"You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company

Florian M. Farke, *Ruhr University Bochum;* Lennart Lorenz, *tracekey solutions GmbH;* Theodor Schnitzler, Philipp Markert, and Markus Dürmuth, *Ruhr University Bochum*

https://www.usenix.org/conference/soups2020/presentation/farke

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

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

"You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company

Florian M. Farke
Ruhr University Bochum

Lennart Lorenz
tracekey solutions GmbH

Theodor Schnitzler
Ruhr University Bochum

Philipp Markert
Ruhr University Bochum

Markus Dürmuth
Ruhr University Bochum

Abstract

The goal of the FIDO2 project is to provide secure and usable alternatives to password-based authentication on the Web. It relies on public-key credentials, which a user can provide via security tokens, biometrics, knowledge-based factors, or combinations. In this work, we report the results of a qualitative study accompanying the deployment of FIDO2-enabled security tokens for primary authentication in a web application of a small software company operating in the life sciences industry. We assisted the company in implementing and setting up FIDO2-enabled authentication on its public test and evaluation server. Over four weeks, we observed the authentication routine of 8 employees out of 10 employees regularly using the web application, including sales representatives, software developers, project managers, and account managers. We gathered data through login diaries, server logs, and semi-structured interviews to assess themes regarding usability, perceived security, and deployability. We found that participants had several concerns, like losing the security token and longer authentication times, while the security benefits were largely intangible or perceived as unnecessary.

1 Introduction

User authentication by username and password is still the most dominant method on the Internet and remote authentication in general. However, password-based authentication has many usability and security flaws, and researchers and practitioners have been discouraging from using it for decades [5]. On the Internet, passwords are prone to phishing attacks. Phishing attacks become more and more sophisticated, leading to often transparent and nearly indistinguishable imitations of valid authentication requests [3, 27].

Many alternatives have been proposed, but their usage is minimal [5]. Biometric schemes such as fingerprint or face recognition are regularly used to unlock phones, but they are not used for remote authentication. Authentication with hardware tokens, typically in the form of two-factor authentication (2FA) combined with a knowledge-based scheme like passwords, provides high security, but distributing and managing the hardware keys can become a great hurdle. 2FA using possession-based factors such as smartphone apps or SMS tokens as a second factor is less secure, yet easier to set up and manage, but has only found limited adoption (e.g., less than 10 % of active Google accounts use 2FA [18]).

The FIDO2 project, including both the Fast IDentity Online (FIDO) Alliance [13] – an industry association – and the World Wide Web Consortium (W3C) [29], aims at offering an alternative to password-based authentication that is both usable and secure. It consists of two main components: the *Client to Authenticator Protocol 2 (CTAP2)*, governing the communication between the client and (external) authentication hardware, and the *Web Authentication (WebAuthn)* specification defining the server-facing API on the client. WebAuthn became an official web standard in March 2019, and several browsers (e.g., Google Chrome, Mozilla Firefox, and Microsoft Edge) support it already.

FIDO2 promises a largely improved authentication experience and is backed by several big companies, like the *Alibaba Group*, *Amazon*, *Apple*, *Facebook*, and *Google*. Thus, it is very interesting to understand the likely impact it can have in practice, including aspects of deployment and usability.

In this work, we present our experience with deploying FIDO2 in the context of a company. We report on a four-week evaluation phase in which we accompanied the deployment in a life sciences company. Eight voluntary participants used a FIDO2-based authentication scheme on a daily basis and kept login diaries, which we combined with server logs, a survey, and semi-structured interviews after the four weeks.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

To use the FIDO2-based authentication method, we gave the participants security keys (USB-based hardware tokens) and guided them through the setup. The security keys could be used as a full-fledged alternative to username and password in one of the company's software products. We used security keys because they are relatively inexpensive and were compatible with all computers the participants used at work. In particular, we were interested in:

- How do users behave when they have a security key as an authentication alternative to username and password and not only as a second factor?
- Do users use the security key in their daily routine?
- What differences do users identify between the authentication schemes, especially do they perceive the new method as more secure?
- What advances or hinders the adoption of the new security key-based mechanism?

We learned that even though the participants liked using the security key-based authentication scheme, they tended to fall back to username and password. On the one hand, this is because participants do not want to abandon a habit when there is no apparent necessity in doing so. On the other hand, they fear to lock themselves out when losing or breaking the security key. Participants who use a password manager with an auto-fill feature of a web browser also report that the authentication with the security key takes longer in comparison. In contrast, the participants assumed that the keys were providing a better security level, although they did not fully comprehend the authentication procedure's technical details.

Our qualitative study is a first attempt to explore FIDO2 in a business environment and sheds light on which problems arise when deploying FIDO2. In summary, we make the following key contributions:

- We explore a *passwordless* web authentication scheme rolled out as the first authentication factor in a real-world application.
- We provide insights into the daily usage of security keys in a company environment over four weeks by combining login diaries, server logs, and interviews. The data indicate that participants liked the passwordless authentication scheme because of its simple usage, yet from the users' perspective, there is no clear advantage over password-based authentication. The positive impression of the security keys is less pronounced if participants previously used password managers that already limit some negative aspects of password-based authentication.
- Analyzing the participants' feedback, we identify a set of adoption barriers, including the fear of getting locked out, a cumbersome integration of the security keys in the work environment, and the general routine in using passwords. Those barriers should be minimized before introducing new security measures in work environments.

2 Background

The FIDO2 project has a more general and thus flexible approach to user authentication than its predecessor, the Universal 2nd Factor (U2F) standard, and other authentication schemes. Compared to other 2FA/multi-factor authentication (MFA) approaches, the advantages of FIDO2 are (i) growing support by all major browser and operating system vendors, (ii) open and standardized protocols, (iii) making authentication via username and password not mandatory (although it is still possible), and (iv) building upon vetted asymmetric cryptographic principles and algorithms.

The FIDO2 project consists of the WebAuthn specification of the W3C [4] and the Client to Authenticator Protocol (CTAP) defined by the FIDO Alliance [6]. FIDO2 allows abstracting from the actual authenticator (e.g., a hardware token). Thus, the *Relying Party* (e.g., a web server) does not require knowledge about the implementation details of the authenticator. Figure 1 depicts the interplay of CTAP2 and WebAuthn as we used it in our study.

WebAuthn specifies a standardized, browser-independent JavaScript API that allows web services to interact with all sorts of facilities. Through this API, web services can implement user authentication in a way that is resilient to phishing, password theft, and replay attacks. Instead of relying on shared secrets like passwords, public-key cryptography is used to create unique credentials for every web service and only generated and stored on the client's device.

On the other hand, CTAP2 governs the communication between external authenticators and web browsers or other applications supporting WebAuthn. The proposed CTAP standard comprises two protocol versions – CTAP1, the protocol used for U2F, and CTAP2 a new protocol used for WebAuthn. At the time of the study, implementations for the operating systems *Android* and *Windows 10* were available.

The FIDO Alliance uses the term "passwordless" to describe single-factor authentication and multi-factor authentication with an authenticator or with an authenticator and a personal identification number (PIN) or biometric. While it is easy to agree with, for example, hardware tokens as a single factor being passwordless, this is not inevitably the case if additionally a PIN is used as a second factor. Although similar to a password, a FIDO2 PIN has some notable differences compared to passwords in the context of web authentication:

- No shared secret has to be entered, sent over network, or store on the server-side. Phishing attempts and data breaches do not affect the authenticity of the credentials.
- A single PIN unlocks the authenticator and all account credentials registered with the device. There is no need to set a unique password for every web service.
- Guessing or brute-forcing the PIN is limited to eight consecutive attempts. Reaching this limit resets the authenticator to factory settings, effectively invalidating all generated credentials [6].

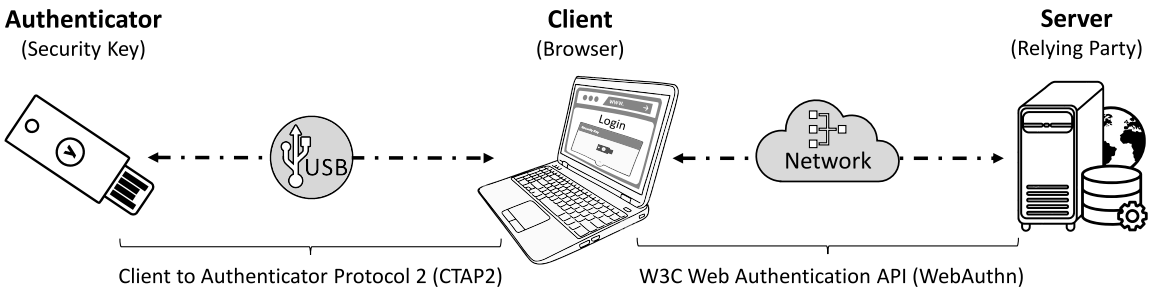

Figure 1: Communication via FIDO2. The cryptographic authenticator and the client communicate via USB using CTAP2. The client's browser implements the JavaScript-based Web Authentication API to communicate with the server over the network.

3 Methods

Our study's primary goal was to gain insights into the usability, user perception, and barriers or facilitators for the adoption of FIDO2. To increase ecological validity, we conducted the study on a web application in a small software company in the life sciences industry. We collected and analyzed qualitative data in the form of login diaries and semi-structured interviews, but also quantitative data in the form of server logs.

3.1 Study Environment

We conducted our study at *tracekey solutions GmbH*,[1] a small software company from Bochum (Germany). As a *software-as-a-service* provider, they develop and operate a product serialization service for small and medium-sized businesses in the pharmaceutical industry. The service offers a solution to fulfill the traceability requirements of this industry [12].

The service includes a web application that requires customers and employees to authenticate with a username and password. For our study, we extended the existing login form and authentication back end and added a new login option using WebAuthn with a roaming hardware token.

We decided only to allow PIN-protected security keys (in contrast to Lyastani et al. [17]) because some participants occasionally worked remotely, and losing the security key was a realistic scenario. However, this may have reduced the comfort of using the key (see Section 4.3). The company had an authentication policy for its software that required re-authentication after 30 minutes of inactivity. Due to this policy, we did not consider adopting a "remember me" option, which does not ask the user to authenticate for a particular time after a successful login on a device. We did not implement any fallback authentication procedure for the security key because the participants could still use their passwords, and manual account recovery was also a viable option.

[1] https://www.tracekey.com/, as of April 30, 2020

Following tracekey's three-week release cycles, the security key-based authentication method was developed on an internal test server and pushed to the public test and validation server before the study started. The test server was accessed regularly by tracekey employees and customers. Due to a delay in the release process, the new authentication method was available on the production server only in the last week of the study (see *Section 5.5*).

The participants used two variants of FIDO2-compliant hardware tokens, the *Security Key by Yubico* and *YubiKey 5 NFC*, both from *Yubico* [30]. Both variants had the same form factor and supported WebAuthn, CTAP, and U2F. YubiKey 5 NFC offered additional features (e.g., support for OTP algorithms, OpenPGP, etc.) and could also be used via NFC. We did not require any of the additional features so that both key variants could be used in the same way.

3.1.1 Recruitment

We asked all employees who were eligible for our study (i.e., having accounts on both the public test server and the production server, using the web application on a daily basis, and being available at the time of the study). We invited the 10 employees who fulfilled these criteria to an in-house workshop, in which 9 attended. During the training session, we briefed the attendees about the purpose of the study, the procedure, risks and benefits, and the option to withdraw from the study at any time without penalty. We asked them to read and sign a consent form containing the same information. Participation was voluntary and uncompensated since they took part in the study during working hours.

We informed the participants about the required operating system and browser version. The minimum requirement was Microsoft Windows 10 version 1903 because it implemented CTAP2 in Windows Hello. The participants used Mozilla Firefox, Microsoft Edge, and Google Chrome. Of those three, only the stable version of Chrome did not support Windows Hello at the time of the study. We asked participants who used Google Chrome to switch to one of the other browsers or the beta version of Google Chrome.

3.1.2 Implementation

We used a server-side WebAuthn library provided by Yubico to implement the new FIDO2-based authentication. This library was integrated because the Spring Security framework used by the web application did not support WebAuthn at the time of the study.

To implement the login, we used the *resident credential* feature of FIDO2. This feature allows storing credential information like the username and private key on any authenticator with built-in memory. The participants did not need to enter their username because of this feature.

In addition to this, we redesigned the login screen of the web application (see Step 1 of Figure 2) to present both login methods (i.e., WebAuthn with security key and username and password). We decided to display both options on the same website to allow participants to choose between them without additional clicking on the website.

3.1.3 Data Preparation

At that time of the study, not all browsers stable versions supported the WebAuthn options used by our FIDO2-based authentication like user verification (i.e., via PIN) and resident keys (i.e., the username is chosen from a list instead of manually entered). Thus, most WebAuthn related errors could be attributed to the use of an unsupported browser.

We removed entries of accounts without a registered security key from the logs before the analysis, leaving logs containing entries of study participants or failed logins, which we could not attribute. The information provided by the timestamps of each login attempt was used to calculate average authentication times for the different login types aggregated across all participants (see Figure 4).

3.2 Study Protocol

The study was conducted over six-week in June/July 2019 and was framed as a usability study on security keys. It consisted of three phases. The first phase was a workshop in which we briefed the participants on using the security key. It followed a four-week phase of day-to-day use of the security key during which we collected data via authentication diaries and server logs. Finally, we interviewed the participants to discuss their experience using the security key and debrief them.

3.2.1 Initial Workshop

We started the study with a one-hour workshop. During this workshop, we first introduced the study as well as its purpose. We gave all participants consent forms, which also contained information about our study and their participation, and let them read and sign the form. A fifteen-minute training session introduced the security key, demonstrated the setup and use of the key, and showcased the user interfaces of each phase. It is important to highlight that we are specifically targeting a corporate context, where such training sessions are relatively common. This situation is very different from introducing WebAuthn to consumers.

After the training session, participants were handed the security keys and asked to set up the key on their work laptop computer and one of their accounts in the web application. Since most of the participants had multiple accounts for the web application, we encouraged them to register it with additional frequently used accounts and assisted them if necessary.

At the end of the workshop, participants filled in a questionnaire in which we gathered demographic data and feedback on the user interface and workflow of the implementation. We were especially interested in participants' knowledge about web authentication and used a modified version of the *web-use skill index* of Hargittai and Hsieh [14] for this purpose, focusing on authentication-related terms. We also gathered free-text responses about the participants' experiences with security keys and 2FA, and asked them to explain how a security key may improve the security of their account.

3.2.2 Authentication Diary

Over the next four weeks, the participants' task was to use the security key in their work routine. Additionally, we encouraged them to keep an authentication dairy in which they noted all logins over the first two days, and later only their failed login attempts. We adapted the diary from the work of Steves et al. [26]. Each diary entry comprised authentication time and date, on which server the participant tried to log in (e.g., the public test server) and whether the participants used the security key or username and password. They could also rate their satisfaction with the login on a five-item emoji-based scale we adapted from previous work [2, 20]. Despite their potential drawbacks (e.g., varying representations of the same emotion [19]), emojis were found to be well suited for affective self-reports of participants [28]. Furthermore, each diary entry had a section for errors and comments.

To enrich the authentication diaries and to get insights into how long it took the participants to authenticate, we also collected the timings of each login from the server logs. Each log entry contained multiple timestamps, username, user agent, WebAuthn-related information (e.g., the WebAuthn credential ID or the WebAuthn error message), and information about the login's success or failure. Especially in the case of failed login attempts, the logs provided additional insights.

3.2.3 Interview

After the four-week usage phase, we invited the participants to interviews. The interviews took place in a conference room in the company, and each session lasted 15 to 20 minutes. All but one participant were German native speakers, and we conducted seven interviews in German and one in English.

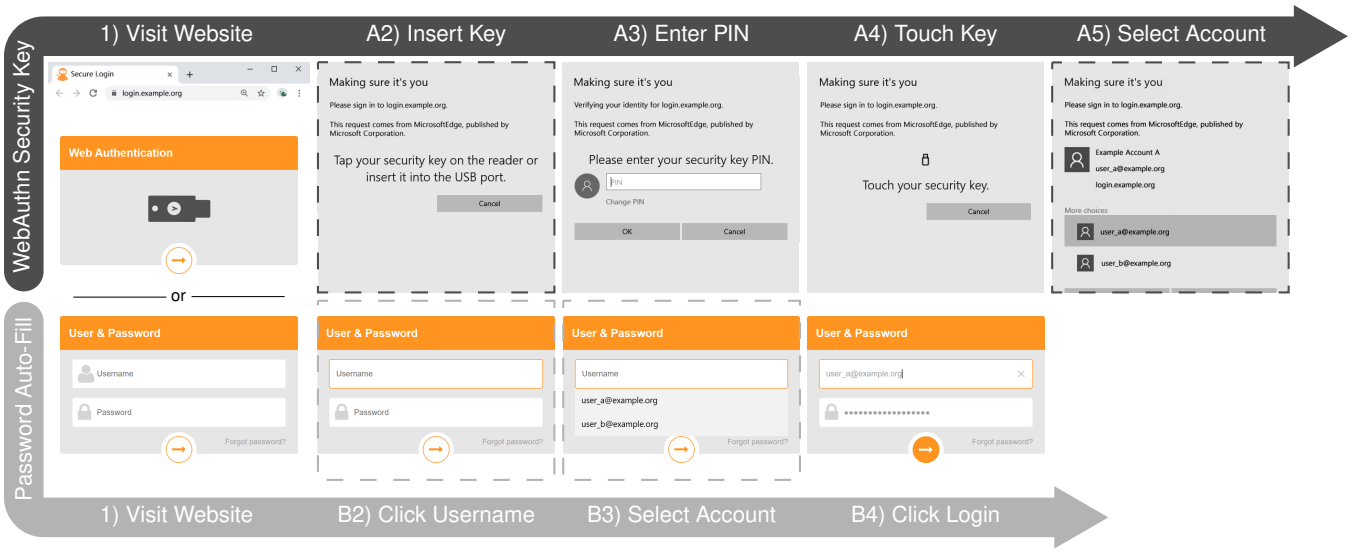

Figure 2: Comparison of the login procedures when using WebAuthn with a security key (top) vs. the browser's password auto-fill feature (bottom). The dashed borders are indicating omitted steps. If the security key is already plugged-in, the dialog in Step A2 does not show up. Having only one account stored on the key or in the browser, skips steps A5, B2, and B3.

The interviews were semi-structured and addressed the perceived usability of the security key, the differences between the key-based and password-based authentication, and the obstacles in using the key. Our goal was to examine why participants used the security key and what kept them from using it. The participants were also asked which of the two login methods they perceived as more secure.

We started each interview with a question about how they liked using the security key. The participants' answers gave us insights into their general impression of the security key and their experience of using it. We then asked them how frequently they used the web application and how often they used the key over the last four weeks. The participants were also asked to describe the difference between username password and security keys. If they mentioned 2FA, we let them explain what 2FA is and what the two factors are.

Additionally, we asked them to share their thoughts on which authentication method is more secure and their rationales. The full interview guide can be found in Appendix A.2.

In contrast to password-based authentication, our possession-based method required the user to have the security key with them. Thus, we wanted to know how hard it was to have the key at hand for the participants since this was the most obvious hurdle. However, we encouraged them to tell us about other obstacles they encountered as well. Finally, we asked them whether they would use the key in the future and for the reasons for their decision.

To analyze the interviews, we used a data-driven coding technique (as described in [10]). Two researchers independently coded all interviews through categorizing participant statements and identify recurring themes in each interview. They then compared the categories and themes across all interviews and created codes. A third researcher merged the themes and codes, derived a final codebook, and used it to code all interviews again. The full codebook is presented in Appendix B.

3.3 Demographics

Since we conducted our study in a small company, the participants had different backgrounds and positions. They were software developers, sales representatives, or project managers. One-third of the participants were female (3 out of 9) and the other two-thirds were male. The participants were 22–44 years old (mean: 30, SD: 6.3). Five (out of 9) participants had completed a master's degree, one holds a bachelor's degree, and two had studied at a university without completing a degree. One had completed a vocational training. All but one of the 9 people who attended the workshop completed the full study. The person who dropped out was on vacation during the second phase of the study and could not use the security key. Nevertheless, we included this person's feedback from the workshop in our evaluation.

Web Authentication Skills

To examine the participants' knowledge about web authentication, we adjusted the *Web-use Skill Measure* [14] to focus on web authentication, resulting in a skill survey containing ten authentication-related terms. We selected surveyed items from security awareness trainings, education materials, and infographics, including the NCSC glossary [22]. Table 1 shows the mean and standard deviation for all ten items.

Table 1: Web authentication skills are determined by rating the understanding of ten authentication-related items. The items are in the order of appearance in the questionnaire.

Item	Mean	SD
Malware	3.1	0.74
Phishing	3.3	0.94
Two-factor authentication	3.4	0.69
One-time password	2.5	1.26
Personal identification number	4.2	0.63
Auto-fill	3.2	1.55
Challenge-response	1.8	1.23
Password manager	3.9	0.99
Brute-force attack	2.4	1.43
Security question	4.0	0.82
Composite score	3.2	0.73
N	9	
Scale	5-point	
Cronbach's α	0.89	

The standard deviations were higher for items with a lower level of understanding (e.g., One-Time Password) than for items with a "high-level" understanding (e.g., personal identification number). These low-level items refer to more technical aspects of authentication. In contrast to the results obtained by Hargittai and Hsieh [14], our participants showed a higher understanding of the medium-level rated terms *Malware* and *Phishing*, indicating that the participants had an excellent understanding of authentication-related risks. A composite score of 3.2 indicates that the level of understanding lay between "some" and "good" understanding.

A Cronbach's α value of 0.89 as an estimate of the interrelatedness of items and internal consistency of the survey can be considered good, almost excellent. Due to the small sample size, statistical evidence is limited. However, the results met our expectations because all participants worked in a software company and reported to be tech-savvy.

3.4 Ethics

Our institution did not have a review board governing this type of study, so we discussed the study design with peers to validate our research's ethical perspective. We made sure to minimize any potential adverse effects from the study by following the ethical principles laid out in the Belmont report [21]. These principles included having an informed consent procedure at the beginning of the study and explaining to the participants that they could withdraw from the study without any negative consequences.

4 Results

Next, we present and discuss the results of our study. We evaluate the data we gathered through login diaries, server logs, and interviews.

4.1 Frequency of Authentication

Among the participants, the number of logins per day varied. Some participants logged into the web application multiple times a day, while others only used it once a week or less. Figure 3 shows how often the participants used the security key over the four weeks of the study broken down by participant and week of the study.

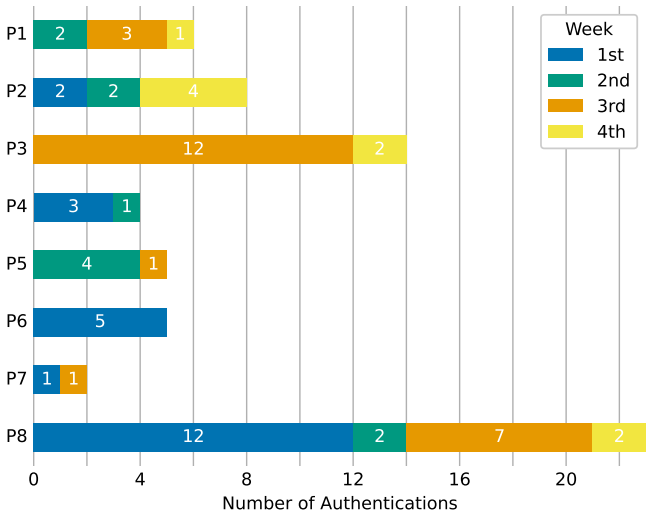

Figure 3: Breakdown of the number of authentications with the security key per participant and week. Except for participant P8, all participants used the security key only occasionally.

The reason for this discrepancy is that we conducted our study on the public test and evaluation server of the web application, which all the participants use but less often than the production server (see Section 5.5). We analyzed the server logs to gain insight into how often the participants used security keys. Table 2 presents a detailed breakdown of how many times the participants logged into the web application during the four weeks of the study.

For our analysis of the server logs, we filtered all log entries in which the WebAuthn method or the usernames of our participants were involved. After the filtering, we had 287 unique logins attempts over the four weeks. Surprisingly, only 67 (23.4 %) of these login attempts used a security key while 141 of the remaining 220 login attempts used browser auto-fill (i.e., browser password manager). We discuss this discrepancy in the number of logins in Section 4.4 in more detail.

Table 2: Breakdown of successful authentications per account, participant, and authentication method. Most of the participants registered their security keys for at least two accounts. Four participant pairs shared five accounts; for these accounts, we cannot distinguish which login belongs to which participant. *Manual logins* contain all login attempts for which the participants typed in the username and password manually or copied them from an external password manager/storage.

		Number of Authentication			
Account	**IDs**	**Security Key**	**Password Auto-fill**	**Manual Logins**	**Total**
A1	P1	4	7	10	21
A2	P1, P3	2	3	4	9
A3	P2	1	0	0	1
A4	P2	2	1	0	3
A5	P2	1	9	7	17
A6	P2, P4	2	33	3	38
A7	P2, P4	5	30	2	37
A8	P3	2	4	5	11
A9	P3	2	0	1	3
A10	P3	1	2	3	6
A11	P3	1	4	13	18
A12	P3, P4	9	6	12	27
A13	P5	0	20	2	22
A14	P5	5	6	8	19
A15	P6	4	9	3	16
A16	P6, P8	3	5	2	10
A17	P7	2	0	3	5
A18	P8	21	2	1	24
Total		67	141	79	287

To analyze login attempts with security key, we used the authentication diaries and the interviews. Participant P1 faced a problem where the touch sensor of the security key (see *A4) Touch key* in Figure 2) did not work at first, so he needed multiple tries until the login was successful. Participant P8 reported a similar problem. In this case, the software detected the security only after plugging it in again. Figure 2 shows the respective step labeled *A2) Search/insert key*. The other six participants reported no security key-related problems.

4.2 General Impressions

We started the interviews asking by participants about their general impressions using the security key over the four-week study period. The themes we found in our analysis of the interviews resulted in five categories of codes (cf. Appendix B): (i) Use of the security key, (ii) comparison of the security key with username and password, (iii) adoption barriers, (iv) general impression, and (v) perceived security.

Our warm-up question in the interviews was how they liked using the security key. Four participants appeared to be pleased about using the security key since they described the key as *easy to use* and its handling as *intuitive*. One participant was even enthusiastic when talking about impressions of the security key.

> P2: *"I don't need to remember anything. It's also faster, I am completely convinced. I think it's terrific."*

The four other participants started referring to minor issues which occurred when they used the key (e.g., being annoyed by touching the key because *"it is on the other side of the desk"* (P7)), two of which still rated its usage to be overall *"ok"* (P3, P5). The remaining two participants stated they did not use the key as often as intended and did not provide a clear judgment.

4.3 Authentication Timings and Convenience

During the interviews, the participants revealed that their convenience in authenticating varied in many aspects. In particular, their feedback on convenience using the security key highly depended on how they managed their password-based credentials since this was their ground truth against which they compared the new method.

We encountered three different ways of managing passwords: (i) The employees used a collaboration software where they stored their shared credentials and copy-and-pasted them into the respective login website, (ii) they saved their passwords using a third-party password manager software, or (iii) they used the browser's built-in password manager.

Five participants (P1, P2, P4, P5, P8) mentioned that the security key reduced the memory effort because they only needed to remember one PIN. Two participants who manually copy-and-pasted passwords (P2, P3) stated that using the security key was faster than entering username and password.

> P2: *"[...] but it is much more convenient if you can simply use this key, push it, enter your 4-digit PIN instead of your 12-character password [...]. It is also faster like this."*

In contrast to these two participants, five participants used browser built-in password managers with a password auto-fill feature and stated that the authentication with auto-fill required fewer steps than using the security key (P4, P6, P7) or was faster (P5, P6, P7, P8). The timings we extracted from the server logs support their statements. We measured the time starting when the login website was fully loaded and ending when the login form was submitted to the server for each authentication attempt. Figure 4 presents the timings of the different login variants. It shows that the security key was slower than the password auto-fill feature of a browser.

For authentication attempts using the security key, we could not determine whether the measured times include the time to reach for and plug in the security key or if it were already plugged in before plugged in before. We expect our result set to comprise both scenarios. However, since we consider physical interactions with the security key part of the authentication ceremony, our results provide a best-case estimate. If the measured times had not included preparing the key, the gap compared to the password auto-fill timings would have become even larger.

Figure 2 illustrates the steps required to log in with the key compared to the browser's auto-fill feature. Using the security key requires three steps in a best-case scenario. This scenario requires that the key is already plugged into the computer (Step A2), only the security key is configured for Windows Hello (Step A2), and only one account is registered for the key (Step A5). The three steps are (i) clicking the login button beneath the security key symbol (see Step 1), (ii) entering the PIN of the security key as shown in Step A3), and (iii) touching the key (see Step A4).

In contrast, the credential auto-fill via browser requires at best (with only one username-password pair stored in the browser for the website) one click on the login button, as shown in Step B4. Otherwise, the user needs to click the text field for the username (Step B2) and select the desired account (Step B3). In both cases, the auto-fill procedure requires fewer steps and no physical interaction with additional hardware, which explains why it is the faster authentication procedure.

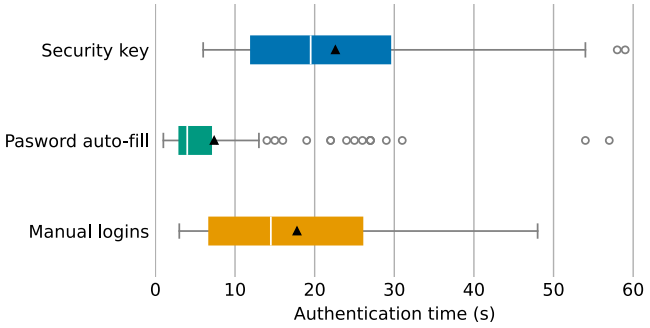

Figure 4: Authentication timings for different login variants. The time spent by participants to authenticate varies depending on the login type used. (▲ denotes the mean.)

Participant P4 provided the most differentiated feedback, taking into account both manually copying and pasting passwords as well as using the browser's password manager when assessing the convenience using the security key.

> P4: *"I already have the passwords saved in my Edge account for all different accounts. So that was more convenient for me because it's hardly one click [...] Even if I save something in the browser, it will work that way as well but if you use the security key it will definitely [be] time saving as well [...]."*

Another participant referred to the use of the 2FA-protected third-party password manager and preferred using the security key because it was less cumbersome.

> P5: *"In comparison I think that the key is more user-friendly, it requires less effort than invoking both WinAuth and KeePass."*

4.4 Weighing Security and Purposes

During the interviews, participants indicated awareness of different security requirements for different services. We unveiled such tendencies when asking participants about the purposes they had used the security key for. Getting a full view is a two-step process since we also needed to capture how the participants estimated the security of the available authentication options.

4.4.1 Security of Authentication Schemes

While six participants (P3–P8) rated the security key as more secure than the password-based authentication schemes, participant P1 guessed that the password copy-and-paste mechanism is presumably more secure than the security key. However, he mentioned the risk of losing the key and, consequently, becoming unavailable to log in, as a reason for the key's reduced level of security.

> P1: *"I guess you can use such a security key, and how do you log in if you don't have it? [...] So, I believe the standard way [i.e., using passwords] is maybe more secure? Well, I'm not sure if it's 'more secure' but I can log in in any case [...]"*

Another participant stated that the security offered a good security level but refrained from deeming one scheme more secure than another. Participants P2, P5, and P8 explained that the security of the key-based authentication is more secure because it relies on "two factors", i.e., possession of the key and knowing the correct PIN. Furthermore, participant P5 elaborated his understanding of how the security key works, alleging that the passwords are stored on the key.

> P5: *"It is secure, if I understand correctly, because the passwords are stored on the key and, therefore, are not affected if I have a compromised machine [...]"*

Even though this explanation is not correct from a technical perspective, the idea of P5 can give non-expert users some useful intuition why the key is more secure than passwords.

4.4.2 Use of the Security Key

In total, three participants talked about different security requirements depending on a service's purpose. Two participants named online banking (P6, P7), another authentication at work (P5) as use cases that require a higher level of security.

When asked whether they want to keep using the key after the study, four participants signaled willingness (P2, P3, P4, P8), two were not sure (P5, P6), and two did not want to use the key in the future (P1, P7). Opinions of those who could imagine continuing using the key ranged from plain approvals (P2, P8: *"yes"*) to readiness to use the key exclusively if the working environment supported this:

> P3: *"Yes, and if it would work with the production server, I would work exclusively using the key."*

However, participants revealed different opinions on extending the use to personal accounts. While one participant claimed willingness to use the key for personal purposes (P2), two participants stated that they would not use a security key off the job.

While P4 stated to use a password manager for personal accounts, P7 unambiguously explained that the additional time required to use the key compared to a password manager is an unacceptable trade-off in everyday use.

> P7: *"In the time it takes to dig it up, plug it in, enter the PIN, and push it – I could have already bought two pairs of shoes."*

Another participant remained rather indecisive when asked about using the key for personal use, due to the additional overhead compared to the use of a password manager.

> P8: *"When you have stored your passwords in your browser, it is still faster than picking the key, plugging it in and entering the PIN."*

4.5 Adoption Barriers

The authentication diaries and responses in the interviews show that usage rates of the security key were rather low (see Section 4.1), so we asked the participants what prevented them from using the security key in particular situations. They reported several hurdles when using the key, e.g., the fear of losing access to their accounts, the additional effort/time required to plug the key in or unlock it, and the habitual use of passwords.

Participants P5 and P7 mentioned that the additional effort and time to interact with the key makes it less convenient than authenticating with username and password.

> P5: *"Well, it would start to make a real difference if I didn't have to enter anything at all but only had to touch the key."*

The time factor was not only important for authentication, two participants (P5, P6) also mentioned that they needed to invest time ("*5–10 minutes*") to set up the key for an account, which implies that even comparably small amounts of time can be an adoption hurdle.

> P6: *"There is this small initial effort you need to find five to ten minutes for."*

Besides the time aspects, participants' feedback from the interviews unveiled further details about additional obstacles towards the adoption of the security key.

4.5.1 Fallback Authentication

Several participants expressed concerns about not being able to log in if they do not carry their keys (P2, P3) or even lose them (P1). Participant P3 further mentioned a potential risk of technical flaws, hampering the ability to log in. The majority of participants had no problems with carrying the key, e.g., by attaching it to their key rings.

> P6: *"I have it on my [...] key ring. Thus, I have it with me all the time."*

However, this was not a proper solution for every participant. P7 explicitly deemed this a disadvantage and suggested providing a solution to attach the key to a smartphone.

> P7: *"That's cumbersome, and I also have quite few keys, and I don't want to plug them all in."*

Potential problems about handling the key were also mentioned by another participant (P2), who feared to destroy the key due to its tiny size and shakiness when plugged in and suggested a more sturdy design.

These answers show that participants' views were not limited to the scope of the study but also widened for the security key's general use as a single first authentication factor. Not being able to log in due to losing the key was not a real risk in our scenario since participants could always choose between password-based and key-based authentication during the study.

4.5.2 Workflow and Environment

The workflow of the authentication or the work environment can also be an adoption barrier. As discussed in Section 4.3, the security key requires more interactions for each authentication. Participant P6 explicitly mentioned the higher click-count when using the security key (i.e., the Windows Hello user interface) compared to entering the username and password or using the browser's password manager.

> P6: *"The workflow needs to be simple. Like even faster. Fewer clicks."*

Another participant saw the account selection of Windows Hello as a hurdle for adoption.

> P1: *"I have 40 accounts or so. When I register the key for all of them and I want to log in then, I need to scroll through all of them [...] That's a little bit time-consuming."*

Two participants indicated that the characteristics of their work environment made it more challenging to integrate the key into their routines. For instance, picking an account to log in when multiple accounts were used on the same website, since the names of all accounts followed a naming convention made them very similar.

> P3: *"I cannot see at first sight to which account [the username] actually belongs."*

Similar, another participant denoted that the login is slightly different depending on the operating system and browser (here Windows 10 version 1903 and Google Chrome 76).

> P6: *"[...] on my computer the Windows update has not been rolled out yet, so, I could not use Firefox [...] and [in the other browser] I need to click three times and touch [the key] twice to log in."*

4.5.3 Routine in using Passwords

Considering aspects of introducing and integrating new security measures into a well-functioning working environment raises questions about how to overcome long-established security behaviors. Participant P7, who showed a generally rather reserved attitude towards using the security key, remarked that routine in handling passwords was a reason not to use the security key for authentication, especially in cases when something needed to be checked quickly.

> P7: *"It was not an active decision [to use the password], but rather a situation when I just had to get things done. [...] I'm just used to it, because I know the password for this application. [...] It's like an addiction. You still use the password after all."*

This statement suggests that deeply ingrained security habits cannot be challenged, let alone be replaced easily, not within the four weeks of our study.

5 Discussion

In contrast to prior work investigating security keys in the context of 2FA [8, 9, 15, 16, 24], we focused on a secure authentication scheme without username and password. From a user perspective, the difference is to have a new authentication scheme instead of adding steps to a well-known one. The resulting process still suffers from similar issues, as found by studies on security keys in a 2FA context [8, 16].

However, our analysis of the interviews and authentication dairies identified three problem areas unique to or more important for the security key as a primary authentication factor: (i) concerns about account recovery in case of key loss or defect, (ii) having a more complex and possibly slower authentication process, and (iii) security benefits are intangible.

Losing access to the account through defect or loss of the security key is the primary concern for users, especially if it is the only way to authenticate. A possible solution to this problem is registering multiple security keys for one account, but this seems to be an additional burden to the users. Another option is using username and password as fallback authentication, but this nullifies the security benefits of FIDO2. The question of how to realize secure fallback authentication for FIDO2 is still open for future research.

The differences in the timings between the security key and other login methods, as indicated in Figure 4 and also mentioned by multiple participants, needs to be tested with a larger sample. Other authenticators could make "passwordless" FIDO2-based authentication faster and less complex.

Even though most participants found the security key to be more secure than username and password, the reasons why the key was, in fact, more secure were hard to grasp for them. More research on how to explain the security benefits of FIDO2-based authentication schemes is needed. In the following, we discuss our results using the three categories to assess authentication schemes proposed by Bonneau et al. [5].

5.1 Usability

Our study indicates that the security key is usable in the sense that all the participants understood how to use the key correctly and comprehended the on-screen instructions. The problems the participants encountered were rare, and they could solve all of them.

Authentication times appeared to be more of a limiting factor. Using the browser's auto-fill feature was the fastest authentication method in our scenario. Even "manual logins" (e.g., copy and paste the password) may be faster than using the security key. This speed difference may be one of the primary adoption barriers.

The level of routine and habituation users developed with passwords is high. Some interview statements implied that password-based authentication does not necessarily induce friction but works as an unconscious background process that makes it more challenging to get used to a new scheme like the security key. Protecting the key with a PIN also undermines its benefit of allowing "passwordless" authentication.

Physical aspects and related handling of the key could also be an obstacle. Actions like carrying the security key around, e.g., by attaching it to a key ring, inserting it, or touching its button were a hurdle for some participants. However, the degree of inconvenience appears to depend highly on the user's perception and predispositions.

5.2 Deployability

WebAuthn support, while increasing, is the biggest deployment issue. This lack of support comprises operating systems, browsers, but also software frameworks to ease integration. Only recent versions of operating systems and browsers work with all WebAuthn features, thus requiring web service owners to offer alternative authentication schemes and show appropriate error messages in case of unsupported operations.

Missing best practices on login form design for WebAuthn-based authentication hinders a consistent user experience across different web services. While a typical design has emerged for password-based login forms over time, there is no such design for WebAuthn. Research on the impact of such forms is scarce.

On the other hand, direct costs for hardware or support and indirect costs through lost productivity are negligible. In a company with tech-savvy personnel, the expense for the adoption of a security key-based authentication (not including implementation) should not be too high. As Lang et al. [16] showed with a predecessor of U2F and thus FIDO2, the same can be true for large companies.

5.3 (Perceived) Security

Security is only secondary to usability when choosing an authentication scheme in daily work life. If security is not promoted as an essential part of work instead of being just an obstacle to other tasks, that fact remains [11].

The benefits of the security key, especially when it requires a PIN, need to be conveyed clearly. While creating risk awareness helps users to make informed decisions, reminding users of the benefits provided by a scheme seems to be even more promising [9].

5.4 Overcome Adoption Barriers

We think that the FIDO2 project can replace password-based authentication on the Web in the long run. However, at the moment, only a few applications or Internet services support FIDO2-based authentication, which impedes its adoption, and the lack of reference implementations of the WebAuthn server-side hinders its integration. These obstacles will probably resolve over time. To overcome some of the other adaption barriers we found, we have the following suggestions:

- Support multiple different authenticators (platform and roaming authenticators if possible);
- Require adaption of the security key in organizations (as suggested by Colnago et al. [8] for 2FA);
- Make FIDO2-based authentication available for as many systems as possible
- For PIN-protected security keys, allow to "remember" the PIN until the key is unplugged.

5.5 Limitations

Due to the qualitative nature of the study and the small sample size, it can only provide a first insight into "passwordless" authentication with security keys. Our results may not apply to a broader population but indicate potential interesting topics and raise new research questions.

We deployed the new authentication method on a public test server for our study. Although all participants had access to the server and user accounts on it, half of them (4 participants) mentioned in the interviews that they used the test server less often than the production system. The low use of the key affected how the participants used the security key and might have had an impact on the perceived usefulness of it.

6 Related Work

The FIDO2 project has not been around for a long time, which is why research in this specific area is limited. Most related to our study is the work by Lyastani et al. [17], as it does investigate the use of tokens for primary authentication in the context of FIDO2. Lyastani et al. [17] conducted a lab study with end-users to get insights into the perception, acceptance, and concerns when security keys are used for passwordless authentication. Their results conform to ours in terms of a mixed impression with an overall positive impression of token-based authentication but also the fear of the participants to lose the token locking themselves out.

In contrast to Lyastani et al. [17], we implemented the token-based authentication in combination with a PIN because it counteracts one of the disadvantages the participants in the study by Lyastani et al. [17] mentioned, namely, the risk of illegal access when the authenticator is lost. However, this combination made the workflow more complex, which again can impede adopting the key. Additionally, we concentrate on the long-term and real-world impact of using token-based authentication in a corporate context. Through this different focus in the study, we saw that overcoming the routine users gained in using passwords as an additional adoption barrier.

Besides FIDO2, Pico, proposed by Stajano [25], is another example of a token-based login method. In a study by Aebischer et al. [1], users appreciated the ability to avoid passwords because of the known drawbacks, but adoption was still identified as a problem as users prefer to stick to the familiar password-based authentication. We observed a similar phenomenon, among the participants who used a password manager. Although they were convinced that the security key-based solution was more secure, but they preferred the password managers because they were fast.

While we are interested in hardware tokens as a first factor, research into 2FA is also related to our work as it gives important insights into the use of tokens for authentication. Despite what factor is used, the initial setup of an additional second factor is one of the major issues for most users [7, 15, 23, 24].

A corporate context – in which we were interested in this study – allows counteracting this problem by offering customized guidance for the setup phase. Because of this, we walked the participants through the initial steps.

Studies by Das et al. [9] and Ciolino et al. [7] further analyzed why users decide not to use 2FA security keys. They found two main reasons: (i) Users are afraid of losing their key locking themselves out and (ii) some users also do not fear an account takeover, which is why they see no necessity for the additional effort associated with the use of a security key. These findings are supported by adoption rates reported by Google with less than 10 % of active Google accounts having 2FA enabled [18]. While these findings are relevant for the end-user, the situation in a corporate context is different. Here, the motivation to use security keys is driven by the company, and using them can be made mandatory for the employees.

Furthermore, it was found that users have an overall positive attitude towards security keys once they are in place as a second factor. [7, 9, 24]. They are seen as easy to use and increase the perceived security [8, 16]. We come to a similar conclusion for the case when security keys are used as a primary factor. Regarding the timing of security key-based logins, Reese et al. [23] found that login times decrease the longer and the more often security keys are used. Some participants also mentioned the fast authentication time, yet some abandoned the security keys in favor of a password manager because it allows an even more efficient authentication.

7 Conclusion

We conducted a qualitative study on the usability of FIDO2, using USB-based hardware tokens in the form of security keys in the context of a small company. The core components of FIDO2 – WebAuthn and CTAP – offer promising alternatives to the dominant username-password scheme used for web authentication. FIDO2 security keys present a phishing-resistant form of hardware tokens suited as the primary authentication factor for web applications.

In contrast to previous work on authentication via security keys, we focused on using the key as a primary authentication factor instead of having it as an additional factor in a 2FA setting. Although most participants considered the security key-based login as usable, several of them stopped using the key as it was slower than using the password manager built in their browsers. Furthermore, the security benefits were largely intangible or perceived as unnecessary by the participants. Another issue was the missing support of some browser and operating systems at the time of the study. All these adoption barriers should be minimized before introducing FIDO2 (with security keys) to replace username and password-based authentication in a company.

Acknowledgments

The authors would like to thank *tracekey solutions GmbH* for allowing them to conduct a study in their company and providing the necessary software and hardware. This research was partially funded by the MKW-NRW research training groups SecHuman, “Human Centered Systems Security” sponsored by the state of North Rhine-Westphalia, Germany, and the German Research Foundation (DFG) within the framework of the Excellence Strategy of the Federal Government and the States – EXC2092 *CASA* – 390781972.

References

[1] Seb Aebischer, Claudio Dettoni, Graeme Craig Jenkinson, Katarzyna Kinga Krol, David Llewellyn-Jones, Toshiyuki Masui, and Francesco Mario Stajano. Pico in the Wild: Replacing Passwords, One Site at a Time. In *European Workshop on Usable Security*, EuroUSEC ’16, Paris, France, April 2017. ISOC.

[2] Sarah Alismail and Hengwei Zhang. The Use of Emoji in Electronic User Experience Questionnaire: An Exploratory Case Study. In *Hawaii International Conference on System Sciences*, HICSS ’18, Waikoloa Village, Hawaii, USA, January 2018. ACM.

[3] Anti-Phishing Working Group. Phishing Attack Trends Report – 2Q 2018, October 2018. https://docs.apwg.org/reports/apwg_trends_report_q2_2018.pdf, as of April 30, 2020.

[4] Dirk Balfanz, James C. Jones, Akshay Kumar, Huakai Liao, Jeff Hodges, Emil Lundberg, Czeskis Alexei, Rolf Lindemann, and Michael Jones. Web Authentication: An API for accessing Public Key Credentials Level 1. Recommendation REC-webauthn-1-20190304, World Wide Web Consortium, March 2019.

[5] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *IEEE Symposium on Security and Privacy*, SP ’12, pages 553–567, San Jose, California, USA, May 2012. IEEE.

[6] Christiaan Brand, Alexei Czeskis, Jakob Ehrensvärd, Michael B. Jones, Akshay Kumar, Rolf Lindemann, Adam Powers, and Johan Verrept. Client to Authenticator Protocol (CTAP). Proposed Standard fido-v2.0-ps-20190130, FIDO Alliance, January 2019.

[7] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *Symposium on Usable Privacy*

and Security, SOUPS '19, pages 339–356, Santa Clara, California, USA, August 2019. USENIX.

[8] 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 *ACM Conference on Human Factors in Computing Systems*, CHI '18, pages 456:1–456:11, Montreal, Quebec, Canada, April 2018. ACM.

[9] Sanchari Das, Andrew Dingman, and L. Jean Camp. Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key. In *Financial Cryptography and Data Security*, FC '18, pages 160–179, Santa Barbara Beach, Curação, February 2018. Springer.

[10] Jessica T. DeCuir-Gunby, Patricia L. Marshall, and Allison W. McCulloch. Developing and Using a Codebook for the Analysis of Interview Data: An Example from a Professional Development Research Project. *Field methods*, 23(2):136–155, December 2011.

[11] Geoffrey B. Duggan, Hilary Johnson, and Beate Grawemeyer. Rational Security: Modelling Everyday Password Use. *International Journal of Human-Computer Studies*, 70(6):415–431, June 2012.

[12] European Parliament and Council of the European Union. Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products. *Official Journal of the European Union*, 174(1):74–87, July 2011.

[13] FIDO Alliance. The FIDO ("Fast IDentity Online") Alliance – Industry Association to Promote Authentication Standards, February 2013. https://fidoalliance.org, as of April 30, 2020.

[14] Eszter Hargittai and Yuli Patrick Hsieh. Succinct Survey Measures of Web-Use Skills. *Social Science Computer Review*, 30(1):95–107, February 2012.

[15] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. In *Workshop on Usable Security*, USEC '15, San Diego, California, USA, February 2015. ISOC.

[16] Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas. Security Keys: Practical Cryptographic Second Factors for the Modern Web. In *Financial Cryptography and Data Security*, FC '16, pages 422–440, Accra Beach, Barbados, February 2016. Springer.

[17] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy*, SP '20, San Francisco, California, USA, May 2020. IEEE.

[18] Grzergor Milka. Anatomy of Account Takeover. In *USENIX Enigma Conference*, Enigma '18, Santa Clara, California, USA, January 2018. USENIX.

[19] Hannah Jean Miller, Jacob Thebault-Spieker, Shuo Chang, Isaac Johnson, Loren Terveen, and Brent Hecht. "Blissfully Happy" or "Ready to Fight": Varying Interpretations of Emoji. In *AAAI Conference on Web and Social Media*, ICWSM '16, pages 259–268, Cologne, Germany, May 2016. AAAI.

[20] Adam Moore, Christina M. Steiner, and Owen Conlan. Design and Development of an Empirical Smiley-Based Affective Instrument. In *Workshop on Emotions and Personality in Personalized Services*, EMPIRE '13, pages 41–52, Rome, Italy, January 2013. CEUR.

[21] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, September 1978. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html, as of April 30, 2020.

[22] National Cyber Security Centre. Common Words and Phrases Relating to Cyber Security, January 2018. https://www.ncsc.gov.uk/information/ncsc-glossary, as of April 30, 2020.

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

[24] 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 *IEEE Symposium on Security and Privacy*, SP '18, pages 872–888, Oakland, California, USA, May 2018. IEEE.

[25] Frank Stajano. Pico: No More Passwords. In *Workshop on Security Protocols*, SPW '11, pages 49–81, Cambridge, United Kingdom, March 2011. Springer.

[26] Michelle Steves, Dana Chisnell, M. Angela Sasse, Kat Krol, Mary Theofanos, and Hannah Wald. Report: Authentication Diary Study. Technical Report 7983, NIST, February 2014.

[27] Symantec Corporation. Internet Security Threat Report Volume 23, 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf, as of April 30, 2020.

[28] Alexander Toet, Daisuke Kaneko, Shota Ushiama, Sofie Hoving, Inge Kruijf, Anne-Marie Brouwer, Victor Kallen, and Jan Erp. EmojiGrid: A 2D Pictorial Scale for the Assessment of Food Elicited Emotions. *Food Research International*, 115:541–551, January 2019.

[29] W3C. The World Wide Web Consortium (W3C) – Standards Organization for the World Wide Web, October 1994. https://www.w3.org, as of April 30, 2020.

[30] Yubico AB. Yubico | YubiKey strong two factor authentication, February 2020. https://www.yubico.com/, as of April 30, 2020.

A Study Materials

This appendix contains the materials we used to conduct the study. All information about the authors or participants have been removed.

A.1 Initial Workshop Questionnaire

How familiar are you with the following authentication and security-related items? Please choose a number between 1 and 5 where 1 represents "no understanding" and 5 represents "full understanding" of the item.

	None (1)	Little (2)	Some (3)	Good (4)	Full (5)
Malware	◯	◯	◯	◯	◯
Phishing	◯	◯	◯	◯	◯
Two-factor authentication	◯	◯	◯	◯	◯
One-time password	◯	◯	◯	◯	◯
Personal identification number	◯	◯	◯	◯	◯
Auto-fill	◯	◯	◯	◯	◯
Challenge-response	◯	◯	◯	◯	◯
Password manager	◯	◯	◯	◯	◯
Brute-force attack	◯	◯	◯	◯	◯
Security question	◯	◯	◯	◯	◯

Please answer all of the following questions.

1. Have you ever used a security key before?
   - ◯ Yes, and I still do
   - ◯ Yes, but I stopped using it
   - ◯ No
   - ◯ I do not know
2. Why? Why not?

   Answer: _____
3. Have you ever used two-factor authentication for any of your online accounts?
   - ◯ Yes, and I still do
   - ◯ Yes, but I stopped using it
   - ◯ No
   - ◯ I do not know
4. Why? Why not?

   Answer: _____
5. What did you like about the setup procedure of the security key?

   Answer: _____
6. How would you improve the setup procedure of the security key?

   Answer: _____
7. How does a security key make your account more secure?

   Answer: _____
8. Do you have any comments, ideas, or suggestions for improvement?

   Answer: _____

A.2 Interview Guideline

(a) Introduction

- Thanks again for taking part in the security key evaluation over the past four weeks and also thank you for agreeing to this interview.
- The interview will take 10-15 minutes.
- Are you OK with me recording our interview?
- <*Start recording.*>
- There are obviously no right or wrong answers here, I am just interested in your personal perceptions and your honest opinions.
- Any questions? Can we start?

(b) Interview

- You were able to test a security key over the last 4 weeks, how do you like it?

  . . . . . .
- How many times a day do you log in on average?
- What do you think, how often have you used the security key during the last 4 weeks?
- Have you registered additional accounts with the security key after the training?

  . . . . . .
- <*Ask questions based on the authentication diary.*>

  . . . . . .
- What are the differences between security keys and passwords?
- Do you think the security key offers any benefits compared to username and password?
- What do you think is more secure?
- How easy or difficult was it to have your security key with you whenever you needed it?
- What kept you from using the security keys?

  . . . . . .
- What was the best part of using the security key?
- What would you improve about the user-friendliness of using the security key?
- Would you like to continue to use the security key?

(c) Debriefing

- <*Briefly summarize interview.*>
- Study goal: We investigate security keys as a password "replacement".
- We are interested in usability issues of these keys.
- Do you have any questions about the interview or the study?
- <*Stop recording.*>

B Codebook

Table 1: **Category:** Use of the security key – The participant indicates if or for what purposes they want to use the security key.

Code	Freq.	Description	Example
Continue using key	6	The participant states to continue using the security key after the study.	*"For all new projects which I'll get, I'll use the security key."* (P4)
Personal use	5	The participant considers using the security key also for their personal accounts.	*"[...] and I'd also use it in my private life."* (P2)
Only for work	5	The participant states to only use the security key for work.	*"I feel like I will just use the security key for work and KeePass and all that for personal stuff."* (P4)
Key is impractical for multiple accounts	4	The participant states that using the security key is impractical for users with more than 5 accounts on one website (Windows Hello selection dialog).	*"As I said, I have 40 different accounts for work. In this case, it's not really practical."* (P1)
Only for sensitive accounts	4	The participant indicates to use the security key only for sensitive accounts (e.g., online banking).	*"And I think in cases where one needs more security, it's good and I could understand it [to use a security key]."* (P7)
No need for the key	2	The participant mentions that using the security key for only one account is not worth the effort.	*"If I'd say: 'Okay, I just got 20 new accounts', then maybe, but with one account, no."* (P7)
Stop using key	2	The participant states to not continue using the security key after the study.	*"I don't think I would continue using it."* (P1)

Table 2: **Category:** Comparison of the security key – The participant compares a certain aspect of the security key with username and password.

Code	Freq.	Description	Example
Key requires more steps than browser PW	7	The participant states using the security key requires more steps/clicks compared to using the built-in password manger of the browser.	*"For already existing accounts, I already had the passwords saved. So, that was more convenient."* (P4)
Key slower than browser PW	6	The participant indicates that authentication with the security key takes longer than using the built-in password manger of the browser.	*"When you have stored your passwords in your browser, it is still faster than picking the key, plugging it in, and entering the PIN."* (P8)
Key memory-wise less effort	5	The participant states using the security key is compared to username and password more convenient because they only need to remember one PIN.	*"I'd prefer to use the key. I think it's easier to only remember the PIN, like just this one PIN and nothing else."* (P5)
Key faster	5	The participant indicates that authentication with the security key is faster than with username and password.	*"It's time saving. Absolutely."* (P4)
No difference	1	The participant finds both security key and username and password equally convenient/inconvenient.	*"But for me it doesn't make a huge difference whether I manually type in a password, or if I type in the PIN for the key. Unfortunately, it doesn't make a huge difference."* (P5)
Key more cognitive effort	1	The participant states that using the security key requires more thinking than entering username and password.	*"Touching the key is something different. [...] sometimes I don't think about what I'm doing, I just do it. And then I find myself using the password again."* (P7)

Table 3: **Category:** Adoption barriers – The participant refers to an obstacle or possible obstacle when using the security key.

Code	Freq.	Description	Example
Higher effort	5	The participant finds carrying/plugging in/unlocking the security key cumbersome or time-consuming.	*"Well, it would start to make a real difference if I didn't have to enter anything at all but only had to touch the key."* (P5)
Fear to lock out	4	The participant fears to lose access to web application through loss or defect of the key.	*"Well, if I forget or loose it, I couldn't get into my account"* (P3)
Routine with passwords	3	The participant mentions to use username and password instead of the security key out of habit.	*"It's like an addiction. You still use the password after all."* (P7)
Setup per account	3	The participant thinks the effort to set up the key for multiple accounts can be an obstacle to adoption.	*"There is this small initial effort you need to find five to ten minutes for."* (P6)
More complex workflow	2	The participant reports usability issues, like higher click count or confusing account selection in Windows Hello.	*"The workflow needs to be simple. Like even faster. Fewer clicks."* (P6)
Forgot to take key	1	The participant states to have forgotten the key and therefore not being able to use it to log in.	*"Well, I assume I always forgot to take it with me."* (P2)
Key perceived as fragile	1	The participant reports difficulties with the form factor of the security key (e.g., the fear to break it accidentally).	*"It always bends so easily, and I thought: 'Oh my god, now I'm breaking the poor thing.'"* (P2)

Table 4: **Category:** General impression – The participant mentions their general impression of the security key.

Code	Freq.	Description	Example
Key is usable/convenient	9	The participant finds the security key generally usable or convenient.	*"You click it [the account name], quickly enter your PIN, touch the key with your finger, and you're done. It's smooth."* (P5)
Key is easy/intuitive	6	The participant finds the security key generally easy or intuitive to use.	*"It's easy, like really easy. I'm a huge fan I have to say."* (P2)
Key is cool/novel	2	The participant shows enthusiasm because the security key is "new" or "cool" technology.	*"Well, at the beginning I started very enthusiastically. I really thought it's cool thing. "* (P6)

Table 5: **Category:** Perceived security – The participant comments on the security of the security key.

Code	Freq.	Description	Example
Key more secure	11	The participant states that the security key is more secure than username and password	*"Yes, I think one thing I like is that no password is sent, if I understand that correctly, over the Internet but it [the password] just decrypts the key locally."* (P6)
Unsure	3	The participant is unsure whether the security key is more secure or not.	*"I guess you can use such a security key, and how do you log in if you don't have it? [...] So, I believe the standard way [i.e., using passwords] is maybe more secure? Well, I'm not sure if it's 'more secure' but I can log in in any case [...]"* (P1)