Why Aren't We Using Passkeys?
Obstacles Companies Face Deploying FIDO2 Passwordless Authentication
(Extended Version)

Leona Lassak⋆, Elleen Pan†, Blase Ur†, Maximilian Golla‡
⋆ *Ruhr University Bochum,* † *University of Chicago,*
‡ *CISPA Helmholtz Center for Information Security*

Abstract

When adopted by the W3C in 2019, the FIDO2 standard for passwordless authentication was touted as a replacement for passwords on the web. With FIDO2, users leverage passkeys (cryptographic credentials) to authenticate to websites. Even though major operating systems now support passkeys, compatible hardware is now widely available, and some major companies now offer passwordless options, both the deployment and adoption have been slow. As FIDO2 has many security and usability advantages over passwords, we investigate what obstacles hinder companies from large-scale deployment of passwordless authentication. We conducted 28 semi-structured interviews with chief information security officers (CISOs) and authentication managers from both companies that have and have not deployed passwordless authentication, as well as FIDO2 experts. Our results shed light on the current state of deployment and perception. We highlight key barriers to adoption, including account recovery, friction, technical issues, regulatory requirements, and security culture. From the obstacles identified, we make recommendations for increasing the adoption of passwordless authentication.

1 Introduction

On the web, passwords remain the dominant form of user authentication [13, 48]. Unfortunately, phishing and credential-stuffing attacks against passwords continue to cause extensive damage even among well-protected online services [92, 95]. Reinforcing passwords by deploying two-factor authentication [40, 76], risk-based authentication [58, 94], and account-security notifications [41, 57, 86], as well as promoting the use of password managers [59, 72] are incomplete solutions to the security problems of relying on passwords [13, 14, 48].

A decade ago, Grosse and Upadhyay [45] described an internal pilot of a USB hardware token that "protects against phishing" and "makes the server side immune to database theft." Shortly after, the Fast IDentity Online (*FIDO*) Alliance was founded to develop and promote authentication standards that "reduce the world's reliance on passwords."

Building on earlier efforts to enhance multi-factor authentication, the FIDO Alliance's *FIDO2* suite of protocols foregrounds passwordless, single-factor authentication for the web. As detailed in Section 2, a user's *authenticator*—either specialized hardware (e.g., a YubiKey) or software running on an existing device—generates a unique asymmetric cryptographic keypair bound to a particular website. The private key is kept on the user's authenticator; the website holds the public key. To log in, the user authenticates locally to their authenticator (e.g., with a biometric or PIN), which then uses the private key to authenticate to the remote website. Around the time the World Wide Web Consortium (*W3C*) adopted FIDO2 as a web standard in 2019, media coverage focused on how FIDO2 would "kill the password" [39, 63, 73].

Starting in 2021, Apple, Google, Microsoft, and others announced *passkeys*, which are multi-device credentials following the FIDO2 standard. In part, passkeys are a rebranding of the existing FIDO2 approach, though they add features for syncing private keys across a user's devices (to avoid needing to re-register on each device) or using a single existing device (e.g., phone) as the authenticator across all devices. The popular media again heralded passkeys as the technology that would "kill the password" [16, 65, 68, 80].

Today, most major operating systems and browsers support FIDO2-based passwordless authentication [34]. Researchers have analyzed FIDO2's security [9, 11, 46] and usability [27, 28, 55, 56, 69, 70], finding FIDO2 more secure and usable than passwords. The FIDO Alliance and W3C have working groups dedicated to driving FIDO2 adoption [36]. It is thus surprising that, to date, only a few companies have deployed passwordless authentication, widely or at all.

We investigate why we are not using FIDO passwordless authentication by answering the following research questions:

RQ1 *How aware are companies about FIDO?*
RQ2 *What are their experiences deploying FIDO?*
RQ3 *What challenges do companies face deploying FIDO?*
RQ4 *How do companies prioritize certain obstacles?*

To this end, we conducted 28 semi-structured interviews with three types of stakeholders: (1) companies and organizations with user-facing web properties, including both those that have and have not deployed passwordless authentication; (2) vendors selling passwordless solutions to businesses; and (3) experts contributing to the FIDO2 standard. We recruited participants in a number of ways, including with help from the FIDO Alliance, enabling us to recruit chief information security officers (*CISOs*), security engineers working on authentication, and identity management leaders. Such participants are typically difficult to recruit for academic research.

Our interviews aimed to understand participants' experiences with passwordless authentication in their own organizations, identify obstacles their organizations faced deploying passwordless authentication, and elicit participants' personal opinions about the FIDO2 standard. The protocol included a card-sorting task to rate potential deployment challenges.

Around half of our participants had experience deploying FIDO-based protocols either for passwordless or two-factor authentication (*2FA*). The biggest obstacles to FIDO2 deployment participants reported relate to fallback authentication and recovery options, complexity and friction due to the drastic change, technical issues like browser support and revocation options, regulatory requirements, and security culture. We also identify both concerns and misconceptions regarding passkeys. The results of our card-sorting task reveal a mismatch between what organizations considering deploying FIDO2 believe to be pressing obstacles compared to the beliefs of FIDO experts and identity and access management (*IAM*) vendors. Even though we observe widespread agreement that FIDO2 will play a major role in making passwords obsolete in many web use cases, legacy systems make it impossible to eliminate passwords quickly. Our results suggest that FIDO2 will not eliminate passwords completely, but has the potential to reduce the number of passwords used.

Collectively, our findings provide the first comprehensive examination of obstacles and perceptions related to FIDO-based passwordless authentication. We discuss recommendations for industry and outline future research for increasing the adoption of passwordless authentication.

2 Background

Next, we introduce the FIDO2 standard and explore related work on passwordless authentication and studying CISOs.

2.1 FIDO2, WebAuthn, and Passkeys

The FIDO Alliance is an industry association developing and promoting passwordless authentication based on public-key cryptography. Its earlier Universal 2nd Factor (*U2F*) protocol enables cryptographic two-factor authentication [45]. All of its protocols have advantages over passwords: they are fast when used with biometrics [55], they are phishing resistant [89], and secrets are only stored locally.

The *FIDO2* W3C standard consists of two protocols. Web Authentication (*WebAuthn*) [50] describes a JavaScript interface that allows a *relying party* (e.g., a website) to perform a passwordless challenge-response protocol with a *client* (e.g., a web browser). The companion Client to Authenticator Protocol (*CTAP*) [15] specifies the communication between a cryptographic authenticator (e.g., a hardware security key or smartphone) and a client. In FIDO2, the user authenticates by proving their possession of the private key. Specifically, they create a signature that can be verified using the corresponding public key stored on the server during registration. To prevent unauthorized use, the user authenticates locally to their device (e.g., using a PIN or biometric) before the private key is used for signing. The protocol has been formally verified [9, 11].

FIDO2 differentiates between *platform authenticators* (those integrated with a device) and *roaming authenticators* (those that can be used across multiple devices). Example platform authenticators include *Microsoft's Windows Hello* and *Apple's Touch ID* when used exclusively for authentication on a given device. While roaming authenticators canonically included hardware like USB keys that could be plugged into different devices, recent smartphones can be used as roaming authenticators for cross-device authentication [70, 71]. For security, the private key and biometrics templates should be isolated from the main processor and OS (e.g., on a TPM).

Relying parties can specify authenticator types they support (roaming, platform, or both) and whether to require *user verification* via local authentication (e.g., with a PIN or biometric) or just *user presence* (e.g., pressing a button on the security key). Common use cases for user verification include passwordless authentication as offered by Adobe, eBay, Google, Microsoft, PayPal, or Yahoo [2]. In contrast, user presence is commonly used in 2FA scenarios in which a security key is used in conjunction with a password.

To increase the usability of FIDO2, the FIDO Alliance recently standardized *passkeys* [30]. Passkeys are multi-device FIDO2 credentials that third parties may synchronize over the cloud, removing the burden on the user to register multiple devices to the same website and offering convenient recovery in case of device loss or theft. Apple and Google report that their passkey synchronization is end-to-end encrypted [7, 12].

2.2 Related Work

FIDO2: Prior work on FIDO2 adoption has mainly studied client-side usability challenges. Lyastani et al. randomly assigned 94 participants to configure an account using either a YubiKey or a password [56], finding that participants preferred FIDO2 passwordless authentication over a password. However, several concerns were raised: recovering accounts if the security key is lost, hardware compatibility, and a lack of mental models explaining passwordless authentication. Farke et al. conducted a similar study with a small software company [28]. Nine participants used a YubiKey during their daily work routine, keeping a diary of when they authenticated. Participants responded positively to security keys, citing ease of use, intuitiveness, and convenience. Some also gave up on using the key, mistakenly thinking it did not provide security benefits or feeling it was slower than using their browser's password manager. Nawrath had 161 participants attempt passwordless registration using devices they already owned, finding a lack of platform/browser support to be a key barrier [64]. Lassak et al. studied user perceptions of biometric WebAuthn [55], finding that 67% of participants mistakenly thought biometric data was stored remotely.

Some work has examined FIDO2 from the developer's perspective, though only on a small scale. Alam et al. [4] briefly outlined some conceptual limitations of developers implementing WebAuthn by analyzing discussions in the WebAuthn developer community. These limitations included a lack of deployment-ready solutions, wrong mental models about WebAuthn, and confusing technical details in the FIDO2 specification. Bicakci and Uzunay [10] briefly discussed potential challenges using FIDO2 as passwordless authentication, such as the lack of a convenient recovery method or support for sharing credentials. Casey et al. proposed a new protocol on top of WebAuthn because businesses may not be able to implement current FIDO2 solutions to comply with their policies [18]. We instead interviewed various FIDO2 stakeholders to gather their perspectives on the current challenges and necessary changes for large-scale deployment of FIDO2.

Studying CISOs: Our methods are also motivated by previous studies interviewing CISOs and security professionals in industry. Reinfelder et al. explored how security managers handle user requirements and behaviors by interviewing seven managers from large German companies [77], utilizing snowball sampling to recruit this hard-to-reach population. Haney et al. interviewed 28 cybersecurity advocates to understand how they overcome negative user perceptions of security and motivate the adoption of best-practice security measures [47]. Hielscher et al. interviewed 30 CISOs to understand whether foundational concepts from human-centered security are used in practice [49], while Ashenden et al. interviewed five CISOs from global companies to understand their approach to security [8]. Wolf et al. interviewed 27 CISOs to identify how to improve security in small businesses [96]. Similar to prior work, we utilized semi-structured interviews and snowball sampling, among other recruitment methods. Doing so enabled us to recruit 32 participants across 28 interviews.

3 Methods

We first describe how we generated a list of potential FIDO2 obstacles based on a literature review. We then outline our interview protocol, recruitment, and participant demographics before presenting limitations and ethical considerations.

Table 1: Potential obstacles based on our literature review.

	ID	Description
Necessity	**N1**	Customers are happy
	N2	Passwords are good enough
	N3	Passwords are not problematic with password managers
	N4	Secure enough with 2FA
	N5	Usability good enough with SSO
Usability	**U1**	No standardized fallback
	U2	Unclear handling of lost or stolen devices
	U3	Unclear handling for new devices
	U4	Unclear handling with multiple devices
	U5	Customers do not use biometrics
	U6	Roaming authenticators are not usable
	U7	Change causes friction
	U8	Customers would not switch
Deployability	**D1**	Libraries and frameworks do not exist
	D2	Libraries and frameworks are incomplete
	D3	Libraries and frameworks are not understandable
	D4	Libraries and frameworks written in wrong language
	D5	Need to support both passwords and FIDO
	D6	Cannot get rid of passwords entirely
	D7	Browsers do not have all functionality
	D8	User interface is OS-dependent
IT Management	**M1**	No need to talk to them
	M2	They do not let us talk
	M3	They do not understand
	M4	Policy forbids open-source software
	M5	Policies do not allow biometrics
	M6	Waiting for peer organizations
Finance	**F1**	Investment is unclear
	F2	Implementing FIDO too expensive
	F3	New communication and interfaces are expensive
Comm.	**C1**	FIDO incompatible with UX guidelines
	C2	Need to brand FIDO2
	C3	Unclear how to communicate about FIDO2
	C4	Design questions are hard

3.1 List of Potential Obstacles

Between January and May of 2022, we compiled a list of obstacles to FIDO2 deployment discussed in prior work and artifacts from the W3C and FIDO Alliance's working group meetings, as detailed below. Table 1 presents the resultant list, which we used as part of our card-sorting task.

Prior Papers: Using search terms like "FIDO," "FIDO2," "passkeys," and "WebAuthn" on Google Scholar, we collected potentially related scientific papers. From this list, we identified papers that covered security aspects of FIDO2 [5, 89], implementation issues [4, 74], deployments [69], user experiences [20, 23, 55, 56, 64, 88], roaming authenticators [28, 70, 71], and fallback solutions [54, 84]. Work about security proofs [9, 19] was out of scope. We also looked at non-FIDO2 work about the adoption of other security mechanisms, such as HTTPs [53, 87], 2FA [21, 79], and password managers [59].

Online Resources: We also analyzed online resources, such as articles and blog posts from IAMs like Okta [83] and services like Microsoft [60] and eBay [52] that had already

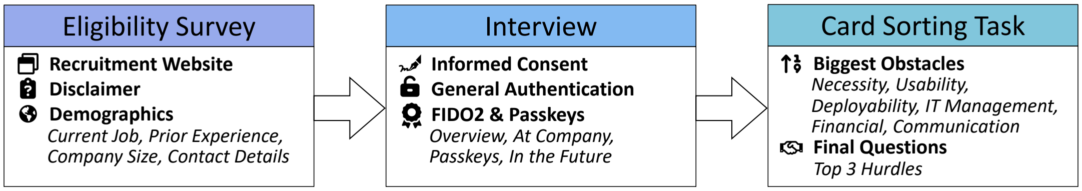

Figure 1: Prospective participants provided demographics and contact details in an eligibility survey. Selected participants were invited to a 45-minute interview about FIDO2 that included a card-sorting task about potential deployment obstacles.

deployed FIDO. We also examined case studies published by the FIDO Alliance covering deployments at services like login.gov, Visa, and NTT [31] from 2017 to 2021.

W3C and FIDO Working Group Resources: Artifacts produced by W3C and FIDO working groups, especially those dealing with adoption (e.g., the user experience working group) [36], also contributed to our list of potential obstacles. We focused on the W3C Web Authentication WG and WebAuthn Adoption CG's open GitHub issues [98], mailing list, and meeting minutes [97, 99], and the official "FIDO Dev" mailing list [33]. We decided against including highly specific issues as our target interviewees would most likely not be deeply versed in the protocols' implementation details.

Two researchers coded all resources in an open-coding process resulting in the first version of what we call our "list of potential obstacles." These coders had backgrounds in cybersecurity and deep familiarity with the FIDO standards and ecosystem. In cooperation with the entire research team, we categorized and refined the list through multiple discussion sessions. We also sought input from external practitioners working at IAMs, as well as FIDO experts with whom we are in personal contact. The final list can be seen in Table 1. In the text, we refer to specific obstacles with their identifier (e.g., N1 = "Customers are happy").

3.2 Interview Structure

Figure 1 summarizes the interview structure. Appendix A contains the full study instrument. Questions differed slightly across our three stakeholder groups: (1) "Organizations," or companies deploying FIDO for their employees or customers; (2) "IAMs," or companies that sell authentication solutions to other companies; and (3) "FIDO experts," or participants in FIDO Alliance working groups [36].

Interviews began with the moderator asking participants whether they had any questions about the consent form, which we shared via email prior to the interview. After the participant consented, we started an audio recording. We reassured participants that no identifiable information—particularly company names—would be disclosed outside the research team. We then asked participants about their company and role, as well as their experience in the field of authentication.

The interview's main section began with a discussion of the general authentication infrastructure in the participant's organization for both employees and customers. When not mentioned explicitly, we prompted for specific features (e.g., 2FA) to ensure a comprehensive overview. We also instructed participants to share their positive and negative experiences about authentication at their organization. Aside from FIDO experts, we then assessed participants' knowledge of FIDO and answered any questions they raised about FIDO protocols. Next, we directed the conversation toward the use of FIDO in their organization. For participants whose organizations had already adopted any FIDO authentication options (termed *adopters*), we asked about their experience with deployment, feedback they had received, and what the biggest obstacles had been to date. We also discussed the decisions that had led to the deployment. For the others (*non-adopters*), we asked whether there had been any internal discussions about adoption and what they felt were the key arguments in favor of, and against, FIDO. We explicitly asked what it would take for their organization to adopt it. If participants did not bring up passkeys specifically, we solicited their opinion on them.

In an interactive card sorting task on a digital whiteboard (see Appendix B), 18 participants then rated our list of potential obstacles (Table 1) by perceived severity. We asked them to narrate their thought process in a "think-aloud" manner. They could rate obstacles as *major* ("a deal-breaker almost on its own"), *minor* ("in conjunction with other minor obstacles impedes the deployment"), or *not an obstacle*. The remaining participants ran out of time for this activity.

3.3 Recruitment / Participant Demographics

Apart from FIDO experts, our target participant group was CISOs. We also accepted security engineers and developers with extensive experience in authentication alongside decision-making responsibility in their organization. We emphasized that no specialized knowledge about FIDO was required to participate as we were particularly interested in the perspectives of organizations that had not yet adopted FIDO. As we had a very specific, hard-to-reach target group, we used a variety of recruitment strategies. First, we created a recruitment website that summarized the study, addressed concerns about privacy and confidentiality, and linked to the eligibility survey. We posted on social media, including LinkedIn and Twitter, and we also directly contacted people from our personal networks. We also reached out to the FIDO Al-

Table 2: Summary of participants and their organizations. For anonymity, numbers are binned and some fields are blinded. “FIDO Experts” contributed to FIDO development. “IAM” participants sell identity and access management solutions.

		FIDO		Participant		Organization		
	ID	Depl.	Expert.	Job Role	Years	Sector	Size	CC
FIDO Expert	E1	N/A	⋆⋆⋆	Blinded	>20	FIDO All.	10-49	US
	E2	○	⋆⋆⋆	IAM	>20	Telco.	> 250	US
	E3	○	⋆⋆	IAM	5-10	Gov.	> 250	DE
	E4	●	⋆⋆⋆	Manager	1-5	Auth.	< 10	DE
	E5	●	⋆⋆⋆	IAM	1-5	Auth.	> 250	US
	E6	●	⋆⋆⋆	Manager	>20	Auth.	50-250	DE
IAM	A1	●	⋆⋆	CISO	>20	Finance	50-250	NO
	A2	●	⋆⋆⋆	Developer	5-10	Software	> 250	NL
	A3	N/A	⋆⋆	Consultant	10-20	Consulting	> 250	DE
	A4	●	⋆	CISO	>20	Consulting	10-49	DE
Organization	O1	○	⋆	CISO	5-10	Health	> 250	DE
	O2	●	⋆⋆	CISO	10-20	Telco.	> 250	US
	O3	○	⋆	CISO	1-5	Gov.	> 250	DE
	O4	●	⋆⋆	CISO	>20	NGO	50-250	US
	O5	●	⋆⋆	CISO	5-10	Gov.	> 250	DE
	O6	○	⋆	CISO	1-5	Marketing	10-49	US
	O7	●	⋆⋆	IAM	5-10	Chemistry	> 250	DE
	O8	○	⋆	Developer	1-5	Finance	> 250	US
	O9	○	⋆⋆	CISO	10-20	Tools	> 250	DE
	O10	○	⋆⋆	CISO	10-20	Electronics	> 250	AU
	O11	○	⋆	Manager	>20	Electronics	> 250	US
	O12	●	⋆⋆⋆	CISO	5-10	Fashion	> 250	DE
	O13	○	⋆	Manager	10-20	Insurance	> 250	CH
	O14	○	⋆	CISO	5-10	Health	50-250	DE
	O15	●	⋆⋆	IAM	10-20	Energy	> 250	DE
	O16	●	⋆⋆	CISO	10-20	Integration	> 250	DE
	O17	○	⋆	CISO	>20	Telco.	> 250	DE
	O18[1]	○	⋆⋆	CISO	>20	Finance	> 250	DE

Depl.: ● = deployed FIDO2, ○ = has not deployed FIDO2, N/A = not applicable.
Expert.: Participant’s FIDO expertise (based on moderator’s subjective judgment), ⋆ = knows from media, ⋆⋆ = helped deploy, ⋆⋆⋆ = involved with FIDO design.
Years: Number of years of experience within the job (self-reported).

liance to distribute our recruitment text. Furthermore, the lead researcher attended the Authenticate conference in October 2022 to recruit and connect with the community. We also reached out to organizations like the German Federal Office for Information Security (BSI), asking them to distribute our recruitment text via their mailing lists. We conducted interviews between November 2022 and April 2023.

Table 2 summarizes our participants. We conducted 28 interviews in total, encompassing 6 with “*FIDO experts*,” 4 with “*IAM*” vendors, and 18 with “*Organizations*” (companies, governments, NGOs) representing a wealth of different industries. Throughout this paper, we reference participants from these three groups with the respective prefixes “E” (for experts), “A” (for authentication vendors), and “O” (for organizations). All interviews involved a single participant except for O18, which included five individuals from different divisions of the same company; we report their collective opinions as one. Thus, 32 individuals were interviewed. We reached saturation (no longer learning new information) after 25 interviews.

Our participants were mostly CISOs or security engineers working in IAM. We also interviewed consultants and individuals in management positions related to security.We had representatives of one start-up (<10 employees), three small businesses (10-49), four medium-sized organizations (50-250), and 20 large organizations (>250). Among large organizations, eight had under 10,000 employees, six had 10,000–100,000, two had 100,000 to 200,000, and four had over 200,000. Participants’ organizations were based primarily in Germany (16) or the U.S. (8). The remaining four came from Norway, the Netherlands, Australia, and Switzerland.

3.4 Analysis

We transcribed our audio recordings, storing files locally. Two researchers then performed independent qualitative coding following a thematic inductive coding approach. We decided not to use our obstacles list for deductive coding as our main aim was to identify as many previously unknown obstacles as possible. In weekly meetings, the full research team refined the codebook and discussed recent interviews. Subsequently, we clustered codes into high-level categories following an affinity diagramming process. As the codebook and themes were developed jointly and iteratively, we decided against calculating intercoder reliability metrics.

3.5 Limitations

Like many qualitative studies, we report on a small sample of 32 individuals across 28 interviews. While the number of people overall is small, we interviewed hard-to-recruit individuals who are key decision-makers in the deployment of FIDO within their organization or in the development of FIDO standards themselves. They also conveyed knowledge they accumulated from discussions with professional colleagues. Thus, our sample size is commensurate with other qualitative studies of hard-to-reach groups. We do not claim to provide a complete overview of all FIDO2 deployment obstacles, but have likely identified those most inhibiting widespread adoption. Most of our participants work at organizations based in the U.S. or Germany; our findings may not generalize to organizations from different parts of the world.

3.6 Ethical Considerations

All data was collected by individuals at an institution that does not have an Institutional Review Board (IRB) or similar ethics review board. However, we followed key principles of the Menlo Report [90]—“respect for persons,” “beneficence,” and “justice”—in designing our protocol. While we collected no personal identifiers beyond participants’ email addresses and full names for correspondence, the ethical treatment of information shared with us about company internal details was a key focus. Protecting the confidentiality of participants’ companies and their inner workings, especially when discussing issues in their security infrastructure, was of paramount importance. Voice recordings were immediately transcribed

[1] Interview O18 included five people from the same organization.

after the interview to minimize the storage of potentially identifiable information. Transcripts were stored pseudonymously in case of unintentional information leaks. All data was stored and processed in accordance with the GDPR.

We described the study procedure carefully, including all risks, and asked participants for their consent. Participants could stop the interview at any point, which nobody did. As our participants were typically highly compensated tech experts and executives, we expected that participants gaining insight into FIDO2 would be the primary value of participating. Thus, we did not offer monetary compensation, instead offering our own FIDO expertise and feedback in follow-up meetings to participants who desired them.

4 Results: Experiences Deploying FIDO2

This section and the two that follow present our main findings from the interviews. We start by summarizing participants' experiences deploying FIDO. We distinguish between FIDO being used for two-factor authentication *(U2F)* and the more recent proposals for FIDO2-based *passwordless* authentication. As U2F is older and more widely deployed, some participants' responses referenced concrete U2F experiences (instead of passwordless). They did, however, indicate these experiences and opinions to be applicable to passwordless deployments concomitantly. Overall, 13 participants reported that their companies had already rolled out or are currently in the process of rolling out FIDO in some way, such as via Windows Hello or YubiKeys (see "Depl." in Table 2). Seven participants reported that their organization had deployed passwordless authentication, while the remaining six reported that FIDO was being used for multi-factor authentication *(U2F)*. All four IAM vendors offered passwordless authentication solutions for business customers. All organizations refrained from in-house developments and instead used an IAM vendor or the built-in functionalities of their Microsoft Azure ID instances. In contrast, thirteen organizations have not yet rolled out any FIDO solution. The remaining two participants ("N/A" in Table 2) worked in contexts (e.g., as a consultant) where FIDO deployment was not relevant. Except for one company currently in the process of preparing a passwordless rollout, none of the organizations offered FIDO-based passwordless authentication for end users. Instead, passwordless authentication was for employees.

Reasons for Deploying: The 13 participants who had deployed FIDO gave various motivations for doing so. The majority (n = 7) brought up security as the main reason for deployment. Some talked about getting rid of passwords (O6, O16) or switching to a phishing-resistant 2FA solution (O4, O5). Others focused on the ability to create unique identities in warehouse or factory settings (O10, O12). One pointed out that increasing "cloudification" made measures like location-based authentication harder to implement (O15). Three participants brought up usability concerns of passwords, including the toll of frequent password resets (O15). O6 felt passwords are cumbersome even with password managers, and E5 liked FIDO's open standardization.

Reasons Against Deploying: Participants whose organizations had not yet deployed FIDO can be categorized into the following three subgroups: "talked about, but decided against" (*reject*, n = 6), "currently talking about" (*consider*, n = 3), and "never talked about" (*unaware*, n = 4). We represent the groups by adding r (reject), c (consider), or u (unaware) to their identifiers. As arguments and concerns partially overlap between these groups, we report their results collectively.

No Need. Most commonly, participants were uncertain whether they would need FIDO. Some said they already felt sufficiently secure (O1_r, O3_u, O11_u, O17_c, O18_r). According to O18_r, "*attack vectors that FIDO would protect against are rarely seen in real life*" and are already handled by measures like risk-based authentication (*RBA*). Others argued that there is no demand for FIDO from customers (O1_r, O18_r) or employees who use trusted intranet services (E3_r).

Costs. Unsurprisingly, many participants brought up deployment costs (O11_u, O14_c, O17_c, O18_r). O11_u said that for them to even consider FIDO, they could not have any increased expenses. The cost of security keys also came up. Even some participants who had already deployed FIDO felt that cost was one of the main obstacles.

Change Too Big. Some argued deploying FIDO would require too much refactoring in their IT infrastructure (O3_u, O11_u). Others focused on the consumer side, claiming that end users would be unhappy or overwhelmed with such a change (O8_r, O14_r). O8_r argued that their company had to "*be very conservative with the technology [they] employ*" as their customers are very non-technical.

Non-Universality. Three participants felt FIDO would be less universal than their current methods. For example, O17_c's current smartcard-based authentication covers other use cases like printing and access to buildings that no currently available FIDO-based solution offers. A3 and O9_u pointed out regulatory differences across countries that make it particularly complicated to deploy FIDO in international corporations.

Additional concerns included past negative experiences with alternative (biometric-based) solutions (O9_u, O13_u) and struggling to convince executives of FIDO's value (O11_r).

4.1 Experience with Deployments

Participants whose organizations had already deployed FIDO reported relatively positive experiences overall. O12 and O15 reported surprisingly positive feedback from their workforce: "*our satisfaction ratings increased to the ones we last had 10 years ago*" (O12). O7 reported that their rollout initially had a relatively low acceptance and adoption rate. After a few weeks of acclimatization, their workforce became more satisfied with the new mechanism. While O2 was satisfied overall with their deployment, they reported that a certain cohort of people was "*just not using it*" and could not be convinced until the company made security keys mandatory.

O4 reported a relatively unsatisfying deployment experience. Uptake did not exceed 65% even after a year. The adoption of biometric-based methods was even lower, stagnating at 15-20%. They attributed their experience to various factors, including mistrust towards the (government-affiliated) employer and technical issues that caused some employees to be locked out of accounts during the initial rollout. Participants also reported both temporary obstacles and persistent issues during and after their deployments. For example, O12 reported that onboarding security keys in Microsoft Azure self-service accounts was relatively complex, requiring a lot of assistance from their IT department. Three participants reported technical issues that required fixes from providers (in their case Microsoft and Apple). A4 felt changing the Active Directory structure was their biggest obstacle during deployment. Furthermore, O7 and O10 emphasized their struggles in convincing management, while O15 and O16 pointed out struggles incorporating legacy software into FIDO-based flows. A1, working in finance, brought up legal issues they encountered after the release of passkeys, causing their deployment to be put on hold entirely. As O2 pointed out, especially in global organizations, physically distributing security keys can become very challenging.

4.2 Consumer-Facing Authentication

Most participants' organizations did not have immediate plans to roll out FIDO for consumer-facing authentication. Only A1 (already in the process of deploying consumer-facing FIDO2), O13, and O15 expressed interest in doing so soon.

As a company, the number of customers is critical. O15 argued that it is good to offer many authentication options to accommodate as many customers' desires as possible. However, three other participants argued that introducing anything that may exclude potential customers (e.g., those whose phones lack FIDO2 support) would be harmful to the business (A3, O14, O15). According to O14, in sectors like health services, it is reasonable to prioritize availability over security and usability. Thus, for these businesses, mandatory FIDO deployment is out of the question. Surprisingly, three participants expressed that the security of individual accounts (which consumer-facing FIDO would protect) is of little value and not a priority (A3, O15, O18). According to O18, account security is the customer's responsibility: "*Everybody knows they should not write down or share [passwords]. They act against better knowledge by contravening it.*" Thus, unless accounts can be compromised at scale, there is little incentive for those companies to protect individual user accounts. As many app-centered services use long-lived access tokens and already offer biometric-based local authentication, O14 found FIDO2's usability advantages unconvincing. O13 and O14 mentioned that supporting security keys would be unnecessary as their user bases are small.

5 Results: Perceptions of FIDO

All participants agreed that the FIDO ecosystem has passed its inflection point and is here to stay. For example, E4 said, "*FIDO is the technology with the [greatest] potential to replace passwords.*" Nevertheless, others felt adoption was much slower than expected and that, even with passkeys, some key issues remain unsolved or are entirely "unsolvable."

Awareness: The vast majority of participants had at least some level of awareness of the FIDO standards prior to the interview. While this can be attributed in part to our recruitment process, about half of the participants were recruited from outside "the FIDO community." Participants from IAM providers and consulting firms consistently reported similar impressions from their work with business customers (A3, E6, O10, O16). E5 said, "*Awareness is there; people want to implement it!*"

Some participants (e.g., O2) reported that the mindset of passwords being "good enough" is not an obstacle in their organization. A2 pointed out that enterprises especially are considering FIDO2 rollouts, but not yet committing. In contrast, others felt that the FIDO standard remains unfamiliar, particularly among people in IT management; at best, they may recognize it as "*logging in with biometrics*" (A3). From the IAM vendors' perspective, E4 noted that business customers usually do not come asking for FIDO, but instead are happy if it is included by default in the package offered to them. O9 similarly said that, despite awareness of FIDO, deploying it is not really a priority for many companies.

While most participants were familiar with FIDO, the nuance between FIDO as an additional authentication factor (U2F) and single-factor, passwordless FIDO2 was frequently lost. When talking about "FIDO," most non-expert interviewees primarily discussed FIDO as a means of 2FA, not a means of replacing passwords entirely.

Misconceptions: Adding to findings about wrong mental models [4], our participants also expressed a variety of misconceptions related to the complexity of the FIDO ecosystem [4, 6]. Many non-experts appeared to have a mental model of FIDO focusing on roaming authenticators; three explicitly expressed this misconception. Such a misconception is particularly undesirable with regards to consumer-facing authentication as participants worried they would burden customers with purchasing extra devices if they deployed FIDO.

O8 expected that FIDO2 required the user to install an extra app, which then securely stores the private key. Similarly, O3 thought passkeys would only work with a central trusted entity similar to a public key infrastructure (PKI). O5 was not aware that roaming authenticators can require "user verification" (e.g., entering a PIN) and incorrectly feared that unfettered access to accounts would always be possible if someone got hold of the security key. O18 also reported the mistaken belief that security keys could just be erased and used for storage like a USB flash drive and that one could simply order untrustworthy security keys online, creating security threats. These assertions suggested an unawareness of the FIDO Alliance's authenticator certification program [37].

Passkeys: As passkeys were a recent development when we conducted the interviews (November 2022 through April 2023), there was lower awareness than for FIDO2 overall. Note that, especially in early interviews, we did not use the explicit term "passkeys" with every participant. While some participants had spent time learning about passkeys, others requested that we explain the concept during the interviews. Opinions about passkeys were split, with 10 participants fully in favor and 8 expressing criticism. The remainder indicated no clear positive or negative attitude.

Apart from high-level judgments like "*it's a fantastic step forward*" (O6, O12), some participants felt that passkeys are what will give FIDO2 the momentum to replace passwords in the long run (E4, O4). Several explicitly said passkeys solve what they felt was FIDO's biggest issue, account recovery (A2, E1, E4, E5, O4). Despite generally being in favor, O15 hoped that passkeys would continue to follow FIDO's standards-based approach to ensure that "*Apple doesn't turn right while Google turns left.*" In contrast, A1 was skeptical about passkeys' ability to replace passwords, expecting they would be useful only for "low-value accounts."

Some participants arguing against passkeys were passionate in their criticism. They considered the hardware binding of keys to be FIDO's very heart, and they felt passkeys lacked this binding (A1, O7). For example, A1 said that "*passkeys is essentially a really good password manager.*" A4 and O17 were similarly concerned about synchronization to the cloud. E6, who is involved in standards developments in the FIDO Alliance, admitted that passkeys were not the first choice from a security standpoint, yet were the only solution that could adequately address the issue of transferability. They felt that transferability constituted FIDO2's most fundamental drawback at the time of passkeys' development.

Some participants did not trust Apple and Google's ability to securely store the private keys. O13 disagreed with this concern, pointing out that when currently using *Apple's iCloud Keychain* or *Google Chrome's built-in password manager*, users already trust these services to store login credentials. In that case, however, users are currently given the choice of whether to use password managers and their cloud-based synchronization functions. In the case of passkeys, they must trust the service. Thus, as A2 pointed out, passkeys may exclude users concerned about privacy as they would not trust Apple or Google. E1 and E6 both raised concerns about the usability of passkeys in a cross-ecosystem context. While there is a QR code-based solution for transferring passkeys (e.g., from an Apple iPhone to a Microsoft Windows PC), this process may be confusing and error-prone for users. More generally, A1 and E5 argued that unless the ecosystems (Apple, Google, and Microsoft) themselves are completely passwordless, one cannot really claim a security enhancement as security overall boils down to the security of the passwords used to protect those cloud-based accounts.

6 Results: Deployment Obstacles

Next, we report on the deployment obstacles participants expressed during the interviews. The full codebook can be found in Table 4 in Appendix C. Obstacles only relevant to company-internal deployments are marked with "***(W)***." Consumer-deployment obstacles are marked with "***(C)***." Unmarked sections apply to both. In this section, we refrain from subjective judgment, revisiting the matter in Section 7.

6.1 Regulation and Requirements

Regulatory requirements—both in terms of national laws and companies' internal policies—were the obstacle to FIDO2 deployment discussed most frequently in our study. Participants reported various concerns that FIDO would collide with their internal compliance and existing regulatory frameworks.

Non-Compliant Policies (W). O1, O3, and O8 pointed out policies requiring them to practice "digital sovereignty," or not to rely on a single vendor for their IT infrastructure. For a FIDO deployment, this not only runs up the bill, but also requires in-house expertise to ensure interoperability, making it hard to commit to drastic changes in authentication infrastructure. For example, O1 noted that if passwordless FIDO were deployed, regulations like password-composition requirements would need to be suspended. O9 mentioned that some security policies demand two completely separate factors for authentication. Others shared that occupational safety regulations hinder the applicability of using biometrics.

eIDAS (C). Participants working in finance shared that a severe obstacle from a federal regulatory perspective originated with Apple's decision to synchronize all passkeys automatically, leaving no option for device-bound credentials [51]. According to the European "Electronic Identification, Authentication, and Trust Services" (eIDAS) regulation, an individual's identity must be bound to a specific hardware device. Thus, credentials stored on a hardware device cannot be easily transferred or replicated.[2] This issue is particularly relevant for all organizations involved in the payment industry. E4 said that "*no serious bank will use [FIDO].*" A1's organization had prepared a consumer-facing rollout of passwordless

[2] See Annex 2.2.1 of the regulation EU 2015/1502 [25].

FIDO authentication for their app in September 2022. Upon Apple's release of their passkey implementation, these developments had to be stopped entirely. They now implement hardware binding in-house, independent of FIDO, considering this to be their only compliant option for passwordless authentication. A1 was particularly frustrated, saying, "*Apple has taken a big dump on FIDO!*" FIDO experts reported being aware of these issues and are currently talking to European regulators (E1, E6). They felt the main challenge would be convincing legislators that passkeys are sufficiently secure.

PSD2 (C). While the FIDO Alliance claims [35] to comply with PSD2,[3] banks struggle with its requirements. While the FIDO standards cover the requirement of *Dynamic Linking*[4] in the form of transaction confirmation displays [22], it is not enforced that all available FIDO-compliant authenticators implement the necessary functionalities. O18 explained that since they have no influence on how security key vendors implement transaction-confirmation displays, O18's organization cannot offer FIDO in a PSD2-compliant manner.

Further Legislation (W). A3 pointed out that in U.S. states like California [44], employers must indemnify expenditures incurred in direct consequence of their employees' duties (e.g., reimbursing cellular plans when prompting employees to use private phones at work). As this requires processing reimbursements, A3 suggested it may deter companies from using biometric FIDO authentication in workplaces.

6.2 Usability Challenges

Complexity and Friction. Nine interviews highlighted the challenges of explaining FIDO to users and non-technical stakeholders, such as management. Participants reported comparing security keys to physical keys as an analogue for non-technical individuals. However, as security keys may be protected by a PIN, sharing them with others does not automatically enable access. Explaining this difference to non-technical people was challenging (E2). As passwordless FIDO authentication requires both possession of the device storing the private key and knowledge of the PIN, some might consider it 2FA, causing confusion (E6). E4 expressed difficulties conveying recommendations for everyone to possess multiple security keys in case of loss or destruction. E6 pointed out the challenge of differentiating proprietary (server-side) biometric authentication solutions from FIDO **(W)**. A3 and O12 reported the onboarding process for security keys to be convoluted, with employees having trouble navigating menus to enroll their key **(W)**. Expert participants who developed FIDO reported difficulty explaining key concepts to UX designers, leading to poorly designed user interfaces (E6, O7).

Consumer aspects played only a minor role. Some participants expressed fears that FIDO2 is not necessarily easy to understand. E6 explained that, in practice, user experience is one of the concerns companies considering consumer-facing, passwordless FIDO2 most frequently raise **(C)**. E1 and O13 emphasized that operating systems and browsers' different approaches displaying FIDO interface elements make it hard for users to recognize it as the same login mechanism across devices **(C)**. E1 extended this criticism to online services putting minimal effort into clear interface design and ignoring the FIDO Alliance's UX guidelines [38]. O18 pointed out that users might mistakenly believe they are more secure with passwords as they are more aware of the risks.

Recovery and Fallback. Opinions were mixed on the degree to which the lack of standardized recovery remains an obstacle. A2, E1, and E5 felt that passkeys fully allay concerns about account recovery. In contrast, A1 and E4 stated that passkeys depend on an individual platform, almost in a "proprietary manner" (despite the technology itself being open), meaning that recovery has not been solved. Several participants reported that questions around fallback authentication are still among the most common concerns when talking to prospective customers. E1, E5, and O6 argued that the options for setting up fallback mechanisms for security keys remain convoluted, while E3 thought that setting up a second security key is a trivial and effective solution. This is also the strategy the FIDO Alliance recommends [42]. E5, however, disagreed: "*That's not really a great user experience, it's a practical solution... In an enterprise [or for] high-value transaction cases that level of inconvenience might be okay. But for the broad consumer, not at all.*"

6.3 Technical Challenges

Overall, participants felt the technical aspects of FIDO appear to be mostly sorted. A2 even pointed out that there is a Conformance Test Tool available for FIDO2 [29]. Supporting both FIDO and passwords alongside each other was only considered a small issue. The biggest concern among participants was that libraries and standards are not easily understandable.

Complex for Developers. As addressed by prior work [4], in contrast to passwords, FIDO protocols are complex and not meant to be implemented by non-specialist developers. Participants familiar with implementing FIDO2 agreed that it is difficult to implement and mentioned a lack of documentation. In fact, E6 recommended that companies should not attempt to implement FIDO in-house as the complexity poses the potential for insecure implementations and misconfigurations. E5, who implemented FIDO for a well-known IAM vendor, shared this view, saying that in the API there are numerous "*options that are not obvious and combinations that don't make sense or offer the protection you think.*" E4 claimed that implementing FIDO increases the "*complexity of the authentication stack by a factor of 10.*" Nonetheless,

[3] The "Payment Services Directive 2" (PSD2) regulates payment services in the European Economic Area. It introduced regulations on strong customer authentication (e.g., via mandatory 2FA) and enforces secure open standards.

[4] *Dynamic Linking* demands that "the payer is made aware of the amount of the payment transaction and of the payee" [26].

E6 does not consider this complexity a major hurdle because they think vendors already offer sufficient solutions.

Specific Technical Issues. Not all browsers, especially in the mobile domain, are yet fully supported. In the past, certain built-in browsers (e.g., Samsung Internet Browser) lacked FIDO support. At the time of conducting the interviews, FIDO2 worked on 95% of mobile browsers [24], with Mozilla Firefox being a prominent exception as it only partially supported FIDO2 (Touch ID and PIN entry were not supported on certain operating systems). Similarly, for passkeys, browser support was very limited [17]. On certain OS and browser configurations, device-bound FIDO credentials and autofill UI were not supported. Participants argued that this impedes the universality, especially keeping consumers in mind **(C)**. O4 pointed out that if a company primarily uses Microsoft, it is not trivial to also handle authentication from Google or Apple devices uniformly. Additionally, O12 mentioned that Windows Hello for Business is limited to ten local identities, which makes it unsuitable for settings like reception workstations where more than ten people share a device **(W)** [62].

Legacy Software (W). While issues with legacy software are well-known in the security community, they play a particularly crucial role in FIDO2 adoption. Eight participants specifically mentioned such issues. As mentioned above, FIDO is rarely implemented in-house. Existing FIDO2 solutions offered by IAM vendors are usually closely integrated with cloud-based services like Azure Active Directory. However, such cloud-based solutions are usually not supported by old applications like process controllers for industrial machines or warehouse software. Some participants viewed this as a justification for not implementing FIDO2 at all to avoid a heterogeneous authentication infrastructure (O12, O18). Others felt that tooling to circumvent such challenges should be made available by IAM vendors, which is not yet the case (O2).

End-of-Life Systems. From a consumer perspective, participants pointed out that supporting old operating systems and browsers is crucial (O1, E5, A2). Web services have to be mindful that many organizations still run on Windows versions that do not support passkeys or other FIDO protocols. A2 voiced that you cannot tell consumers that they can "*only access the website using a specific OS version.*" This argument becomes particularly evident with services that target non-tech-savvy demographics or must be available for the entire population (e.g., digital government services) **(C)**.

6.4 Lack of Universality

One strength of passwords is their near-universal applicability, independent of the devices and environments where they are used. FIDO2 cannot live up to this universality.

Production Environments (W). In environments such as production sites, biometric authentication is often not well-suited as workers wear gloves, masks, or have dirty hands, preventing reliable usage of biometric sensors (A3, O9, O11).

Buried Entry (W). O6, a small-business CISO, highlighted that certain software licensing systems restrict access to important security features, like SSO integration with Microsoft Azure, to larger teams. This practice of hiding security functionalities behind paywalls disadvantages smaller businesses.

Exclusion of User Groups (C). From an ethical perspective, A1 and E2 pointed out that FIDO excludes users who do not have the financial means of purchasing mobile phones or security keys, or even just users who struggle with technology. This is particularly critical for services like bank accounts. If a service is entirely passwordless, in the worst case some user groups would be completely excluded. A3 supported this argument when pointing out that, in lower-income countries, people often have older phones that do not support FIDO protocols or share devices with family members [3, 81]. From an accessibility standpoint, A3 and O1 argued that sharing passwords is often the only means of interacting with web services for some people (e.g., the elderly).

Biometrics (W). Contrary to our expectations [55], concerns about where the biometric data is stored with FIDO2 were not universal and were only raised by European workers' councils in France and Germany (O7, O10). Some participants who had negative experiences with proprietary biometric-based solutions raised concerns about biometric FIDO2, projecting their prior negative experiences (O6, O11). O18 raised concerns about the limited value of FIDO for mobile apps that already offer local biometric authentication **(C)**.

6.5 Organizational Challenges

Manageability and Logistics. While measures for centralized management of username/password credentials have long been available and standardized, the management possibilities for FIDO credentials are still in their infancy.

On- and Off-boarding (W). O12 considered it problematic that the FIDO onboarding process is unnecessarily complex due to its device-centric nature. They criticized that FIDO credentials cannot be managed centrally by IT departments for non-technical employees who struggle to register credentials. A3 and O2 referenced similar experiences. Some participants did not like that security keys would need to be recalled when a customer closes an account (O18) or an employee leaves a company (E11). While employee accounts can be closed centrally regardless of whether they use security keys or passwords, an organization might still want to physically retrieve security keys for asset management and cost control (A3, O1).

Credential Sharing (W). Scenarios like showcasing, exhibitions, or temporary accounts can only be effectively handled with shareable credentials (A1, O1). Despite the security challenges, these cases form a substantial portion of the workflow for businesses like small companies and start-ups.

Passkey Management (C). E5 pointed out an issue that might emerge once passkeys are common. As the number of accounts users have is huge, the number of passkeys a user

Table 3: This table shows how the 18 interviewees who completed the card-sorting task rated potential obstacles.

	Customers happy	Pwd good	Pwd managers	2FA secure enough	SSO usable enough	No std fallback	Stolen unclear	New dev unclear	Multiple unclear	Wouldn't use bio	Roaming auth	Friction	Used to pwd	Libs don't exist	Libs incomplete	Libs not understand	Libs wrong language	Issue support both	Can't get rid entirely	Browser support	Unified experience	No need	Won't allow	Don't understand	No open-source	Bio forbidden	Peer organizations	Why invest	Impl. costs	New comm costs	Incompatible w/ UX	Can't brand	Can't communicate	Color, icons hard
	N1	N2	N3	N4	N5	U1	U2	U3	U4	U5	U6	U7	U8	D1	D2	D3	D4	D5	D6	D7	D8	M1	M2	M3	M4	M5	M6	F1	F2	F3	C1	C2	C3	C4
ID	Necessity					Usability								Deployability								IT Management						Financial			Comm.			
*E*1	○	●	●	○	●	○	○	○	○	●	○	○	○	○	○	●	○	·	○	·	○	●	●	●	○	●	○	○	○	○	●	·	○	○
*E*2	·	·	·	○	○	○	○	·	·	·	○	●	○	·	○	·	○	·	○	○	○	·	·	●	·	·	·	·	·	·	·	·	○	·
*E*4	○	○	○	○	○	●	○	○	○	·	○	○	○	·	·	●	·	●	●	●	○	○	○	○	·	○	○	○	○	●	·	·	●	·
*E*5	·	·	·	○	○	●	●	●	○	○	●	●	·	●	●	●	○	○	●	●	●	●	-	-	●	○	●	○	○	·	·	·	○	·
*A*1	●	·	·	○	·	○	○	○	·	○	·	○	·	○	·	·	·	○	○	●	○	·	·	·	·	·	·	·	○	○	·	·	○	·
*A*2	●	●	·	·	●	·	○	○	·	○	·	○	○	·	·	○	○	·	○	○	·	●	●	●	○	●	●	●	●	○	○	○	·	○
*A*3	○	·	·	○	○	●	·	○	○	·	○	·	·	·	○	○	●	○	○	○	●	○	○	○	●	·	●	●	○	○	●	●	·	·
*A*4	-	·	○	●	-	●	○	●	●	●	○	●	●	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	·	·	·	·
*O*1	○	·	·	●	●	○	·	·	·	○	·	○	○	○	○	·	-	○	○	●	·	○	·	·	·	○	○	○	·	·	·	·	○	·
*O*3	○	●	·	●	○	○	●	●	○	·	-	●	●	-	-	-	-	-	-	○	-	●	●	●	○	○	●	○	○	○	○	·	○	○
*O*4	·	●	○	·	·	○	●	●	○	●	·	○	○	-	-	-	-	·	○	·	○	○	·	·	·	·	·	○	·	·	·	·	○	○
*O*5	·	·	·	●	○	○	·	·	·	·	·	·	·	○	○	○	·	·	·	·	·	·	·	○	·	·	·	·	·	·	·	·	●	·
*O*6	○	●	○	●	●	○	○	·	○	●	●	○	○	·	·	○	·	○	●	○	●	·	○	○	·	·	○	●	○	●	·	·	○	·
*O*8	·	·	○	·	·	·	●	○	●	·	·	●	●	·	·	·	·	○	○	-	·	●	·	-	·	-	·	○	-	·	·	·	○	○
*O*10	·	·	·	○	·	○	·	○	○	○	·	○	○	○	○	○	○	○	●	○	○	·	·	○	·	·	·	·	○	○	·	○	·	○
*O*13	·	·	·	·	·	○	·	·	○	·	·	○	·	·	·	·	·	·	·	○	·	·	·	·	·	·	·	○	·	○	·	·	○	·
*O*16	·	·	·	·	·	·	·	·	·	○	·	○	○	○	-	-	-	-	-	·	·	·	·	·	·	·	·	·	○	○	·	·	·	·
*O*17	·	·	·	·	·	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○	○	○	·	·	·	·	·	○	○	·	·	·	·	·
Priority	.59	.61	.39	.94	.82	1.06	.88	.88	.76	.82	.56	1.18	.88	.67	.71	.93	.69	.73	1.20	1.06	.88	.89	.59	.88	.44	.53	.61	.89	.76	.72	.33	.22	.78	.33

Major Obstacle = ●, **Minor Obstacle =** ○, **Not an Obstacle =** ·, **Skipped =** -, **Priority** = Mean rating.

must manage will be, too. This raises the challenge of user-friendly management and revocation of FIDO credentials.

Stakeholders with Power. FIDO at its core is built as an open standard and has always valued its cooperative decision-making processes. Nevertheless, a number of participants pointed out that a few powerful stakeholders are most influential in the FIDO realm. This makes it substantially different from passwords, which cannot be influenced by a corporation.

Solo Efforts. This hurdle has become particularly evident when passkeys were first released by Apple despite them being a joint endeavor of many FIDO affiliates (E4, E5). E5 fears that the companies, being as big as they are, have the power to block the development of FIDO if it does not fit their company-internal agenda. E5 explained, "*If Google has objections, and they do not implement [a feature] in Chrome, it'll never gain adoption*." As one example of this, device-bound FIDO credentials are not supported by Apple. One can see from that example that FIDO's success is partially dependent on the cooperation of all stakeholders.

Conflict of Interest. Other participants speculated about potential reasons for FIDO2's slow adoption. For some companies involved, a conflict of interest may have emerged since the focus of FIDO shifted from roaming authenticators to platform authenticators. Security key vendors like Yubico have an interest in maintaining their market (E6, O11, O12).

6.6 Prioritization of Obstacles

With our card-sorting task, we aimed to learn more about participants' views of the relative severity of obstacles to FIDO deployment. As Table 3 shows, there was no particular consensus obstacle. FIDO and IAM experts overall were more concerned than representatives from organizations. In Table 3, we calculate participants' mean severity per obstacle, artificially weighing "major" as 2, "minor" as 1, and "no obstacle" as 0 to indicate and reflect trends.

Necessity. Overall, participants confirmed that FIDO is "necessary." They agreed that customers overall are not satisfied (N1), that passwords should be replaced (N2), and that password managers do not sufficiently solve the problem (N3). A more salient obstacle is that existing 2FA solutions are already considered to be secure enough by about half of the organizations (N4). The same applies to single sign-on (SSO), which is considered to be usable enough (N4).

Usability. The most pressing usability obstacle is the lack of a standardized fallback procedure (U1), one of the three biggest obstacles identified overall. Device theft and handling multiple (or new) devices (U2-U4) was rated at least a minor obstacle by most. Some, however, considered these issues to be solved with passkeys. Participants overall did not think that roaming authenticators should be considered unusable (U6). Change causing friction and users being habituated to passwords were considered bigger obstacles; the complexity of change (U7-U8) may outweigh FIDO's advantages.

Deployability. Most participants considered deployability (D1-D4) not to be an issue. The most pressing concern among experts was that libraries are not easily understandable (D3). The lack of full support by mobile browsers (D7) was considered a major obstacle by experts and also raised as a minor concern by representatives of organizations.

IT Management. Three participants rated all management-specific hurdles as major (M1-M3). However, they generally expressed how management can severely impede deployments while emphasizing this not being the case for FIDO in reality. All others rated these issues to be minor at worst. Open-source software (M4) or biometrics being not allowed (M5) do not appear to be obstacles. Some participants in larger companies reported waiting for peer organizations. However, participants also pointed out that being innovative can be an asset and thus not necessarily a hurdle to FIDO (M6). Generally, FIDO and IAM experts rated these aspects much worse than organizations. As organizations have better insights here, this indicates that management is likely not a blocker in reality.

Financial. Most participants rated all financial concerns (F1-F3) as at least minor obstacles. To them, it all boils down to a cost-benefit analysis. Thus, it appears that FIDO's value proposition is not yet entirely clear or it does not solve concerns that are urgent and worth investing in.

Communication. Figuring out how to properly communicate FIDO to the user (C3) was a minor obstacle for most. The other categories (C1, C2, C4) were not considered obstacles.

In summary, the worst-rated obstacles were increased friction for users (U7), the lack of universal support in mobile browsers (D7), and the lack of a standardized fallback (U1).

6.7 Distinguishing Stakeholders Views

Experts and IAM vendors sometimes judge the severity of obstacles differently than organizations. Only experts and IAM vendors raised concerns regarding FIDO being hard to explain and understand. Practitioners might be more oblivious to the challenging task of communicating FIDO's functionality. It could also indicate that in practice the technical functionalities are actually easier to convey than experts think. Shortcomings in support and issues with legacy software were raised by seven organizational representatives, but only one FIDO expert. This might hint at how experts sometimes disregard concerns surrounding this topic as insignificant and easy to fix. However, these pieces of software often comprise a major part of the core business infrastructure. Similarly, only organizations addressed the lack of universal applicability for "non-desk" staff (e.g., in healthcare). Only experts and IAM vendors discussed ethical concerns with FIDO surrounding universal accessibility independent of socioeconomic status and abilities. The experts may take a more idealistic viewpoint on the "purpose" of authentication, whereas organizations apply a pure "business lens."

7 Discussion

Next, we discuss our thoughts on the future of passwordless authentication, give recommendations for industry, and outline important avenues for future research.

7.1 A Passwordless Future

Will We Get Rid of Passwords? According to our findings, not in the near future. However, there is agreement that FIDO2 will play a major role in making the password obsolete in many cases. E5 said that the term "passwordless" should not be understood as eliminating passwords, but rather as having "less passwords [sic]." With legacy software that is often commissioned for over 30 years and written in languages few still understand today, it is unlikely that FIDO will be implemented in such cases (O10). Even once FIDO is deployed, it is still a long way before its security benefits can flourish [89]. FIDO-protected accounts only fully benefit from being more secure if they are used without a password. However, especially for the consumer case, the password will most likely remain the primary fallback. So far, only Microsoft offers "password-free accounts" [91], allowing users to delete the password after enrollment into their authenticator app. This was also mentioned by interviewees who criticize Apple's and Google's passkey implementation, arguing that they themselves must be passwordless before passkeys can offer their full security advantage. While this is technically true, it should not be used as an argument against FIDO as these major services are known for paying very close attention to account protection (e.g., Apple enforces 2FA for all accounts attempting to use passkeys [7]). FIDO also offers a variety of usability advantages over passwords. The same cannot necessarily be said about all other services on the web.

FIDO as a Convenience Feature. FIDO, often perceived primarily as a security technology, should also be recognized for its convenience. When pitching FIDO, it is crucial to emphasize the convenience it brings (E4). In fact, according to some, overall usability will likely be a stronger motivating factor for adoption than security alone (O1). To broaden its appeal, the security community should adopt a narrative that highlights how FIDO makes logins easier and faster, in turn increasing customer/employee satisfaction. Shifting the focus to the seamless user experience could help persuade those who are currently hesitant due to misconceptions, such as believing that current 2FA systems are "secure enough."

7.2 Top 5 Obstacles

No Standardized Fallback. Confirming Bicakci et al. [10], one of the biggest obstacles we observed was the lack of a standardized fallback. While the FIDO Alliance gives recommendations for handling fallback in different scenarios (e.g., having two security keys) [42], these can neither be considered universally applicable nor are they usable and secure. Some fallback procedures described by our participants involved having a one-time code sent to a predefined colleague who would then share the code in a personal conversation or over the phone. Apart from availability issues (person receiving the code not being available), such measures can involve fear and shame of admitting the loss to superiors [78] and be susceptible to social engineering attacks.

Complexity and Friction. Introducing any new technology will temporarily lead to confusion, resistance, and friction for users and stakeholders. At all times during deployments, it is important to inform, educate, and communicate with all parties involved. To convince management, a clear communication plan emphasizing FIDO's usability, user experience, and security benefits is crucial. It is vital not to disregard these stakeholders. A successful and secure deployment will partially depend on factors that are independent of FIDO's theoretical security. Highlighting success stories or case studies from other organizations could help. FIDO will most likely not integrate seamlessly with existing systems. Thorough testing and engaging with all IT teams are thus indispensable for proper integration with existing infrastructure (A4). Our results echo previously raised concerns about FIDO documentation being confusing [4]. Developers should be assisted with training sessions, clear explanations, and good documentation [17, 43, 75, 100] to help them understand how FIDO and especially its security work (E5). If the user interface or onboarding process for FIDO are poorly designed or difficult to navigate, it will create frustration and resistance. To ensure intuitive and user-friendly interfaces that foster adoption, educated UX designers need to be involved from the early stages of the deployment process. Usability testing with different user groups, not only technical staff, is key (O4).

Technical Issues. While prior work identified a lack of deployment-ready solutions [4], this was of little concern in our sample. However, participants described various examples of technical problems, with incompatible legacy systems and incompatible browser and OS configurations being most common, confirming findings from Nawrath concerning a lack of platform support [64]. As end-of-life systems are a reality in industry and frequently encountered when it comes to consumers, the FIDO Alliance must develop guidelines and propose alternative solutions for such systems. Similarly, the current situation surrounding the support of device-bound credentials or Mozilla Firefox's lack of support for user verification are harmful to a smooth user experience. Note that Mozilla added support with Firefox 114 in June 2023 and announced it will support passkeys with Firefox 120 in November 2023 [67].

Regulatory Requirements. Another frequently named obstacle was regulatory requirements like the payment directive PSD2 and European eIDAS regulation. Members of the FIDO Alliance explained working on convincing legislators that passkeys are compliant with the regulations. Other entities like the U.S. National Institute of Standards and Technology (NIST) are actively asking whether passkeys and FIDO2 are sufficiently addressed in their newest revision of the digital identity guidelines SP 800-63-4 (Draft) [85]. Participants also reported various concerns that FIDO conflicts with internal rules and existing policies and will ultimately require new policies and best practices.

Security Culture. Even 24 years after a canonical paper exhorted that "users are not the enemy" [1], we found that this mindset still has not entirely vanished. Some interviewees felt that security should be pushed on the workforce if the "experts" think a specific security measure is relevant [82]. For example, one company was unsure how to define a policy for handling the security key and whether it could be left in the computer or if it should be securely stored in a locker. Deciding on the latter, they found that most people disregarded the policy as ignoring it allowed for more flexibility.

When talking about reasons for and against deploying consumer-facing FIDO, participants elicited a mindset that taking care of account security is the responsibility of the customer. For FIDO deployments, this mindset may become an issue as those companies likely have little to no intent for changing the authentication landscape for their customers. The compromise of single accounts often causes companies little harm. At worst, they need to reimburse the owner. They follow the idea that telling customers how to behave "correctly" is sufficient and that it is governments' task to properly educate citizens about digital safeguards.

7.3 Recommendations for Industry

Prepare Smooth Deployment. To ensure a smooth deployment process, O10 emphasized the importance of adapting security policies right from the beginning. This is also recommended in the "enterprise journey" resources of the FIDO Alliance [32]. To handle the distribution of security keys in international corporations, O2 recommended using a security key distribution service like YubiEnterprise Delivery [101]. O4, who had a relatively unsuccessful deployment, self-reflected saying that others should not be "the typical tech guy." O4 reported only having piloted FIDO deployment with peers from the tech department. However, as their experience and opinions are not representative of the entire workforce, they should not be used as a reference.

Increase Acceptance in Workforce. To decrease the friction originating from change, O4 recommended onboarding training in very small groups and making rollouts on a per-department level as each will likely bring up their own requirements and issues. To foster confidence in FIDO's trustworthiness, O5 recommended communicating transparently that the workplace does not have access to the key even if it is used for private accounts. O12 pointed out their positive experience with their CISO advertising the new authentication options occasionally to familiarize the workforce. Several participants from all participant groups recommended using an IAM provider or using the methods the operating system already supports to obviate the issues caused by the complexity of implementing FIDO in-house.

Little Care for User Experience. Many participants from organizations perceived any topics related to user experience as unimportant. Experts and IAM vendors seemed to be more aware of the topic. Early adopters reported negative experiences about never reaching high adoption rates due to technical and UX issues during rollouts, stressing the importance of a good user experience. When it comes to consumer-facing FIDO2, it is particularly concerning that certain settings are wildly inconsistent. Every browser and OS has its own way of doing and naming procedures. On websites where passwordless sign-in is possible, the process gets even more confusing.

Implement a Secure Fallback. It must be acknowledged that FIDO is only more secure than passwords if any existing passwords are disabled. If passwords continue to be used as an alternative or fallback option, FIDO's security guarantees can be easily bypassed via downgrade attacks [89]. The FIDO Alliance gives recommendations for handling fallback in different scenarios [42]. Many consumer-facing websites continue to rely on their already existing fallback infrastructure (e.g., out-of-bad communication via email or SMS). However, this level of security is often insufficient in high-risk scenarios like online banking (e.g., no real-time phishing resistance). Kunke et al. [54] evaluated 12 different account recovery options for their use in the FIDO2 passwordless authentication context (before passkeys had been announced). They suggested either registering multiple authenticators during account setup (as suggested by the FIDO Alliance) or relying on help desk personal verifying the user (e.g., via an identity card).

7.4 Future Research Directions

Passkey Management and Revocation. Another issue raised was the question of what happens once passkeys are more commonly in use for a variety of accounts. The problem of password reuse [66] originated due to the ever-increasing number of accounts everyone holds. This means that users at some point will hold a large number of passkeys. This issue is even aggravated as with passkeys people will hold multiple for every account when they register with more than one ecosystem. As of now, it is unclear how to properly handle those passkeys, especially in cases such as revocation. Notably, commercial and open-source password managers are already in the process of deploying functionalities to manage passkeys [93]. However, the vast majority of the population does not use password managers except for those built into browsers [72, 102]. This issue should be addressed before passkeys find more widespread adoption. As of October 2023, vendors have started working on a cross-ecosystem future (e.g., Chrome accessing passkeys stored in iCloud Keychain) and integrating passkey managers into their products [61].

Assisting Migration. Online services have become ubiquitous. Thus, in most situations, users will not be creating new passwordless accounts, but instead be migrating existing accounts to FIDO-based authentication. To facilitate this, companies have started to deploy small notifications that advertise the usability and security advantages of FIDO2 and address misconceptions [55]. Once passkeys are offered by more services, convincing users to migrate away from passwords will become an important aspect. Studying users' migration concerns and issues will help to drive the adoption of a usable and secure passwordless future for everyone.

Acknowledgments

We thank the FIDO Alliance for supporting this project and connecting us with FIDO experts.

References

[1] Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. *Communications of the ACM*, 42(12):40–46, December 1999.

[2] AgileBits, Inc. Passkeys.directory, June 2023. passkeys.directory, as of October 10, 2023.

[3] Syed Ishtiaque Ahmed, Md. Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. "Everyone Has Some Personal Stuff": Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *ACM Conference on Human Factors in Computing Systems*, CHI '19, pages 180:1–180:13, Glasgow, Scotland, United Kingdom, May 2019. ACM.

[4] Aftab Alam, Katharina Krombholz, and Sven Bugiel. Poster: Let History Not Repeat Itself (This Time) – Tackling WebAuthn Developer Issues Early On. In *ACM Conference on Computer and Communications Security*, CCS '19, pages 2669–2671, London, United Kingdom, November 2019. ACM.

[5] Fatima Alqubaisi, Ahmad Samer Wazan, Liza Ahmad, and David W. Chadwick. Should We Rush to Implement Password-Less Single Factor FIDO2 Based Authentication? In *Annual Undergraduate Research Conference on Applied Computing*, URC '20, pages 1–6, Dubai, United Arab Emirates, April 2020. IEEE.

[6] Anna Angelogianni, Ilias Politis, and Christos Xenakis. How Many FIDO Protocols Are Needed? Surveying the Design, Security and Market Perspectives. *CoRR*, abs/2107.00577:1–35, June 2021.

[7] Apple, Inc. About the Security of Passkeys, 2022. support.apple.com, as of October 10, 2023.

[8] Debi Ashenden and Angela Sasse. CISOs and Organisational Culture: Their Own Worst Enemy? *Computers & Security*, 39(B):396–405, November 2013.

[9] Manuel Barbosa, Alexandra Boldyreva, Shan Chen, and Bogdan Warinschi. Provable Security Analysis of FIDO2. In *Advances in Cryptology – CRYPTO 2021*, CRYPTO '21, pages 125–156, Virtual Conference, August 2021. Springer.

[10] Kemal Bicakci and Yusuf Uzunay. Is FIDO2 Passwordless Authentication a Hype or for Real?: A Position Paper. In *Conference on Information Security and Cryptography*, ISCTURKEY '22, pages 68–73, Ankara, Turkey, October 2022. IEEE.

[11] Nina Bindel, Cas Cremers, and Mang Zhao. FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation. In *IEEE Symposium on Security and Privacy*, SP '23, pages 1471–1490, San Francisco, California, USA, May 2023. IEEE.

[12] Arnar Birgisson. Security of Passkeys in the Google Password Manager, 2022. security.googleblog.com, as of October 10, 2023.

[13] 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.

[14] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. Passwords and the Evolution of Imperfect Authentication. *Communications of the ACM*, 58(7):78–87, June 2015.

[15] John Bradley, Jeff Hodges, Michael B. Jones, Akshay Kumar, Rolf Lindemann, and Johan Verrept. Client to Authenticator Protocol (CTAP) – Version 2.1, 2021. fidoalliance.org, as of October 10, 2023.

[16] Matt Burgess. Apple's Killing the Password. Here's Everything You Need to Know, 2022. wired.com, as of October 10, 2023.

[17] Tim Cappalli, Matthew Miller, and Community. Passkey: Device Support, 2023. passkeys.dev, as of October 10, 2023.

[18] Matthew Casey, Mark Manulis, Christopher J. P. Newton, Robin Savage, and Helen Treharne. An Interoperable Architecture for Usable Password-Less Authentication. In *Workshop on Emerging Technologies for Authorization and Authentication*, ETAA '20, pages 16–32, Guildford, United Kingdom, September 2020. Springer.

[19] Dhiman Chakraborty and Sven Bugiel. SimFIDO: FIDO2 User Authentication with SimTPM. In *ACM Conference on Computer and Communications Security*, CCS '19, pages 2569–2571, London, United Kingdom, November 2019. ACM.

[20] 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.

[21] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Faith 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.

[22] Janis Danisevskis. Android Protected Confirmation: Taking Transaction Security to the Next Level, 2018. android-developers.googleblog.com, as of October 10, 2023.

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

[24] Alexis Deveria ("Fyrd") and Community. Support of the Web Authentication API on Mobile Devices, 2023. caniuse.com, as of October 10, 2023.

[25] The European Parliament and the Council of the European Union. Regulation (EU) 2015/1502 on Setting Out Minimum Technical Specifications and Procedures for Assurance Levels for Electronic Identification Means, 2015. eur-lex.europa.eu, as of October 10, 2023.

[26] The European Parliament and the Council of the European Union. Regulation (EU) 2018/389 on Strong Customer Authentication and Common and Secure Open Standards of Communication, 2017. eur-lex.europa.eu, as of October 10, 2023.

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

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

[29] FIDO Alliance. FIDO2 Conformance Test Tool, 2020. fidoalliance.org, as of October 10, 2023.

[30] FIDO Alliance. Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins, 2022. fidoalliance.org, as of October 10, 2023.

[31] FIDO Alliance. FIDO Case Studies, 2022. fidoalliance.org, as of October 10, 2023.

[32] FIDO Alliance. FIDO Deployment in the Enterprise: Journey Map, 2022. fidoalliance.org, as of October 10, 2023.

[33] FIDO Alliance. FIDO-Dev Mailing List, 2022. groups.google.com, as of October 10, 2023.

[34] FIDO Alliance. FIDO2: Web Authentication (WebAuthn), 2022. fidoalliance.org, as of October 10, 2023.

[35] FIDO Alliance. Meet PSD2 Requirements with FIDO, 2022. fidoalliance.org, as of October 10, 2023.

[36] FIDO Alliance. FIDO Adoption Working Groups, 2023. fidoalliance.org, as of October 10, 2023.

[37] FIDO Alliance. FIDO Authenticator Certification Program, 2023. fidoalliance.org, as of October 10, 2023.

[38] FIDO Alliance. Passkeys Creation and Sign-ins UX Guidelines, 2023. fidoalliance.org, as of October 10, 2023.

[39] Samuel Gibbs. RIP Passwords: New Web Standard Designed to Replace Login Method, 2018. theguardian.com, as of October 10, 2023.

[40] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M. Redmiles. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In *USENIX Security Symposium*, SSYM '21, pages 109–126, Virtual Conference, August 2021. USENIX.

[41] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In *ACM Conference on Computer and Communications Security*, CCS '18, pages 1549–1566, Toronto, Ontario, Canada, October 2018. ACM.

[42] Hidehito Gomi, Bill Leddy, and Dean H. Saxe. Recommended Account Recovery Practices for FIDO Relying Parties, 2019. fidoalliance.org, as of October 10, 2023.

[43] Google, Inc. Google Identity: Passwordless Login with Passkeys, 2023. developers.google.com, as of October 10, 2023.

[44] Government of California. California Labor Code: Section 2802 - Obligations of Employer, 2016. leginfo.legislature.ca.gov, as of October 10, 2023.

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

[46] Iness Ben Guirat and Harry Halpin. Formal Verification of the W3C Web Authentication Protocol. In *Symposium on Hot Topics in the Science of Security*, HoTSoS '18, pages 6:1–6:10, Raleigh, North Carolina, USA, April 2018. ACM.

[47] Julie M. Haney and Wayne G. Lutters. "It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Symposium on Usable Privacy and Security*, SOUPS '18, pages 411–425, Baltimore, Maryland, USA, August 2018. USENIX.

[48] Cormac Herley, Paul C. Van Oorschot, and Andrew S. Patrick. Passwords: If We're So Smart, Why Are We Still Using Them? In *Financial Cryptography and Data Security*, FC '09, pages 230–237, Accra Beach, Barbados, February 2009. Springer.

[49] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *USENIX Security Symposium*, SSYM '23, Anaheim, California, USA, August 2023. USENIX.

[50] Jeff Hodges, J.C. Jones, Michael B. Jones, Akshay Kumar, and Emil Lundberg. Web Authentication: An API for Accessing Public Key Credentials – Level 2, 2021. w3.org, as of October 10, 2023.

[51] Vincenzo Iozzo. The Good, the Bad and the Ugly of Apple Passkeys, 2022. slashid.dev, as of October 10, 2023.

[52] Shikha Khanna, Anand Bahety, Md Kamal Hossen, and Neb Pesic. eBay Makes Mobile Web Login Easier, 2019. tech.ebayinc.com, as of October 10, 2023.

[53] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. "I Have No Idea What I'm Doing" – On the Usability of Deploying HTTPS. In *USENIX Security Symposium*, SSYM '17, pages 1339–1356, Vancouver, British Columbia, Canada, August 2017. USENIX.

[54] Johannes Kunke, Stephan Wiefling, Markus Ullmann, and Luigi Lo Iacono. Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication. In *Open Identity Summit*, ODI '21, pages 59–70, Copenhagen, Denmark, June 2021. GI.

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

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

[57] Philipp Markert, Leona Lassak, Maximilian Golla, and Markus Dürmuth. "It Knew It Was Me": Understanding Users' Interaction with Login Notifications. *CoRR*, abs/2212.07316:1–24, December 2022.

[58] Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth. "As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication. In *Symposium on Usable Privacy and Security*, SOUPS '22, pages 483–501, Boston, Massachusetts, USA, August 2022. USENIX.

[59] Peter Mayer, Collins W. Munyendo, Michelle L. Mazurek, and Adam J. Aviv. Why Users (Don't) Use Password Managers at a Large Educational Institution. In *USENIX Security Symposium*, SSYM '22, pages 1849–1866, Boston, Massachusetts, USA, August 2022. USENIX.

[60] Microsoft, Corporation. Windows Hello for Business: Password-less Strategy, 2022. learn.microsoft.com, as of October 10, 2023.

[61] Microsoft, Corporation. Building the Passwordless Future, September 2023. microsoft.com, as of October 10, 2023.

[62] Microsoft, Corporation. Windows Hello for Business: Common Questions, 2023. learn.microsoft.com, as of October 10, 2023.

[63] Ron Miller. FIDO Alliance and W3C Have a Plan to Kill the Password, 2018. techcrunch.com, as of October 10, 2023.

[64] Florian Nawrath. Quantitative Analysis of FIDO2 Client Support. In *Who Are You?! Adventures in Authentication Workshop*, WAY '21, pages 1–5, Virtual Conference, August 2021.

[65] Lily Hay Newman. A Big Bet to Kill the Password for Good, 2022. arstechnica.com, as of October 10, 2023.

[66] Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, and Blase Ur. A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords. In *USENIX Security Symposium*, SSYM '23, pages 5127–5144, Anaheim, California, USA, August 2023. USENIX.

[67] Jan Odvarko. Mozilla Connect Community: Support WebAuthn Passkeys, 2023. connect.mozilla.org, as of October 10, 2023.

[68] Kate O'Flaherty. Apple to Kill Passwords with Game-Changing New Face ID Move, 2021. forbes.com, as of October 10, 2023.

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

[70] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Symposium on Usable Privacy and Security*, SOUPS '21, pages 57–76, Virtual Conference, August 2021. USENIX.

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

[72] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why People (Don't) Use Password Managers Effectively. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 319–338, Santa Clara, California, USA, August 2019. USENIX.

[73] Jon Porter. The Web Just Took a Big Step toward a Password-Free Future, 2019. theverge.com, as of October 10, 2023.

[74] Florentin Putz, Steffen Schön, and Matthias Hollick. Future-Proof Web Authentication: Bring Your Own FIDO2 Extensions. In *Workshop on Emerging Technologies for Authorization and Authentication*, ETAA '21, pages 17–32, Darmstadt, Germany, October 2021. Springer.

[75] Suby Raman. Guide to Web Authentication, 2019. webauthn.guide, as of October 10, 2023.

[76] 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.

[77] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. Security Managers Are Not The Enemy Either. In *ACM Conference on Human Factors in Computing Systems*, CHI '19, pages 433:1–433:7, Glasgow, Scotland, United Kingdom, May 2019. ACM.

[78] Karen Renaud, Rosalind Searle, and Marc Dupuis. Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil? In *New Security Paradigms Workshop*, NSPW '21, pages 70–87, Virtual Conference, October 2021. ACM.

[79] Joshua Reynolds, Nikita Samarin, Joseph Barnes, Taylor Judd, Joshua Mason, Michael Bailey, and Serge Egelman. Empirical Measurement of Systemic 2FA Usability. In *USENIX Security Symposium*, SSYM '20, pages 127–143, Virtual Conference, August 2020. USENIX.

[80] Lucas Ropek. Google Rolls Out Passkeys to (Eventually) Kill Passwords, 2023. gizmodo.com, as of October 10, 2023.

[81] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy Is Not for Me, It's for Those Rich Women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Symposium on Usable Privacy and Security*, SOUPS '18, pages 127–142, Baltimore, Maryland, USA, August 2018. USENIX.

[82] Angela Sasse. Scaring and Bullying People into Security Won't Work. *IEEE Security & Privacy*, 13(3):80–83, May 2015.

[83] Swaroop Sham. Why Your Customers Need Passwordless Authentication, 2019. okta.com, as of October 10, 2023.

[84] Alex Takakuwa. *Moving from Passwords to Authenticators*. PhD thesis, University of Washington, 2019.

[85] David Temoshok, Diana Proud-Madruga, Yee-Yin Choong, Ryan Galluzzo, Sarbari Gupta, Connie LaSalle, Naomi Lefkovitz, and Andrew Regenscheid. Digital Identity Guidelines – Authentication and Lifecycle Management: NIST Special Publication 800-63-4B (Initial Public Draft), December 2022.

[86] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, and Elie Bursztein. Protecting Accounts From Credential Stuffing With Password Breach Alerting. In *USENIX Security Symposium*, SSYM '19, pages 1556–1571, Santa Clara, California, USA, August 2019. USENIX.

[87] Christian Tiefenau, Emanuel von Zezschwitz, Maximilian Häring, Katharina Krombholz, and Matthew Smith. A Usability Evaluation of Let's Encrypt and Certbot: Usable Security Done Right. In *ACM Conference on Computer and Communications Security*, CCS '19, pages 1971–1988, London, United Kingdom, November 2019. ACM.

[88] Mindy Tran, Sabrina Amft, and Dominik Wermke. Poster: User Awareness of Phishing and WebAuthn. In *IEEE Symposium on Security and Privacy*, SP '22, San Francisco, California, USA, May 2022. IEEE.

[89] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols. In *USENIX Security Symposium*, SSYM '21, pages 3811–3828, Virtual Conference, August 2021. USENIX.

[90] U.S. Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, 2012.

[91] Tom Warren. Microsoft Accounts Can Now Go Fully Passwordless, 2021. theverge.com, as of October 10, 2023.

[92] Jess Weatherbed. A Huge Phishing Campaign Has Targeted over 130 Companies, Affecting Twilio and Signal, 2022. theverge.com, as of October 10, 2023.

[93] Jess Weatherbed. 1Password Is Finally Rolling Out Passkey Management, 2023. theverge.com, as of October 10, 2023.

[94] Stephan Wiefling, Markus Dürmuth, and Luigi Lo Iacono. Verify It's You: How Users Perceive Risk-based Authentication. *IEEE Security & Privacy*, 19(6):47–57, November 2021.

[95] Davey Winder. This Is How Hackers Accessed 34,942 PayPal Accounts, 2023. forbes.com, as of October 10, 2023.

[96] Flynn Wolf, Adam J. Aviv, and Ravi Kuber. Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. In *USENIX Security Symposium*, SSYM '21, pages 1199–1216, Virtual Conference, August 2021. USENIX.

[97] World Wide Web Consortium. W3C WebAuthn Adoption Community Group: Public Mailing List, 2022. lists.w3.org, as of October 10, 2023.

[98] World Wide Web Consortium. W3C WebAuthn Working Group: GitHub Issues, 2022. github.com, as of October 10, 2023.

[99] World Wide Web Consortium. W3C WebAuthn Working Group: Public Mailing List, 2022. lists.w3.org, as of October 10, 2023.

[100] Yubico, Inc. Yubico: WebAuthn Developer Guide, 2023. developers.yubico.com, as of October 10, 2023.

[101] Yubico, Inc. YubiEnterprise Delivery, 2023. yubico.com, as of October 10, 2023.

[102] Samira Zibaei, Dinah Rinoa Malapaya, Benjamin Mercier, Amirali Salehi-Abari, and Julie Thorpe. Do Password Managers Nudge Secure (Random) Passwords? In *Symposium on Usable Privacy and Security*, SOUPS '22, pages 581–597, Boston, Massachusetts, USA, August 2022. USENIX.

A Interview Script

Hello, thank you for joining our study. First of all, can you hear and see me properly? If you feel comfortable, I would appreciate it if you could turn on your camera but it is not required. As mentioned in the consent form, we will audio record this session. We will not record the video. Please let me know if you are okay if I start the audio recording now. *[start audio recording]*
Do you have any questions before we start?
[Explain: The interview is split into two parts: first I will ask you some questions and then we will do a little task on a digital whiteboard]

{The questions for organizations and IAMs were very similar.}

Authentication in General (Asked: organizations, IAMs)
Great! To begin, I would like to talk about some general aspects of the authentication infrastructure in your company/you offer.

Q1 Can you name and describe the devices and authentication options your company currently offers for its customers. We are interested in everything ranging from passwords or multifactor authentication to FIDO2.

Q2 Please do the same for the company's internal authentication infrastructure. In what ways can employees currently authenticate?

Q3 Do you see any shortcomings with those methods and if so which are those? Which are the benefits relative to other authentication methods you offer? What can only this authentication method offer?

Q4 *[IAMs only]* Regarding passwords specifically, what do your customers complain to you about the most? What are the most common reasons they seek alternative authentication? Do they have experience with attacks or leaks, issues with support tickets, or calls?

FIDO2 in General (Asked: organizations)

Q5 Now, I would like to ask you to what extent you are familiar with the FIDO2 protocol, recently also introduced under the term "passkeys?"

FIDO2 at Company (Asked: organizations, IAMs)
Ok, interesting. Thank you for sharing that. Now switching over to your company.
[As you mentioned earlier] *[none of the/some of the]* FIDO protocols are supported by your company, right?/Which FIDO protocols do you offer?

Q6 Which protocols do you support specifically?
[potentially prompt for specific protocols: FIDO U2F, FIDO UAF]
{If FIDO2 mentioned}

Q7 Which authentication options do you use/offer with FIDO2?

Q8 Do you use/offer FIDO2 for passwordless authentication?
{If no passwordless}

Q9 Why do you not offer FIDO2 for passwordless authentication?

Q10 *[organizations]* Why did your company decide to deploy it? What were the biggest selling points?

Q11 *[IAMs]* How do you sell FIDO2 to your customers? What are the most important arguments you present to them?

Q12 *[IAMs]* From your customer's response: What are the biggest selling points in hindsight?

Q13 *[IAMs]* When you are in a product pitch: What are the most common issues and concerns expressed by your potential customers?

Usage/Experience Questions:

Q14 What has your/your customer's experience with FIDO2 been so far?

Q15 Which feedback did you/your customer's receive from your/their users? If you are allowed to give us that information and you had to roughly estimate: What fraction of users/of users of customers use FIDO2?

Q16 Do you have plans or are you considering expanding the use cases/your offering of FIDO2?

Q17 Do you think the shortcomings of other authentication options you mentioned, in the beginning, can/will be/are solved by the FIDO2 protocols?

{If FIDO2 not mentioned}

Q18 Has there ever been any discussion on whether the FIDO2 standard should be implemented/offered as a service at/by your company?
{If yes}

Q19 What is the reason that it has not (yet) been implemented?

Q20 What would it take for your company to deploy/offer FIDO2?
{If no}

Q21 Why do you think FIDO2 was not considered yet?

Q22 What would it take for your company to deploy/offer FIDO2?

Q23 Do you think the shortcomings of other authentication options you mentioned, in the beginning, could be solved by any of the FIDO protocols?

Passkeys (Asked: organizations, IAMs)
Recently, the FIDO Alliance announced its plans for the augmentation of FIDO2 referred to as "passkeys" (multi-device FIDO credentials). Have you heard of it, and what do you know?
{If yes}

Q24 If any, which issues do you think passkeys will solve in terms of FIDO2 deployment [in your company]?

Q25 What is your general opinion on passkeys? (potentially prompting for tradeoff security for usability?) Do you think it addresses any of the issues discussed before?

Q26 *[IAMs only]* Does the development of passkeys change your companies offerings in terms of FIDO2?
{If no}
Passkey has been introduced to counteract one of FIDO2s major challenges. With passkeys, users will be able to transmit private keys between devices. For that, the private key is stored in the Cloud instead of only on the local device. The FIDO Alliance also claims to ensure interoperability between different operating systems using, i.e., QR codes.

Q27 If any, which issues do you think passkeys will solve in terms of FIDO2 deployment in your company?

Q28 What is your general opinion on passkeys? (potentially prompting for trade of security for usability?) Do you think it addresses any of the issues discussed before?

{The questions for the FIDO experts were different.}

Your FIDO Working Group (Asked: FIDO experts)
Great! In today's interview, I am interested in learning about FIDOs plans and goals for the FIDO2 standard as well as how you work on improving and fostering the more widespread deployment of FIDO2.

Q29 So to start, I would like to talk about your general thoughts on other authentication options compared to FIDO? What are shortcomings, what are benefits, and what can only specific methods offer?

Awesome, thanks for your reply. Now I would like to understand a bit more about the inner workings of the FIDO working group.

Q30 What are the objectives of the working group and how do you make decisions? Do you have a counseling rule? Do you work on explicit solutions? How do you cooperate with companies?

Q31 Generally, how do you approach the process of developing and improving FIDO2? Are you conducting research? Do you focus on public relations? Do you and if so how measure success?

Q32 What role do usability aspects play in the design and improvement process?

FIDO2 in General (Asked: FIDO experts)
Let's now switch over to the FIDO2 standard itself.

Q33 From your perspective: What are FIDO2s advantages over older FIDO standards?

Q34 What are you personally most proud of in the design / that it has this advantage?

Passkeys (Asked: FIDO experts)

Recently, the FIDO Alliance announced its plans for "passkeys" (multi-device FIDO credentials).

Q35 What were the main reasons for your work on passkeys?

Q36 If any, which issues do you think passkeys will solve in terms of more widespread FIDO2 deployment?

Q37 What is your opinion on passkeys? How do you judge the tradeoff between security and usability?

FIDO2 in the Future (Asked: FIDO experts)

Q38 Do you have plans or are you considering expanding the use cases of FIDO2?

Q39 In previous interviews with other stakeholders, we have learned some issues they face with the deployment of FIDO2. What do you think about those specifically?

Q40 Which solutions do you develop to tackle the shortcomings of FIDO2?

Q41 What do you think are the main reasons companies have not implemented FIDO2? Do you think they have not considered it? Do you think they have decided against it, and why?

B Card Sorting Task

Now, I will share a link to a digital whiteboard with you. In the process of this research, we have accumulated a comprehensive list of a variety of potential obstacles to the FIDO2 deployment. We may have talked about some of those hurdles already during our interview, but we would like to make sure that we cover all potentially influential factors.

{Ask if familiar with digital whiteboard, if not explain.}

So, generally speaking, I would like to know what you think *[are/were/will be]* the biggest obstacles for the deployment of FIDO2 within your company. On the whiteboard, you see a number of potential obstacles from different categories, each on an individual Post-it. Please think of the following question:

"*How much has the factor encumbered the deployment of FIDO2 [in your company?]*"

Your task is to sort the Post-its into one of these three categories:

- "It was a major obstacle."
- "It was a minor obstacle."
- "It was not an obstacle."

By "major," we mean something that is a deal-breaker almost on its own. A "minor obstacle" means something that is not a deal-breaker, but in conjunction with other minor obstacles impedes the deployment. Please also shortly explain the main reasons for your answer choice. Do you have any questions before we start?

Necessity:

We/Companies do not need FIDO2 as an authentication mechanism, because...

N1 Our/their customers/employees are happy with how it is

N2 Passwords are good enough

N3 Password managers exist, so passwords are not a problem anymore

N4 We/Companies use two-factor authentication (2FA), so our/their authentication procedure is already secure enough

N5 We/Companies offer single sign-on (SSO) so we/companies do not need better usability

Usability:

FIDO2 has [too many] usability shortcomings that need to be solved first before we can deploy it, specifically . . .

U1 There is no standardized fallback method

U2 It is unclear what to do if customers/employees lose their device or it gets stolen

U3 It is unclear what to do if a customer/employee gets a new device

U4 It is unclear what to do when a customer/employee wants to sign in from multiple different devices

U5 Our customers/'s users/employees would not use biometrics

U6 Roaming authenticators are not usable so we do not offer them for login

U7 Our customers/'s users/employees are used to the password login and changing the system would cause friction

U8 Our customers/'s users/employee are used to the password login so they would not see the need to switch the login method

Deployability:

The server-side implementation is an issue, because libraries and frameworks ...

D1 do not exist

D2 are incomplete

D3 are not understandable

D4 are written in the wrong language

D5 we would need to support passwords alongside FIDO2

D6 it is unclear how to get rid of passwords entirely

The client-side implementation is an issue, because...

D7 some browsers do not have all the functionality we/customers need

D8 the user interface is OS-dependent but we/companies want a unified experience for all our customers/employees/their users

IT Management:

M1 We have never seen the need to talk to management about FIDO2

M2 Management will not let us/IT staff explain the need/talk about it

M3 Management just does not see/understand the need for FIDO2

M4 Our/Many company policies forbid the use of open-source software

M5 Our/Many company policies do not allow biometric authentication

M6 We are waiting for peer organizations to deploy it first to judge whether FIDO2 is a good option for us

Financial:

F1 It is unclear why we should invest in FIDO2 deployment because everything is working well

F2 The costs for implementing FIDO2 are too high

F3 The costs for developing new communication & interfaces to market FIDO2 are too high

Communication:

C1 FIDO2 is incompatible with the company's UX guidelines.

C2 We cannot brand FIDO2, however, this is necessary for our company/customers.

C3 It is unclear how to communicate the issue & necessity of FIDO2 to the user.

C4 Deciding on design questions like wording, color, and icons is hard.

Final Question

Ok now I have one final task for you: Please name the top 3 points that, in your opinion, FIDO needs to change that are the biggest hurdles to the deployment.

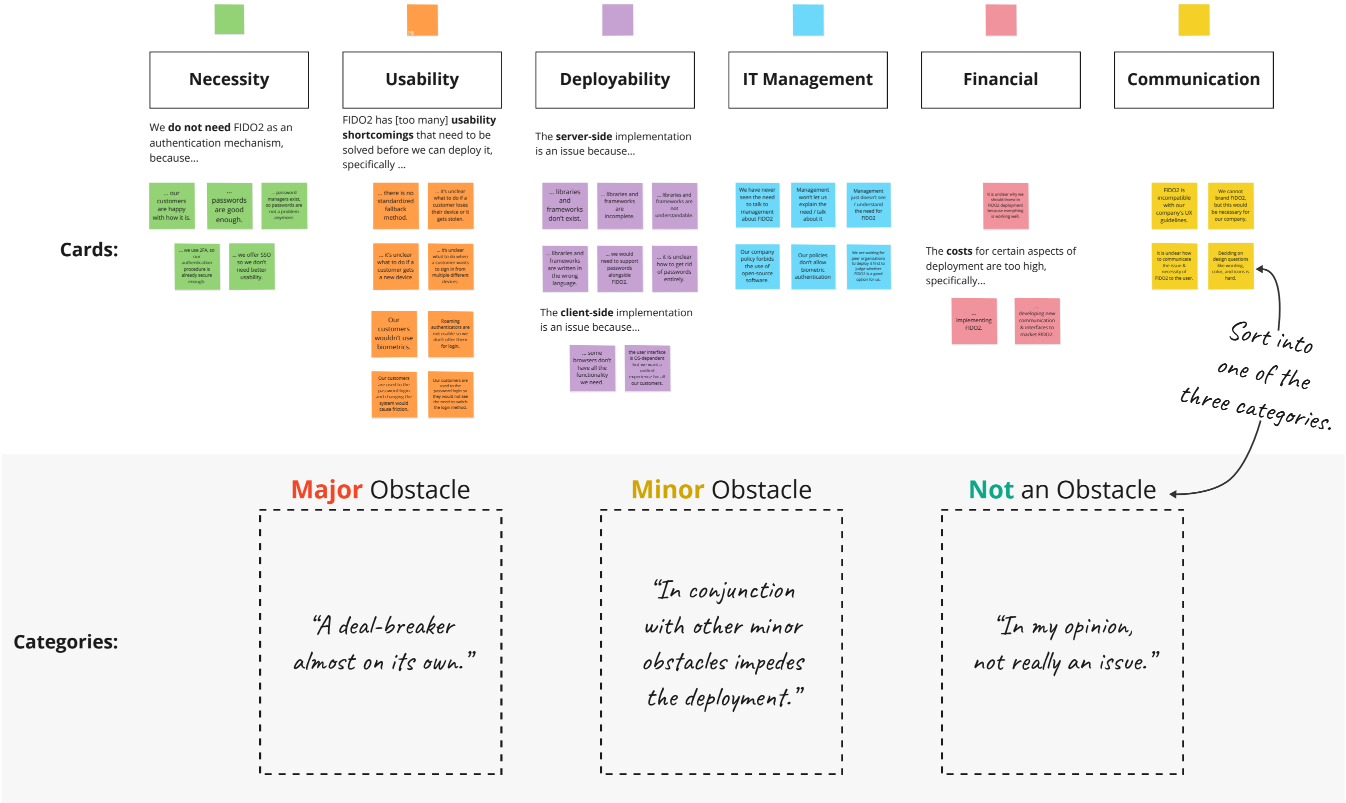
Cards:
Necessity
We do not need FIDO2 as an authentication mechanism, because...
... our customers are happy with how it is.
... passwords are good enough.
... password managers exist, so passwords are not a problem anymore.
... we use 2FA, so our authentication procedure is already secure enough.
... we offer SSO so we don't need better usability.
Usability
FIDO2 has [too many] usability shortcomings that need to be solved before we can deploy it, specifically ...
... there is no standardized fallback method.
... it's unclear what to do if a customer loses their device or it gets stolen.
... it's unclear what to do if a customer gets a new device
... it's unclear what to do when a customer wants to sign in from multiple different devices.
Our customers wouldn't use biometrics.
Roaming authenticators are not usable so we don't offer them for login.
Our customers are used to the password login and changing the system would cause friction.
Our customers are used to the password login so they would not see the need to switch the login method.
Deployability
The server-side implementation is an issue because...
... libraries and frameworks don't exist.
... libraries and frameworks are incomplete.
... libraries and frameworks are not understandable.
... libraries and frameworks are written in the wrong language.
... we would need to support passwords alongside FIDO2.
... it is unclear how to get rid of passwords entirely.
The client-side implementation is an issue because...
... some browsers don't have all the functionality we need.
the user interface is OS-dependent but we want a unified experience for all our customers.
IT Management
We have never seen the need to talk to management about FIDO2
Management won't let us explain the need / talk about it
Management just doesn't see / understand the need for FIDO2
Our company policy forbids the use of open-source software.
Our policies don't allow biometric authentication
We are waiting for peer organizations to deploy it first to judge whether FIDO2 is a good option for us.
Financial
It is unclear why we should invest in FIDO2 deployment because everything is working well.
The costs for certain aspects of deployment are too high, specifically...
... implementing FIDO2.
... developing new communication & interfaces to market FIDO2.
Communication
FIDO2 is incompatible with our company's UX guidelines.
We cannot brand FIDO2, but this would be necessary for our company.
It is unclear how to communicate the issue & necessity of FIDO2 to the user.
Deciding on design questions like wording, color, and icons is hard.
Sort into one of the three categories.
Categories:
Major Obstacle
"A deal-breaker almost on its own."
Minor Obstacle
"In conjunction with other minor obstacles impedes the deployment."
Not an Obstacle
"In my opinion, not really an issue."

Figure 2: We presented each participant with an interactive card sorting task using our list of potential obstacles (Table 1). Participants were asked to sort every statement from six different areas—"Necessity," "Usability," "Deployability," "IT Management," "Financial," and "Communication"—into one of three categories: (1) *Major Obstacle*, (2) *Minor Obstacle*, or (3) *Not an Obstacle*.

C Codebook

Table 4: Codebook of deployment obstacles.

Code	**Explanation**
Regulation & Requirements	
Non-Compliant Policies	
Digital sovereignty	Reliance on external vendor prohibited.
Separate 2FA devices	Factors for 2FA must be on different physical devices.
Occupational safety	Mandatory safety gear (i.e., protective gloves) hinders biometric usage.
Obsolete password rules	Password composition regulations must be suspended.
Law	
eIDAS	eIDAS requires individual's identity to be bound to hardware.
PSD2	Not all FIDO authenticators implement transaction confirmation displays (PSD2).
Other	Further regulations.
Usability Challenges	
Hard to Explain	
Concept shift to public key	Sharing of keys is possible & it is 2FA.
Inconsistent UX across services	Inconsistent UX impairs users ability to accustom to new authentication.
Difference to other authenticators	Difference to proprietary biometric authentication.
Need for multiple keys	Multiple keys must be registered for fallback.
Account Recovery	
Solved by passkeys	Passkeys sufficiently address the issue of secure account recovery.
Standardized fallback missing	A standardized, vendor-agnostic secure account recovery is needed.
Backup setup convoluted	UX for setting up backup authenticators is poor.
Technical Challenges	
Complex for Developers	
Secure implementation expertise	High expertise is required for secure implementation.
Solutions available	Vendors offer sufficient FIDO(2) authentication solutions.
Support/Legacy	
Legacy software	Crucial software cannot be used with modern authentication.
Tooling unavailable	Tooling to integrate legacy into modern authentication is missing.
Platform support	Support of certain browsers/OSs is not sufficient.
No EOL support	Older OS versions will never be supported.
Lack of Universality	
Non-Universal for Workforce	
Production environment	Typical work gear (i.e., gloves) makes using biometrics cumbersome.
Call centers	Rules that prohibit private devices (platform authenticators only).
Exclusion of User Groups	
Costs for devices	Lower income demographics cannot purchase extra devices.
Homeless/Elderly	Unusable for those who have no (personal) phones.
Delegating access	Delegating account access to, i.e., family members, is impossible.
Buried Entry	Vendors offer FIDO2 functionality only for big teams.
Biometrics	
Storage location	Storage location of biometric data as a concern.
Negative past experiences	Negative experiences with proprietary biometric authentication solutions.
Apps already offer	Little usability value as mobile app already offers biometric authentication.
Organizational Challenges	
Manageability & Logistics	
Key distribution for onboarding	Key distribution for onboarding is complicated.
Key retrieval for offboarding	Retrieving physical security keys when someone leaves company is hard.
Credential sharing	Account sharing for, i.e., showcasing, is impossible.
Passkey management	Number of passkeys will be huge once more common.
Stakeholders with Power	
Block developments	Strong players can block developments due to their powerful position.
Conflict of interest	Certain FIDO Alliance members benefit from roaming authenticators.