenticator is a CTAP-conforming external device that manages all public key credentials. During authentication, the relying party's challenge is forwarded to the roaming authenticator, solved locally with the secret key, and returned to the relying party. There is a large ecosystem of suitable roaming authenticators which are compatible with smartphones via NFC [75], BLE [36], or Apple Lightning/USB Type C [25]. The smartphone itself must be equipped with a CTAP-conforming interface and a WebAuthn-compatible web browser. Since 2019, FIDO2 roaming authentication has been supported on Android smartphones running Android 7 or later [27] and on Apple iPhones running iOS 13.3 or later via Apple Lightning [73] and NFC [2].

Lyastani et al. [44] conducted the first large-scale user study of FIDO2 roaming authentication on computers. In their between-groups study, participants either authenticated with passwords or used a YubiKey, concluding that roaming authentication is more usable and accepted than passwords. Farke et al. [23] studied FIDO2 roaming authentication as an unlocking mechanism for computers, using YubiKeys with enabled personal identification number (PIN) protection. They reported that participants stopped using roaming authentication because it was slower than their password manager.

Previous studies investigated whether smartphones, themselves, could be used as external FIDO2 roaming authenticators to address deployment and availability issues of traditional security keys. Owens et al. [51, 52] reported a between-groups observation study, comparing passwords to smartphones as roaming authenticators. They concluded that users understand the security benefits of FIDO2 but still find password-based authentication more usable. Rasmussen [57] conducted a between-groups user study showing that smartphones as roaming authenticators have similar usability and acceptance as YubiKeys. Both studies [51, 57] reported availability concerns regarding empty smartphone batteries.

We continue with a brief overview of user studies on the Universal 2nd Factor (U2F) [26], which is CTAP's predecessor and has similar user interaction. Lang et al. [41] reported on a two-year enterprise deployment of security keys within Google, laying the foundation for the U2F standard that is CTAP's predecessor. Das et al. [18, 20] studied U2F in non-enterprise environments and found that a two-factor authentication (2FA) method's acceptance did not correlate with its usability. Reynolds et al. [60] and Reese et al. [58] conducted longitudinal studies of U2F, reporting that the initial setup is cumbersome compared to the fast and easy authentication afterward. Ciolino et al. and Das et al. investigated lay users' perception of U2F, finding that, while sentiment towards U2F is lower than for SMS-based 2FA [13], some lay users do not feel the need to protect their accounts with MFA at all [19]. Colnago et al. [14] conducted a large-scale longitudinal study to explore 2FA adoption at a university, finding that $< 1\%$ use U2F as a 2FA method. More recent works on U2F by Das et al. and Reynolds et al. found that users are more likely to adopt MFA for essential accounts [21] and that the users' initial negative perception of MFA methods fades over time [59].

2.3 Platform Authentication

Client devices qualified to manage cryptographic key pairs can be used as platform authenticators. During authentication, the relying party's challenge is solved directly on the client's platform authenticator. Most platform authenticators require the user to authenticate locally with a PIN or biometrics, augmenting FIDO2 to an MFA method. Any Android phone running Android 7 or later provides a FIDO2 platform authenticator, as Android's FIDO2 certification includes the built-in biometrics sensors [27]. Since iOS 14, Apple has equipped iPhones with a platform authenticator, namely Touch ID for the web [3], which we also refer to as *Touch ID* for simplicity. For Touch ID platform authentication, the iPhone's Secure Enclave manages FIDO2 credentials and requires the user to authenticate locally with Touch ID.

Oogami et al. [50] studied the usability of FIDO2 platform authentication on smartphones, conducting interviews to improve the website user experience for first-time FIDO2 users. However, they did not collect FIDO2 weaknesses or adoption barriers of platform authentication. Lassak et al. [43] studied misconceptions about FIDO2 platform authentication on Android phones and developed smartphone notifications to address them.

2.4 Miscellaneous

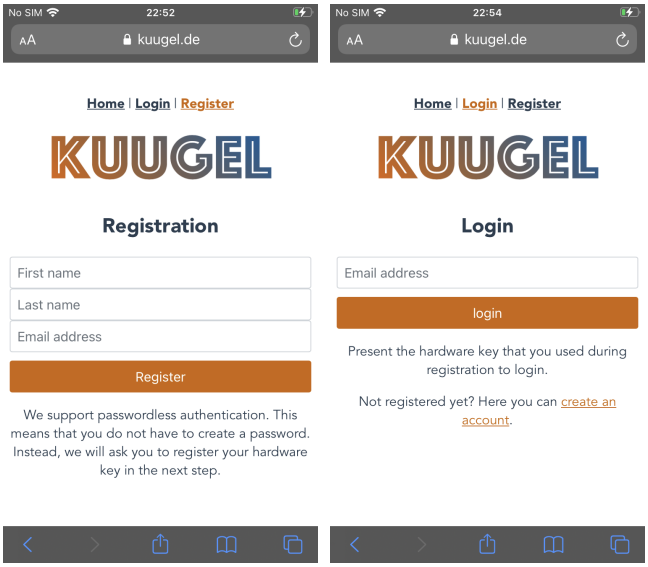
Independently of FIDO2, van den Boogaard [66] conducted an online study of users' understanding of biometrics-based authentication on mobile phones, finding that most participants use biometric options when available. Conners et al. [15] conducted an online study of *Let's authenticate* [16], which is similar to FIDO2 but uses authenticators (roaming or platform) to issue certificates for user authentication. Alqubaisi et al. [1] studied elements hindering the adoption of FIDO2 passwordless authentication, basing their analysis on the FIDO developer mailing list.

3 RESEARCH QUESTIONS

We continue the work of recent FIDO2 user studies but focus on passwordless authentication on smartphone clients. Thus, the research questions addressed in this work are:

- **RQ1** *What is the usability and acceptance of FIDO2 passwordless authentication using platform and roaming authentication on smartphones?*
- **RQ2** *What benefits and concerns do users consider when using FIDO2 passwordless authentication on smartphones?*
- **RQ3** *Which account types do users want to secure using FIDO2 passwordless authentication on smartphones?*

In contrast to related work, to the best of our knowledge, we are the first to study FIDO2 roaming authentication on smartphone clients and the first to conduct a lab study on any device type that compares FIDO2 platform authentication and roaming authentication. Our main goal is to identify the strengths and weaknesses of passwordless authentication on smartphones. To this end, we determine account-specific adoption barriers by encouraging our participants to reflect on whether they want to use passwordless authentication for their own accounts.



(a) Registration page. **(b) Login page.**

Figure 3: Screenshots of our mockup website's registration and login page. In our experiment, each participant experienced the complete authentication flow of FIDO2 passwordless authentication consisting of account registration and subsequent login.

4 METHODS

To answer our research questions on the usability and acceptance of platform and roaming authentication on smartphones, we conducted a lab study with practical web authentication tasks (Section 4.1) and a follow-up survey containing quantitative and qualitative questions (Section 4.2). We address our study sample (Section 4.3) and ethical considerations (Section 4.4), including the pilot study (Section 4.5), and analysis toolbox (Section 4.6).

4.1 Material

Our lab study's goal was to create a passwordless authentication scenario resembling our participants' everyday lives. In our study, the participants gained hands-on authentication experience on a smartphone, namely the Apple iPhone SE (2nd generation), referred to as *iPhone* for simplicity, running iOS 14.5.1 and Safari 14.1. During our study, this setup represented the most popular mobile operating system in North America [64]. We developed the mockup website KUUGEL as a relying party (Figure 3), which supports FIDO2 registration/login, e.g., using either (1) platform authentication with Touch ID [7] or (2) roaming authentication with a Yubico YubiKey 5C NFC [76], referred to as *YubiKey* for simplicity. The YubiKey supports FIDO2 via an NFC interface. Furthermore, it features optional PIN protection, adding a knowledge-based authentication factor. Farke et al. [23] reported negative user feedback on this feature. Thus, we opted against activating the YubiKey's PIN protection to avoid additional authentication overheads.

4.2 Study Design

We used a between-groups design to identify the differences between platform and roaming authentication on smartphones. Our between-groups design eliminates the influence of order and concentration level with an extended study duration. We decided for a lab study over alternative study designs to ensure consistent conditions for all participants, minimizing confounding factors. We randomly distributed the participants into two groups: The study group used platform authentication with Touch ID (Group P), while the control group used roaming authentication with a YubiKey (Group R). We conducted our lab study in neutral meeting rooms, where the participants met the study conductor in one-on-one sessions[1]. Each room contained a chair in front of a desk with an iPhone and, for Group R, also a YubiKey. For all participants, we ensured the same neutral environment and hardware to help participants only evaluate the effect of the presented authentication method. The study conductor was always present during each trial to verify that the participant performed the tasks and watched the educational videos.

Our study consisted of eight stages, which are shown in Figure 4. We first asked participants to read and sign our consent form, which explained the study's goal, procedure, and privacy policy. We then instructed participants in Group P to register one of their fingerprints in the iPhone's Touch ID settings, which was required for the following experiment. We explicitly decided to do this step early before the introductory videos and practical tasks so that the rest of the study procedure was comparable for both groups.

4.2.1 Task Instruction. All participants watched group-specific educational videos (approx. 5 minutes total) before the experiment, introducing FIDO2 passwordless authentication and ensuring that all participants had identical conditions[2]. The video continued with a brief explanation of our mockup website's registration and login process. We decided to use pre-recorded videos for instruction to increase the internal validity of our study by ensuring that all participants received the same information. Both groups watched identically structured videos that only differed in the platform and roaming authentication details, allowing for fair comparison in our between-groups design. Our goal was to avoid misunderstandings resulting in confounding effects, that are invisible in the worst case.

4.2.2 Experiment. After the task instruction, we handed our participants the smartphone (and for Group R, also the YubiKey). The participants used the iPhone to browse our mockup website and register an account using their assigned authenticator type. Our mockup website complies with Apple's recommendations for websites with Touch ID for the Web [7]. Besides the pages necessary for registration and login, the mockup website provides only minimal additional functionality to help participants assess only the usability of FIDO2.

After registration, participants in Group P logged into our mockup website with an email address and their fingerprint, as shown in Figure 1a. Participants in Group R used their email address and the YubiKey for authentication at our mockup website.

[1] Protocols were in place for the in-person lab study ensuring the safety of participants and the study conductor, as we conducted our study during the COVID-19 pandemic.
[2] Our introduction video was partly based on the introductory videos from the study of Lyastani et al. [44].

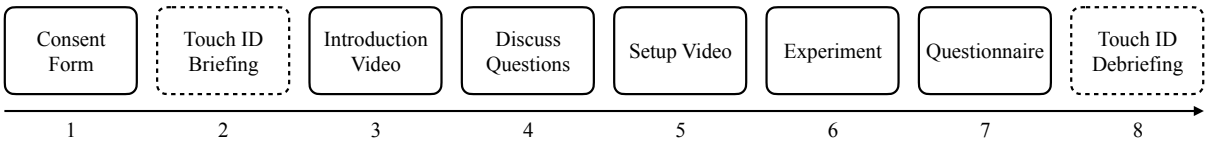


Figure 4: Our lab study's eight stages. Dashed borders indicate stages that only participants of Group P participated in to register and delete their fingerprints from the iPhone's Touch ID settings.

The user brings the YubiKey near the iPhone to register a new credential on the YubiKey, as shown in Figure 1b. After registration, the participants logged into their accounts using the same method.

4.2.3 Questionnaire. After collecting the hardware, we asked the participants to fill in our questionnaire to reflect on their experiences during the experiment. Appendix B contains the corresponding questionnaire. We included variables from related work on authentication factors [44, 50, 57, 60] for comparability with previous user studies:

- Dependent Variables: The dependent variables captured our participants' experience and assessment of roaming or platform authentication. To answer RQ1, we used the System Usability Scale (SUS) [12] to determine the authentication methods' usability, as well as the acceptance scale from van der Laan et al. [67] to measure how much our participants accepted their assigned authentication method. To answer RQ3, we used 11 five-level Likert items to measure how likely our participants would use the demonstrated authentication method on 11 different types of online accounts. As support for FIDO2 is currently limited in practice, we asked our participants to assume that each service supported the presented authentication method. Participants could also select "not available" if they did not use this type of account.
- General Impression: Our questionnaire included four open-ended text questions to answer RQ2. Participants reflected on their general impression of the studied authentication method, but we also specifically asked our participants to state any strengths and weaknesses that came to their minds. Our fourth text question, which directly follows the quantitative question on adoption for 11 different account types, was designed to learn why participants do (not) want to use the authentication methods for specific account types. Our goal was to recognize account characteristics increasing or decreasing participants' likelihood of using passwordless authentication and identify adoption barriers for common account types.
- Control Variables: As control variables, we measured our participants' technology affinity using the Affinity for Technology Interaction Scale (ATI) [32] as well as their level of privacy concerns using four Likert items from Langer et al. [42]. Furthermore, we asked participants which 2FA methods they had already used and whether they had prior experience with Apple iOS, which was the operating system running on our study's smartphone.
- Demographic Variables: We collected the gender, age, education, and field of study/work of our participants as demographic variables.

After filling in the questionnaire, we ensured participants of Group P deleted their fingerprints from the iPhone's Touch ID settings. Before concluding the study, we thanked the participants for their time. It usually took participants 15-25 minutes to participate in our study.

4.3 Participants

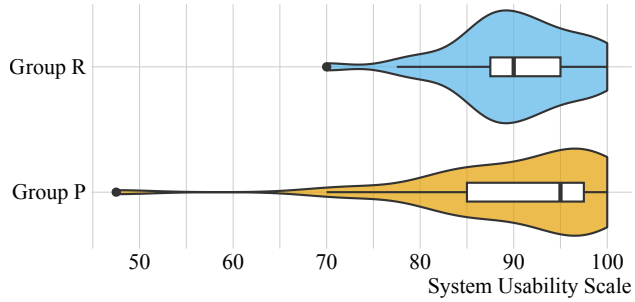
We conducted our lab study with 89 participants between July and September 2021. For recruitment, we used mailing lists, social media groups, word-of-mouth, and snowball sampling, both within and outside our university (participants had to be over 18 years old to be eligible). Interested participants self-registered with a registration form to choose a time slot for voluntary participation in our study. Participants did not receive compensation for their participation in our study, except for one student from our university's psychology department who received a participation point as part of their study program. Within this study program, the student had sufficient studies to choose from.

Two participants did not fully complete the questionnaire, so we removed them from our final sample (N = 87). Of these, 55 (63%) identified as male and 32 (37%) as female, with no participants opting for the *"other"* or *"no answer"* options. The education level of our participants was high, with the most common highest educational degree in our sample being a Bachelor's degree (40%; 35). Our diverse recruitment sources resulted in at least 39 (45%) of non-students. Most participants (59%; 51) were between 20 and 29 years old, but a substantial share of participants (34%; 30) were older than 30, of which 10 participants (11%) were over 50. According to Pearson's chi-squared test, the demographic structure (gender, age, and education) did not differ significantly between Group P and Group R (Table 7).

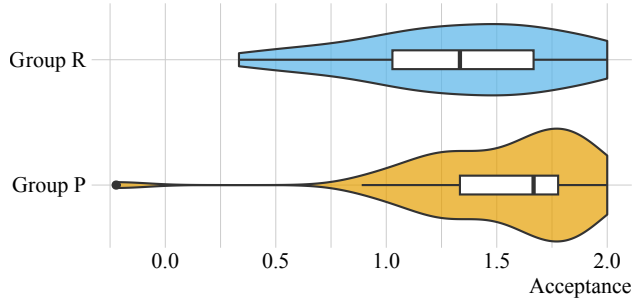
4.4 Ethical Concerns

Our university's institutional review board (IRB) reviewed and approved this study. We informed all participants about the study's purpose and data collection while adhering to the General Data Protection Regulation (GDPR). We collected written consent prior to the lab study.

During the study, participants in Group P temporarily registered their fingerprints on the iPhone. We briefed the participants about this and ensured the deletion of their fingerprints after each trial. For participants in Group R, we reset the YubiKey to factory settings after each trial to ensure equal conditions for all participants. The names and email addresses for authentication at our mockup website were only temporarily stored on the iPhone and deleted after each trial. We did not collect any other sensitive information. We pseudonymously stored each participant's answers without



(a) SUS scores.



(b) Acceptance scores.

Figure 5: Comparison of our participants' SUS scores and acceptance scores for platform authentication (Group P) and roaming authentication (Group R). The boxplots show quartiles, median, and outliers.

identifying information by assigning sequential numbers. Participation in our study was voluntary and without compensation in accordance with common practice of our university's computer science department.

4.5 Pilot Study

We conducted a pilot study (N=6) to identify technical problems with the study setup and ambiguities in the instructional videos and the questionnaire. The pilot study showed that the setup worked reliably and that the participants understood the instructional videos and all categories of the questionnaire.

4.6 Data Analysis

We used the statistical software R 4.2.0 for all quantitative data analysis [56]. We calculated the central tendencies and correlations to answer our research questions. We compared Group P and Group R using the Wilcoxon-Mann-Whitney test [45] for ordinal variables and Pearson's chi-squared test [53] for nominal variables. For multiple tests, we controlled the false discovery rate (FDR) using the Benjamini-Hochberg method [10]. We used Kendall's rank correlation coefficient [39] to determine the relationship between our control and dependent variables. For all statistical tests, we used an alpha level of .05.

Furthermore, we conducted a qualitative analysis of the four open-ended text questions, performing the following qualitative coding steps: (1) Two researchers independently constructed an initial codebook for each question using inductive coding [34, 48]. (2) The researchers merged these codebooks through discussions and formed clusters to identify a suitable level of detail. (3) Two further independent researchers deductively coded all data according to the final codebook. (4) They discussed to resolve coding differences. After discussions, the researchers agreed on most coding decisions and reached satisfactory inter-coder reliability (mean Krippendorff's Alpha = .984, minimum .789 [40]). Finally, the researchers who created the initial codebook discussed and agreed on any remaining coding inconsistencies. Appendix C contains our final coding system.

5 QUANTITATIVE RESULTS

In this section, we report on the evaluation of our questionnaire, which represents the results of our study. The questionnaire (Section 4.2) contains quantitative scales, control variables, and open-ended qualitative questions. We used well-known metrics [12, 67] to study the participants' perceptions of FIDO2 regarding its usability (Section 5.1) and acceptance (Section 5.2). Furthermore, we determined the participants' likelihood to adopt FIDO2 for specific online account types (Section 5.3) and analyzed the control variables (Section 5.4).

5.1 Usability

After getting hands-on experience with passwordless authentication on smartphones, the participants completed our questionnaire, including the SUS [12]. We use the Shapiro-Wilk test [63] to determine whether this variable is normally distributed. The SUS scores for Group R ($W = 0.95$, $p = .058$) are approximately normal, but the scores for Group P ($W = 0.81$, $p < .001$) are significantly non-normal. Figure 5a depicts the statistics of the SUS scores per group. The distribution in Group P has visible negative skew, indicating that most participants selected values on the higher end of the scale. Additionally, there is a single outlier in both groups. Parametric methods such as the t-test assume normally distributed sampling distributions and can give inaccurate results in the presence of outliers [68]. We, therefore, use non-parametric statistical methods for data analysis (Section 4.6).

SUS scores in Group P (Mdn = 95) did not differ significantly from Group R (Mdn = 90) according to the Wilcoxon-Mann-Whitney test, $W = 835.5$, $p = .351$, $r = -.10$. **Both platform and roaming authentication on smartphones have a similarly high level of usability.**

5.2 Acceptance

We collected data on the acceptance of passwordless authentication using the scale of van der Laan et al. [67]. Figure 5b shows the acceptance scores for both groups, which are approximately normal for Group R ($W = 0.96$, $p = .196$), but significantly non-normal for Group P ($W = 0.83$, $p < .001$). As with the SUS scores, the acceptance scores in Group P have strong negative skew and an outlier, which reaffirms our choice of the non-parametric Wilcoxon-Mann-Whitney test. The acceptance scores in Group P (Mdn = 1.7) differed significantly from Group R (Mdn = 1.3), $W = 691$, $p = .031$, $r = -.23$, indicating that **platform authentication has higher acceptance on smartphones than roaming authentication**.

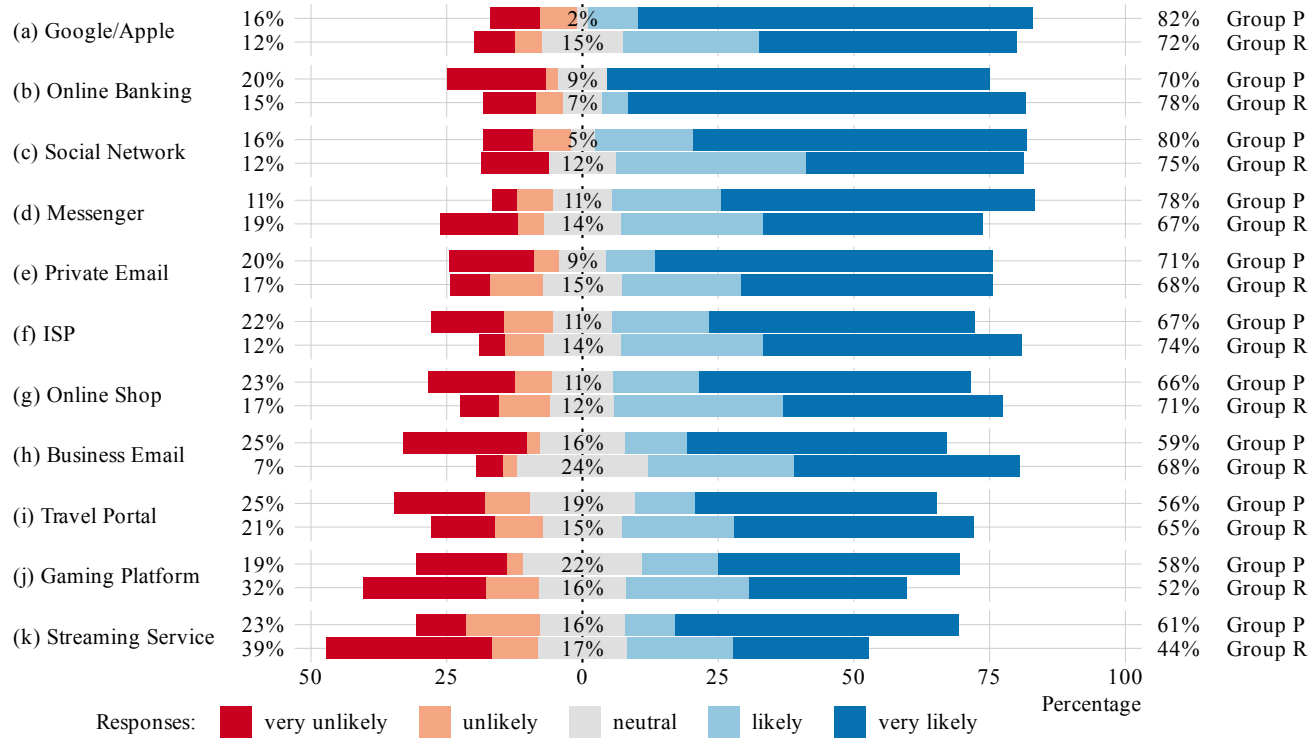


Figure 6: Comparison of our participants' adoption likelihood for different account types ordered by their average likelihood. The percentages (left, middle, right) represent the share of negative, neutral, and positive responses, respectively.

5.3 Adoption

The category dedicated to adoption listed 11 account types and asked participants how likely they were to use the studied passwordless authentication method, provided that the online service supported it. Figure 6 shows the responses for all accounts.

Most participants were optimistic about using passwordless authentication on their smartphones. The three account types with the highest share of positive responses were Google/Apple accounts (77%; 65), online banking accounts (74%; 63), and social network accounts (77%; 65), although the last had less *"very likely"* responses compared to the former two. Our participants were least likely to use passwordless authentication for streaming services (54%; 43 positive responses) and gaming platforms (55%; 37 positive responses). For every account type, however, the share of positive responses was higher than the share of negative responses, indicating that **overall, our participants want to use passwordless authentication on smartphones when possible.**

We compared the adoption scores of both groups using Pearson's chi-squared test. The adoption did not differ significantly between both groups for any account type after controlling the FDR using the Benjamini-Hochberg method and a target FDR of 10% [10]. We excluded participants without a certain account from the analysis of that account type. This occurred only for a few participants per account, with the following exceptions: Twenty participants did not have a gaming account (11 P + 9 R), 17 participants did not have an account at a travel portal (9 P + 8 R), and 7 participants did not have an account at a streaming service (1 P + 6 R).

5.4 Control Variables

Our control variables are part of the descriptive overview in Table 1. Additionally, Appendix A contains our participants' demographic information. Group P and Group R did not differ significantly for ATI, privacy concerns, and iOS familiarity. We calculate bivariate Kendall's rank correlation coefficients in Table 2 to determine the relationship between the control and dependent variables. As shown, the acceptance scores significantly correlated with the SUS scores ($\tau = .36, p < .001$) and the predictor variable representing the differences between the two groups ($\tau = .20, p = .030$). There also was a significant negative correlation between the ATI scores and iPhone familiarity ($\tau = -.23, p = .009$).

2FA Familiarity. We asked our participants whether they were familiar with any 2FA methods. Most of our participants had prior experience with SMS-based 2FA (87%; 76), push-based smartphone apps (83%; 72), and transaction authentication number (TAN) lists (76%; 66). About half had used one-time password (OTP) generator apps before (51%; 44), and only a few had experience with security keys such as the YubiKey (8%; 7). Group P and Group R did not differ significantly for any of the five 2FA methods.

6 QUALITATIVE RESULTS

The questionnaire contained open-ended text questions to investigate the participants' general experience with passwordless authentication as well as its strengths and weaknesses. We also included an open-ended question to understand better why participants do

Table 1: Comparison of our participants' descriptive data, including the control and dependent variables.

Variable	Group P ($N = 45$)	Group R ($N = 42$)	Statistic	ES
iOS Familiarity			$\chi^2(1) = 0.05$	.03
Yes	67% (30)	64% (27)	$p = .815$	
No	33% (15)	36% (15)		
ATI	4.2	4.5	$W = 1072$	-.12
	(2.2)	(1.5)	$p = .282$	
Privacy Concerns	5.0	5.0	$W = 966$	-.02
	(1.8)	(1.8)	$p = .861$	
SUS	95	90	$W = 835.5$	-.10
	(12.5)	(7.5)	$p = .351$	
Acceptance	1.7	1.3	$W = 691$	-.23
	(0.4)	(0.6)	$\mathbf{p = .031}$	

Note: For iOS familiarity, we report in-group percentages (and frequencies), Pearson's chi-square test, and Cramér's V [17] as the ES. For the other scores based on Likert scales, we report the median (and the interquartile range), the Wilcoxon-Mann-Whitney test, and the effect size estimate based on Rosenthal's method [61].

Table 2: Kendall's correlation between control and dependent variables.

		2	3	4	5	Accept.
1	Group (P)	-.10	-.02	.03	.09	**.20***
2	ATI		.05	**-.23****	.15	.12
3	Privacy Concerns			-.09	-.12	-.14
4	iOS Familiarity				.00	-.02
5	SUS					**.36*****

Note: $N = 87$ * $p < .05$ ** $p < .01$ *** $p < .001$

(not) want to adopt passwordless authentication for specific account types. In summary, our participants' general impression was *"good"* (87% P, 81% R) or *"good, but"* (13% P, 19% R), with only two participants in Group R not describing a positive general experience. Based on our participants' comments, Section 6.1 summarizes the strengths of FIDO2 (Table 3), and Section 6.2 reports its weaknesses (Table 4). We also quote from our participants' free-text responses to better present the details of their reasoning.

6.1 FIDO2 Strengths

Overall, our participants reacted positively to platform and roaming authentication on smartphones. The SUS scores for both groups were concentrated at the top of the scale (> 90), indicating *excellent* usability [9]. The acceptance scores in both groups were high but significantly higher in Group P, albeit with a small effect size.

In our lab study, participants gained hands-on experience with passwordless authentication on our mockup website. However, we also asked them if they wanted to use the authentication methods on their own accounts, encouraging the participants to reflect on their everyday authentication use cases and whether they would like to use passwordless authentication beyond this user study. There was a clear positive trend for each of the 11 account types, with the majority wanting to adopt passwordless authentication. The median share of positive responses (*"likely"* and *"very likely"* to adopt) across all account types was 69.8%. When we asked users about their general experience with the studied authentication methods, most participants (86%) had a positive impression.

Why did users like the studied authentication methods? The coded responses to the open-ended text questions revealed four main strengths of passwordless authentication related to security, passwords, usability, and authentication times (Table 3).

Secure. Most participants in both groups commented on the methods' security benefits, e.g., one participant wrote:

> *"From my point of view, it feels more secure than, for example, a password manager."* (P32, Group R)

This is encouraging, as for any new authentication method to succeed, it must not only be secure, but users must also perceive it as secure and trust it [44].

Password Replacement. Users generally dislike passwords and the associated overhead of creating, memorizing, and updating them [65]. Many participants stated eliminating this effort as an advantage of passwordless methods.

Usable. Participants in both groups praised the usability of the studied authentication methods and described them as *"intuitive"*, *"simple"*, and *"efficient"*:

> *"Easy to use, even for non-technical people."* (P44, Group P)

Fast. Participants, mainly in Group P but also in Group R, mentioned that the authentication method is fast.

6.2 FIDO2 Weaknesses

The median share of negative responses (*"unlikely"* or *"very unlikely"* adoption) across all account types was 17.6%. Why do some participants not want to adopt FIDO2 authentication on their smartphones, despite security benefits and excellent usability scores? To illustrate this, note that those participants still had a respectable median SUS score of 93.8, demonstrating that usability alone is insufficient for users to adopt FIDO2 in their everyday lives. Instead, there are further adoption barriers, which we now present in more detail. We start with problems common to both platform and roaming authentication and then turn to each of them individually. Table 4 summarizes all weaknesses mentioned by our participants within a smartphone environment.

6.2.1 Platform and Roaming Weaknesses. Overall, in both Group P and Group R, the usability of registration and login on the smartphone was fine, but some participants raised concerns about account recovery and delegation, authenticator revocation, and availability. We identified the following weaknesses in both groups, indicating that these weaknesses are common to both platform and roaming authentication.

Account Recovery. When users lose access to their accounts, they need a convenient and reliable recovery mechanism. Participants from both groups raised questions about how to proceed in case they suddenly cannot access their accounts:

Table 3: Strengths of passwordless authentication reported by our participants.

	Strength	Group P	Group R
Both	Secure	69%	69%
	No password memorization issues	47%	52%
	Easy to use/Intuitive	38%	33%
	No passwords	16%	14%
	Easier than passwords	16%	12%
	No password creation	7%	5%
	No password updates	4%	2%
Platform	Fast	47%	12%
	Always available	11%	2%
	Privacy	11%	2%
	Easy to setup	4%	2%
Roaming	One solution for many accounts	4%	10%
	Good for lay users	2%	5%
	Security less reliant on smartphone	0%	2%

Note: Numbers in **Group P** and **Group R** are in-group percentages (%). As both groups mostly identify similar strengths of passwordless authentication, Section 6.1 reports them jointly and points out differences.

Table 4: Weaknesses of passwordless authentication reported by our participants.

	Weakness	Group P	Group R
Both	Revocation/Recovery	11%	26%
	Complicated for lay users	13%	5%
	Privacy concerns	4%	10%
	Website compatibility	4%	2%
	Coerced authentication	0%	5%
	Account sharing	4%	0%
	Unfamiliarity	4%	0%
Platform	Use on multiple clients	27%	5%
	Technical problems	20%	5%
	Technology mistrust	13%	0%
	Empty battery	7%	0%
	Biometric security	4%	0%
Roaming	Loss/Destruction	20%	81%
	Something to carry	2%	36%
	Theft	4%	21%
	Costs	0%	12%
	Cumbersome	2%	7%

Note: Numbers in **Group P** and **Group R** are in-group percentages (%).

> *"If I lose the YubiKey, I will have to look for a replacement, block my accounts, and then register initially with my new YubiKey..."* (P20, Group R)

Authenticator Revocation. The problem of revocation closely relates to recovery. When the smartphone or the security key is stolen, users not only need to recover access, but they also want to revoke the stolen authenticator to prevent abuse. This problem applies to both platform and roaming authentication, but participants from Group P rarely mentioned revocation as an issue.

Account Delegation. Users are familiar with sharing access to some of their accounts, e.g., streaming services. Furthermore, some users would like to give their partner access to a shared bank account. Account delegation is easy with passwords, but with passwordless authentication (especially platform authentication), there is nothing to share:

> *"In case another person needs to log in to your account for whatever reason that's difficult, or if it's an account that multiple people use [...]"* (P34, Group R)

Availability. Password-based authentication is available as long as the user remembers their password. In contrast, passwordless authentication can be temporarily unavailable, e.g., when a user forgets to carry their YubiKey (Group R) or the smartphone's battery is empty (Group P). Participants of both groups worried about the potential inconvenience of authentication being unavailable.

6.2.2 Platform Weaknesses. Even though our study reports good usability of platform authentication, some participants wondered how to access their accounts from other devices. Others were concerned about hardware issues or did not trust the technology.

Multiple Clients. While passwords are applicable on most client devices, our participants did not know how to access their accounts on devices other than their smartphones, e.g., their personal computer (PC) or laptop. For example, one participant wrote:

> *"Authentication is bound to the device. For me, it is important that these accounts are accessible from everywhere [...]"* (P57, Group P)

Similarly, some participants wondered how to access their accounts on public computers:

> *"Not usable on all devices, e.g., the PC in the library."* (P73, Group P)

Malfunctions. Participants were concerned about technical problems with the biometric sensor, preventing them from accessing their accounts. Especially participants who had used biometric authentication before to access their smartphones seemed to be aware of potential problems:

> *"Sometimes the fingerprint does not work so well when the hands are wet, for example (from my own experience with unlocking the iPhone)."* (P71, Group P)

Technology Mistrust. A few participants were skeptical of platform authentication due to its novelty. They were unsure if they could trust it, as Touch ID felt like a black box to them. For instance, one participant wrote:

> *"Less visibility into what's actually happening. It feels like you're giving up a lot of control."* (P56, Group P)

6.2.3 Roaming Weaknesses. Most of our participants gave good SUS scores to roaming authentication during our lab study, indicating that the general authentication flow is usable. However, our participants raised concerns about the requirement to purchase and carry additional hardware, which could get lost, destroyed, or stolen in the worst case.

Additional Hardware. Roaming authentication requires additional hardware, which users must remember to carry. The associated physical effort is a hidden usability penalty [31]. While we provided all hardware to our participants in our study, users would need to bring their own authenticator in practice, which requires thought and effort.

Loss/Destruction/Theft. The roaming authenticator is often a small external device, so it can get lost, destroyed, or stolen. The immediate consequence is a lack of availability because users lose access to their accounts . Most participants in Group R (81%) mentioned this as an issue, for example:

> *"You must always have the [YubiKey] with you → can be lost, forgotten → no login possible. Actually, you always want to have it with you, but then you can lose it, in which case you can no longer log in."* (P80, Group R)

Deployment Costs. Another problem with requiring additional hardware is that it costs money. The NFC-capable FIDO2 roaming authenticators used for our study cost 55 USD at the time of our study [76], but cheaper models are available for 25 USD [75]. Nevertheless, some users are unwilling to pay this much for authentication , especially considering that the best practice is buying a second token as a backup.

> *"The [YubiKey] costs money, to begin with, and passwords are free. I think this will prevent many users from using it."* (P1, Group R)

For P34, however, the costs were no dealbreaker:

> *"Has a certain price (but would be worth it to me personally)."* (P34, Group R)

7 DISCUSSION

We now discuss the main findings of our study. In Section 7.1, we discuss usage patterns in our participants' responses that lead to account-specific adoption decisions. Section 7.2 revisits the weaknesses of FIDO2 and guides on how to alleviate major issues. Finally, we address the limitations of our work (Section 7.3) and discuss future work (Section 7.4).

7.1 Adoption Depends on Account Type

Most weaknesses presented in the previous section were only mentioned by a fraction of our participants, emphasizing their positive general impression and indicating that some of these weaknesses only apply to specific usage patterns or accounts. After the participants stated their likelihood of using passwordless authentication for real-world online accounts, we asked them to explain what affected their decision. Table 5 and Table 6 summarize the characteristics of accounts for which participants (did not) want to use passwordless authentication. We observe that specific account characteristics affect how participants weigh the strengths and weaknesses of passwordless authentication. Our goal is to identify account characteristics that make an account more suitable for either platform or roaming authentication.

7.1.1 Account Sensitivity. We observe opposite trends regarding how users reason about adopting passwordless authentication for sensitive accounts.

Security vs. Availability. Some users reject roaming authentication for non-sensitive accounts, where availability concerns outweigh security benefits. These participants cited account sensitivity as a reason for adopting passwordless authentication but its absence as a reason against adoption:

> *"In principle, I would choose to use the authentication method for most accounts, except for accounts [...] to which I do not assign any importance."* (P32, Group R)

Convenience vs. Mistrust. We identify a countertrend of users rejecting passwordless authentication for sensitive accounts, as they cannot put aside their technology mistrust in favor of the usability benefits. These participants cited *"easy to use"* and *"fast"* as strengths of passwordless authentication and generally considered it to be *"secure"*. However, they would instead rely on password-based authentication for sensitive accounts, trusting their memory more than the mechanisms of passwordless authentication:

> *"I consider the [Yubikey] to be secure. However, for important accounts, I would rather rely on my memory and that the login does not get into the wrong hands."* (P68, Group R)

7.1.2 Usage Frequency. During our study, there was a clear relationship between the adoption likelihood and the usage frequency of an account.

Security vs. Physical Effort. Some users reject roaming authentication for frequently-used accounts because the physical effort outweighs the security benefits. We find that these participants described the YubiKey as *"easy to use"* and *"secure"*, but also as *"something to carry"*:

> *"For: Accounts that I do not use daily. [...] Not: For Insta and Co. Since I use them several times a day (even on the side or so), and the effort to always use the USB stick is not in proportion to the benefit, i.e., the danger if someone steals my password or hacks my account."* (P80, Group R)

Speed vs. Initial Effort. We observe the opposite trend for platform authentication: Some users reject platform authentication for rarely-used accounts because the effort to set up passwordless authentication outweighs the reduced authentication times. This

Table 5: Account characteristics favoring adoption.

Yes, for …	Group P	Group R
sensitive accounts	16%	38%
rarely used accounts	0%	7%
accounts that are not shared	4%	2%
frequently used accounts	4%	2%
business-related accounts	2%	2%
accounts where fast access is crucial	4%	0%
non-sensitive accounts	2%	0%
accounts mainly used on smartphone	2%	0%
accounts not used on other devices	2%	0%

Note: Numbers in **Group P** and **Group R** are in-group percentages (%).

Table 6: Account characteristics preventing adoption.

No, for …	Group P	Group R
non-sensitive accounts	11%	21%
sensitive accounts	11%	10%
shared accounts	7%	10%
frequently used accounts	0%	10%
accounts used outside of home	4%	5%
business-related accounts	7%	2%
rarely used accounts	7%	2%
accounts supposed to be anonymous	0%	2%
accounts used on multiple devices	2%	0%

Note: Numbers in **Group P** and **Group R** are in-group percentages (%).

trend is likely related to our previous observation that more participants perceived platform authentication as fast compared to roaming authentication:

> *"For: accounts where you have to log in more often (often on the same device). Against: social networks: login [only once]"* (P72, Group P)

7.1.3 Mobility. We observe that some users reject passwordless authentication for accounts used outside of their homes because, in these scenarios, the chances of authentication unavailability increase. These participants worried about an *"empty battery"* (Group P) or described the need to remember to carry the roaming authenticator (Group R):

> *"For streaming services, I may log in from somewhere else than home, and then, if I don't have the [YubiKey] with me, I won't be able to log in."* (P30, Group R)

7.2 Roadmap to Addressing the Weaknesses of FIDO2

We now discuss the weaknesses identified in our study and propose how to address them while considering the findings of previous user studies in different passwordless authentication scenarios (Section 2). Some weaknesses, including account recovery, authenticator revocation, and account delegation, affect both platform and roaming authentication, but other issues directly stem from the concrete authentication mode.

7.2.1 Account Recovery. Recovery is an open problem in FIDO2 [23, 44, 51, 57], which the standards currently do not sufficiently address. The best practice is to register multiple authenticators per account and keep one as a backup, consolidating the issues of acquisition costs and additional hardware. However, this does not scale. Furthermore, our analysis shows that users need clear instructions on dealing with recovery as they did not realize that mitigations known from password-based authentication can also work for FIDO2. For instance, online services can allow users to request instructions for authentication reset via email and enroll new FIDO2 credentials, similar to a password reset form. The usability and acceptance of this form of recovery require further research. Some works propose to improve recovery in FIDO2 with extensions [33, 55, 74], certificates [15], or electronic IDs [62].

7.2.2 Authenticator Revocation. Authenticator revocation has been identified as a weakness in prior studies of FIDO2 roaming authentication [23, 44, 51, 57] but not in related studies of platform authentication. A possible explanation is that there already exist mitigations to deal with the loss of smartphones. For instance, platform authentication often requires local authentication, making it harder for attackers to access accounts with stolen smartphones. Additionally, users can remotely erase the data on a lost iPhone [6], further addressing revocation. Most roaming security keys do not support local authentication, although some models are equipped with biometric protection [24, 77]. However, as the FIDO2 standards do not sufficiently solve authenticator revocation, web services (i.e., FIDO2 relying parties) need to provide account management options to revoke access from specific authenticators.

7.2.3 Account Delegation. While giving your authenticator to someone else is possible, it only allows account delegation to one person at a time and does not work remotely [43, 44, 57]. As FIDO2 supports the registration of multiple authenticators for a single account [69], we argue that account delegation can become a strength of FIDO2 rather than a weakness once online services start using this feature.

7.2.4 Platform Authentication. Our study confirms that the main weakness of platform authentication is the use on multiple clients [43]. While FIDO2 allows users to add multiple authenticators per account, the individual registration of all devices for each account imposes an additional burden on users. Furthermore, it does not work in special authentication environments, e.g., public computers in a library where roaming authentication would be better suited.

Platform authentication requires trusting the involved hardware components to handle the key material. Even if the involved protocols and components are proven secure, they are often implemented as blackboxes, and some TPMs had vulnerabilities in the past [37, 49]. Many users mistrust such novel, unfamiliar technologies [23, 43, 44, 51, 57, 66], which is a dealbreaker for the acceptance of an authentication method. One potential solution is better education on how platform authentication, FIDO2, and public-key-based authentication methods work.

7.2.5 Roaming Authentication. The primary weaknesses of roaming authentication are by design: Roaming authenticators require additional hardware that users have to purchase [11, 23, 44], they have to be carried around [23, 44, 51, 57], and they can be lost, destructed and stolen [23, 43, 44, 51, 57]. These weaknesses can also apply to smartphones as physical devices, but more participants in Group R described these issues, indicating that the perceived risk is higher for roaming authentication. Furthermore, smartphones can mitigate these issues, which is infeasible with the limited capabilities of roaming authenticators: Some smartphone vendors allow users to locate their smartphones, such as via Apple Find My [4] or Android Find My Device [35], which mitigates the consequences of loss and theft. Additionally, platform authentication does not cause additional deployment costs, as it runs directly on the user's smartphone, which most users already own [54].

7.3 Limitations

This section addresses limitations of our work as a result of our recruitment and study design.

7.3.1 Task Instruction. Our instructional videos ensured that all participants had a basic understanding of passwordless authentication, resulting in a study sample that is likely better informed about FIDO2 than today's general public. This limits the ecological validity of our results for the first-time user experience of users unaware of passwordless authentication. A previous user study by Lassak et al. showed, however, that basic user training can address such misconceptions of first-time users [43]. In contrast, usability problems in the day-to-day user interaction of FIDO2 cannot be solved with education alone and are thus a more interesting scenario for our study. We argue that briefing our participants supports studying the usability of FIDO2 for informed lay users, which is increasingly representative given the ongoing proliferation of FIDO2 [46]. The instructional videos affected Group P and Group R in the same way, as both of our study groups watched identical videos except for the details of platform and roaming authentication. Thus, our participants all had identical conditions, allowing for fair comparison in our between-groups design.

7.3.2 Recruitment. Our sample was comparatively young, with a larger-than-average share of students and most participants in the 20-39 age range. Furthermore, not compensating participants for their participation in our study may have introduced a skew towards participants who are wealthy enough to participate in lab studies for free. Overall, our sample shows a slight deviation from the average population in terms of demographics but, as we argue, without significant effect on the measured items. Rather than selectively sampling participants to achieve a representative distribution, we instead controlled for factors potentially affecting usability and acceptance (Section 5.4). Additionally, our instructional videos helped balance prior knowledge, further mitigating the effects of our unfiltered sample. Neither our control variables nor age correlated significantly with usability or acceptance. While our sample only includes 10 participants (11%) older than 50, there have been related usability studies focusing on older adults' (older than 60) interaction with roaming authentication [19].

7.3.3 Mobile Operating System. We conducted our study on Apple iOS, which at the time of our study represented the most popular mobile operating system in North America [64]. As the FIDO2 user interaction is the same on iOS and Android, except for the wording and illustration in the web browser prompts in Safari and Chrome, we argue that our results also generalize to Android smartphones. Furthermore, none of the strengths, weaknesses, or adoption decisions stated by our participants directly relate to iOS but are equally relevant to FIDO2 on Android.

7.4 Outlook and Future Work

Before concluding our work, we dare a look into the future of FIDO2 and provide recommendations for future research, as well as for the FIDO Alliance and FIDO2 users.

7.4.1 User Education. Introducing our participants to the basics of passwordless authentication and the setup of FIDO2 might have led to improved usability compared to related studies, which should encourage the FIDO Alliance and website operators to strive for better FIDO2 education for the general public. Nevertheless, we found that our participants described several weaknesses that are actually solvable with mechanisms of the FIDO2 standards, e.g., account delegation or authenticator reset. The FIDO Alliance should prioritize explicitly informing users about these mechanisms of FIDO2 to mitigate such misconceptions [43], e.g., they could publish videos similar to our instructional videos (Section 4.2).

7.4.2 Compatibility. Our study shows that users consider a variety of client devices (e.g., laptops, smartphones, smart TVs, game consoles, wearables) when reflecting on their authentication use cases. As a consequence of our work, future authentication methods should be compatible with versatile authentication environments to qualify for the users' needs.

7.4.3 Platform vs. Roaming. Proper consideration of other FIDO2 weaknesses requires adding technical solutions to the FIDO2 standards or developing improved authenticators. For future research and industry, we encourage improving platform authentication because its main weaknesses (Section 6.2.2) are more easily addressable than those of roaming authenticators (Section 6.2.3).

Similarly, we suggest that relying parties (i.e., website operators) expand support for FIDO2 authentication. All modern smartphones support FIDO2 platform authentication nowadays, so FIDO2 is a viable second factor in addition to passwords or even a suitable single factor replacing passwords. Users can benefit from FIDO2's easy-to-use and secure authentication flow without too much overhead for website operators, as FIDO2's browser API is straightforward to implement. By relying on platform or roaming authentication, website operators also avoid storing users' passwords, eliminating a potential liability in case of data breaches.

A combination of smartphone platform authentication with the ideas of using smartphones as roaming authenticators for external devices [52, 57] would be promising to address most weaknesses identified in this study. For instance, Apple has announced *passkeys* for iOS 16 [5], replacing Touch ID for the Web as the iPhone's FIDO2 platform authenticator [8].

Passkeys are FIDO2 key credentials that are synchronized between the user's Apple devices. The usability results of our study

regarding FIDO2 platform authentication with Touch ID also apply to passkeys. Furthermore, passkeys address several platform authentication-related weaknesses identified for Touch ID, e.g., allowing the use of passkeys on multiple clients and enabling users to authenticate on other Apple devices (by connecting their own Apple device as a roaming authenticator). Additionally, the synchronization of passkeys in the iCloud Keychain simplifies FIDO2 account recovery. While passkeys are a promising solution within the Apple environment, the FIDO Alliance should strive for an open system that is usable on all platforms independent of a single vendor's infrastructure.

8 CONCLUSION

We conducted a between-groups lab study (N=87) of FIDO2 passwordless authentication, comparing roaming and platform authentication on smartphones. Our main goal was to identify the strengths and weaknesses of passwordless authentication on smartphones as perceived by lay users, focusing on account-specific adoption barriers. Our key findings for each research question are as follows:

RQ1. *"What is the usability and acceptance of FIDO2 passwordless authentication using platform and roaming authentication on smartphones?"* Both platform and roaming authentication show the potential of satisfactory day-to-day usability on smartphones, but less common events such as device malfunctions, account recovery, and account delegation impair the experience. Overall, users slightly prefer platform authentication.

RQ2. *"What benefits and concerns do users consider when using FIDO2 passwordless authentication on smartphones?"* Users appreciate platform and roaming authentication as simple and secure password replacements without the overhead of memorizing and managing passwords for each account. The primary weakness identified by users is the loss/theft/destruction of the authenticator and the associated burden of revoking and recovering access to each account. For roaming authentication, users criticize having to carry an additional device. In contrast, for platform authentication, users are concerned with accessing their accounts on other client devices and technical problems with the biometric sensor.

RQ3. *"Which account types do users want to secure using FIDO2 passwordless authentication on smartphones?"* While most users are likely to adopt passwordless authentication for their accounts, users prioritize usability, security, and availability differently depending on the account type. As a result, the weaknesses of passwordless authentication turn into dealbreakers for specific account types and usage patterns. Participants generally preferred platform over roaming authentication for non-sensitive accounts or frequently used accounts due to the excellent availability and the fast authentication time of the smartphone's integrated platform authenticator. Conversely, participants preferred roaming authentication for sensitive or rarely used accounts. Some users reject passwordless authentication for shared accounts as they do not see an option to delegate access to other users. Overall, most users prefer passwordless authentication for sensitive accounts. However, despite the usability benefits, some do not fully trust the technology and would therefore only use it for non-sensitive accounts.

In summary, although there is no one-size-fits-all authenticator for all account types, we recommend improving platform authentication, which has more easily addressable weaknesses than roaming authentication.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their helpful suggestions. Furthermore, we thank Annemarie Mattmann for her support during the qualitative data analysis, and Jasin Machkour for the helpful discussions on robust data analysis. This work has been co-funded by the LOEWE initiative (Hesse, Germany) within the emergenCITY center and the Federal Ministry of Education and Research of Germany in the project Open6GHub (grant number: 16KISK014).

AVAILABILITY

Together with this paper, we release a replication package with our evaluation scripts and the pseudonymized dataset generated in our study [71] consisting of usability and acceptance scores, the adoption likelihood for 11 account types, and 9 control variables for each of our 87 participants. We also provide our mockup website's source code [70] to facilitate future work.

REFERENCES

[1] Fatima Alqubaisi, Ahmad Samer Wazan, Liza Ahmad, and David W Chadwick. 2020. Should We Rush to Implement Password-less Single Factor FIDO2 based Authentication?. In *12th Annual Undergraduate Research Conference on Applied Computing (URC)*.
[2] Apple. 2020. About iOS 13 Updates. https://support.apple.com/en-us/HT210393#133. [Online; accessed 2022-06-07].
[3] Apple. 2020. Safari 14 Release Notes. https://developer.apple.com/documentation/safari-release-notes/safari-14-release-notes. [Online; accessed 2022-06-07].
[4] Apple. 2022. iCloud Find My. https://www.apple.com/icloud/find-my. [Online; accessed 2022-06-07].
[5] Apple. 2022. iOS 16 Release Notes. https://developer.apple.com/documentation/ios-ipados-release-notes/ios-16-release-notes/. [Online; accessed 2022-09-14].
[6] Apple. 2022. Locate a Lost or Stolen Device, Remotely Erase a Device. https://support.apple.com/en-us/HT210515. [Online; accessed 2022-06-07].
[7] Apple Developers. 2020. Meet Face ID and Touch ID for the web. https://developer.apple.com/videos/play/wwdc2020/10670/. [Online; accessed 2022-06-07].
[8] Apple Developers. 2022. Meet passkeys. https://developer.apple.com/videos/play/wwdc2022/10092/. [Online; accessed 2022-09-07].
[9] Aaron Bangor, Philip Kortum, and James Miller. 2009. Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. *Journal of usability studies* (2009).
[10] Yoav Benjamini and Yosef Hochberg. 1995. Controlling the False Discovery Rate: A Practical and Powerful Approach to Multiple Testing. *Journal of the Royal Statistical Society: Series B (Methodological)* (1995).
[11] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *2012 IEEE Symposium on Security and Privacy*.
[12] John Brooke. 1996. SUS: A Quick and Dirty Usability Scale. *Usability Evaluation in Industry* (1996).
[13] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. 2019. 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)*.
[14] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "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*.
[15] James Conners, Stephen Derbidge, Corey Devenport, Natalie Farnsworth, Kyler Gates, Stephen Lambert, Christopher McClain, Parker Nichols, and Daniel Zappala. 2022. Let's Authenticate: Automated Certificates for User Authentication. In *Network and Distributed Systems Security (NDSS) Symposium 2022*.
[16] James Conners and Daniel Zappala. 2019. Let's authenticate: Automated cryptographic authentication for the web with simple account recovery. In *Who Are You?! Adventures in Authentication Workshop (WAY)*.
[17] Harald Cramér. 1946. *Mathematical Methods of Statistics*. Princeton University Press.

[18] Sanchari Das, Andrew Dingman, and L Jean Camp. 2018. Why Johnny Doesn't Use Two Factor: A Two-Phase Usability Study of the FIDO U2F Security Key. In *International Conference on Financial Cryptography and Data Security*.

[19] Sanchari Das, Andrew Kim, Ben Jelen, Joshua Streiff, L Jean Camp, and Lesa Huber. 2019. Towards Implementing Inclusive Authentication Technologies for Older Adults. In *Who Are You?! Adventures in Authentication Workshop (WAY)*.

[20] Sanchari Das, Gianpaolo Russo, Andrew C Dingman, Jayati Dev, Olivia Kenny, and L Jean Camp. 2018. 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*.

[21] Sanchari Das, Bingxing Wang, Andrew Kim, and L Jean Camp. 2020. MFA is a Necessary Chore! Exploring User Mental Models of Multi-Factor Authentication Technologies. In *53rd Hawaii International Conference on System Sciences*.

[22] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

[23] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. 2020. "You still use the password after all"–Exploring FIDO2 Security Keys in a Small Company. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*.

[24] Feitian. 2018. BioPass FIDO Series Biometric Security Keys. https://www.ftsafe.com/products/FIDO/BIO. [Online; accessed 2022-06-07].

[25] Feitian. 2020. iePass FIDO Series iOS Security Key. https://www.ftsafe.com/products/FIDO/iOS. [Online; accessed 2022-06-07].

[26] FIDO Alliance. 2017. FIDO U2F Raw Message Formats. https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-raw-message-formats-v1.2-ps-20170411.html. [Online; accessed 2022-06-07].

[27] FIDO Alliance. 2019. Android now FIDO2 certified, accelerating global migration beyond passwords. https://fidoalliance.org/android-now-fido2-certified-accelerating-global-migration-beyond-passwords/. [Online; accessed 2022-06-07].

[28] FIDO Alliance. 2021. Client to Authenticator Protocol (CTAP). https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html. [Online; accessed 2022-06-07].

[29] FIDO Alliance. 2022. FIDO Alliance Member Companies & Organizations. https://fidoalliance.org/members/. [Online; accessed 2022-06-07].

[30] FIDO Alliance. 2022. FIDO Alliance Specifications Overview. https://fidoalliance.org/specifications/. [Online; accessed 2022-06-07].

[31] Mikhail Fomichev, Julia Hesse, Lars Almon, Timm Lippert, Jun Han, and Matthias Hollick. 2021. Fastzip: Faster and more secure zero-interaction pairing. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 440–452.

[32] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* (2019).

[33] Nick Frymann, Daniel Gardham, Franziskus Kiefer, Emil Lundberg, Mark Manulis, and Dain Nilsson. 2020. Asynchronous Remote Key Generation: An Analysis of Yubico's Proposal for W3C WebAuthn. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA. https://doi.org/10.1145/3372297.3417292

[34] Dennis A. Gioia, Kevin G. Corley, and Aimee L. Hamilton. 2013. Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods* 16 (2013).

[35] Google. 2022. Find, lock, or erase a lost Android device. https://support.google.com/accounts/answer/6160491. [Online; accessed 2022-09-08].

[36] GoTrustID. 2022. Smart Badge Authenticator — Idem Card. https://www.gotrustid.com/idem-card. [Online; accessed 2022-06-07].

[37] Seunghun Han, Wook Shin, Jun-Hyeok Park, and HyoungChun Kim. 2018. A bad dream: Subverting trusted platform module while you are sleeping. In *27th USENIX Security Symposium*.

[38] Blake Ives, Kenneth R. Walsh, and Helmut Schneider. 2004. The Domino Effect of Password Reuse. *Commun. ACM* 47 (2004).

[39] Maurice G. Kendall. 1938. A New Measure of Rank Correlation. *Biometrika* 30 (1938).

[40] Klaus Krippendorff. 2004. *Content Analysis: An Introduction to Its Methodology*. Sage Publications, Inc.

[41] Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas. 2016. Security Keys: Practical Cryptographic Second Factors for the Modern Web. In *International Conference on Financial Cryptography and Data Security*.

[42] Markus Langer, Cornelius J König, and Andromachi Fitili. 2018. 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* (2018).

[43] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *30th USENIX Security Symposium*.

[44] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. 2020. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *2020 IEEE Symposium on Security and Privacy*.

[45] Henry B. Mann and Donald R. Whitney. 1947. On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other. *The Annals of Mathematical Statistics* 18 (1947).

[46] MDN. 2022. Web Authentication API: Browser compatibility. https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API#browser_compatibility. [Online; accessed 2022-06-07].

[47] Nathan Mercer. 2018. Extending the capabilities of Windows Hello. https://techcommunity.microsoft.com/t5/windows-blog-archive/extending-the-capabilities-of-windows-hello/ba-p/166534. [Online; accessed 2022-06-07].

[48] Sharan B. Merriam and Elizabeth J. Tisdell. 2015. *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons.

[49] Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec, and Vashek Matyas. 2017. The return of Coppersmith's attack: Practical factorization of widely used RSA moduli. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*.

[50] Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, and Tatsuru Higurashi. 2020. Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*.

[51] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. 2021. User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS)*.

[52] Kentrell Owens, Blase Ur, and Olabode Anise. 2020. A Framework for Evaluating the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Who Are You?! Adventures in Authentication Workshop (WAY))*.

[53] Karl Pearson. 1900. 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 (1900).

[54] Pew Research Center. 2021. Mobile Fact Sheet. https://www.pewresearch.org/internet/fact-sheet/mobile/. [Online; accessed 2022-06-07].

[55] Florentin Putz, Steffen Schön, and Matthias Hollick. 2021. Future-Proof Web Authentication: Bring Your Own FIDO2 Extensions. In *Emerging Technologies for Authorization and Authentication (ETAA)*. Springer.

[56] R Core Team. 2022. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing.

[57] Brian Rasmussen. 2021. *A Usability Study of FIDO2 Roaming Software Tokens as a Password Replacement*. Master's thesis. Brigham Young University.

[58] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five Two-Factor Authentication Methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS)*.

[59] Joshua Reynolds, Nikita Samarin, Joseph Barnes, Taylor Judd, Joshua Mason, Michael Bailey, and Serge Egelman. 2020. Empirical Measurement of Systemic 2FA Usability. In *29th USENIX Security Symposium*.

[60] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. 2018. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *2018 IEEE Symposium on Security and Privacy (SP)*.

[61] Robert Rosenthal. 1991. *Meta-Analytic Procedures for Social Research*. Sage Publications, Inc.

[62] Fabian Schwarz, Khue Do, Gunnar Heide, Lucjan Hanzlik, and Christian Rossow. 2022. FeIDo: Recoverable FIDO2 Tokens Using Electronic IDs. In *2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[63] Samuel S. Shapiro and Martin B. Wilk. 1965. An analysis of variance test for normality (complete samples). *Biometrika* 52 (1965).

[64] Statista. 2021. Market share of mobile operating systems in North America from January 2018 to June 2021. https://www.statista.com/statistics/1045192/share-of-mobile-operating-systems-in-north-america-by-month/. [Online; accessed 2022-06-07].

[65] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I Added '!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*.

[66] Leon van den Boogaard. 2022. *User understanding and user acceptance of biometric authentication on mobile phones*. Master's thesis. Radboud University.

[67] Jinke D. Van Der Laan, Adriaan Heino, and Dick De Waard. 1997. A Simple Procedure for the Assessment of Acceptance of Advanced Transport Telematics. *Transportation Research Part C: Emerging Technologies* (1997).

[68] Rand Wilcox. 2017. *Introduction to Robust Estimation and Hypothesis Testing*. Elsevier, Academic Press.

[69] World Wide Web Consortium. 2021. Web Authentication: An API for Accessing Public Key Credentials Level 2. https://www.w3.org/TR/2021/REC-webauthn-2-20210408/. [Online; accessed 2022-06-07].

[70] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. 2023. *FIDO2 The Smartphone: Mockup Website for Platform and Roaming Authentication on Smartphones*. https://github.com/seemoo-lab/fido2-the-smartphone

[71] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. 2023. *Lab Study Dataset: FIDO2 Platform and Roaming Authentication on Smartphones.* https://doi.org/10.5281/zenodo.7572697
[72] Jeff Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. 2004. Password Memorability and Security: Empirical Results. *IEEE Security Privacy* 2 (2004).
[73] Yubico. 2019. Yubico Launches the World's First Lightning-Compatible Security Key, the YubiKey 5Ci. https://www.yubico.com/press-releases/yubico-launches-the-worlds-first-lightning-compatible-security-key-the-yubikey-5ci/. [Online; accessed 2022-06-07].
[74] Yubico. 2022. GitHub: webauthn-recovery-extension. https://github.com/Yubico/webauthn-recovery-extension. [Online; accessed 2022-06-07].
[75] Yubico. 2022. Security Key NFC. https://www.yubico.com/us/product/security-key-nfc-by-yubico/. [Online; accessed 2022-06-07].
[76] Yubico. 2022. YubiKey 5C NFC. https://www.yubico.com/us/product/yubikey-5c-nfc/. [Online; accessed 2022-06-07].
[77] Yubico. 2022. YubiKey Bio - FIDO Edition. https://www.yubico.com/us/product/yubikey-bio/. [Online; accessed 2022-06-07].

A DEMOGRAPHICS

In this section, we extend our participants' descriptive data (Table 1) with further demographic information (Table 7).

Table 7: Our participants' demographic data. We report in-group percentages (and frequencies), Pearson's chi-square test, and Cramér's V as the effect size (ES).

	Variable	Group P ($N = 45$)	Group R ($N = 42$)	Statistic	ES
Gender	Female	44.4 (20)	28.6 (12)	$\chi^2(1) = 2.35$ $p = .125$	.16
	Male	55.6 (25)	71.4 (30)		
	Other	0 (0)	0 (0)		
	No answer	0 (0)	0 (0)		
Age	18-19	6.7 (3)	7.1 (3)	$\chi^2(5) = 4.94$ $p = .423$	.11
	20-29	48.9 (22)	69.0 (29)		
	30-39	28.9 (13)	14.3 (6)		
	40-49	2.2 (1)	0 (0)		
	50-59	11.1 (5)	7.1 (3)		
	60-69	2.2 (1)	2.4 (1)		
Education	Still in school	4.4 (2)	0 (0)	$\chi^2(6) = 3.89$ $p = .692$	.09
	Middle school	8.9 (4)	9.5 (4)		
	High school	37.8 (17)	26.2 (11)		
	Bachelor	35.6 (16)	45.2 (19)		
	Master	8.9 (4)	11.9 (5)		
	Doctorate	2.2 (1)	2.4 (1)		
	Other	2.2 (1)	4.8 (2)		

B QUESTIONNAIRE

We provide a translation of our questionnaire, with descriptive question names for convenience. The actual questionnaire only had non-descriptive section names ("Category 1" and so on) so as to not influence the participants. We gave the questionnaire to the participants in the native language of the country where we ran the study.

Usability. Please mark the answer that reflects your immediate response to each statement. Please do not think too long about each statement and be sure to provide an answer to all statements.
⟨*Five responses ranging 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 cumbersome 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. Now please evaluate the system. To do this, read each pair of words carefully and make one cross per line.
⟨*Five responses in between the words*⟩

(1) Useless vs. Useful (2) Pleasant vs. Unpleasant (3) Bad vs. Good (4) Nice vs. Annoying (5) Effective vs. Superfluous (6) Irritating vs. Likeable (7) Assisting vs. Worthless (8) Undesirable vs. Desirable (9) Raising Alertness vs. Sleep-Inducing

Privacy Concerns. Please indicate how strongly you agree with the following statements
⟨*Seven responses ranging 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.

Technology Affinity. In the following questionnaire, 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).
⟨*Six responses from "Completely disagree" to "Completely 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.

iOS Familiarity. (1) Do you use an iPhone for private or business purposes? ⟨*Yes / No*⟩

Open-Ended Questions. (1) How would you describe your general experience with the presented authentication method? ⟨*Free text response*⟩ (2) Which advantages do you see in the usage of the presented authentication method? ⟨*Free text response*⟩ (3) Which disadvantages do you see in the usage of the presented authentication method? ⟨*Free text response*⟩

Adoption. In the following, think of a website or account that you use yourself. Assume that the service to which this account belongs supports the presented authentication method. How likely is it that you would use the presented authentication method for this account?
⟨*For items 1-11, there are five responses ranging from "very unlikely" to "very likely", with an additional response for "Not available"*⟩

Table 8: Codebooks created during the qualitative analysis (Section 4.6) of the open-ended text questions.

(a) Strengths	
Usability	⟨Easy to use/Intuitive⟩ ⟨Good for lay users⟩ ⟨Fast⟩ ⟨Easy to setup⟩
Availability	⟨One solution for many accounts⟩ ⟨Always available⟩
Cognitive effort	⟨No passwords⟩ ⟨No password creation⟩ ⟨No password updates⟩ ⟨Easier than passwords⟩ ⟨No password memorization issues⟩
Security	⟨Secure⟩ ⟨Security less reliant on smartphone⟩ ⟨Privacy⟩ ⟨Security less reliant on website⟩
(b) Weaknesses	
User experience	⟨Slow⟩ ⟨Complicated for lay users⟩ ⟨Cumbersome⟩
Deployability	⟨Costs⟩ ⟨Website compatibility⟩
Availability	⟨Technical problems⟩ ⟨Something to carry⟩ ⟨Empty battery⟩ ⟨Loss/ Destruction⟩
Mental models	⟨Unfamiliarity⟩ ⟨Revocation/Recovery⟩ ⟨Account sharing⟩ ⟨Technology mistrust⟩ ⟨Use on multiple clients⟩
Security	⟨Theft⟩ ⟨Coerced authentication⟩ ⟨Biometric security⟩ ⟨Privacy concerns⟩
(c) General Expression	
Conclusion	⟨Good⟩ ⟨Good, but⟩ ⟨Bad, but⟩ ⟨Bad⟩
Usability	⟨Easy to use / Understandable⟩ ⟨Cumbersome⟩ ⟨Fast⟩ ⟨Complicated Safari UI⟩
Security	⟨Secure⟩ ⟨Too easy, can feel insecure⟩ ⟨Privacy concerns⟩
Cognitive effort	⟨No password memorization issues⟩ ⟨Easier than a password manager⟩ ⟨(Needs) no passwords⟩
Availability	⟨Forgetting/Loss/Theft/Destruction⟩
Mental models	⟨Technology mistrust⟩ ⟨Important⟩ ⟨Innovative⟩ ⟨More transparency/ information required⟩
(d) Adoption reasons	
Importance	⟨Sensitive accounts⟩ ⟨Non-sensitive accounts⟩
Business Stuff	⟨Business-related accounts⟩
Anonymity	⟨Accounts supposed to be anonymous⟩
Multiple Devices	⟨Accounts not used on other devices⟩ ⟨Accounts mainly used on smartphone⟩ ⟨Accounts used on other devices⟩
Account Sharing	⟨Shared accounts⟩ ⟨Accounts that are not shared⟩
Frequency	⟨Rarely used accounts⟩ ⟨Frequently used accounts⟩
Speed	⟨Accounts where fast access is not important⟩ ⟨Accounts where fast access is crucial⟩
Mobility	⟨Accounts used outside of home⟩

(1) Social network account (2) Streaming service account (3) Messenger service account (4) Travel portal account (5) Gaming portal account (6) Internet service provider account (7) Google/Apple account (8) Private email account (9) Business email account (10) Online shop account (11) Online banking account (12) Please briefly explain for which accounts you would decide to use or not use the presented authentication method. ⟨*Free text response*⟩

2FA Familiarity. Which two-factor authentication methods have you previously used?

(1) Text messages ⟨*Checkbox*⟩ (2) TAN lists ⟨*Checkbox*⟩ (3) Code generators ⟨*Checkbox*⟩ (4) Smartphone apps ⟨*Checkbox*⟩ (5) Hardware keys ⟨*Checkbox*⟩ (6) Other: ⟨*Free text response*⟩

Demographics. (1) Please state your gender. ⟨*Male / Female / No answer / Other*⟩ (2) How old are you? ⟨*10-19 / 20-29 / 30-39 / 40-49 / 50-59 / 60-69 / 70-79 / ≥80*⟩ (3) Please state your highest educational degree: ⟨*Still in school / Middle school / High school / Bachelor's degree / Master's degree or Diploma / Doctorate / Other*⟩ (4) Please state your area of work or area of studies. ⟨*Free text response*⟩ (5) Is there anything else you would like to tell us? ⟨*Free text response*⟩

C CODEBOOKS

This section lists the codebooks (Table 8) that we created during the qualitative analysis of the four open-ended text-questions.