"It's Just a Lot of Prerequisites": A User Perception and Usability Analysis of the German ID Card as a FIDO2 Authenticator

MARKUS KEIL and PHILIPP MARKERT, Ruhr University Bochum, Germany

MARKUS DÜRMUTH, Leibniz University Hannover, Germany

Two-factor authentication (2FA) overcomes the insecurity of passwords by adding a second factor to the authentication process. A variant of 2FA, which is even phishing-resistant unlike, e.g., SMS-based implementations, is offered by the FIDO2 protocol. In 2018 its compatibility with eID, the German electronic identification system, which is built into every German ID card, was published. Thus, users who own a German ID card may use it as a second factor to secure their online accounts.

We conducted a qualitative study with $n = 20$ participants to collect users' impressions of the usability when utilizing an ID as a second factor, their perception of security, and the overall acceptance. After showing participants an introductory video to familiarize them with the procedure, they completed a hands-on task for which they first set up an ID as a second factor and then used it to log in. Users' opinions, thoughts, and concerns were collected through multiple-choice questions and structured interviews. We find that most non-tech-savvy users struggle with the setup but generally perceive the login to be easy. Users with a tech background faced fewer issues when setting up the ID as a second factor but pointed out to prefer other alternatives. Finally, we observe a misconception regarding the transmission of personal information to the authenticating service despite several indicators of privacy-conform data handling. Based on our findings, we depict which aspects need to be addressed in order to provide a competitive alternative to established second factors.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; **Multi-factor authentication**.

Additional Key Words and Phrases: FIDO2, national identity card

1 INTRODUCTION

To this day, passwords are still the most widespread form of user authentication for online services [6, 31]. Although it is no secret that text-based passwords bear various security risks [2, 3, 5, 7, 13, 16, 22, 33, 49], there has not been a mass migration from passwords to a viable alternative just yet. To minimize the security hazards and limitations that passwords bring, security researchers and companies have advocated switching to *two-factor authentication* (2FA) [4, 12, 15, 26, 42, 50]. Google even went one step further and starting auto-enrolling its users in 2FA in October 2021 [42, 48]. 2FA improves authentication to the extent that the user has to prove two of three factors: something they *know* (e.g., a password), something they *have* (e.g., a hardware token), or something they *are* (e.g., a fingerprint). This further layer of security is called the *second factor*.

One of the newest promising candidates for the implementation of 2FA is the *FIDO2* standard. FIDO2 was jointly developed by the *FIDO Alliance*, an industry association backed by several big companies like *Amazon*, *Apple*, and *Facebook*, as well as the *World Wide Web Consortium* (W3C), the main international standards organization for the web. FIDO2 builds upon the *Universal 2nd Factor* (U2F) standard and offers websites a standardized communication method with hardware authentication devices, such as security keys. Although this factor is of less interest in our work, it should be noted that FIDO2 not only supports hardware authentication devices as a second factor but also as a *single-factor* for *passwordless* authentication. Being an open web application standard, FIDO2 is supported by all major browsers and is compatible with many potential authenticators because it abstracts from the actual authentication device. Roaming devices like security keys, but also platform authenticators like *Trusted Platform Modules* are all potential alternatives for authentication using FIDO2. Interestingly, FIDO2 is also compatible with *eID*, the electronic identification system built into German ID cards since 2010. Considering that only 3.5%–4% of German citizens made use of eID in 2020 [28], utilizing the German ID card as a second factor for authentication presents an intriguing new use case with the following unanswered research questions:

RQ1: Are users aware of the possibility of using their German ID card as a FIDO2 authenticator?
RQ2: How do users perceive the German ID as a second factor in terms of usability?
RQ3: Are users accepting the German ID as a second factor?
RQ4: What thoughts and concerns arise in the users' minds when using the German ID as a second factor?

To answer these questions, we conducted a qualitative user study with $n = 20$ participants consisting of two runs with 10 participants each. Participants for the first run were selected randomly. For the second run, we required participants to have an education or work in an IT-related area to determine if this background would affect their usage patterns and perception. In both runs, the participants were randomly assigned to one of the two options which can be used to scan the ID card's chip: a separate card reader or a smartphone. After being familiarized with the presented system and its setup process in the form of three videos, the participants completed a hands-on task for which they registered the provided ID card as a second factor and then used it to log in. Finally, the participants were asked to reflect on their experience in an online survey and personal interviews.

Although some participants indicated their willingness to use the system, its setup was perceived to be the biggest hurdle. Installing the different pieces of software, especially a browser plugin, seems to be a serious complication for less tech-savvy users. Considering that the ID card's chip contains sensitive personal information, privacy misconceptions arose in round one, and participants felt unsure about their personal information's security. While those in round two had considerably fewer concerns, they pointed out to prefer other 2FA alternatives regarding their usability and ease of use to be superior to the presented system.

To summarize, we make the following contributions:

- We explore eID's usability as a second factor in the form of a user study, considering both setup and the login, as well as both options for scanning the ID card's chip (card reader and smartphone). We present results for both a mixed and a tech-savvy user group.
- We show that while eID as a second factor is a promising concept, it lacks in usability. Most users either perceive the system as too complex and challenging to set up or prefer other 2FA alternatives. Moreover, we observe privacy misconceptions as users falsely assume that personal data is shared during the authentication process.
- Considering the participant's reactions and answers, we outline what steps need to be taken to make the usage of eID as a second factor a more promising alternative to other 2FA options.

2 RELATED WORK

This work relies on two main aspects, the eID functionality of the German national identity card and FIDO2 as the specification which enables the authentication. Below, we outline works from both areas most related to ours.

2.1 eID

A study by Harbach et al. [34] investigated the acceptance of the German identity card as an authenticator using the eID authentication scheme. The study's participants stated that they did not understand the technology and were not interested in it. Unlike the FIDO2-based authentication we analyze in our study, the eID authentication scheme requires companies to apply for an extra authorization certificate. Hence, they also saw little to no need to replace the existing mechanisms beyond legal requirements. The study's main takeaway was that simply ensuring that enough users get an eID-compatible ID card through a national roll-out is not enough to kick-start adoption. In our study, we observe similar problems although we focus on eID as an additional security factor in the context of FIDO2 authentication; Harbach et al. [34] exclusively investigated the eID system as a standalone.

Poller et al. [55] discussed eID's key concepts, promises, and practicality. Although they conclude it would be unlikely for the standalone eID authentication to replace other currently used schemes, they saw some advantages. Namely, eID offers authentication regulated by law, and it supports attribute verification, e.g., of the age. Furthermore, the article poses the *Chicken-and-Egg Problem*: "Service providers need a sufficient user base, and users need a sufficient number of everyday services. [. . .], service providers and citizens are waiting for each other to make the first step." Finally, the article depicts some open questions like "How does the ID card affect user behavior?" or "Do the users trust the service more or less?" In the context of this work, we try to find answers to these questions.

In terms of technical advancements, Otterbein et al. [52] described how eID can be provided on *Android* devices without requiring a physical identity card or a card reader. They implemented a prototype, which showed that an actual implementation faces technical issues, including two vulnerabilities that cannot be prevented as they are enabled by the architecture. However, they are also not critical as they cannot be used to extract any sensitive information.

A literature review by Tsap et al. [59] identified 12 influencing factors on the acceptance of eID and concluded that it is recommended to take a more societal angle on future eID research. Trust, privacy, and security are usually the main focus of research and are well known, but according to Tsap et al. [59], it is not sufficient if eID only works in theory. Especially for large-scale deployment, its usability is just as crucial. That is also why we focus on direct user feedback instead of the technical advantages the system may have over other authentication schemes.

2.2 FIDO2

Regarding work on FIDO2, the research paper by Lyastani et al. [47] is the first large-scale laboratory study on FIDO2 *passwordless* authentication and its acceptance amongst end-users. Their study's participants were educated on the topic by a series of informative videos, then asked to complete a hands-on task, and finally a survey collected insights about the users' perception, acceptance, and concerns regarding passwordless authentication. The study's encouraging results revealed that users are generally willing to accept a direct replacement of text-based passwords. However, also new concerns arose that could potentially impede the system's adoption.

Another study on single-factor authentication using a hardware security token was performed by Farke et al. [27]. Although most participants considered the hardware keys usable, no explicit security benefits were noticed. We loosely

based our studies' structure and approach on the works of Lyastani et al. [47] and Farke et al. [27]. However, instead of investigating hardware keys as a single-factor authentication method, we focused on eID as a *second* factor to passwords.

Several works on passwordless authentication by Lassak et al. [46], and Owens et al. [53] [54] have shown that big security misconceptions regarding the user's sensitive information like biometrics prevail amongst potential end-users. Common critiques of FIDO2 passwordless authentication also contain the authenticator's availability, setup difficulties, and account recovery and backup. As we will show, all of these positions also hold for eID as a second factor. Regarding account recovery methods, Kunke et al. [44] have shown that currently used methods have many drawbacks, with some still relying on passwords, making the efforts for passwordless authentication abundant.

Ulqinaku et al. [60] proved that FIDO2 does not eliminate the threat of phishing completely. They used a social engineering downgrade attack on FIDO2 as a second factor. While 55% of participants were tricked by the attack another 35% would potentially be prone to it if they encountered it in the real world.

Additionally, several other two-factor authentication alternatives have been studied, for example, by Strouble et al. [58], Weir et al. [63, 64], Gunson et al. [32], Krol et al. [43], or De Christofaro et al. [21]. Summarized, they all revealed that users are not in favor of using specialized hardware for authentication and tend to lose said hardware. Moreover, users pay more attention to a system's convenience than its perceived usability and security when adopting such a new authentication scheme. This, as we will show, is also in line with our findings.

Reynolds et al. [57] underlined the sentiment that the two processes setup and day-to-day usage yield very different results in terms of usability. While most participants struggled with setting up a YubiKey, other participants described it as usable and gave it a high usability rating when using it in their daily lives for four weeks. Furthermore, Reynolds et al. [57] recommended standardizing the setup step to diminish potential problems or difficulties. The sentiment that many users struggle with the setup process is supported by Ciolino et al. [14], who evaluated a diverse set of security keys alongside SMS-based OTPs. When searching for different influences on the usability and security perceptions of security keys during setup and login, Ciolino et al. [14] found that the setup time for security keys was considerably greater than the login time. We aimed to improve the setup part of our studies, by producing specifically tailored videos that not only give an outline of the different technologies involved, but also include a precise setup guide.

3 BACKGROUND

In this section, we first provide information about the history and the idea of eID which is the central concept in this work. Afterward, we explain the integration of FIDO2 into the functionality of eID.

3.1 eID

In digitizing business and governmental processes, secure electronic identification is crucial to enable trust in electronic services. Thus, in 2010 a new identity card, *neuer Personalausweis* (nPA), with an online authentication functionality called eID was introduced by the *Federal Office for Information Security* (BSI) in Germany. As of 2017, eID is activated in every newly issued nPA, and more than 61 million Germans already owned a compatible ID [51] in 2019. The nPA includes a built-in chip, containing all personal data found on the outside of the card. The eID infrastructure can be separated into three main parts: the user environment, the service providers, and the background systems. A detailed overview is depicted in Figure 1.

A user environment for eID consists of the following components: a German nPA with its eID functionality enabled, the self-chosen 6-digit eID-PIN, a stationary (desktop/notebook) or mobile (tablet/smartphone) terminal, the eID client software (AusweisApp2) installed on the terminal, and a card reader or an NFC-enabled smartphone. Most service
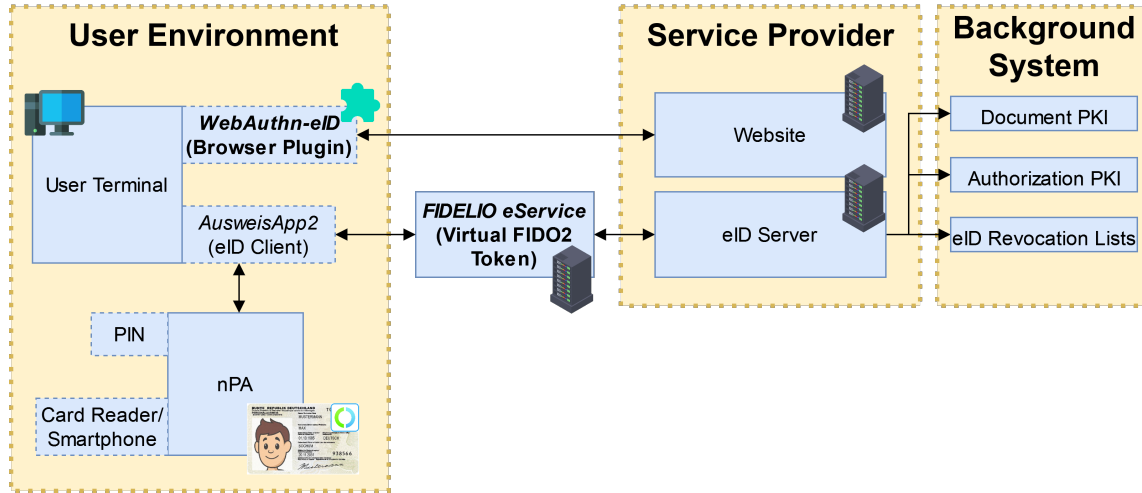
Fig. 1. Overview of the eID infrastructure which is necessary to use the nPA as a second factor at a service provider.

providers are government offices, e.g., for vehicle registration, but private companies like banks can also become service providers. An eID server is a hard- and software component used to integrate the ID card's online authentication functionality. It is responsible for secure communication with the eID client and passes the data to the service provider. Every service provider has to either implement an eID server or let another service provider run one for them.

The background system consists of a *document PKI*, an *authorization PKI* and eID *revocation lists*. When an ID card is personalized during the manufacturing process, data on the ID card's chip is digitally signed. The authenticity of the signature is verified via the document PKI. The authorization PKI ensures authenticity and determines the service provider's full access rights. It works as a trust anchor to access the ID card chip's data. When an nPA is reported as lost or revocation is requested via a revocation hotline, it is entered into the eID revocation list. This list is kept by the revocation service for the eID application and is made available for all service providers at any time, so that the eID server recognizes when someone tries to use a revoked nPA.

3.2 FIDO2-eID Integration

After the BSI joined the FIDO Alliance in 2015, the compatibility between the online authentication functionality of eID and the FIDO protocol was developed as part of the *FIDELIO* project [37]. FIDELIO aims to add easy-to-use second-factor authentication to the German eID card based on FIDO2. For that purpose, it embeds eID within FIDO2 and introduces two new components: a browser plugin and an additional web-based service. The browser plugin intercepts the FIDO2 requests and forwards them as FIDELIO requests to the eID client [35]. In the context of FIDO2, the browser plugin is the transport layer connection or driver to the token. The web-based service called *FIDELIO eService* [36] establishes connections to eID compatible ID cards and checks for their validity and revocation status. In the context of FIDELIO, it acts as a universal virtual FIDO2 security token.

Currently, FIDELIO only works with a very limited number of services, mainly because FIDO2 requests do not fully match the expected format or requests are delayed during transmission and appear in an unexpected order. Hence, we chose to use *Google* for our study, as it turned out to be the most reliable service and also one many users are already

familiar with. To register the nPA as a security key, users have to follow Google's standard two-factor authentication setup. After selecting the "Security Key" option, the AusweisApp2 client automatically opens and shows which data is requested from the nPA's chip. The nPA offers a pseudonym functionality that enables the cardholder to authenticate with a service provider without sharing any personal data. This pseudonym is created by the *Restricted Identification* protocol, which is always used in the context of FIDELIO. After confirming the presented data, the user is prompted to connect a device capable of reading the nPA's chip to their local terminal, if not done so before. Then, the user scans the nPA's chip using the configured device. As soon as the AusweisApp2 client recognizes an nPA, the user is prompted to enter the eID PIN. On successful authentication, the AusweisApp2 client closes, and Google takes the user to a new screen showing that the process was successful.

4 METHOD

In this section, we describe the method we used to collect data regarding the usability, acceptance, and security as perceived by potential end-users of the German nPA as a second factor. We start by describing our recruitment process and the demographics of our participants, followed by the structure of the study. Afterward, we describe the ethical implications of our research and end by highlighting the limitations of our approach.

4.1 Recruitment & Demographics

Recruitment took place via a variety of channels at our institution. Flyers in German and English (see Figure 2 and 3 in Appendix E) outlining the study were posted in Facebook groups, Discord servers, sent to departments via email, and distributed over the campus. Through these channels, we recruited two rounds of $n = 10$ participants each. We did not have any requirements for the first 10 participants, as we aimed to determine how average users perceive the setup and login of an ID as a second factor. For round two, we considered our findings from the first run and recruited participants who we required to "have an education in, or work in, the field of computer science, computer engineering or IT." We assumed that this background would affect how the system is perceived as technological constraints play a minor role.

The first round took place in December 2021 and January 2022, the second in April 2022. On average, the study took 35 minutes to complete, and each participant was compensated with a 20€ Amazon gift card.

A detailed overview of the participants' demographics can be found in Table 1. Eight participants in the first round were female, two male, and no non-binary participants took part. Most were undergrad students between the age of 18 and 24. The tech-savvy group in round two had a balanced mix of female and male participants; again no one was non-binary. The majority were again undergraduate students between 18 and 24 years, but we had more older participants with higher degrees compared to round one overall.

4.2 Study Procedure

Before beginning the study, participants were randomly assigned to one of two groups, differing only in the method used to read the nPA's chip. $Group_{CR}$ was given the *cyberJack RFID basis*, a standard, commercially available *card reader*, which prices at around 35€. $Group_{SM}$ received an NFC-compatible smartphone in the form of a *Google Pixel 3A*. We also provided both groups a workplace with a laptop, an nPA, its PIN, and login credentials for a Google account.

To eliminate any biases, the smartphone ran on a clean Android distribution without additional applications. *Windows 10* was used as the operating system on the laptop which only had *Mozilla Firefox* pre-installed because we expect the average user to already have a browser installed on their system. Thus, the process of downloading and installing a

Table 1. Participants' demographics in round one and two of the study.

		Round 1		Round 2	
		$Group_{CR1}$	$Group_{SM1}$	$Group_{CR2}$	$Group_{SM2}$
Gender	Woman	3	5	4	1
	Man	2	0	1	4
Degree	High School	3	5	3	2
	Bachelor's	2	0	0	1
	Master's	0	0	1	2
	Doctoral	0	0	1	0
Age	18−24	3	4	3	3
	25−34	1	0	2	2
	35−44	1	1	0	0
Tech	Yes	1	1	5	5
	No	4	4	0	0

new browser was of no interest to us. Firefox was used because it is the only browser at the moment where the browser plugin *WebAuthn-eID* which connects eID and FIDO2, is available.

At the beginning of the study, participants read the privacy policy and gave their consent. Afterward, they watched three educational videos on eID, FIDO2, and how to set up the nPA as a second factor in a Google account [38–41]. The last of the three videos differed for $Group_{SM}$ and $Group_{CR}$. While $Group_{SM}$ was shown how to configure the smartphone as a card reading device within the AusweisApp2 client, the video for $Group_{CR}$ only demonstrated how to connect the card reader to the laptop via USB. We chose to educate the participants before the study because previous work has shown that a lack of clarity about the process and functionality of an authentication method leads to lower acceptance, lower security ratings, and hesitation to switch to a new authentication method [20, 63, 64].

After watching the videos, the participants were asked to complete two hands-on tasks to gain experience with the system. First, they should register the given ID card as a second factor in the given Google account. Then, they should use the previously registered ID by logging into the account. The hands-on task was recorded to facilitate the analysis.

Once participants finished both tasks, they were asked to complete a survey made up of seven sets of questions which we will outline below. Please refer to Appendix A for the exact wording of each question. (1) The *System Usability Score* (**SUS1–SUS10**) [8] to get a general idea of the usability. (2) The *User Acceptance* (AC) [62] to measure the participant's acceptance of the presented system. (3) The *Affinity for Technology Interaction* scale (**ATI1–ATI9**) [30] to assess how much a user enjoys technology and their affinity to it. (4) We measured the participants' *Privacy Concerns* (**PC1–PC4**) [45], which can arise, e.g., when they are unsure how their data is processed. (5) To answer our first research question on users' awareness of the presented system (RQ1), two additional questions were added to the survey. **A1** "Were you aware that the German ID card offers an online functionality (eID)?" and **A2** "Were you aware that the FIDO2 standard for web authentication is compatible with eID?" FIDO2 was intentionally separated from eID in this context because we expected very different results from the two questions. Since almost every German citizen owns an ID card and eID has been a standard since 2017, we expect most participants to at least be aware of its existence, while FIDO2 is a comparably new system that the average user probably does not know yet. (6) To understand how participants perceive the privacy implications, they were then asked what data they thought would be shared with the services they register their nPA as a second factor with (**PP1**). For that purpose, they were presented with all the personal

information saved on the nPA, randomly ordered in a multiple-choice-manner with "None of the above" always as the last option. (7) Finally, we collected general demographic information with questions **D1–D4**, which asked about participants' gender identity, degree, and age.

The study concluded with a personal interview consisting of 11 open-ended questions **Q1–Q11** to collect qualitative data on the participant's thoughts and opinions on the presented second-factor alternative. We intended to get tangible feedback on the system's setup- and usage-procedure, general advantages and disadvantages, its usage in the real world, and potential concerns. The complete interview guideline can be found in Appendix B.

4.3 Ethics

Since our institution does not have an ethical review board, we followed the ethical principles discussed in the Menlo report [61] to minimize any negative effects on the participants. For instance, we informed participants about the study's procedure beforehand, told them what their participation would involve, and that they could always withdraw from the study without any negative consequences. Moreover, all collected data was stored in accordance with the General Data Protection Regulation (GDPR) [25] and we discussed the study's design with peers to double-check that we did not miss any harmful implications.

For the hands-on task, it was necessary to have access to an ID alongside its PIN. As demo IDs are highly regulated, and we did not want to require participants to know their PIN, we decided to use the ID from one of the researchers. To hide the personal data on the ID, we printed an overlay which we fixed with tape. Lastly, the researchers were always present when the ID was used during the study, and the PIN was reset after the study to prevent any subsequent misuse.

4.4 Limitations

We designed the study to ensure a high level of ecological validity. Still, there are limitations to our approach. First, participants were comparatively young, which is a common problem for studies in a university environment. While subsequent studies with a more diverse sample could yield additional insights [1, 17–19, 23, 56], we do find indications that our findings are transferable to a more age-diverse sample. For example, the participants' ATI scores usually correlate negatively with their age, yet, the scores in this study were comparable to studies with much more diverse age distributions [30].

Secondly, we conducted a qualitative user study with $n = 20$ participants. Hence, the results are not exhaustive, the informative value of the quantitative results is limited, and no statistical significance can be concluded. To reflect this, we only use the quantitative results to get a general idea and to detect trends that we explain further with the qualitative interview data. Also note that self-reported data can always be biased towards socially desirable answers.

5 RESULTS

In the following, we present the study's results and assess the collected data on trends and tendencies. We use the online survey and timings of the participant's runs for initial insights, followed by an in-depth analysis based on the qualitative interview data. The quantitative scores for each group can be seen in Table 2, timings are depicted in Table 3. An in-depth overview over every single participant, the scores they have given, and their respective times for partial tasks and complete runs, are depicted in Table 4a and 4b in Appendix C.

Questions **A1** and **A2** confirmed our presumptions about the participant's knowledge on eID and FIDO2 and gave us a definitive answer to research question one (RQ1). While in round one, eight out of ten people knew that eID existed, only one participant had heard of FIDO2 before. In round two, nine out of ten participants were aware of eID, but again,

Table 2. Scores for the four standardized metrics: *System Usability Scale*, *User Acceptance* (depicted with its two separate values *Usefulness* and *Satisfying*), *Affinity for Technology Interaction*, and *Privacy Concerns*.

	Round 1		Round 2	
	$Group_{CR1}$	$Group_{SM1}$	$Group_{CR2}$	$Group_{SM2}$
SUS	72	62	75	59
Acceptance				
Usefulness	1.2	1.0	1.1	0.7
Satisfying	0.8	0.5	1.1	0.2
ATI	3.5	3.3	4.2	4.8
Privacy Concerns	4.6	5.3	5.4	5.2

only one participant knew FIDO2. We also asked the participants whether they had used the eID system before the study. Although most were aware of eID's existence, close to no one had used it before. Nine participants in round one and eight in round two had never used eID before the study. Hence, users can generally not be expected to be aware of the possibility of using their nPA as a FIDO2 authenticator.

5.1 Survey Results and Timings

As shown in Table 2, $Group_{CR1}$ gave the system a SUS score of 72, $Group_{SM1}$ rated it with 62. While $Group_{CR1}$ barely exceeds the mark of an average system, which has a score of 68 [9], $Group_{SM1}$'s SUS score is even lower. This shows a distinct trend that in terms of usability, the participants perceived neither of the two versions of using the nPA as a second factor as above-average. Round two yielded very similar results. $Group_{CR2}$ perceived the nPA's usability as a second factor to be barely above-average with a score of 75, while $Group_{SM2}$ rated the system's usability with a 59. Neither of the scores deviates to a greater extent from their respective counterparts in round one. This sentiment gives us an appropriate baseline for answering research question two (RQ2), on users' perception of usability. The fact that the SUS is lower in $Group_{SM}$ than in $Group_{CR}$ in both rounds might be explained by $Group_{SM}$ having to complete the extra steps of opening the eID app on the smartphone and connecting it with the laptop. These longer setup and usage times could have potentially led to a lower usability score.

The SUS scores showed that neither of the two versions of FIDELIO was perceived as notably positive. The same tendency can be observed in the *Acceptance Scale* scores (Table 2). The scale is divided into the *Usefulness Scale*, denoting a system's usefulness, and the *Satisfying scale* which is designated to a system's satisfaction, as experienced by a potential end-user. Both scales range from −2 to +2. While both $Group_{SM1}$ and $Group_{CR1}$ seemingly perceived their respective system as rather useful, it scored lower on the satisfaction scale in both cases. Here, round two differs from round one to the extent that three out of four scores of the AC lie just below their counterparts of round one. This disparity could be due to the fact that participants in round two have more comparisons to other 2FA alternatives than participants in round one and thus perceive the system as less useful and satisfying. Subsequently, it can be said that both groups generally appear to accept the nPA as a second factor, while also seeing room for improvement.

Regarding the timings presented in Table 3, the time for complete runs was measured from the point of opening a new tab when beginning the tasks, to successfully registering the nPA as a second factor and logging into the Google account using it. We started timing a partial task when it was obvious that the participant understood what their next step would be and stopped the time when they successfully finished that step. Adding up all the partial task timings of a participant accumulates less than their total run time. This is owed to the fact that when timing the partial tasks, we

Table 3. Timings [mm:ss] of participants for setting up the nPA as a second factor and logging in with it.

	Round 1		Round 2	
	$Group_{CR1}$	$Group_{SM1}$	$Group_{CR2}$	$Group_{SM2}$
Min	3:28	5:57	4:25	5:14
Max	11:08	21:50	8:12	11:22
Range	7:40	15:53	3:47	6:08
Mean	7:47	16:15	5:49	7:21
Median	8:00	18:08	5:20	5:55
Standard Deviation	2:30	5:43	1:23	2:16

did not account for the time the participants took to re-watch the videos or spent idle thinking. The partial task times, alongside each participant's survey scores are depicted in Table 4a and Table 4b in Appendix C.

Most of the participants in round one did not immediately understand what the tasks involved exactly, as it was the first contact with this technology for most of them. This sentiment is supported by the fact that there is only little spread in the run timings it took to fulfill single partial tasks but a rather big spread in the timings of whole runs. Meaning, longer runs account for difficulties in understanding the tasks, not difficulties in fulfilling them. Moreover, as we observed during the study, the participants with longer run times generally had more trouble understanding the tasks than actually completing them. Another clear indicator for this sentiment is that several participants re-watched the videos multiple times and at some point seemingly just blindly followed the depicted steps, without thinking about what they were actually doing.

The participants in round two were not only faster than in round one, there is also substantially less spread in the different run-times as there were fewer outliers. This can be accounted by the fact that the basic installation steps did not lead to any problems in round two. Seemingly, there were also fewer participants who did not understand what they were doing or had to re-watch the videos. Overall, it took $Group_{SM}$ longer to complete the tasks than $Group_{CR}$ in both rounds. Again, we assume that the fact that $Group_{SM}$ had an extra step in their setup process, namely connecting the smartphone to the laptop, is partially to blame. Nonetheless, this extra time does not fully account for the run timings in $Group_{SM1}$ being double the length in $Group_{CR1}$.

Both the participants' *Affinity for Technology Interaction* and *Privacy Concerns* scores in round one are close to the expected population's average [30, 45]. While ATI scores lie on a scale of 1–6, PC scores are distributed over the range 1–7. With ATI scores of 3.5 and 3.3 and PC scores of 4.6 and 5.3 our round one sample did not score unusually high or low in any of the two metrics. While the participants in round two achieved similar results with ATIs of 4.2 and 4.8 and PC scores of 5.4 and 5.2, both scales scored higher than in round one, on average. As can be expected, participants who study or work in a Computer Science-adjacent field tend to have a higher affinity for technology interaction and privacy concerns than a group with less contact with Computer Science and IT.

To summarize, we see considerable potential for improvement in the analyzed aspects. The SUS scores are low in $Group_{SM}$ and slightly above average in $Group_{CR}$ in both rounds. The Usefulness- and Satisfying Scale both scored okay. Lesser tech-savvy users in round one had a lot of difficulties understanding the exact steps the tasks involved. However, they seemed relatively easy to complete once understood, which is depicted in the run timings. Participants in round two had fewer problems understanding and completing the tasks, yet they were more critical overall and gave the system lower scores than round one participants.

5.2   Interview Results

The structure of this section follows three different topics: the system's setup, the system's usage, as well as security concerns and misconceptions. For the analysis, two members of the research team independently coded all answers to the interview's open-ended questions. Afterward, they met to discuss the codes until full agreement was reached. The resulting codebook can be found in Appendix D.

In the following, we address each participant with a unique identifier, which is made up of three components. *SM* or *CR* stands for the participant being in group *smartphone* or group *card reader*, respectively. Secondly, a 1 or 2 represents the round the participant took part in, and lastly, a digit 1–5 depicts the individual participant in the said round.

5.2.1   Setup. Throughout the interview, the participants voiced their concerns about barriers and difficulties, but also their opinions on what they liked and disliked about the system's setup. Eleven participants indicated that they had no particular problems setting up the system, eight of which were in round two. The remaining nine, seven from round one and two from round two, said that they would not have been able to complete the system's setup without the ability to re-watch the videos at least once.

> $CR1_4$: *"I don't think I could have completed the setup without having someone showing me clear instructions on every single step."*

For six of these, five from round one and one from round two, the setup included too many steps. They described the setup process to be too long and complicated. For instance, participant $SM1_1$ said: *"I was overwhelmed by the number of steps I had to remember and fulfill in the right order."* Countering this statement, ten called the system easy and fast to set up. Six of them were participants in round two, and most named the instructional videos to have eased the process a lot:

> $CR2_1$: *"I would have had difficulties without the videos."*

The main advantage mentioned in one way or another was the AusweisApp2's design and structure. Two participants also liked the AusweisApp2's integrated instructions.

> $SM1_1$: *"I liked that the software described the processes with pictures and less text."*

While six participants said not to want to change anything about the setup process, six other participants mentioned the number of different needed tools and programs as too high.

> $SM2_4$: *"There are too many things that I have to have and use."*

The main sentiment was that other 2FA options are much easier to set up than FIDELIO.

A barrier pointed out three times by participants in round one was installing the Firefox plugin. Especially for those who had not installed a browser plugin in Mozilla Firefox before, this was indicated to be a big challenge. The plugin's name was also perceived to be too complicated, making the search unnecessarily difficult.

> $CR1_3$: *"I think that because I already knew how to activate the Add-on, I had fewer difficulties than people who haven't done that before [. . .]. I think that was the hardest part."*

Three participants in round two had an idea to tackle this problem, namely integrating more in-depth instructions into the applications that lead a user through the setup process step-by-step.

> $SM2_3$: *"Something like an assistant [. . .] that gives you step-by-step instructions [. . .] with a lot of pictures."*

As pointed out by three participants, finding the correct option in Google was another big hurdle. As we saw in the screen recordings of round one as well, most had difficulties navigating through the Google interface. In particular, the option to select a security key as a second factor was challenging to find. Seven participants in round one had trouble

finding it or thought they had found it, although actually, they were in the wrong settings menu. The participants in round two had no problems with this aspect.

> $CR1_4$: *"I would simplify [navigating the Google interface] somehow. I wouldn't have found that by myself."*

In most of the interview results, there were no notable differences between $Group_{CR}$ and $Group_{SM}$. When talking about the method to scan the nPA's chip, however, there was a clear trend in $Group_{CR}$ in both rounds to want an alternative, even though at no point in the study we specifically asked about this aspect. Seven participants in $Group_{CR}$ over both rounds mentioned the card reader negatively in one way or another. Participant $CR1_2$, for example, indicated what they most wanted to change about the system was *"that you don't have to use a card reader."* Participant $CR2_1$ added: *"It would be good if you could read the ID card without the USB card reader."*

5.2.2 Usage. Eight participants, three from round one and five from round two, said not to want to use the system at all. In contrast, nine pointed out that they could see themselves using it, four in round one and five in round two. The remaining three, all from round one, indicated only to use the system if it was necessary. Eleven of the twelve who would either be willing to use the system now or in the future were of the opinion, only to use the ID card as a second factor on "important" accounts like financial ones.

> $SM1_2$: *"Yes, I could imagine [using it for] finance accounts, there is no way I would use it for social media."*

Out of those who would not want to use the system, four described it to be too complex. Three, like participant $SM2_1$, mentioned to prefer other alternatives: *"[…] because OTP is better usability-wise and I see fewer disadvantages in it."*

All of this gives us a good idea of the system's acceptance and usability as perceived by potential users, in terms of research questions RQ2 and RQ3. Overall, the system's usage was perceived more positively than its setup. Eleven participants mentioned finding the system's usage easy and fast:

> $SM1_5$: *"I believe that for lesser tech-savvy users, it might be easier to use than second-factor apps because of the comparably simple process."*

Again, the card reader was put in a negative light by three participants, one of whom ($CR2_5$) did not like *"always having to connect the card reader."* Naturally, only participants in $Group_{CR}$ were able to have an opinion on the device at all, since $Group_{SM}$ exclusively used the smartphone and were not informed about the option of using a card reader.

Twelve participants mentioned the system's security to be another advantage. As did participant $SM1_3$ when they said that what they liked most about the system was *"the system's security and that other people have a harder time gaining access [to my accounts]."*

Nine participants described the idea of always having to find their nPA when wanting to log in to their accounts as too arduous and expressed their need for an alternative. So did $SM1_4$, who would most like to change *"that you don't have to scan the ID card because you don't always have it at hand. Maybe there could be some alternative there."* However, nine participants also liked the fact that the system is easily available for most German citizens, as they already have all the necessary hardware at hand.

> $SM2_3$: *"Virtually everyone owns a smartphone, and basically every German citizen has an ID card, meaning that the system is always available as a second factor. Most people carry these things with them anyways."*

On the other hand, remembering one's PIN was mentioned to be another challenge.

> $CR1_3$: *"Always having my ID card with me and remembering my PIN. It's just a lot of prerequisites."*

Finally, some participants in the tech-savvy group from round two had specific suggestions for improvement on the AusweisApp2's UI. For example, $CR2_2$ said that *"the whole app pops up as soon as you start the process and I think that a small popup would be sufficient, considering that it is irritating when you are taken away from the website.".*

5.2.3 Security Concerns and Misconceptions. The following section finds several potential answers to our fourth research question (RQ4) on users' thoughts and concerns when using an ID as a second factor. One statement everyone agreed upon was that using the nPA as a second factor would be more secure than solely using a password to protect an account. Nevertheless, six participants in round one had concerns regarding their personal information's security. Even though nothing but a pseudonym is shared when registering and using the nPA as a second factor, some felt unsure about what could go wrong and who would have access to their personal information.

$CR1_5$: *"I don't know what happens with the data that is read from the chip, especially when Google does it."*

This sentiment is supported by the results from **PP1** of the online-survey (see Table 5 in Appendix C). In round one, every participant except one believed that at least some of the nPA's data would be shared with the service with which the card is being registered. The same participant that did not think that any sensitive data would be shared supported had the highest ATI in round one (4.9) and supported their claim in the interview.

$SM1_5$: *"I don't think that much data is shared. I expect this to be quite compliant with data protection rules."*

Participants in round two generally had fewer concerns regarding their privacy and personal information. Three of them even specifically mentioned not having any concerns. For example, participant $SM2_5$ said that they *"don't really have any concerns. Everything is encrypted, so there shouldn't be a problem."* Two other participants mentioned that even though they were unsure how exactly the back-end works, they would still trust the system. If concerns arose, it was for specific use-cases like using the system on a shared computer.

$SM2_1$: *"If you use the second factor on a laptop that is used by other people who used it in a way that there is some kind of harmful software on it which then can grab data, that might be a problem."*

PP1 from the online-survey yielded different results in round two compared to round one (see Table 5 in Appendix C). While in round one the main focus was on personal information like *Name*, *Date of Birth*, *Nationality*, and *Address*, the participants in round two expected more technical data like *Date of Expiry* or *Date of Issue* to be shared.

$SM2_1$: *"I only selected 'date of expiry' because I thought the second factor could expire, but I am not sure."*

The nPA's availability and possible fallback alternatives were also brought up. Five participants were unsure about what would happen if they lost their nPA and how long it would take for them to regain access.

$SM2_2$: *"I am afraid of what happens when I lose my ID card. I don't know how long it takes until I get a new one, and I might be locked out of my account for four weeks."*

6 DISCUSSION

First and foremost, it should be taken into consideration that FIDELIO, for now, is merely a prototype [36] and a proof of concept rather than a full-fledged, ready-to-publish system that could be used on a big scale. That is also why, apart from FIDELIO's GitLab repository[1], there is little to no information on the system online. However, we are still going to assess its advantages and disadvantages compared to other FIDO2 authenticator alternatives in the context of a fully usable system as we try to paint a picture of how FIDELIO would perform in the real world.

---

[1]https://gitlab.com/adessoAG/FIDELIO, as of August 12, 2022

6.1 Setup & Usage

Despite the given laboratory environment with comprehensive instructional videos and all required hardware at hand, the majority of users in round one had trouble setting up the nPA as a second factor. As there is no user guide or other source of information on how to set up and use eID as a FIDO2 authenticator, we assume FIDELIO's performance in the real world to be worse than most alternatives. Thus, we expect FIDELIO's setup to lead to problems and inconveniences for the average user. The lack of information and guides could be easily counteracted by publishing in-depth user guides, articles, and booklets on how to set up and use FIDELIO from a user perspective. This way, user misconceptions about the system's security and privacy could also be addressed, essentially solving two problems at once. Participants in round two performed a lot better in setting up and using the system, suggesting that FIDELIO could be a viable option for users who know their way around basic installations. Such users with basic IT knowledge, however, seem to be tending to other 2FA options, as was pointed out multiple times during the interviews.

Some of the participants in round one had difficulties installing the browser plugin. Most of them also had trouble finding the correct option in the Google interface as registering a security key was unnecessarily hidden behind a generic "More Options" button. Neither posed noteworthy problems for participants in round two. The service providers are an essential part of making FIDELIO, and generally FIDO2, more accessible for the average user. If it is to succeed and overtake other 2FA alternatives, the corresponding functionalities have to be easily available and convenient to use. Instead of waiting for a large part of their user base to adopt FIDO2 tokens, service providers should, for the sake of their user's security and privacy, maximize FIDO2 tokens' usability as soon as possible. We assume this would also help motivate more users to adopt this way of authentication. A specific way to address this issue in the case of Google would be to remove the "More Options" button and change the wording from "Security Key" to something more general like "Security Token". As of right now, if a user wants to register their nPA or any token that is not a security key as a second factor in their Google account, they have to choose the "Security Key" option. This can be confusing as their token might look very different from the depicted ones.

So far, only a handful of notable service providers support FIDO2 on their platform, which is an obvious prerequisite for FIDELIO. We conducted the study using Google because the FIDELIO browser plugin cannot intercept FIDO2 requests from other service providers like *Twitter* or *Facebook*. Even though both services, in theory, support security keys and thus FIDELIO. If FIDELIO wants to be a competitive FIDO2 authenticator and a viable option for users, it needs to at least support every service provider that implements FIDO2. Naturally, if there is no proper use case for FIDELIO, no one will use it. This sentiment can be related back to the *Chicken-and-Egg Problem* posed by Poller et al. [55]: both service providers and users are waiting for each other to make the first move in adopting new authentication schemes.

As was mentioned by most participants in $Group_{CR}$ in both rounds, the card reader seems to be a poor option for scanning the card's chip. It diminishes eID's advantage of not having to buy a new device, as you would have to for using a hardware key, for example. Also, most modern smartphones already support the necessary NFC functionality, essentially deeming the card reader redundant. Moreover, most users already own a smartphone, carry it with them all the time, and notice their smartphone's loss quickly [10, 24]. On the other hand, scanning the ID card's chip using a smartphone might yet again add additional complexity to the system's setup, raising the barrier for lesser tech-savvy users. This claim is supported by the fact that $Group_{SM2}$ was nine minutes faster on average than $Group_{SM1}$. This discrepancy cannot be ascribed to the participants in round one being generally slower, because the difference between $Group_{CR1}$ and $Group_{SM2}$ is substantially lower. We still recommend depicting the smartphone as the standard way of

scanning the nPA's chip. Taking the participants' reactions to the card reader into consideration, we expect users to be easily scared off by systems that include such a card reader.

An issue users had with the FIDELIO scheme, or rather eID itself, is the eID PIN, as they have to memorize an additional secret. Other FIDO2 authenticators (e.g., hardware keys) work without an additional PIN. By using eID, however, this advantage is eliminated. At the same time, this is FIDELIO's only advantage over security keys like YubiKeys, as the eID PIN adds another security factor, essentially exchanging security with usability.

6.2 Security Concerns and Misconceptions

While all participants agreed that eID as a second factor is more secure than only using a password to protect an account, the vast majority in round one had noteworthy privacy concerns. Nine participants thought that at least some personal information would be shared with the respective service provider (see Table 5 in Appendix C). However, this is not at all the case. No personal information is ever touched in the process of authentication with FIDELIO. Thus, neither the FIDELIO eService nor the service provider gains any knowledge of the user's personal information. This misconception is even more surprising in that the AusweisApp2 client shows the user precisely what data will be read from the nPA's chip before entering the eID PIN and, in the case of FIDELIO, uses the term "pseudonym". Highlighting the word "pseudonym", or explaining in greater detail that no personal information is being processed, could help diminish some user concerns. Also, the wording could be changed to something more descriptive and more user-friendly, as the word "pseudonym" might not sufficiently convey the message to non-tech-savvy users. Participants in round two showed substantially fewer security and privacy misconceptions and expressed their trust in the system during the interview.

Some participants were unsure how easy it would be to misuse a stolen nPA. Firstly, a potential attacker would not only need physical access to the nPA but also its PIN. Even if an attacker got hold of both, the nPA's owner can report the card as lost or stolen and put it on a revocation list. Its current revocation status is checked on every authentication attempt, even using restricted identification, meaning once the card is on a revocation list, it cannot be misused for any purpose. A major disadvantage, on the other hand, is that if the revocation services are unavailable, no authentication can be performed, as happened multiple times even during our study.

If a user loses their nPA, which they had registered as a second factor in the majority of their accounts, they have to go through the process of proving their identity to all of the service providers they had registered their nPA as a second factor with. Since users have an increasing number of accounts in general [11, 29], this procedure can become arduous and tiresome. Direct contact with each service provider has to be established, and we expect only a few service providers to offer a user-friendly and quick way of re-run identity proofing. Some, however, provide the user with *recovery codes* on registration of a FIDO2 token that can be used once to reset the account's second factor. On the one hand, this way of re-run identity proofing is easy and fast, but on the other, substantially less secure.

6.3 Additional Thoughts

Although mandatory, FIDELIO's availability might cause problems as it is not widely deployed yet. For example, using the nPA on at work is most likely not possible as the setup requires installing additional software, which is often restricted. In contrast, YubiKeys can be used on any setup as they do not require additional hard- or software.

Since the FIDELIO plugins have to be implemented in a browser-specific way for intercepting FIDO2 requests, they also need ongoing support in case something about the browser or its workflow changes. Currently, the browser plugin is not actively supported or being worked on, making the whole system volatile. As soon as the browser plugin stops working, the whole system cannot be used. In a worst-case scenario, a potential user cannot access any of the accounts

they have registered their nPA as a second factor with, because their browser cannot intercept the FIDO2 request. This problem does not only apply to the browser plugin. Besides it, the FIDELIO infrastructure consists of a user, a relying party, the nPA, the eID client, the eID server, and the FIDELIO eService. As soon as one party fails to complete its part, the authentication request will not yield a successful result. We witnessed the system's instability several times throughout our study. Twice in three weeks, some party involved in the authentication process had technical issues, leading to the authentication process failing. Since a lesser tech-savvy user also has no way of knowing whether they made a mistake or the complication occurred somewhere along the long FIDELIO authentication process, this is just another source of confusion and frustration.

7 CONCLUSION

In the context of a qualitative usability study, we asked potential users to voice their concerns and opinions on using the German National identity card (nPA) as a second factor in a Google account. We aimed to highlight barriers and difficulties average and tech-savvy users may stumble upon when adopting the system.

Our findings confirm that FIDELIO's security has a lot of potential for a second factor. However, difficulties in the system's setup, unnecessarily complex steps, and security misconceptions for less tech-savvy users led to an overall negative picture. While participants did not immediately reject the system, many struggled to finish the setup in a short time, even with the help of in-depth instructional videos. Furthermore, some participants had difficulties understanding the basic concepts of the interactions between eID and FIDO2. Notably, there was a fear of potential misuse of users' personal information amongst less tech-savvy participants—a subjective threat model that differs from our objective risk assessment. Tech-savvy participants faced substantially fewer issues in the system's setup and usage, however, they pointed out to prefer other second-factor alternatives. Another sentiment that most agreed on was that the system's complexity did not match the convenience needed for the everyday usage of a potentially protected account. Therefore, the majority stated that if they were to use the system, they would only use FIDELIO on "important" accounts.

FIDELIO is a volatile prototype that heavily relies on third parties and service providers, making it less attractive to users looking for a secure and easy-to-use second-factor option. It also offers almost the same security benefits as any FIDO2 hardware token, while being substantially less usable. Hence, we believe that if users are willing to adopt 2FA into their authentication routines, most FIDO2 authenticators are more inviting than FIDELIO.

Despite these negative aspects, FIDELIO is a promising concept making use of FIDO2's characteristic of abstracting from the authenticator and building a good baseline for other authentication schemes that could be compatible with FIDO2. With a potential increase in usage of the eID system, FIDELIO might become a viable 2FA option in the future. If end-users already have the needed eID infrastructure assembled and know their way around the eID client and their nPA's PIN, the barrier to using the nPA as a second factor is substantially lower. For that to happen, however, there are four major points that FIDELIO has to improve on:

- End-users have to experience better education on the eID, FIDO2, and FIDELIO systems.
- The FIDELIO system has to be made more accessible, e.g., the number of pieces of software could be reduced by embedding the eID-client functionality into the FIDELIO browser plugin or vice-versa.
- The FIDELIO browser plugin and FIDELIO eService need ongoing support with regular software updates conforming to potential web browser updates.
- The FIDELIO browser plugin has to be compatible with more online services, to create more potential use-cases.

ACKNOWLEDGMENTS

REFERENCES

[1] Aniqa Alam, Robert Biddle, and Elizabeth Stobert. 2021. Emics and Etics of Usable Security: Culturally-Specific or Culturally-Universal?. In *International Conference on Human-Computer Interaction (HCII '21)*. Springer, Virtual Conference, 22–40.

[2] Daniel V. Bailey, Markus Dürmuth, and Christof Paar. 2014. Statistics on Password Re-use and Adaptive Strength for Financial Accounts. In *Security and Cryptography for Networks (SCN '14)*. Springer, Amalfi, Italy, 218–235.

[3] Joseph Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *IEEE Symposium on Security and Privacy (SP '12)*. IEEE, San Jose, California, USA, 538–552.

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

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

[6] Joseph Bonneau and Sören Preibusch. 2010. The Password Thicket: Technical and Market Failures in Human Authentication on the Web. In *Workshop on the Economics of Information Security (WEIS '10)*. ACM, Cambridge, Massachusetts, USA.

[7] Joseph Bonneau and Sören Preibusch. 2010. The Password Thicket: Technical and Market Failures in Human Authentication on the Web. In *Workshop on the Economics of Information Security (WEIS '10)*. ACM, Cambridge, Massachusetts, USA.

[8] John Brooke. 1996. SUS: A Quick and Dirty Usability Scale. In *Usability Evaluation in Industry*, Patrick W. Jordan, Bruce Thomas, Bernard Weerdmeester, and Ian Lyall McClelland (Eds.). CRC Press, London, United Kingdom, Chapter 21, 189–194.

[9] John Brooke. 2013. SUS: A Retrospective. *Journal of Usability Studies* 8, 2 (Feb. 2013), 29–40.

[10] Steve Brunswick. 2009. eCommerce Fraud – Time to Act? *Card Technology Today* 21, 1 (Jan. 2009), 12–13.

[11] Oliver Burkeman. 2012. Online Passwords: Keep It Complicated. https://www.theguardian.com/technology/2012/oct/05/online-security-passwords-tricks-hacking, as of August 12, 2022.

[12] Pedro Canahuati. 2019. Keeping Passwords Secure. https://newsroom.fb.com/news/2019/03/keeping-passwords-secure/, as of August 12, 2022.

[13] Claude Castelluccia, Abdelberi Chaabane, Markus Dürmuth, and Daniele Perito. 2013. When Privacy Meets Security: Leveraging Personal Information for Password Cracking. *CoRR* abs/1304.6584 (April 2013), 1–16.

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

[15] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Faith Cranor, and Nicolas Christin. 2018. "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)*. ACM, Montreal, Quebec, Canada, 456:1–456:11.

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

[17] Sanchari Das, Andrew Kim, Ben Jelen, Lesa Huber, and L. Jean Camp. 2021. Non-Inclusive Online Security: Older Adults' Experience with Two-Factor Authentication. In *Hawaii International Conference on System Sciences (HICSS '21)*. AIS, Kauai, Hawaii, USA, 6472–6481.

[18] Sanchari Das, Andrew Kim, Ben Jelen, Joshua Streiff, L. Jean Camp, and Lesa Huber. 2019. Towards Implementing Inclusive Authentication Technologies for Older Adults. In *Who Are You?! Adventures in Authentication Workshop (WAY '19)*. Santa Clara, California, USA, 1–5.

[19] Sanchari Das, Andrew Kim, Ben Jelen, Joshua Streiff, L. Jean Camp, and Lesa Huber. 2020. Why Don't Older Adults Adopt Two-Factor Authentication?. In *SIGCHI Workshop on Designing Interactions for the Ageing Populations (CHI EA '20)*. Honolulu, Hawaii, USA, 1–5.

[20] Sanchari Das, Gianpaolo Russo, Andrew C Dingman, Jayati Dev, Olivia Kenny, and L. Jean Camp. 2017. A Qualitative Study on Usability and Acceptability of Yubico Security Key. In *Workshop on Socio-Technical Aspects in Security and Trust (STAST '17)*. ACM, Orlando, Florida, USA, 28–39.

[21] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2014. A Comparative Usability Study of Two-Factor Authentication. In *Workshop on Usable Security (USEC '14)*. ISOC, San Diego, California, USA.

[22] Matteo Dell'Amico, Pietro Michiardi, and Yves Roudier. 2010. Password Strength: An Empirical Analysis. In *Conference on Information Communications (INFOCOM '10)*. IEEE, San Diego, California, USA, 983–991.

[23] Bryan Dosono, Jordan Hayes, and Yang Wang. 2015. "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In *Symposium on Usable Privacy and Security (SOUPS '15)*. USENIX, Ottawa, Canada, 151–168.

[24] Nesi Dragoljub. 2007. Stronger Security. *Card Technology Today* 19, 1 (Jan. 2007), 9–10.

[25] The European Parliament and the Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119/1.

[26] Facebook, Inc. 2011. A New Suite of Safety Tools. https://www.facebook.com/notes/10160198855746729, as of August 12, 2022.

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

[28] Frank Felden, Taavi Einaste, Thilo Zelt, Mario Müller, Patrick Bauer, Hendrik Lume, Sabine Siegert, and Hoffmann Till. 2020. Ten Years Electronic Identity: How Germany Can Establish a Successful eID Ecosystem. https://nortal.com/de/blog/ten-years-electronic-identity-how-germany-can-establish-a-successful-eid-ecosystem/, as of August 12, 2022.

[29] Dinei Florêncio and Cormac Herley. 2007. A Large-scale Study of Web Password Habits. In *The World Wide Web Conference (WWW '07)*. ACM, Banff, Alberta, Canada, 657–666.

[30] Thomas Franke, Christiane Attig, and Daniel Wessel. 2018. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human-Computer Interaction* 35, 6 (March 2018), 456–467.

[31] Maximilian Golla, Theodor Schnitzler, and Markus Dürmuth. 2018. "Will Any Password Do?" Exploring Rate-Limiting on the Web. In *Who Are You?! Adventures in Authentication Workshop (WAY '18)*. USENIX, Baltimore, Maryland, USA.

[32] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking. *Computers & Security* 30, 4 (June 2011), 208–220.

[33] Weili Han, Zhigong Li, Minyue Ni, Guofei Gu, and Wenyuan Xu. 2018. Shadow Attacks Based on Password Reuses: A Quantitative Empirical Analysis. *IEEE Transactions on Dependable and Secure Computing* 15, 2 (April 2018), 309–320.

[34] Marian Harbach, Sascha Fahl, Matthias Rieger, and Matthew Smith. 2013. On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards. In *Privacy Enhancing Technologies Symposium (PETS '13)*. Springer, Bloomington, Indiana, USA, 245–264.

[35] Christian Kahlo. 2021. WebAuthn-eID for Firefox. https://addons.mozilla.org/en-US/firefox/addon/webauthn-eid-for-firefox/, as of August 12, 2022.

[36] Christian Kahlo and Frank Aufmhoff. 2017. FIDELIO eService specification. https://gitlab.com/adessoAG/FIDELIO/Documentation/-/raw/master/FIDELIOeService_V1_1.pdf, as of August 12, 2022.

[37] Christian Kahlo and Markus Krebs. 2020. Description of the Business Process FIDELIO. https://gitlab.com/adessoAG/FIDELIO/Documentation/-/raw/master/FIDELIO_Dienstbeschreibung_V1_3.pdf, as of August 12, 2022.

[38] Markus Keil. 2021. Introduction eID and FIDO. https://youtu.be/jFpprzm0kp0, as of August 12, 2022.

[39] Markus Keil. 2021. Setup Configuration. https://youtu.be/Fefg5U8k8P0, as of August 12, 2022.

[40] Markus Keil. 2021. Setup of the nPA as a Second Factor for Google (Card Reader). https://youtu.be/Z3KJyNZjb3w, as of August 12, 2022.

[41] Markus Keil. 2021. Setup of the nPA as a Second Factor for Google (Smartphone). https://youtu.be/Z-XkBIAl6Ro, as of August 12, 2022.

[42] Guemmy Kim. 2022. Making You Safer With 2SV. https://blog.google/technology/safety-security/reducing-account-hijacking/, as of August 12, 2022.

[43] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. 2015. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. In *Symposium on Network and Distributed System Security (NDSS '15)*. ISOC, San Diego, California, USA.

[44] Johannes Kunke, Stephan Wiefling, Markus Ullmann, and Luigi Lo Iacono. 2021. Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication. In *Open Identity Summit (OID '21)*. Gesellschaft für Informatik e.V., Virtual Conference, 59–70.

[45] Markus Langer, Cornelius J. König, and Andromachi Fitili. 2018. Information as a Double-Edged Sword: The Role of Computer Experience and Information on Applicant Reactions Towards Novel Technologies for Personnel Selection. *Computers in Human Behavior* 81 (April 2018), 19–30.

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

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

[48] AbdelKarim Mardini and Guemmy Kim. 2021. Making Sign-in Safer and More Convenient. https://blog.google/technology/safety-security/making-sign-safer-and-more-convenient/, as of August 12, 2022.

[49] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2016. Usability and Security of Text Passwords on Mobile Devices. In *ACM Conference on Human Factors in Computing Systems (CHI '16)*. ACM, San Jose, California, USA, 527–539.

[50] Microsoft, Inc. 2020. Sign in to Your Accounts Using the Microsoft Authenticator App. https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-sign-in, as of August 12, 2022.

[51] Federal Ministry of the Interior and Community. 2019. Digital Identification With the German Online ID Card - Information for Companies and Authorities. https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/EN/anwenderhandbuch.pdf, as of August 12, 2022.

[52] Florian Otterbein, Tim Ohlendorf, and Marian Margraf. 2016. The German eID as an Authentication Token on Android Devices. *International Journal of Computer Science and Information Security* 14, 12 (Dec. 2016), 198–205.

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

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

[55] Andreas Poller, Ulrich Waldmann, Sven Vowé, and Sven Türpe. 2012. Electronic Identity Cards for User Authentication - Promise and Practice. *IEEE Security & Privacy* 10, 1 (Jan. 2012), 46–54.

[56] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2021. Why Older Adults (Don't) Use Password Managers. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 73–90.

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

[58] Dennis Strouble, Gregory M. Shechtman, and Alan S. Alsop. 2009. Productivity and Usability Effects of Using a Two-Factor Security System. In *Southern Association for Information Systems Conference (SAIS '09)*. AIS, Charleston, South Carolina, USA, 196–201.

[59] Valentyna Tsap, Ingrid Pappel, and Dirk Draheim. 2019. Factors Affecting e-ID Public Acceptance: A Literature Review. In *International Conference on Electronic Government and the Information Systems Perspective (EGOVIS '19)*. Springer, Virtual Conference, 176–188.

[60] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. 2021. Is Real-Time Phishing Eliminated With FIDO? Social Engineering Downgrade Attacks Against FIDO Protocols. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 3811–3828.

[61] U.S. Department of Homeland Security. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of August 12, 2022.

[62] Jinke D. Van Der Laan, Adriaan Heino, and Dick De Waard. 1997. A Simple Procedure for the Assessment of Acceptance of Advanced Transport Telematics. *Transportation Research Part C: Emerging Technologies* 5, 1 (Feb. 1997), 1–10.

[63] Catherine S. Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. 2009. User Perceptions of Security, Convenience and Usability for eBanking Authentication Tokens. *Computers & Security* 28, 1–2 (Feb. 2009), 47–62.

[64] Catherine S. Weir, Gary Douglas, Tim Richardson, and Mervyn Jack. 2010. Usable Security: User Preferences for Authentication Methods in eBanking and the Effects of Experience. *Interacting with Computers* 22, 3 (May 2010), 153–164.

A STUDY PART 1: HANDS-ON TASK

Each participant went through the following steps before answering the quantitative questions and taking the interview:

(1) Watching three educational videos explaining eID, FIDO2, and how to register the nPA as a second factor in a Google account.

(2) Setting up a given nPA in a Google account as a second factor. The PIN for the nPA and the login data for the Google account were provided.

(3) Logging into the Google account using the nPA as a second factor.

System Usability Score (SUS)

For the assessment of the authentication system you just used, please select your agreement/disagreement with the following statements.

Please select the answer choice that most closely matches how you feel about the following statements:

SUS1 I think that I would like to use this system frequently.

SUS2 I found the system unnecessarily complex.

SUS3 I thought the system was easy to use.

SUS4 I think that I would need the support of a technical person to be able to use this system.

SUS5 I found the various functions in this system were well integrated.

SUS6 I thought there was too much inconsistency in this system.

SUS7 I would imagine that most people would learn to use this system very quickly.

SUS8 I found the system very awkward to use.

SUS9 I felt very confident using the system.

SUS10 I needed to learn a lot of things before I could get going with this system.

○ Strongly disagree ○ Disagree ○ Neither agree or disagree ○ Agree ○ Strongly agree

Acceptance (AC)

Please judge the presented authentication method on the following adjectives.

Useless	○	○	○	○	○	Useful
Unpleasant	○	○	○	○	○	Pleasant
Bad	○	○	○	○	○	Good
Annoying	○	○	○	○	○	Nice
Superfluous	○	○	○	○	○	Effective
Irritating	○	○	○	○	○	Likeable
Worthless	○	○	○	○	○	Assisting
Undesireable	○	○	○	○	○	Desireable
Sleep-Inducing	○	○	○	○	○	Raising Alertness

Affinity for Technology Interaction (ATI)

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

ATI1 I like to occupy myself in greater detail with technical systems.

ATI2 I like testing the functions of new technical systems.

ATI3 I predominantly deal with technical systems because I have to.

ATI4 When I have a new technical system in front of me, I try it out intensively.

ATI5 I enjoy spending time becoming acquainted with a new technical system.

ATI6 It is enough for me that a technical system works; I don't care how or why.

ATI7 I try to understand how a technical system exactly works.

ATI8 It is enough for me to know the basic functions of a technical system.

ATI9 I try to make full use of the capabilities of a technical system.

○ Completely disagree   ○ Largely disagree   ○ Slightly disagree   ○ Slightly agree   ○ Largely agree   ○ Completely agree

Privacy Concerns (PC)

Please state how much you agree or disagree to the following statements.

PC1 I am concerned that companies are collecting too much information about me

PC2 I am concerned about my privacy

PC3 To me it is important to keep my privacy intact

PC4 Novel technologies are threatening privacy increasingly

○ Strongly disagree   ○ Disagree   ○ Somewhat disagree   ○ Neither agree or disagree

○ Somewhat agree   ○ Agree   ○ Strongly agree

Awareness

A1 Were you aware that the German ID card offers an online functionality (eID)?

○ Yes   ○ No

A2 Were you aware that the FIDO2 standard for web authentication is compatible with eID?

○ Yes   ○ No

Privacy Perception

PP1 What data do you think is shared with the services you register with? (Select all that apply)

☐ Nationality ☐ Name ☐ Date of birth ☐ Colour of eye ☐ Address ☐ Date of issue ☐ Height

☐ Date of expiry ☐ Place of birth ☐ None of the above

(Note: "None of the above" was always the last option, all others were randomized for each participant.)

Demography

D1 Which of these best describes your current gender identity?

○ Woman ○ Man ○ Non-binary ○ Prefer to self-describe: _____ ○ Prefer not to answer

D2 What is the highest degree or level of school you have completed?

○ No schooling completed ○ Some high school, no diploma ○ High school graduate, diploma, or equivalent

○ Trade, technical, or vocational training ○ Bachelor's degree ○ Master's degree ○ Doctoral degree

○ Prefer not to answer

D3 Select your age.

○ 18–24 ○ 25–34 ○ 35–44 ○ 45–54 ○ 55–64 ○ 65–74 ○ 75+ ○ Prefer not to answer

D4 Which of the following best describes your educational background or job field?

○ I have an education in, or work in, the field of computer science, computer engineering or IT.

○ I do not have an education in, nor do I work in, the field of computer science, computer engineering or IT.

○ Prefer not to answer

B STUDY PART 2: INTERVIEW

Q1 Have you used eID before? If so, what for?

Q2 Did you run into any technical problems or difficulties while setting up the ID card as a second factor? If so, please describe them.

For the following two questions, we will focus on the procedure of *setting up* the ID card as a second factor.

Q3 What things did you like best about the procedure of setting up the ID card as a second factor?

Q4 What would you most want to change about the procedure of setting up the ID card as a second factor?

For the following two questions, we will focus on the procedure of *using* the ID card as a second factor.

Q5 What things did you like best about the procedure of using the ID card as a second factor?

Q6 What would you most want to change about the procedure of using the ID card as a second factor?

Q7 What advantages do you see in using the ID card as a second factor?

Q8 What disadvantages do you see in using the ID card as a second factor?

Q9 Would you use your ID card as a second factor yourself? If you would, on what kinds of accounts would you use it? If you wouldn't, why not?

Q10 What concerns would you have using your ID card as a second factor?

Q11 Would you rank using eID as a second factor as more or less secure than using a password as a single factor? Please explain your choice.

C   ADDITIONAL TABLES

Table 4. Participants' scores for each of the four standardized metrics and timings [mm:ss] for setting up the nPA as a second factor and logging in with it. Note, the sum of all partial timings does not equal the total completion time because the partial timings do not account for the time the participants took to re-watch the videos or spent idle thinking.

(a) Scores and timings for the participants with a mixed background from round one.

	$CR1_1$	$CR1_2$	$CR1_3$	$CR1_4$	$CR1_5$	$SM1_1$	$SM1_2$	$SM1_3$	$SM1_4$	$SM1_5$
SUS	50	83	70	93	63	18	73	70	63	85
Acceptance										
Usefulness	1.0	1.6	0.8	2.0	0.8	−0.2	1.6	1.0	1.2	1.4
Satisfying	0.5	1.3	0.3	2.0	0.0	−1.0	1.0	0.8	1.0	0.8
ATI	4.2	4.8	2.4	5.0	1.0	2.8	2.9	4.0	1.8	4.9
PC	5.3	3.5	4.3	4.8	5.0	5.5	5.8	6.0	3.8	5.3
Partial Task Timings										
Install AusweisApp2	1:15	0:39	0:36	0:50	0:58	1:12	0:43	0:48	1:09	0:53
Install Plugin	0:35	0:30	0:24	2:20	0:59	1:07	0:30	1:08	4:37	0:38
Connect Smartphone	na	na	na	na	na	3:57	3:11	1:00	1:40	0:28
Navigate Google	1:30	2:22	1:06	2:00	2:17	7:57	4:45	1:16	5:43	1:09
Total Completion Time	11:08	7:23	3:28	8:00	8:55	21:50	18:08	14:35	20:44	5:57

(b) Scores and timings for the participants with a tech background from round two.

	$CR2_1$	$CR2_2$	$CR2_3$	$CR2_4$	$CR2_5$	$SM2_1$	$SM2_2$	$SM2_3$	$SM2_4$	$SM2_5$
SUS	35	80	93	88	80	40	70	60	53	73
Acceptance										
Usefulness	0.2	0.8	2.0	1.6	1.0	0.4	0.8	0.0	0.8	1.6
Satisfying	0.3	0.5	2.0	2.0	1.0	−0.5	0.3	0.3	−0.3	1.5
ATI	4.6	5.6	4.2	2.0	4.4	5.4	4.6	5.2	5.0	3.9
PC	5.6	5.0	4.0	5.5	6.5	6.3	5.3	4.0	4.8	5.5
Partial Task Timings										
Install AusweisApp2	1:04	0:45	0:56	1:25	0:45	0:42	0:44	0:55	0:51	0:45
Install Plugin	0:25	0:39	0:33	0:52	1:15	0:15	0:26	0:21	0:25	1:01
Connect Smartphone	na	na	na	na	na	1:23	1:20	1:10	1:02	1:16
Navigate Google	1:42	1:28	1:23	2:00	1:50	0:50	1:14	1:09	1:00	1:25
Total Completion Time	4:41	5:20	4:25	6:26	8:12	5:14	8:22	5:55	5:54	11:22

Table 5. Overview of answers to **PP1**: What data do you think is shared with the services you register with? (Select all that apply)

	Round 1			Round 2		
	$Group_{CR1}$	$Group_{SM1}$	Combined	$Group_{CR2}$	$Group_{SM2}$	Combined
Name	4	5	9	1	2	3
Date of Expiry	3	5	8	3	3	6
Date of Birth	4	3	7	1	1	2
Nationality	2	4	6	1	0	1
Address	4	2	6	1	0	1
Date of Issue	2	4	6	0	3	3
Place of Birth	2	3	5	1	0	1
Height	0	3	3	1	0	1
Colour of Eye	0	2	2	0	0	0
None of the Above	1	0	1	2	1	3

D CODEBOOKS

Table 6. Codebook for Q1–Q6.

Code	Freq.	Description	Example
Q1: Have you used eID before?			
No	17	Has not used eID before the study.	*"No, because I haven't found a proper use-case."*($SM2_1$)
Yes	3	Has used eID before the study.	*"Yes, I tried applying for BaföG online, but I failed."*($CR1_5$)
Q2: Did you run into any technical problems or difficulties while setting up the ID card as a second factor?			
Did not need help/videos	11	The participant states that they did not have problems and did not need to re-watch the videos	*"No, not really. It was easy."* ($CR2_2$)
Needed help/videos	9	The participant states that they would not want to dispense given help	*"I don't think I could have completed the setup, without having someone showing me clear instructions on every single step."* ($CR1_4$)
Too many steps	6	The participant calls the setup process too long and complicated	*"I was overwhelmed by the amount of steps I had to remember and fulfill in the right order."* ($SM1_1$)
Technical Issues	2	The participant encountered provider-sided technical issues	*"Yes, I encountered a problem. There was an unknown technical issue that hindered me from continuing."* ($CR1_4$)
Q3: What did you like best about the procedure of setting up the ID card as a second factor?			
Easy and fast	10	The participant calls the setup process easy and fast	*"I perceived it to be structured relatively simple, it wasn't unnecessarily complex."* ($SM1_5$)
Easy->with video	6	The participant mentions the videos to have simplified the setup procedure	*"I would have had difficulties without the videos."* ($CR2_1$)
AusweisApp2 advantages	6	The participant mentions an advantage of the AusweisApp2	*"I really liked that there was a setup software, that gave instructions."* ($CR1_1$)
Browser AddOn	2	The participant mentions the browser AddOn to be convenient	*"It was convenient that this Firefox AddOn already exists."* ($SM2_2$)
Instructions	2	The participant positively mentions the instructions integrated into the softwares	*"I liked that the software described the processes with pictures and less text."* ($SM1_1$)
Smartphone as cardreader	2	The participant likes that a smartphone can be used as reading device	*"What I also like is that I don't have to buy a cardreader but use my smartphone."* ($SM2_4$)
Q4: What would you most want to change about the procedure of setting up the ID card as a second factor?			
No changes	6	The participant does not want to change anything	*"I think it was alright, I wouldn't want to change anything."* ($CR2_5$)
Multiple parts	6	The participant mentions the number of different tools as too high	*"There are too many things that I have to have and use."* ($SM2_4$)
Browser AddOn	3	The participant mentions the Mozilla Firefox AddOn to be difficult to find and install	*"I think that because I already knew how to activate the AddOn, I had less difficulties than people who haven't done that before […]. I think that was the hardest part."*($CR1_3$)
Google option	3	The participant states that it was difficult for them to find the correct option in the Google interface	*"I would maybe make [navigating the Google interface] easier somehow, because I wouldn't have found that by myself."* ($CR1_4$)
Integrated instructions	3	The participant states that integrating instructions into the applications would simplify the process	*"Something like an assistant […] that gives you step-by-step instructions […] with a lot of pictures."* ($SM2_3$)
Card reader	2	The participant expresses their need for an alternative to the card reader	*"I, for one, don't have such a card reader […] so that would be impractical for me."* ($CR1_5$)
Q5: What did you like best about the procedure of using the ID card as a second factor?			
System security	12	The participant believes the system to be comparably secure	*"[…] the system's security and that other people have a harder time gaining access [to my accounts]."* ($SM1_3$)
Easy and fast usage	11	The participant perceived the system's usage as easy and fast	*"I believe that for lesser tech-savvy users it might be easier to use than second-factor Apps, because of the simple process."* ($SM1_5$)
No additional hardware	3	The participant likes that no additional hardware has to be obtained	*"[…] by now everyone has such an ID card, so there is no extra effort. Also everyone owns a smartphone."* ($SM2_5$)
Q6: What would you most want to change about the procedure of using the ID card as a second factor?			
Simpler procedure	6	The participant finds the usage procedure too burdensome	*"Compared to an authenticator app the process takes way longer."* ($SM2_4$)
No changes	5	The participant does not want to change anything	*"I wouldn't change anything about the usage process."* ($SM1_4$)
UI	4	The participant criticizes the system's UI	*"[…] the whole app pops up, as soon as you start the process and I think that a small popup would be sufficient, considering that it is irritating when you are taken away from the website."* ($CR2_2$)
Less equipment	4	The participant criticizes the high amount of needed equipment	*"Also there is just a little much equipment needed."* ($CR2_1$)
Carrying ID	2	The participant criticizes the aspect of always having to carry all the hardware	*"The fact that I always have to carry my second factor with me is annoying."* ($CR2_4$)

Table 7. Codebook for **Q7–Q11**.

Code	Freq.	Description	Example
		Q7: What advantages do you see in using the ID card as a second factor?	
Availability of ID	9	The participant likes the system's availability	*"Virtually everyone owns a smartphone and basically every German citizen has an ID card, meaning that the system is always available as a second factor. Most people carry these things with them anyways."* (SM2$_3$)
Security	8	The participant sees the system's security as an advantage	*"Two-factor authentication is obviously way more secure than just a password if you want to protect your accounts from phishing and other attacks."* (SM2$_5$)
Easy and fast	3	The participant mentions the ease of use as and advantage	*"Maybe it's more secure and faster than another password or a text message or call."* (SM1$_2$)
		Q8: What disadvantages do you see in using the ID card as a second factor?	
Finding ID	9	The participant mentions the process of finding and getting out their ID card when using the system to be too exhausting	*"that you don't have to scan the ID card because you don't always have it at hand. Maybe there could be some alternative there."* (SM1$_4$)
Losing ID	4	The participant mentions losing the ID card to be a potential threat	*"If your ID is gone, your authentication is gone and you don't have access."* (SM2$_4$)
Card reader	3	The participant sees the card reader as a disadvantage	*"[…] always having to connect the card reader."* (CR2$_5$)
Privacy	6	The participant expresses a lack of clarity regarding the system's privacy	*"I am unsure what happens with the data that is read from the chip, especially when Google does it."* (CR1$_5$)
		Q9: Would you use your ID as a second factor yourself?	
Yes	9	The participant would use the system	*"Yes, I think I would use it."* (SM1$_3$)
Only if necessary	3	The participant would only use the system if it were necessary	*"If at some point it is mandatory to use the system, I would, but right now if I don't necessarily need it, I wouldn't use it."* (SM1$_4$)
No	8	The participant would not be willing to use the system	*"I don't think I would use the system, I like other alternatives better."* (CR1$_3$)
Yes->important accounts	9	The participant would only use the system for important accounts (e.g., finances)	*"Yes, I could imagine [using it for] finance accounts, there is no way I would use it for social media[…]."* (SM1$_2$)
Only if necessary ->important accounts	2	The participant would only use the system for important accounts (e.g., finances)	*"I wouldn't really use it on social media, only accounts that are important to me."* (CR1$_4$)
Yes->all accounts	1	The participant would use the system for all their accounts	*"I don't care about the kind of account. I would use it everywhere."* (CR2$_2$)
No->too complex	4	The participant would not use the system because of its complexity	*"Probably not, because always having to do this is just too burdensome if I merely want to log in to PayPal for instance."* (SM2$_4$)
No->better alternatives	3	The participant would not use the system because they like other alternatives better	*"No, because OTP is better usability-wise and I see less disadvantages in it."* (SM2$_1$)
		Q10: What concerns would you have using your ID card as a second factor?	
Privacy	6	The participant has concerns about what data is shared with whom	*"That my personal information is stolen from the ID card."* (CR1$_5$)
Lose/Change ID	5	The participant is worried to be locked out of their account if the ID card was unavailable for a longer period of time	*"I am afraid of what happens when I lose my ID card. I don't know how long it takes until I get a new one and I might be locked out of my account for four weeks."* (SM2$_2$)
No concerns	3	The participant has no concerns regarding the system	*"I don't really have any concerns. Everything is encrypted so there shouldn't be a problem there."* (SM2$_5$)
Shared Computer	2	The participant is concerned about using the system on shared computers	*"If you use the second factor on a laptop that is used by other people as well, who used it in a way that there is some kind of harmful software on it, which then can grab data, that might be a problem."* (SM2$_1$)
Trust	2	Even though the participant is unsure how the system works, they trust its security	*"The whole concept and how exactly it works is still unclear to me. […] You are never fully safe but in this case I wouldn't worry too much."* (CR2$_5$)
		Q11: Would you rank this system as more or less secure than only using a password?	
More secure	20	The participant thinks that the system is more secure than only using a password	*"Definitely more secure because it is a second factor. Passwords are being leaked a lot nowadays, meaning that every additional factor improves the security."* (SM2$_3$)

E RECRUITMENT MATERIAL

Fig. 2. Flyer used for round one to recruit users with a mixed background.

Fig. 3. Flyer used for round two to recruit users with a tech background.