2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) | 979-8-3503-2720-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/EuroSPW59978.2023.00070

"As Usual, I Needed Assistance of a Seeing Person": Experiences and Challenges of People with Disabilities and Authentication Methods

Ahmet Erinola
Materna Information & Communications SE
Dortmund, Germany
ahmet.erinola@materna.group

Annalina Buckmann
Ruhr University Bochum
Bochum, Germany
annalina.buckmann@ruhr-uni-bochum.de

Jennifer Friedauer
Ruhr University Bochum
Bochum, Germany
jennifer.friedauer@ruhr-uni-bochum.de

Aslı Yardım
Ruhr University Bochum
Bochum, Germany
asli.yardim@ruhr-uni-bochum.de

M. Angela Sasse
Ruhr University Bochum
Bochum, Germany
martina.sasse@ruhr-uni-bochum.de

***Abstract*— According to the World Health Organization, about 16% of the world's population live with a disability. While they could benefit from digital products and services, users with disabilities often face severe accessibility issues: tasks can only be completed with difficulty, a considerable investment of time, or with assistance of technologies or other people. Further, to access these products and services, they need to authenticate. The accessibility of authentication methods for users with disabilities has not been studied in depth. We use an accessible study design to conduct 13 semi-structured interviews with people with physical, hearing, visual, cognitive, or multiple impairments to better understand the accessibility issues they face when using knowledge- or token-based, and biometric authentication. Our qualitative content analysis shows that none of the commonly available authentication methods is fully accessible to participants, causing them to abandon services or develop workarounds that reduce their own security and privacy. Our results also reveal the role of assistive technologies and human assistants in the authentication experience of users with disabilities. We conclude by encouraging fellow researchers and practitioners to reflect on assisted access when designing security mechanisms, to include people with disabilities using accessible study designs, and to keep in mind that accessible security is about more than usability – to further benefit users without disabilities as well.**

1. Introduction

People with disabilities often face severe accessibility challenges when using digital products and services which could benefit them. These challenges are not well-researched. Renaud [55] argued that accessibility should be considered as equally important as usability in the design of security systems to include the needs of vast parts of the population with a range of disabilities, to prevent exposing them to more risks. In fact, according to the World Health Organization (WHO) [53], 16% of the world's population, i.e., 1 in 6 people, has some form of disability – and everyone can become disabled during the course of life. In 2010, Fritsch et al. [25] argued that "the acknowledgment of user diversity, in contrast to modelling an average user, or a typical user, is important", and several guidelines and legal norms, such as the Web Content Accessibility Guideline (WCAG) [69], oblige to ensure accessibility for everyone [2], [49], [66]. However, these often do not specifically address security and privacy (S&P). Only the new WCAG 2.2 [70] (in draft) introduces the criterion for accessible authentication. Despite these existing guidelines, norms, and laws, researchers conclude that "for many, security measures are often exasperatingly inaccessible" [56]. To ensure the secure use of digital technologies for people with different abilities, an "inclusive approach to cybersecurity" is necessary [56] – especially as more and more products and services are moved online. Most of these require some form of authentication. They can be found in applications, apps, and websites, from e-mails to online commerce or online banking to social media, to prevent unauthorized users from accessing sensitive information [58], [64].

The (lack of) usability of different authentication methods for "average, typical users" [25] has been studied in-depth (e.g., [1], [13], [29]), and new approaches are being developed, like FIDO2 [14], [17], [28]. Still, the accessibility of authentication for users with disabilities is rarely considered. The purpose of our study therefore was to understand how accessible these authentication methods are – including the 3 tasks of enrolment, authentication, and recovery. Steves et al. [65] found that users who struggle with authentication methods develop coping strategies. So our second goal was to identify the workarounds and coping strategies people with disabilities develop. Finally, we wanted to understand what risks to S&P those coping strategies might harbour.

Within an exploratory study design, we conducted 13 semi-structured interviews with people with different disabilities to better understand their challenges with knowledge-based authentication (KBA), token-based authentication (TBA), and biometric authentication (BA) and the workarounds they engage in. In particular, we wanted to know how these users perceive and manage challenges with authentication methods that influence their S&P.

These 3 questions guide our study:

DOI 10.1109/EuroSPW59978.2023.00070

RQ1: What are the experiences of people with disabilities when using authentication methods? What challenges do they face?

RQ2: What workarounds and coping strategies do they use to deal with these challenges in everyday life?

RQ3: What security and privacy risks are associated with these challenges and workarounds?

Our results show that **none** of the existing authentication methods are fully accessible for our participants, leading them to either abandon the method or engage in workarounds that affect their S&P. Further, all except 1 participant relied on assistive technologies or human assistance to use digital technologies in their everyday life, which is not accounted for by the design of authentication methods. In some cases, they needed extra support merely to cope with unusable authentication methods. Assisted access introduces new challenges for trust, security, and privacy in authentication and further emphasizes the importance of interoperability between socio-technical systems to ensure accessibility for people with disabilities – and further large parts of the population without disabilities. The remainder of this paper is structured as follows: First, we ground our research in related work in Section 2 before introducing our accessible study design in Section 3. We then present and discuss our results and recommendations for improvement in Section 4 and Section 5 before concluding our work in Section 6.

2. Related Work

We now present the discussion on inclusive and accessible S&P before giving an overview on research on people with disabilities and authentication.

2.1. Inclusive and Accessible Security & Privacy

Studies on people with disabilities are scarce in S&P. Reviewing user studies in S&P from 2008-2018, Kaur et al. [38] found that recruitment is dominated by convenience sampling, often involving university students "as a convenient proxy for end-user [...] populations". This results in a narrow picture of users that assumes they are fully abled, cognitively unimpaired, and have the necessary resources and required dexterity to interact with security systems [56]. Apart from recruitment, people with disabilities can effectively be excluded by the study designs, depending on the impairment. Lack of research and support can leave them more vulnerable in the realm of S&P [56], [72] – and may violate existing guidelines and regulations [72]. In 2017, Wang [72] advocated for a third wave of security research, aiming at designing S&P mechanisms "that are inclusive to people with various characteristics, abilities, needs and values". This inclusive S&P should actively involve under-served populations in user studies, risk assessments, and in the "design and evaluation of S&P technologies [...] that involve human efforts". Similarly, Renaud [55] argued to include the dimension of accessibility, next to security and usability, into human-centered security. Otherwise, we "risk ignoring the needs of vast swathes of the population with a range of disabilities" [55] – or: "an estimated 1.3 billion people" [53]. While guidelines and legal mandates are focusing on web accessibility [2], [49], [54], [66], [69], Renaud finds that especially assistive technologies pose problems for security, as they are "designed to ease the usual web-related activities, not cyber security actions" and that "usability of cyber security mechanisms is not the same as usability of a web page" [55]. Extending this argument, Renaud & Coles-Kemp [56] argue to further take into account socio-economic and political factors, as users with disabilities are not only affected by inaccessible S&P mechanisms, "but also because they often struggle with depleted resources and capabilities together with less social, economic, and political resilience". While it is argued that accessibility may benefit people without disabilities as well [55], [69], it usually still holds a "medical disability perspective" [56]. Rather, Renaud & Coles-Kemp argue to obtain a "social model of disability", which emphasizes "limitation[s] to interact with other people, the environment or artefacts in the environment", and that "disability is not only physical but also related to a range of barriers that prevent people from operating as fully fledged members of society" [56]. They further define 4 types of vulnerabilities that result from this lack of access: physical, cognitive, financial, and emotional. Looking at accessible security this way highlights it is a promising venue to benefit users without disabilities as well. In 2022, Coles-Kemp et al. [16] further shed light on the issue of "assisted digital access" in the security domain, arguing to take into account social aspects of access, i.e., the assistance of other human beings, as well assistive technologies, therefore designing for shared, or "safer assisted digital access". This is underlined by Hayes et al. [31], who emphasize that building on the cooperative practices of users with visual impairments and their support networks can improve the design of mechanisms and tools while "mitigating the potential privacy risks this practice might introduce". As more and more services are provided online, these issues become especially pressing with authentication, as people depending on these services do not have a choice to use it or not [55], [56]. Having introduced inclusive and accessible S&P, we now present related work on users with disabilities and authentication.

2.2. Disability & Authentication

While there is a growing body of research on users with disabilities and security issues (e.g., [31], [45], [50]), little research specifically addresses users with disabilities and authentication. We categorize the related work into 4 types, based on the impairment that the research addresses most, as well as the types that affected the study's participants: (I) visual impairments, (II) physical impairments, (III) hearing impairments, and (IV) cognitive impairments. The amount of research on those types differs vastly, with most research being done on visual impairments and the least on hearing impairments [5].

Visual Impairments. Most research on authentication and users with disabilities targets visual impairments (e.g., [3], [4], [20], [23], [30], [35], [36]). This work often highlights the usage of assistive technologies when authenticating, such as screen readers and magnifiers [36]. For example, Desono et al. [20] found that users with visual impairments face difficulties due to the limitations of assistive technologies incompatibility issues with interfaces, resulting in noticeable authentication delays,

causing frustration and insecure behavior. Inan et al.'s interview study [35] showed that participants more knowledgeable on digital security issues tended to be more concerned in internet usage than those less familiar. They also describe issues with image verification and login sessions with timeouts. Faustino & Girouard [23] found their participants tended to preferably use family names or numbers as passwords because they are easier and faster to enter. Ahmed et al. [3] and Akter et al. [4] showed that participants are more prone to different types of S&P risks (e.g., shoulder-surfing, eavesdropping on private conversations, or detecting fake URLs), while also showing concern about being intercepted when publicly using assistive technologies, such as screen readers or audio output. In an interview study with users with visual impairments on their experiences with passwords, Hayes et al. [30] found that on the surface, the issues they face are similar to users without impairments, yet the underlying causes differ, and argue that neglecting this may lead to failure of designed solutions. In an online survey, Schmeelk & Petrie [61] find that "[p]assword creation, entry and change systems, as well as password management systems, all suffer from a typical range of accessibility problems" for visual impaired people, and that especially CAPTCHAs present a significant obstacle to them.

Physical Impairments. Little work addresses physical impairments and authentication. For example, Blanco-Gonzalo et al. [11] found that people with physical impairments have difficulties using BA and don't present an improvement over KBA for them. In a literature review and a survey of people with physical and other impairments as well as people working with them, Furnell et al. [26], [27] found that KBA was used predominantly, despite showing the most issues regarding security and usability, and that TBA as well as BA do not constitute viable alternatives. Conducting semi-structured interviews with 8 adults with upper extremity impairments, Lewis and Venkatasubramanian [41] found that KBA presents a challenge to them. As participants struggled with typing in general, they used simpler and shorter passwords, i.e., prioritising usability over security [41].

Hearing Impairments. We found least work addressing users with hearing impairments and authentication. However, Murbach [44] did extensive work on their self-efficacy in information security. They found that deaf users have low security knowledge compared to the general population, show poor security behaviors, and may need assistance to cope with security mechanisms and input keystrokes given by auditory instructions.

Cognitive Impairments. Recently, researchers started to look more closely at the needs of people with cognitive impairments, such as dyslexia [22], [32], [39], [52], [57]. Hayes et al. [32], Renaud et al. [57], and Ophoff et al. [52] found that difficulties occur in entering passwords, memorizing patterns, PINs, tokens, and identifying objects in pictures (CAPTCHAs). Participants help themselves with password managers that are fast and easy to use, as they automatically achieve the requirements of passwords, such as minimum length or upper and lower case. Other strategies are, e.g., writing them down on paper or asking for support. Kelly and Petrie [39] further found significant differences between people with and without dyslexia. Especially multi-factor authentication (MFA) posed challenges for people with dyslexia, e.g., in memorizing and entering one-time passwords (OTP). Evtimova & Nicholson [22] found that people with dyslexia engaged in potentially dangerous workarounds when creating passwords, engaged in password re-use, and need more time in the authentication process. Investigating the relationship between cognitive decline in ageing and KBA, Nicholson et al. [47], [48] found that older adults show poorer performance compared to younger adults, regardless of the authentication method. They – similar to Evtimova & Nicholson [22] – suggest that graphical passwords may benefit their participants. Our study adds to this body of work by applying a socio-technical lens to shed light on the experiences with (in-)accessible authentication of people with various impairments and possible venture points for improvement. To do so, we engaged in an exploratory study, which we present in the following.

3. Research Method

We conducted an exploratory study using semi-structured interviews to understand the experiences of users with disabilities and authentication methods, their challenges they face in everyday usage, and how they cope with them. We recruited appropriate participants with an online questionnaire. The accessibility of our study design is discussed in Section 3.2. As our principal researcher vastly shaped the study, we first reflect on the role of the researcher's positionality.

3.1. Researcher Positionality

Research is a collaborative process, in which results are produced through the interaction between researchers and participants [10]. Therefore, we discuss the research team's positionality [10], [71] to explain how this affected our work and the results. While our research team is engaged in human-centered security research, we have different backgrounds: 2 IT security researchers, a social scientist, an educational scientist, and a psychologist and HCI specialist, all bringing their disciplines' perspectives into the discussion. Our risk analysis was made possible by drawing on expertise in IT security, while having backgrounds in the social sciences enriched our analysis of the socio-technical aspects of our research. Further, 2 team members have disabilities themselves, which significantly shaped the study. Their experiences and perspectives enabled us to (I) make the study design as accessible as possible and (II) analyze the data from the perspective of the affected population. As they are well connected with other affected people and researchers, and they could reach out to them to ensure accessibility, e.g., the usage of plain language (see Section 3.2). This also benefited recruitment, as they knew how to best reach the target group. Having disabilities themselves enhanced trust and rapport with participants, making them more willing to participate and more open in their answers. This is vital for doing research with marginalized communities, and people with disabilities in particular, as expressed by the slogan "nothing about us without us" [59]. Our data analysis also benefited greatly from their perspectives and expertise. Sharing at least some part of the experience

enabled them to see important points within the data that could have easily been missed or left unseen by other researchers, see Section 3.6.

3.2. Accessible Study Design

As we target a population that is not only under-researched, but also often excluded by the study design itself, we now briefly describe which methods we applied to increase our study's accessibility.

Plain Language. To ensure accessible language in our recruitment flyer, interview guide, and survey, we consulted an expert on plain language who provided us with valuable guidance. Plain language was developed to make communication as easily understandable by as wide an audience as possible, e.g., by avoiding verbose, complex grammar structures, or jargon, seeking to be as concise and clear as possible, and keeping in mind the needs of the target audience [42]. We used Hurraki [34], a dictionary for plain language, as a reference for defining important terms regarding authentication, e.g., BA or MFA. These definitions were also included in the interview guide to have them at hand if a participant needed clarification. Using plain language vastly improved the accessibility of our study design and the quality of our data. We believe that plain language could also benefit other S&P research involving people unfamiliar with the topic. However, care must be taken not to make participants feel belittled.

Making the Survey Accessible. We reached out to potential participants by posting a digital flyer in plain language on selected social networks and mailing lists. The flyer also included an accessible text version to ensure that individuals using screen readers could access it. The online screening questionnaire was rolled out on the survey software Qualtrics. Being aware that people with disabilities may use assistive technologies, e.g., alternative pointing and input devices, or screen readers, for filling out the questionnaire, we reviewed its accessibility and comprehensibility several times during and after its development. For this, we used the built-in function *Check Survey Accessibility* to analyze the questionnaire against the standards of the WCAG 2.1 [69]. We adjusted our questions based on the recommendations and checked whether it was user-friendly on mobile devices as well as screen readers. We also changed the colors to create a contrast between the font and the background and made sure the font size was readable by people with visual impairments. The default navigation button labels were replaced with more readable labels and labeled with *Next* and *Back* so screen readers could read them aloud to participants. Questions with validation were marked to indicate that they have special requirements, e.g.,*"This question is a required question"* was added at the end of the question text. Finally, we checked if the online questionnaire was accessible via common browsers and on mobile view. Including this step is crucial as older browser versions may cause difficulties when attempting to access the questionnaire. [62]. The final version was tested by 2 people with disabilities (motor impairment and blindness) to ensure the survey was accessible. However, our instruction included a note that participants could contact the researcher for assistance in completing the questionnaire in case they encountered any difficulties.

Involving Assistants. Some people with disabilities rely on human assistants for support in their daily life and tasks. We encouraged participants with such assistants to invite them to join the interview. Being aware that the presence of another person might affect the interview situation, we conducted a pilot study, including a participant's assistant. In a few instances, the assistant interrupted the participant by attempting to answer for them or offering their own experiences and perspectives. Based on these experiences, we deduced the following rules to guide us during interviews that involved assistants:

- Informing participants beforehand and during the interview that we are primarily interested in *their* experiences and opinion,
- Assuring participants that they may take as much time as necessary to respond to questions,
- Only if the participant is unable or chooses not to answer a question may the assistant answer or add their insights with the participant's permission.

3.3. Instrument Development

Questionnaire. The questionnaire was developed as a screening instrument to recruit appropriate participants and gather information on their demographics, impairments, and technology usage. It was designed to be short, concise, and as simple as possible. It included questions about gender, age, type of disability, education level, and whether participants had a background in computer science. Further questions assessed the role of technology in the everyday life of participants, e.g., whether they needed assistance in using it, what problems they encountered in usage, and how they assessed the accessibility of technology. In the end, participants were given the opportunity to leave their e-mail addresses to schedule an interview. The full questionnaire can be found in the Appendix Section 7.1.

Interview Guide. For our exploratory approach, semi-structured interviews allow researchers to follow the underlying interview guide but leave room for participants to talk about their issues and concerns related to authentication. We prepared open-ended questions in thematic blocks, starting with the usage of digital technologies in everyday life, followed by discussions on authentication, including which authentication methods were used, and why (or why not). The next block discussed the accessibility of these methods, as well as risks and concerns. The following 3 blocks delved deeper into the different kinds of authentication methods, asking for experiences and challenges with (I) KBA, (II) TBA, and (III) BA. The final block focused on MFA, using online banking as an example. To conclude the interview, we asked about the participant's perception of security, usability, and accessibility of authentication. We piloted the interview guide (see Appendix Section 7.2) for suitability, feasibility, and practicality, which resulted in adjusting some questions and adding explanations of certain terms in plain language (see Appendix Section 7.3) to increase comprehensibility.

3.4. Recruitment

Recruiting participants from marginalized groups can be challenging [12], [60], as standard recruitment channels

do often not cater for such participants. This is particularly true for people with disabilities, who additionally might prefer to partake in a study run by a researcher with disabilities. A sense of shared familiarity makes it easier to connect to. To recruit appropriate interviewees for our study, we engaged in selective sampling. Participation required that the participants were over 18, with some form of disability, who used any authentication methods on a digital device, application, website, or app. A digital flyer, including information about the study, the target group, a link, and a QR code to the online survey, was distributed within predetermined networks and channels, including social media platforms, as well as mailing lists of public organizations working with people disabilities. At the end of each interview, respondents were requested to name other people who might be interested in participating (snowball sampling, see [24]). This resulted in interviews with 13 participants in total.

3.5. Conducting the Study

The interviews were conducted remotely, using the video conferencing tool Zoom and OBS Studio for recording. Participants were free to choose whether they turned on their cameras. Remote interviews had the benefit that neither the interviewer nor the interviewees had to travel long distances to conduct the interview, and further protected their health during the receding COVID-19 pandemic. 2 of the interviews were conducted in the presence of the participants' assistants, while 1 participant indicated the presence of a family member to assist in case of need. Before beginning the interview, the researcher introduced themselves and engaged in small talk to create an open atmosphere and increase rapport. Then, participants were guided through the consent form. The recording was started only after participants had agreed and given their consent. During the interview, the interviewer paid attention not to rush participants, leaving them time to think about their answers and to elaborate on issues that mattered to them. If necessary, the interviewer would offer explanations of words or concepts to avoid misunderstandings. The interviews lasted from 33 minutes to 87 minutes, with an average of 50 minutes. The interviews were held in German. For the purpose of this paper, quotes have been translated.

3.6. Data Analysis

The interviews were transcribed and analyzed using MAXQDA. Transcription was performed verbatim, including interjections and interruptions by speakers and speech pauses, to obtain the flow of speech for analysis, including, e.g., the need to think about an answer. The language was edited lightly to create a readable transcript (clean verbatim). During the process, all personally identifying information was removed, and the recordings were deleted after the transcript had been checked for completeness and accuracy. The data was analyzed based on guidelines for Qualitative Content Analysis [43]. In the first step, deductive codes were derived from the research questions and the interview guideline. All transcripts were reviewed the codes assigned to fitting passages. Then, codes were refined iteratively, optimized, and organized into sub-categories. Following this, inductive codes were built, accounting for experiences that have not been thought about before, resulting in an elaborate code system. In the final step, all data was reviewed again, using the finalized code system, checking that all statements had been correctly assigned and that nothing had been overlooked. The codebook can be found in Table 4 in the Appendix in Section 7.4. The coding procedure was supported and advised by another researcher with a disability. The same researcher reviewed the code system and transcripts, offering critiques and suggestions for improvement. While this process was mainly performed by these 2 researchers, 2 other researchers without disabilities reviewed the coding process and offered their perspectives in several discussion sessions. Our data analysis benefited greatly from our researchers' positionality. Sharing some of the experiences and perspectives of the study participants revealed insights that researchers without disabilities would have overlooked. As a result, we are able to present results that reflect the perspectives of our participants.

3.7. Ethical Research Practices & Data Privacy

Research with marginalized groups, and those who face higher risks than the "average" population [73], requires special attention to ethics [10]. Our institution did not have an institutional review board (IRB) nor an ethics review board (ERB) responsible for security research with or without human participants. We therefore thoroughly discussed ethical questions within the research team, followed established guidelines of Information and Communication Technology Research [67], and made sure our data collection and handling was in accordance with the European privacy regulation (GDPR). We systematically assessed possible risks and benefits for participants and the affected group we targeted, basing our discussions on the recently proposed "Ethical Practices for Security Research with At-Risk Populations" [10], as well as the insights of our research team members who are also members of the community we study. One important aspect for us is not only to treat, but present our data with respect to our participants in talking respectfully about them, i.e., using their preferred terminology. For example, we talk about "people with disabilities", instead of "severely or multiply disabled persons", i.e., using a person-first, not an identity-first description [21]. Participants gladly participated in the study, as the principal researcher shared their experiences of having a disability, and showed gratitude of being able to talk about their concerns with the outlook of them being shared publicly. By giving voice to their experiences, we hope to inspire more security researchers to work with the communities of people with disabilities, ensuring secure access and authentication for all by giving voice to their concerns in this publication.

3.8. Limitations

Our data is the experience of our participants, self-reported, with the usual risk of memory and other biases, such as social desirability. The interviewer, having a disability themself, encouraged them to share their experiences openly. Our sample includes people with very different kinds of disabilities, meaning we do not have a depth

of data for any particular disability. As the recruitment was performed mainly through the primary researchers' channels, most participants in our sample share a sense of familiarity with the researcher. However, this also increased trust and rapport, giving quality to the data. As the survey and the interview were conducted online, a certain degree of accessibility to digital technology was necessary, biasing the sample towards people who can acquire this.

4. Results

Our results show that people with disabilities experience significant challenges when using different authentication methods, leaving them to engage in different workarounds and coping strategies, which at times make them more vulnerable. This chapter presents our major findings (see also Table 3) after giving an overview of our study sample.

4.1. Sample Description

Our sample was diverse in regards to gender, education, and most importantly, the impairments participants reported, suiting our exploratory study approach well. In total, 8 participants identified as man, 4 as woman, and 1 preferred not to disclose their gender. Participants' age ranged from 23 to 48, with an average age of 28. Their education levels differed widely: 2 participants had no formal education certificate, 1 a special education degree, 5 had university-level degrees, while the remaining had high-school degrees. None of them had an academic background in computer science or related fields. Participants reported all kinds of impairments, from physical, to visual, to hearing impairments, and learning difficulties. Only 1 participant became disabled later in life. All participants except 1 required assistance to use digital technologies. They used assistive technologies, like text-to-speech tools, hearing aids, screen magnifiers and readers, braille displays, optical character recognition (OCR), specific glasses, and a prosthesis. 2 participants had a human assistant to support them in their everyday life. An overview of our sample can be found in Table 1. In the following, we present how different kinds of impairments and assistance shaped participants' experiences with different authentication methods.

4.2. Experiences and Challenges with different Authentication Methods

All participants used a smartphone in daily life. For 2 participants, this was the only device they used, the other 11 used at least 1 other device: tablet, laptop, or desktop PC. All except P2 highlighted the importance of authentication for their security and privacy:

> *"[It is] out of a certain need for security [...]. I don't have anything to hide, but [...] at work, it is about sensitive data. The smartphone contains potentially sensitive data as well [...]."* (P12)

7 participants, e.g., P6, stated they had no choice, as a specific authentication method was mandatory:

> *"Today, you don't have a choice anymore. It is required by the respective device, system, [or organisation]. [...] I do it because I have to."*

All participants used KBA (passwords, PINs), and 6 used TBA (smart cards, OTP generators). 11 participants have used BA (fingerprints, facial recognition), but 6 of them stopped because of usability issues. An overview of device and authentication usage can be found in Table 2. We present the experiences and challenges participants reported with authentication methods, sorted by type of authentication (KBA, TBA, BA) and authentication task: enrolment, authentication, and recovery. For a detailed overview, see Table 3.

KBA. KBA dominated the interviews, as all participants used them and reported significant challenges at all authentication tasks. Enroling KBA, i.e., setting up a username and a password/PIN, already presented significant challenges for all participants except P4, P5, and P11, starting with the difficulty of creating secure passwords. This was due to, e.g., a lack of explanations in plain language (P2, P3) or complicated password rules that interfere with their disabilities or assistive technologies. While P4, P5, and P8 perceived password-strength meters as helpful, P1, P6, and P10 described them as challenging and limiting to enrolment:

> *"I had to reset a password [...]. It did not work at all, as it constantly said, this is not okay, that is not okay. There are a lot of rules. I felt very constrained."* (P6)

This experience is amplified for participants with learning difficulties or those who use assistive technologies, which often are very costly. For example, P8 elaborates that insurances cover only the bare necessities:

> *"The purchase price for a Braille display, which represents only 40 characters, is about €6000. [...] There are [...] some with more characters. [The] costs for these are not covered."*

Thus, participants prefer short and simple passwords they can easily recall and enter – but which the systems often do not accept. This causes frustration and increases the time and mental workload of having to think about new passwords. Participants with impaired fine motor skills (P1, P10) reported frequent typing errors slowing down authentication because passwords must be entered correctly twice. Participants with visual impairments (P9, P12, P13) reported that too small text fields and lack of contrast make it challenging to distinguish the fields for username and password; non-identical keyboards on smartphones and PCs cause further orientation issues and frustration, as elaborated by P9:

> *"I don't understand how the keyboard is arranged. There is a keyboard for letters, and a second, for symbols and punctuation. I don't understand how they differentiate. So I have to scroll through every symbol [via VoiceOver] until I find the symbol I am looking for."*

Participants also reported significant challenges using other assistive technologies, such as a screen reader or -magnifier – called "their eyes" by P8 and P9 –, without which they can barely operate their devices. UI design frequently posed problems, as certain buttons can not be clicked, and fields not be navigated to (P7).

For P2 and P3, who have human assistants, it was not possible to enrol without their help due to their

TABLE 1. PARTICIPANT SAMPLE

#	Gender [a]	Age	Education	Reported Impairment	Self Description	Assistive Technologies or Human Assistance
P1	M	25	Special Education School	Physical, Visual, Learning	Limited Fine Motor Skills, Moderate Vision	Trackball Mouse, Text-to-Speech
P2	M	25	No Degree	Physical, Learning	Upper Extremity Spasticity, Muscle Weakness	Human Assistance[b]
P3	M	27	No Degree	Physical, Learning	Spasticity over the Body, Use only the Index Finger	Human Assistance[c], Touch Pen
P4	W	25	Bachelor	Hearing	Moderately Severe Hearing Loss	Hearing Aids
P5	M	29	Bachelor	Visual	Color Blindness, 5-10% Vision, ESL[d]	Screen Magnifier
P6	W	25	High School	Physical	Limited Fine Motor Skills, Upper Extremity Spasticity	None
P7	M	29	Master	Visual	Loss of Central Vision, 2% Vision	Screen Reader, -Magnifier, OCR
P8	M	24	High School	Visual	No Vision	Braille Display, Screen Reader
P9	W	26	High School	Visual	No Vision	Braille Display, Screen Reader, OCR
P10	W	48	Secondary School	Physical	Lower Arms & Legs Amputated	Prosthesis
P11	-	23	Bachelor	Hearing	Moderately Severe Hearing Loss	Hearing Aids
P12	M	27	Master	Visual	Blurry Central Vision, 2% Vision	Screen Reader, -Magnifier, OCR
P13	M	33	Elementary School	Visual, Learning	Severe Hearing Loss, ESL[d], Decreasing Visual Acuity	Edge Filter Glasses

[a] M = Man, W = Woman, [b] Interview with assistance without technical background, [c] Interview with assistance with technical background, [d] Extreme Sensitivity to Light

physical impairments and learning difficulties. Both assistants explained that they completed the enrolment task: entering the e-mail address and choosing a password. The reasons given for this are the lack of plain language, the difficulty of typing only with the index finger, and the creation and memorization of passwords. Participants reported similar challenges for the authentication task. However, further highlighting issues with memorizing and entering credentials, especially as authentication itself is a task preferably done quickly. This caused participants to engage in a variety of workarounds and coping strategies, which we discuss in Section 4.3. Further, participants reported significant challenges with CAPTCHAs in the enrolment or authentication process.

Credential recovery was also a significant challenge for most participants. Most of them had difficulties remembering the answers to the security questions and therefore needed multiple attempts:

> *"I could not remember the answers, even though the questions were not that hard, and the answers logical."* (P5)

TBA. Only 6 participants talked about their experiences with TBA, i.e., with card readers they had to use for their organisation (P4, P6, P11, P12) and OTPs (P5, P6, P7, P11, P12). P6 and P12 were unable to setup the card readers without support, underlining that this was not due to their disabilities but because the instructions were

> *"[...] not accessible, as they use advanced technical terms. I [as someone who did not study this] can not understand these terms."* (P6)

P5, P6, P7, and P12 described difficulties with using OTPs, e.g., in regards to difficulties reading the code or the time limit presenting an obstacle causing frustration and slowing down the process:

> *"I would probably not manage to do it within the time-limit, needing several attempts, or asking someone for help."* (P7)

Needing to wait for a new OTP was mentioned by all participants. P5 explains:

> *"Usually, I look at the timer and wait for a new code, as it is not readable for me straight away, and errors would occur when transferring it to the browser. I have to hold the smartphone very close to my face due to my visual impairment."*

P12 further explains that they need to let the code be read aloud by voice output, further slowing down the process.

BA. All participants, except P11 and P12, used fingerprint for authentication. Yet, 5 participants stopped using it due to usability issues and privacy concerns. P1 and P6 report challenges setting up the fingerprint due to their physical impairments – their limited fine motor skills make it difficult for them to accurately position their fingers on the smartphone to capture it from all sides. Enrolling in fingerprint authentication is experienced by them as frustrating and time-consuming as it takes several attempts. After setting up the fingerprint, authentication is much more convenient. According to P1, P6, and P13, it happens from time to time that a touch device does not recognise the fingerprint. For P2, P3, and P10, it was not possible to use fingerprint at all due to their physical constraints. For example, P10, who uses an arm prosthesis without a fingerprint, describe their experience:

> *"I tried once with my arm stump on a tablet. Scanning worked somehow. [...] However, it was not recognised when trying to unlock."*

P2's and P3's assistants explained they could not use the fingerprint, as their hands were too bent, and they have issues with fine motor skills. They have trouble holding the smartphone itself, let alone coordinating their fingers around it, especially as the device is usually placed on a table or within a holder. P2's assistant explains:

> *"P2 grabs the phone from the table with their right hand. Then, they place the back of the phone onto their chest to stabilise it. Then, P2 swipes the phone with their left hand to unlock it, then places it back on the table."*

Only 4 participants actively used facial recognition for authentication, while 4 others had used it but stopped. Af-

ter failing with the fingerprint, P10 tried facial recognition. However, holding the smartphone steady and towards their face with the arm prosthesis proved too difficult. Facial recognition presented significant challenges for participants with visual impairments (P7, P8, P9, P13). While P8 explained that the VoiceOver prompts for setting up face recognition are good, they could not estimate the positioning of the face in terms of distance and angle and needed the assistance of another person to do so. P7, P8, P9, and P13 explain that they often need several attempts to unlock their smartphones with facial recognition. P8, who relies on VoiceOver to operate their smartphone, usually holding it close to their face, elaborates:

> *"One has to get used to this extra gesture, to hold the phone further, otherwise unlocking won't work. In more noisy environments, I use a headset with the phone. [...] It is very cumbersome, to have to hold it in front of your face."*

P8 and P9 describe getting used to opening their eyes to unlock the smartphone, as usually, they mostly keep their eyes closed to focus on listening. They, as well as P7, disabled the attention-sensing [7] features on their phones. This makes it possible to unlock the iPhone even when closed or without looking into the camera. However, participants with physical impairments also reported issues when using facial recognition due to their limited capabilities for movement, as described by P3:

> *"To register my face, [my assistant] would have to move the device back and forth. I am constrained [in my movements] in that regard."*

As autonomous usage is of importance to participants, some decide against using BA altogether:

> *"It is also about autonomy. An authentication method is of no use, when you are depending on others."* (P6)

4.3. Workarounds and Coping Strategies

Authentication methods posed significant and distinct challenges. Participants engaged in several workarounds and coping strategies to access their devices and accounts.

KBA. As shown, the only available authentication method for P2 and P3 is KBA, for which they rely on their assistants to set them up. Due to their learning difficulties, P2 can not memorize their passwords and PINs, so they further rely on A2. A2 copes with this by setting easy to remember passwords, like family names and birth dates. P3's assistant, with a technical background, opted for a password manager for generating and storing passwords:

> *"We opted for the App KeePass [...], as it is open source. [...] I entrusted P3 to use it."*

Memorizing and recalling passwords proved challenging for most participants. P1, P4, P5, P6, P8, and P10 indicated that they have a pool of passwords that they draw on and re-use, preferably relatively short and easy passwords, as they are easy to remember and enter using different assistive technologies. For example, P10 describes typing in long passwords as cumbersome with their prosthesis. 5 participants (P3, P7, P10, P11, P13) used a password manager for authentication. However, only P3, P7, and P11 used them to generate unique passwords, as they were advised by their school or workplace, respectively. Participants' other workarounds were writing down passwords (P1, P6, P12), looking up passwords in the notes app to copy and paste (P9), or using voice input, as speaking is more accessible than typing. For example, P10, who does not wear prosthetic arms during the day and can handle the tablet without prosthetic arms, explains:

> *"You can see that as another reason why I choose my passwords this way. Long and complex passwords are not easy to pronounce."*

As P1 uses more than 1 digital device and does not always have access to the browser where the passwords are stored, the credentials still have to be manually entered. For this, they established 2 additional workarounds. First, they write down the credentials after each enrolment process in an analog list, which is already more than 3 pages long. If they need to remember, they look up the credentials. Second, if possible, P1 signs in to many accounts using Facebook's or Google's single sign-on procedure, so they only have to memorize a single password.

P1 and P10 report another challenge. Sometimes, the systems do not provide a function to toggle the visibility of the password, e.g., in the enrolment task. To circumvent entering a wrong password due to this, P1 explains that they type the password in an editor and copy this into the password field. P9 describes a similar approach when authenticating. They explain that after enrolment, they store their credentials in Apple's Notes app, and use the copy and paste function to login into a system. This is more efficient on the smartphone, they said:

> *"I stored some of my passwords in a note-app, so I can copy and paste them easily. So at least sometimes, I spare myself from typing on the smartphone."* (P9)

To recover authentication credentials, 5 participants would need support from others. P8, P9, and P10 state

TABLE 2. DIGITAL DEVICES AND AUTHENTICATION METHODS USED BY THE PARTICIPANTS. ✓ INDICATES THAT THE DEVICE IS USED, AUTHENTICATION METHOD, ◌ WAS PREVIOUSLY USED, ◔ IS USED WITH USABILITY AND SECURITY ISSUES, ◓ IS USED WITH USABILITY ISSUES, ● IS USED WITHOUT PROBLEMS.

	Digital Devices				**Knowledge**	**Token**		**Biometric**	
	Smartphone	**Tablet**	**PC**	**Laptop**	**Password/ PIN**	**Smart Card**	**OTP**	**Fingerprint**	**Facial Recognition**
P1	✓		✓		◔			◓	
P2	✓				◔			◌	◌
P3	✓	✓			◓			◌	◌
P4	✓	✓		✓	●	●		●	●
P5	✓	✓	✓		●		◓	●	
P6	✓	✓		✓	◓	◓	◓	◓	
P7	✓			✓	◓		◓	●	◔
P8	✓			✓	◓			◌	◔
P9	✓			✓	◓			◌	◔
P10	✓	✓			◓			◌	◌
P11	✓		✓		●	●	●		
P12	✓	✓	✓	✓	◓	◓	◓		
P13	✓				◓			◓	◌
∑	13	6	5	6	13	4	5	11	8

TABLE 3. CHALLENGES, WORKAROUNDS, AND RESULTING RISKS TO S&P DURING THE AUTHENTICATION PROCESS.

Knowledge-based Authentication			
Task	**Identified Challenges**	**Workarounds**	**Risks to S&P**
Enrolment	Whole process is not possible	Assistant takes over whole process (P2, P3)	No autonomy and requires a certain level of trust between them
	Difficult to create a secure password	Using names of family members, partners, friends or date of birth (P1, A2) Using one password more than once (P1, P4, P5, P6, P8, P10) Generating a secure password by a password manager (A3, P7, P11)	The use of passwords with personal information and multiple uses of a password represent a severe security risk
	Compatibility issues with assistive technologies, making fields unreachable	Finding a way by trial and error (P7)	Time consuming and can be frustrating
	Orientation problems on the smartphone keyboard using special characters	Faster voice output of characters on the keyboard (P9)	
	Poor contrast of the smartphone keyboard	Using a customized third-party keyboard (P12) Not choosing a workaround (P13)	
Authentication	Password fields are unreadable because the eye symbol is only sometimes available	Entering the password in an editor and copying it into the password field (P1) Not choosing a workaround (P10)	Time consuming and can be frustrating
	Credentials are difficult to enter or remember	Using Google or Facebook single sign-on (P1) Looking up written passwords (P1, P6, P12) Using a password manager (P3, P7, P10, P11, P13) Looking up passwords in the notes app to copy and paste (P9) Using the voice input (P10)	Reduced privacy with single sign-on as they get access to their personal data, voice input leads to a higher security risk with potential bugging
	Image-based CAPTCHA on the login screen is difficult to solve	Finding a way by trial and error (P5, P8, P9) If available, using audio CAPTCHA as an alternative (P8, P9) Getting help from others (P8, P9)	Time consuming and can be frustrating
Recovery	Insufficient retries lead to lockouts or the security questions are difficult to remember	Getting help from others (P2, P3, P8, P9, P10) Creating a new account (P1, P2, P13)	No autonomy and depend on the help from other people
Token-based Authentication			
Task	**Identified Challenges**	**Workarounds**	
Enrolment	Challenging to install a card reader for smart cards, as the instructions are not understandable	Getting help from others (P6, P12)	No autonomy and depend on the help from other people
Authentication	Challenging to read and enter a one-time password when time is short	Waiting for a new one-time password with a new time limit (P5, P6, P7, P12) Copying and pasting across devices on the Apple ecosystem (P7) Reading aloud by voice output (P12)	Time consuming and can be frustrating
Biometric Authentication			
Task	**Identified Challenges**	**Workarounds**	
Enrolment	Difficult to scan fingerprint	Finding a way by trial and error (P1, P6)	Time consuming and can be frustrating
	Difficult to position the face in front of the device	Getting help from others (P8)	No autonomy and depend on the help from other people
Authentication	Fingerprint or facial recognition cannot be used because of the abilities of people with disabilities	Disabling authentication on device (P2, P3, P10) Using an older iPhone model (P7) Attempting arm stump (Unsuccessful) (P10)	
	Sometimes the face can not be recognized	Making several attempts (P7, P8, P9, P13) Using the alternative authentication (P7, P13) Disabling the attention function so the eyes do not have to be open (P7, P8, P9)	Time-consuming and decreased security by disabling the attention function
	Sometimes the fingerprint can not be recognised	Making several attempts (P1, P6, P13) Using the alternative authentication (P6)	Time consuming and can be frustrating

that they have no problems recovering the account per se. P10 notes that the situation sometimes overwhelms them. P8 and P9 said their assisting technologies (VoiceOver or Braille Display) significantly slowed down the process, so they preferred human assistance:

> *"Yes, well, it just is faster. I wanted to spare myself the hassle of doing it by myself."* (P8)

P2 and P3 again need complete assistance in recovering the account, as in the enrolment process. Moreover, P2's assistant explains that this constitutes a considerable effort and therefore prefers to create a new account simply. P1 and P13 engage in the same workaround.

TBA. As already stated, P6 and P12 needed help from others in setting up their card reader for TBA. While P5, P7, and P12 habitually waited for a new time limit before entering the code, P7 developed a system of copy-and-paste the code across devices within the Apple ecosystem, which is not offered for other devices [6].

BA. As we have seen, BA posed significant challenges to most participants, causing 3 of them to stop using them altogether. The remaining ones faced the challenges by either getting help from others in setting up the facial recognition (P8), engaging in rounds of trial and error in setting up the fingerprint (P1, P6), making several attempts when the face or fingerprint is not recognised (P1, P6, P7, P8, P9, P13), or disabling the attention function, so their eyes don't need to be open (P7, P8, P9). Further, P7 refrains from buying a newer model, as that would no longer support their preferred fingerprint authentication.

5. Discussion

We discuss our key findings, focusing on the workarounds participants engage in to access different authentication methods and the role of assisted access, highlighting the effects on S&P. We then discuss the role of accessible language and multiple impairments before deriving recommendations for practitioners and researchers.

5.1. Lack of accessible authentication forces users with disabilities to prioritize usability over security

While some of our results, especially regarding KBA [29], [32], also pertain to "typical users", it is striking that *none* of the available authentication methods were fully accessible to our participants. Rather, they described a large number of challenges with KBA, TBA, and BA. Depending on the usage, the number of identified challenges and workarounds in the respective authentication method and their effects on S&P differ vastly (see Table 3). Most accessibility challenges and workarounds arose with KBA. Many of these have already been found to affect the general population as well (e.g., [8], [29]). However, for users with disabilities, these challenges become reinforced. The majority stem from usability issues – such as compatibility problems with assistive technologies (P7), lack of contrast on the smartphone keyboards (P12, P13), non-readable password fields (P1, P10), or solving CAPTCHAs in the enrolment or authentication process (P5, P8, P9) – that have also been identified by other research, e.g., [20], [61]. These also have an effect on security, e.g., similar to people with dyslexia [22], [39], [52], [57] P1, with learning difficulties, finds it hard to create and remember secure passwords, so they reduce the length of the passwords and choose family names or a date of birth as a password to be able to memorize it easily. Such adaptations commonly come at the cost of security, as shown in P1's experience:

> *"Yes, unfortunately. Sometimes it has happened that my password was cracked."*

Due to these negative experiences, P1 prefers to use Facebook's or Google's single sign-on function. However, this leaves them choosing a secure and usable authentication method at the potential cost of privacy, as they have to rely on third parties. Forms of interoperability between systems and devices, like the single sign-on procedure, require devices that are up to date, which are not accessible to everyone due to privacy concerns or limited access to financial resources [56], [68].

Furthermore, participant P2 can not register on their own. Hence, their assistant takes over the enrolment process. This decreases user autonomy, requires a certain level of trust between them, and holds potential risks to S&P. Firstly, the assistant must enter a secure password. However, P2's assistant states, like P1, prefer passwords that are easy to remember yet less secure, being trapped in the tradeoff between usability and security:

> *"To be honest... I use family names, a date of birth, or a combination of numbers, because it's not P2 who has to memorize it, it's me."*

This further exemplifies how the burden of security is placed on the human assistant, most likely struggling to manage their own passwords and those of the assisted person on top. Both would highly benefit from using a password manager, like P3 and A3.

For TBA, challenges arose with a smart card and the OTP. P1 and P12 express how difficult it was to set up a card reader for a smart card. Here, the major obstacle did not stem from their impairments but an incomprehensible set of instructions made up of IT terminology for which they sought support. This illustrates how accessible language would benefit not only people with disabilities but most likely large parts of the population.

P5, P7, and P12 with visual impairments report reading and entering OTPs as challenging. Their workarounds are time-consuming and, therefore, frustrating for participants. As with other authentication methods, this could potentially cause abandoning them, or 2FA in general, which would then decrease security [18], [51].

BA was most challenging for people with physical or visual impairments. For example, participants with physical impairments have difficulty placing the finger precisely (P1 and P6) for fingerprint authentication. Face recognition is especially cumbersome for participants with visual impairments (P7, P8, P9, and P13) who report difficulties scanning the face. P7, P8, and P9 developed a workaround: they disabled the attention function of Face ID, so their eyes do not have to be open, only later realizing this infringes on security:

> *"However, I learned afterward that there is a functionality to turn this off. But conversely, this means less security."* (P8)

Due to the severe usability issues, many participants abandoned BA methods or did not even start using them (see Table 3). This shows that BA increased usability for people without disabilities yet remains inaccessible for people with disabilities. Others have also found this, e.g., Blanco-Gonzalo et al. [11] and Furnell et al. [26], [27].

However, we also observed the creative attempt of P10 to use an existing biometric sensor, the fingerprint, in a new way: They test the arm stump print. Similar practices have been found by Lewis and Venkatasubramanian [41] in their study on authentication with users with motor impairments. This is an opportunity to enhance existing credentials or develop new credentials for people with disabilities to use their current abilities effectively and increase autonomy. Building on existing practices has also been suggested by Hayes et al. [31].

Almost all participants show a high level of interest in BA to increase usability and hence, security. In this context, participants P8, P10, and P13 suggested voice recognition as the desired method in addition to existing methods. Including people with different abilities in the development and design process of BAs is pivotal to alleviating the burden of KBA. We further need to consider the role of assisted access in more detail.

5.2. Assisted Access

Many participants, particularly those with visual and physical impairments, use assistive technologies in their everyday lives – for handling digital devices, as well as for authentication (see Table 1). They described them as predominantly positive, and at times, as extensions or replacements of their selves, e.g., P9:

> *"Without my voice output, I wouldn't be able to use my devices at all. They replace my eyes."*

However, 2 critical issues must be addressed. First, assistive technologies are not equally accessible to everyone. P8, P9, and P10, report that getting financing from cost-bearers is burdensome, time-consuming, and involves much work. As a result, people with disabilities often have to muster up a significant amount of resources (financially, time, mental and physical work) to access assistive technologies. This presents a significant obstacle to people with disabilities, who are more frequently affected by unemployment and restricted access to resources [56], [68]. Additionally, a significant earning gap exists between employees with and without disabilities, increasing their struggle to pay bills [68]. Thus, people with disabilities are not always able to acquire assistive technologies or newer, updated devices. For example, P11 says their hearing aids do not work with all devices:

> *"I have an Android smartphone. It's a bit older and I have the problem, for example, that my hearing aids can't connect due to the outdated Bluetooth standard."*

This lack of access to resources can have direct consequences on S&P, e.g., in continued usage of older devices that are not updated anymore. P7, P9, and P11 further experience incompatibility problems. P9 explains that programs and apps do not interact with the voice output. In contrast, P7 states that contents and fields are not operable. This ambivalence of assistive technologies is also discussed in [41] and [55]: On the one hand, assistive technologies ensure access in enabling device interaction, e.g., by making user input easier when entering a password. On the other hand, assistive technologies can slow down authentication and make it unreliable, as also found by Renaud [55].

Another issue is the role of access assisted by other humans. Our results show how P2's and P3's assistants' different knowledge and skill levels regarding IT directly impacted participants' S&P, in either opting to (not) use a password manager, and the creation of (in-)secure passwords. This suggests that increasing the security knowledge and skill of human assistants may benefit themselves as well as the assisted, which is also indicated by [16]. Further, as seen, even participants without a dedicated human assistant frequently relied on human assistance to accomplish authentication tasks (e.g., P6, P8, P9, P10, P12), which was also found by Hayes et al. [31]. However, digital services and authentication mechanisms are neither designed for shared access [63] nor assisted access [16]. While this can introduce risks to S&P, Hayes et al. [31] show that "people with visual impairments often work closely with their allies to protect their privacy and security in a cooperative manner", and argue that building on these practices can improve the design of mechanisms and tools, by ensuring interoperability between tools as well as people within socio-technical systems. Our results further emphasize the role of accessible language – and the lack thereof.

5.3. Accessible language is key

Although we used definitions in the plain language provided by official sources [34] for our interview guide, comprehension problems occurred several times, especially with P1, P2, P3, and P13. A lack of explanations in plain language was also mentioned as an obstacle to creating secure passwords (e.g., P2 and P3). P6 and P12 could not set up a smart card reader for authentication without the help of others, emphasizing this was not due to their impairments but to incomprehensible instructions involving complicated IT jargon. This illustrates that, while people with specific disabilities are in need of plain language to use authentication securely, the usage of accessible language would also benefit large parts of the population without disabilities. This also holds true for authentication challenges in general and KBA in particular. While participants' impairments differed widely, it is striking that they faced similar challenges to people without disabilities – however, reinforced. This is a case in point that accessibility would also benefit others. Within socio-technical systems, accessible language is key.

5.4. Having multiple impairments

In our study, 4 out of 13 participants, approximately 31%, indicate having at least 2 impairments (see Table 1) – casting doubts on current approaches that seek individual solutions for individual impairments. Our results also reveal differences within the disability categories in terms of access to digital devices and assistive technologies, use of authentication methods, and perceived difficulties and workarounds developed. Previous studies by Johansson et

al. [37] and Dobransky and Hargittai [19] call for different categories of disability to be used when considering people with disabilities. In the study by Dobransky and Hargittai [19], 44% of participants reported having more than 1 impairment. In the survey by Johansson et al. [37], about 68% reported having more than 1 impairment. The average is 4 impairments. According to Johansson et al. [37], the combined effects of multiple impairments have yet to be researched. Research focusing on 1 impairment at a time cannot clarify the nature of the difficulties experienced by people with various impairments.

5.5. Recommendations

Based on our results, we now draw recommendations for practitioners and researchers to make authentication more accessible and inclusive:

Alternatives to KBA. It is long known that KBA presents significant challenges for users [1], [29]. Our results show that KBA is even less suited for users with disabilities. Moreover, BA, offering better usability, is often not accessible to them. While promising alternatives are developed, like FIDO2 [13], [14], [17], [28], research and development targets BA like fingerprint and facial recognition [40]. Voice recognition, which might improve accessibility – and was explicitly wished for by participants –, remains less targeted. To avoid the pitfall of developing an inaccessible alternative, we advocate including users with disabilities in the development and design, as it is still in the beginning. Further, compatibility with prevalent assistive technologies should be evaluated.

Existing authentication methods should aim at offering alternatives, so users with disabilities can choose the most accessible to them. To establish this, more research is needed on which authentication methods these are. They further need to be evaluated and improved in regard to compatibility with assistive technologies.

Improving KBA. As long as KBA is prevalent, password managers are promising to alleviate many of the challenges that users with and without disabilities face. However, little research is done on the accessibility of password managers for users with disabilities [9], [46] or their compatibility with different assistive technologies [61]. This research gap must be filled to develop products that increase S&P for users with disabilities and further benefits their human assistants, if any.

Accessible Security is about more than Usability. We have seen that usability is not enough and that, for example, the communication of S&P relevant information also needs to be accessible. Therefore, we encourage practitioners and researchers to develop a canon of S&P knowledge in plain language. This may benefit many users without disabilities as well. We also encourage policymakers to specifically address S&P in policies that affect users with disabilities, to motivate institutions (e.g., insurances) and organisations to address these issues and distribute resources accordingly (e.g., in the development and acquisition of technologies that do not compromise S&P).

Future Work. Researchers can assist in making S&P accessible and inclusive by engaging users with disabilities. More research on this user group is desperately needed, especially on the role of assisted access and multiple impairments. At best, people with disabilities are included from the beginning, i.e., advising on making the study design accessible. This can be done by working with representatives or associations. To identify challenges in everyday life, we need a wide range of participatory and long-term methods, e.g., field studies, diary studies, creative security engagements [15], [33], living labs, and observatories. We need more knowledge on what type of access works best for which impairments and on which platforms and devices, as well as best practices for balancing assistance and autonomy for assistant and assisted. This body of knowledge should then be evaluated in lab studies and quantitative measurements.

6. Conclusion

We conducted 13 semi-structured interviews with people with varying disabilities, from physical, hearing, visual, and cognitive, to multiple impairments on their experiences with KBA, TBA, and BA. We shed light on the challenges they face, the workarounds they engage in, and their effects on S&P. Our results show that **none** of the commonly available authentication methods are fully accessible to them, which results in the need to engage in workarounds and coping strategies or the decision to abandon them. While KBA is specifically challenging for all participants, only 3 of them can use BA without difficulties, so most of them do not benefit from BA's usability advancements. We further shed light on the role of assistive technologies and human assistants, which ensure access for participants yet complicate S&P: Assistive technologies can interfere with authentication, slowing down the process, or human assistants need to take over the whole authentication process. This form of assisted access is not accounted for in S&P design. Additionally, 4 of our participants had multiple impairments, roughly corresponding to the population of people with disabilities. The possible effects on S&P are rarely addressed and accounted for. We conclude that accessible S&P is about more than usability.

As KBA is still the most prevalent and challenging method to date, we strongly advocate including users with disabilities in the development of alternatives from the beginning. The development of alternatives should evaluate the compatibility with assistive technologies and human assistants. To do this, it is best to get advice from people with disabilities to best approach and include them. Existing authentication procedures should offer alternatives to KBA that are accessible to users with disabilities so they can choose their preferred method.

More work is to be done to make password managers accessible to users with disabilities as long as KBA is the prevalent method, as well as on improving compatibility with assistive technologies and human assistants. There is a need to develop a canon of S&P relevant knowledge in plain language. Accessible information on S&P may benefit users without disabilities as well. More knowledge on the accessibility of authentication, and S&P in general, is needed to underpin these approaches, especially on the barriers to access, the role of assisted access, and of multiple impairments. At best, people with disabilities are included from the beginning of the study design stage.

Acknowledgements

We thank our study participants for their trust, willingness, and openness to share their experiences, thereby enabling us to give voice to them in this publication. We further thank our colleague Sümeyra Altintas for supporting us with helpful advise on accessible communication, and Joshua Speckels for performing LaTeX Magic. Our work was (partly) supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972.

***Index Terms*—Human-Centred Security, People with Disabilities, Authentication, Accessibility, Plain Language, Accessible Security, Inclusive Security, Visual Impairment, Hearing Impairment, Physical Impairment, Learning Difficulties**

References

[1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42:40–46, 1999.

[2] U.S. General Services Administration. Section 508. https://www.section508.gov/ access at May 14, 2023.

[3] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. Privacy concerns and behaviors of people with visual impairments. CHI '15, page 3523–3532. Association for Computing Machinery, 2015.

[4] Taslima Akter, Bryan Dosono, Tousif Ahmed, Apu Kapadia, and Bryan Semaan. "i am uncomfortable sharing what i can't see": Privacy concerns of the visually impaired with camera based assistive applications. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1929–1948. USENIX Association, 2020.

[5] Sarah Andrew, Stacey Watson, Tae Oh, and Garreth W. Tigwell. A review of literature on accessibility and authentication techniques. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility*. Association for Computing Machinery, 2020.

[6] Apple. Copy and paste between devices from your mac. https://support.apple.com/guide/mac-help/copy-and-paste-between-devices-mchl70368996/mac access at May 14, 2023.

[7] Apple. Turn attention aware features on or off on your iphone or ipad pro. https://support.apple.com/en-us/HT208245 access at May 14, 2023.

[8] Daniel V. Bailey, Markus Dürmuth, and Christof Paar. Statistics on password re-use and adaptive strength for financial accounts. In *Security and Cryptography for Networks*, pages 218–235. Springer International Publishing, 2014.

[9] Natã M. Barbosa, Jordan Hayes, and Yang Wang. Unipass: Design and evaluation of a smart device-based password manager for visually impaired users. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '16, page 49–60, New York, NY, USA, 2016. Association for Computing Machinery.

[10] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M Redmiles, and Angelika Strohmayer. Ethical practices for security research with at-risk populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 546–553. IEEE, 2022.

[11] Ramon Blanco-Gonzalo, Chiara Lunerti, Raul Sanchez-Reillo, and Richard Michael Guest. Biometrics: Accessibility challenge or opportunity? *PLOS ONE*, 13:1–20, 03 2018.

[12] Billie Bonevski, Madeleine Randell, Chris Paul, Kathy Chapman, Laura Twyman, Jamie Bryant, Irena Brozek, and Clare Hughes. Reaching the hard-to-reach: a systematic review of strategies for improving health and medical research with socially disadvantaged groups. *BMC medical research methodology*, 14:1–29, 2014.

[13] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567, 2012.

[14] Zachary Breit, Hunter Dean, Tai-Juan Generrette, Samuel Howard, Balaji Kodali, Jim Kong, Jonah Tash, Phillip Wang, and John Wu. Exploration of the security and usability of the fido2 authentication protocol. *Gemstone Team Research*, 2022.

[15] Lizzie Coles-Kemp and Peter Hall. Trespass book 3: Creative engagements. 2016.

[16] Lizzie Coles-Kemp, Nick Robinson, and Claude PR Heath. Protecting the vulnerable: Dimensions of assisted digital access. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–26, 2022.

[17] Sanchari Das, Gianpaolo Russo, Andrew C. Dingman, Jayati Dev, Olivia Kenny, and L. Jean Camp. A qualitative study on usability and acceptability of yubico security key. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, page 28–39, 2018.

[18] Sanchari Das, Bingxi Wang, Zachary Tingle, and L. Jean Camp. Evaluating user perception of multi-factor authentication: A systematic review. *CoRR*, 2019.

[19] Kerry Dobransky and Eszter Hargittai. The disability divide in internet access and use. *Information, Communication & Society*, 9:313–334, 2006.

[20] Bryan Dosono, Jordan Hayes, and Yang Wang. "i'm stuck!": A contextual inquiry of people with visual impairments in authentication. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, pages 151–168. USENIX Association, 2015.

[21] Dana Dunn and Erin Andrews. Person-first and identity-first language developing psychologists' cultural competence using disability language. *The American psychologist*, 70, 2015.

[22] Polina Evtimova and James Nicholson. Exploring the acceptability of graphical passwords for people with dyslexia. In Carmelo Ardito, Rosa Lanzilotti, Alessio Malizia, Helen Petrie, Antonio Piccinno, Giuseppe Desolda, and Kori Inkpen, editors, *Human-Computer Interaction – INTERACT 2021*, pages 213–222, Cham, 2021. Springer International Publishing.

[23] Daniella Briotto Faustino and Audrey Girouard. Understanding authentication method use on mobile devices by people with vision impairment. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, page 217–228. Association for Computing Machinery, 2018.

[24] Uwe Flick, Ines Steinke, and Ernst von Kardorff. *Qualitative Forschung: ein Handbuch*. Rowohlt, Germany, 2000.

[25] Lothar Fritsch, Kristin Fuglerud, and Ivar Solheim. Towards inclusive identity management. *Identity in the Information Society*, 3:515–538, 2010.

[26] Steven Furnell, Kirsi Helkala, and Naomi Woods. Disadvantaged by disability: Examining the accessibility of cyber security. In *Universal Access in Human-Computer Interaction. Design Methods and User Experience*, pages 197–212. Springer International Publishing, 2021.

[27] Steven Furnell, Kirsi Helkala, and Naomi Woods. Accessible authentication: Assessing the applicability for users with disabilities. *Computers & Security*, 113, 2022.

[28] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285, 2020.

[29] Maximilian Golla. *On the Usability and Security of Password-Based User Authentication*. Masters Theses and Doctoral Dissertations, Ruhr University Bochum, Germany, 2020.

[30] Jordan Hayes, Bryan Dosono, and Yang Wang. "they should be convenient and strong": Password perceptions and practices of visually impaired users. *iConference 2017 Proceedings*, 2017.

[31] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 1–20, Santa Clara, CA, August 2019. USENIX Association.

[32] Jordan Hayes, Xiao Li, and Yang Wang. "i always have to think about it first": Authentication experiences of people with cognitive impairments. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, page 357–358. Association for Computing Machinery, 2017.

[33] Claude PR Heath, Peter A Hall, and Lizzie Coles-Kemp. Holding on to dissensus: Participatory interactions in security design. *Strategic Design Research Journal*, 11(2), 2018.

[34] Hurraki. Hurraki - wörterbuch für leichte sprache. https://hurraki.de/wiki/Hauptseite access at May 14, 2023.

[35] Fethi A. Inan, Akbar S. Namin, Rona L. Pogrund, and Keith S. Jones. Internet use and cybersecurity concerns of individuals with visual impairments. *Educational Technology & Society*, 19:28–40, 2016.

[36] Paul T. Jaeger. *Disability and the Internet: Confronting a Digital Divide*. Lynne Rienner Publishers, 2012.

[37] Stefan Johansson, Jan Gulliksen, and Catharina Gustavsson. Disability digital divide: the use of the internet, smartphones, computers and tablets among people with disabilities in sweden. *Universal Access in the Information Society*, 20:105–120, 2020.

[38] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. Human factors in security research: Lessons learned from 2008-2018. *CoRR*, 2021.

[39] Nicole Kelly and Helen Petrie. Digital authentication and dyslexia: A survey of the problems and needs of dyslexia people. In *Computers Helping People with Special Needs*, pages 18–25. Springer International Publishing, 2022.

[40] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "it's stored, hopefully, on an encrypted server'': Mitigating users' misconceptions about FIDO2 biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 91–108. USENIX Association, 2021.

[41] Brittany Lewis and Krishna Venkatasubramanian. "i...got my noseprint. but it wasn't accurate": How people with upper extremity impairment authenticate on their personal computing devices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. Association for Computing Machinery, 2021.

[42] Christiane Maaß. *Easy Language - Plain Language - Easy Language Plus: Balancing Comprehensibility and Acceptability*. Frank & Timme, 2020.

[43] Philipp Mayring and Michaela Gläser-Zikuda. *Die Praxis der Qualitativen Inhaltsanalyse*. Beltz, 2005.

[44] Kyle Murbach. *Self-Efficacy in Information Security: A Mixed Methods Study of Deaf End-Users*. Masters Theses and Doctoral Dissertations, Dakota State University, 2019.

[45] Daniela Napoli. Developing accessible and usable security (accus) heuristics. CHI EA '18, page 1–6, New York, NY, USA, 2018. Association for Computing Machinery.

[46] Daniela Napoli, Khadija Baig, Sana Maqsood, and Sonia Chiasson. "i'm literally just hoping this will Work:'' obstacles blocking the online security and privacy of users with visual disabilities. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 263–280. USENIX Association, 2021.

[47] James Nicholson, Lynne Coventry, and Pam Briggs. Faces and pictures: Understanding age differences in two types of graphical authentications. *International Journal of Human-Computer Studies*, 71(10):958–966, 2013.

[48] James Nicholson, Lynne Coventry, and Pamela Briggs. Age-related performance issues for pin and face-based authentication systems. 04 2013.

[49] United Nations Department of Economic and Social Affairs. Convention on the rights of persons with disabilities (crpd). https://social.desa.un.org/issues/disability/crpd/convention-on-the-rights-of-persons-with-disabilities-crpd access at May 14, 2023.

[50] Britta Offergeld and Laura Bell. Blindsided by security; the reality of web security for the visually impaired. 2012.

[51] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. Multi-factor authentication: A survey. *Cryptography*, 2, 2018.

[52] Jacques Ophoff, Graham Johnson, and Karen Renaud. Cognitive function vs. accessible authentication: Insights from dyslexia research. In *Proceedings of the 18th International Web for All Conference*. Association for Computing Machinery, 2021.

[53] World Health Organization. Disability and health. https://www.who.int/news-room/fact-sheets/detail/disability-and-health access at May 14, 2023.

[54] Helen Petrie, Andreas Savva, and Christopher Power. Towards a unified definition of web accessibility. In *Proceedings of the 12th International Web for All Conference*, pages 1–13, 2015.

[55] Karen Renaud. Accessible cyber security: The next frontier? In *Proceedings of the 7th International Conference on Information Systems Security and Privacy - ICISSP,*, pages 9–18, 2021.

[56] Karen Renaud and Lizzie Coles-Kemp. Accessible and inclusive cyber security: A nuanced and complex challenge. *SN Computer Science*, 3, 2022.

[57] Karen Renaud, Graham Johnson, and Jacques Ophoff. Accessible authentication: dyslexia and password strategies. *Information and Computer Security*, 29:604–624, 2021.

[58] Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina. Internet. *Our World in Data*, 2015. https://ourworldindata.org/internet access at May 14, 2023.

[59] Daniela Rosner, Alex Taylor, Mikael Wiberg, and Amanda Windle. The urgency for access. *Interactions*, 28(3):5–5, 2021.

[60] Shruti Sannon and Andrea Forte. Privacy research with marginalized groups: What we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–33, 2022.

[61] Suzanna Schmeelk and Helen Petrie. Digital authentication for visually disabled people: Initial results of an online survey. page 41–50, Berlin, Heidelberg, 2022. Springer-Verlag.

[62] Suzanna Schmeelk and Helen Petrie. Digital authentication for visually disabled people: Initial results of an online survey. In *Computers Helping People with Special Needs*, pages 41–50. Springer International Publishing, 2022.

[63] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I Hong, and Laura Dabbish. Normal and easy: Account sharing practices in the workplace. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–25, 2019.

[64] Statista. Forecast of the number of internet users in the world from 2010 to 2025. https://www.statista.com/forecasts/1146844/internet-users-in-the-world access at May 14, 2023.

[65] Michelle Steves, Dana Chisnell, Angela Sasse, Kat Krol, Mary Theofanos, and Hannah Wald. Report: Authentication diary study. 2014.

[66] European Union. Directive (eu) 2016/2102 of the european parliament and of the council of 26 october 2016 on the accessibility of the websites and mobile applications of public sector bodies. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L2102 access at May 14, 2023.

[67] U.S. Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, August 2012. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of May 14, 2023.

[68] Rebecca Vallas, Kim Knackstedt, Hayley Brown, Julie Cai, Shawn Fremstad, and Andrew Stettner. Economic justice is disability justice. *The Century Foundation*, 2022. https://tcf.org/content/report/economic-justice-disability-justice/ access at May 14, 2023.

[69] World Wide Web Consortium (W3C). Web content accessibility guidelines (wcag) 2.1. https://www.w3.org/TR/WCAG21/ access at May 14, 2023.

[70] World Wide Web Consortium (W3C). Web content accessibility guidelines (wcag) 2.2. https://www.w3.org/TR/WCAG22/ access at May 14, 2023.

[71] Noosheen Walji, Patricia K Sheridan, Penny Kinnear, Robert Irish, and Jason Foster. Who you are and how you work: Embedding positionality in engineering design. *Proceedings of the Canadian Engineering Education Association (CEEA)*, 2020.

[72] Yang Wang. The third wave? inclusive privacy and security. In *Proceedings of the 2017 new security paradigms workshop*, pages 122–130, 2017.

[73] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2344–2360. IEEE, 2022.

7. Appendices

7.1. Questionnaire

Page 1

Q1.1 Please select your gender.

- ○ Male
- ○ Female
- ○ Non-binary
- ○ Prefer not to answer

Q1.2 Please enter your age:

_____

Q1.3 Please select your kind of disability.

- ▫ Visual impairment
- ▫ Hearing impairment
- ▫ Physical impairment
- ▫ Mental disorder
- ▫ Learning disabilities
- ▫ Other: _____

Q1.4 Please select your highest education level.

- ○ No Degree
- ○ Secondary School
- ○ High School
- ○ Bachelor's degree
- ○ Master's degree
- ○ Other: _____

Q1.5 Which statement describes your educational background or career field?

- ○ I have an education in computer science or work in this field
- ○ I have no education in computer science or work in this field

Page 2

Q2.1 To what extent are you self-employed in your use of technology?

- ○ Self-employed
- ○ Mostly self-employed, but need help from others from time to time
- ○ Basically with help from others e.g. assistance
- ○ Prefer not to answer

Q2.2 Please list assistive technologies that you use in everyday life.

_____

Q2.3 Do you experience particular problems in using technology related to your disability?

- ○ Yes
- ○ No

Note: If previous question was answered with yes

Q2.4 Please list the challenges you have perceived.

_____

Q2.5 Please specify if and what problems arise when using technology.

- ▫ I am not aware of any problems
- ▫ Orientation problems
- ▫ Comprehension problems
- ▫ information overload
- ▫ Lack of subtitles or sign language of videos.
- ▫ Other issues: _____

Q2.6 Do you use authentication methods such as Face ID?

- ○ Yes
- ○ No

Note: In Article 9(1), the UN Convention on the Rights of Persons with Disabilities requires its signatory states to take appropriate measures to ensure access to information and communication, including information and communication technologies and systems, for persons with disabilities on an equal basis with others. (2009)

Q2.7 How do you rate the accessibility of information and communication technologies and systems?

- ○ Accessibility has improved
- ○ Accessibility has not changed
- ○ Accessibility has decreased
- ○ I do not know

Q2.8 Due to the COVID 19 pandemic, many activities moved to the internet, e.g. online learning. How do you perceive the accessibility?

- ○ Accessibility has improved
- ○ Accessibility has not changed
- ○ Accessibility has decreased
- ○ I do not know

Q2.9 Please state to which you agree with the following statements (Matrix question, scale of 1-10).

- People with disabilities have sufficient access to technology compared to people without disabilities.
- I have sufficient access to technology compared to people without disabilities.
- I have sufficient access to technology compared to people with disabilities.
- People with disabilities are sufficiently included in the digital society compared to people without disabilities.
- I feel sufficiently included in the digital society compared to people without disabilities.
- I feel sufficiently included in the digital society compared to people with disabilities.

Page 3

Q3.1 Please enter your email so we can contact you for the interview.

_____

7.2. Interview Guide

General Questions

To begin, I want to ask you a few general questions.

1) Can you describe your disability?
2) Which digital devices do you use in everyday life?
3) Do you use any assistive technologies to help you use technology?

[If answered]

3.1) How do you use these technologies?
3.2) How helpful do you think this technology is?

Authentication Methods

Let's move right on to the next block of questions.

1) What do you understand under the term authentication?
2) Are you aware of any dangers related to authentication?

I will read you a brief definition of authentication, which might expand on your definition, so we're talking about the same thing: Authentication is the process by which a user's identity is verified. It is done so by a trusted entity. This verifies the identity of the user based on the information provided, for example, in a database. Based on this definition...

3) Which authentication methods are you using?
4) On average, how many times a day do you authenticate to a device, system, or app?
5) Why do you use authentication methods?
6) Which authentication method are you using most?
[If answered]

6.1) In what context do you use this authentication method?

7) How secure do you feel when using authentication methods?
[If answered]

7.1) Why do you think that is the case?

Accessibility, Knowledge and Risks

1) What do you understand under the term accessibility in relation to technology?
2) How do you rate the accessibility of authentication methods?
[If answered]

2.1) Why do you think that is the case?

3) You have already mentioned [...] methods. Do you know any others?
[If yes]

3.1) Can you tell me which ones?

4) Are you aware of cyber threat risks?
5) Do you feel well informed about protection against cyber threats?
[If answered]

5.1) Would you want a specific seminar or training to help you learn safety behaviors, practices, or measures?

Knowledge-based Authentication

We talked about different authentication methods. Now I want to ask you questions about knowledge-based authentication methods. With knowledge-based authentication methods, users are verified, for example, by having to enter a username and the associated password.

1) Do you use knowledge-based authentication methods?
[If no]

1.1) Why do you not use this authentication method?
[If yes]

1.2) Do you face any challenges during the enrolment task?
[If yes]

1.2.1) Which challenges did you face?
1.2.2) Did you get help from a third person?
1.2.3) How do you rate the accessibility and usability?
1.2.4) How would you compare to people without disabilities?
1.2.5) How could the process be improved for you?

1.3) Do you face challenges during the authentication task?
[If yes]

1.3.1) Which challenges did you face?
1.3.2) Did you get help from a third person?
1.3.3) How do you rate the accessibility and usability?
1.3.4) How would you compare to people without disabilities?
1.3.5) How could the process be improved for you?

1.4) Do you face challenges during the recovery task?
[If yes]

1.4.1) Which challenges did you face?
1.4.2) Did you get help from a third person?
1.4.3) How do you rate the accessibility and usability?
1.4.4) How would you compare to people without disabilities?
1.4.5) How could the process be improved for you?

1.5) How secure do you feel when knowledge-based authentication methods?
[If answered]

1.5.1) Why do you think that is the case?

2) Are you aware of any dangers related to knowledge-based authentication methods?

Possession-based Authentication

Now I want to ask you questions about possession-based authentication methods. With possession-based authentication methods, users are verified by requiring them to have an object such as a key or ID card.

1) Do you use possession-based authentication methods?
[If no]

1.1) Why do you not use this authentication method?
[If yes]

1.2) Do you face any challenges during the enrolment task?
[If yes]

1.2.1) Which challenges did you face?
1.2.2) Did you get help from a third person?
1.2.3) How do you rate the accessibility and usability?
1.2.4) How would you compare to people without disabilities?
1.2.5) How could the process be improved for you?

1.3) Do you face challenges during the authentication task?
[If yes]

1.3.1) Which challenges did you face?
1.3.2) Did you get help from a third person?
1.3.3) How do you rate the accessibility and usability?

1.3.4) How would you compare to people without disabilities?
1.3.5) How could the process be improved for you?
1.4) Do you face challenges during the recovery task?
[If yes]
1.4.1) Which challenges did you face?
1.4.2) Did you get help from a third person?
1.4.3) How do you rate the accessibility and usability?
1.4.4) How would you compare to people without disabilities?
1.4.5) How could the process be improved for you?
1.5) How secure do you feel using possession-based authentication methods?
[If answered]
1.5.1) Why do you think that is the case?
2) Are you aware of any dangers related to possession-based authentication methods?

Biometric Authentication

Now I want to ask you questions about biometric authentication methods. With biometric authentication methods, users are verified using face recognition or fingerprints.

1) Do you use biometric authentication methods?
[If no]
1.1) Why do you not use this authentication method?
[If yes]
1.2) Do you face any challenges during the enrolment task?
[If yes]
1.2.1) Which challenges did you face?
1.2.2) Did you get help from a third person?
1.2.3) How do you rate the accessibility and usability?
1.2.4) How would you compare to people without disabilities?
1.2.5) How could the process be improved for you?
1.3) Do you face challenges during the authentication task?
[If yes]
1.3.1) Which challenges did you face?
1.3.2) Did you get help from a third person?
1.3.3) How do you rate the accessibility and usability?
1.3.4) How would you compare to people without disabilities?
1.3.5) How could the process be improved for you?
1.4) Do you face challenges during the recovery task?
[If yes]
1.4.1) Which challenges did you face?
1.4.2) Did you get help from a third person?
1.4.3) How do you rate the accessibility and usability?
1.4.4) How would you compare to people without disabilities?
1.4.5) How could the process be improved for you?
1.5) How secure do you feel using biometric authentication methods?
[If answered]
1.5.1) Why do you think that is the case?
2) Are you aware of any dangers related to biometric authentication methods?

Multi-Factor Authentication

We've already talked about simple authentication methods, and now we move on to the final question block of multi-factor authentication.

1) What do you understand under the term multi-factor authentication?
[If answered]
1.1) Next, I would like you to compare multi-factor authentication with the simple authentication. Can you name the differences?

I want to read you a short definition of the term MFA, which could expand your definition so that we are talking about the same thing: In multi-factor authentication, for example, an account is not only secured by username and the matching password but by further queries. The additional security level usually consists of a request for another password generated only for this login. Depending on the company, the user receives a code through the respective app, an alternative program, or via SMS. Based on this definition...

2) Do you use multi-factor authentication?
[If yes]
2.1) Why do you use multi-factor authentication?
2.2) In what context do you use multi-factor authentication?
[If no]
2.3) Why do you not use multi-factor authentication?

In 2018, the new payment services directive PSD2 (Payment Services Directive2) was realized in Germany. It requires banks to implement multi-factor authentication. Online and card payments must now be confirmed by two independent factors from the categories of knowledge, possession, and biometric.

3) Do you use online banking?
[If no]
3.1) Why do you not use online banking?
[If yes]
3.2) Do you face challenges during the MFA process?
[If yes]
3.2.1) Which challenges did you face?
3.2.2) Did you call for help from a third person?
3.2.3) How do you rate the accessibility and usability?
3.2.4) How would you compare to people without disabilities?
3.2.5) How could the process be improved for you?
3.3) How secure do you feel using multi-factor authentication?
[If answered]
3.3.1) Why do you think that is the case?
4) Are you aware of any dangers regarding multi-factor authentication?

Ending

We're almost done. Now that our conversation is coming to an end, I would like to ask you to evaluate your sense of security when using authentication methods:

1) How secure do you feel when using authentication methods?

[If answered]

1.1) Why do you think that is the case?

2) Ho do you rate the accessibility and usability?
[If answered]

2.1) Why do you think that is the case?

Now into the last question. There are no limits to your ideas.

3) How do you envision the perfect authentication method for you?

Alright, that's it from my side.

4) Is there anything else you want to tell me that is important to you or has not yet come up in the interview?

Alright, the interview is almost over.

5) Do you have any questions or comments about the study?

Great. The interview is over. I will now stop the recording.

7.3. Authentication Terms in Plain Language

Difficult terms in plain language should always be explained with an example. It is assumed that people have little knowledge about the world. Certain passages are written out in detail. Unimportant or less relevant passages are skipped. In the following, the terms knowledge-based, possession-based, and biometric authentication are given in plain language.

Knowledge-based Authentication

If you want to buy something online, you need to sign up on the website first. This means you'll have to give some personal information like your name, address, and birthdate. Once you've filled out everything, you'll need to choose a username and a password to protect your information. Your username can be your email address, and your password should be something that nobody else can guess. All of your information will be saved in a computer system called a database. If you need to confirm your purchase later, you'll need to enter your username and password again, and the computer will check to make sure it's really you. This process is called "knowledge-based authentication."

Possession-based Authentication

Are you working in a company? Then you will get a chip card from that company. The simple word for it is: key card. If you want to open the entrance door of the company, there is a card reader next to the door. Just hold your chip card in front of the card reader. The card reader knows that you have arrived, and the door opens. The difficult word for this process is called: possession-based authentication.

Biometric Authentication

Did you lose your ID card and need a new one? You will have to go to the town hall. An employee will check your personal information in a database, which may include comparing your fingerprints, facial features, and eye color. This process is called "biometric authentication".

7.4. Tables

TABLE 4. THE FINAL CODEBOOK. (*) DENOTES A CONTAINER FOR SUB-CODES AND THEREFORE IS NOT USED DURING CODING.

Code	Description	Example Quote
Individual (*)	Statements that describe participants individually	-
Type of Disability	Statements that refer to a participant's disability	P1: Okay, my disability is called tetraparesis. That is paralysis of the legs and arms.
Usage of Digital Devices	Statements that refer to a participant's digital device use	P6: So, a smartphone, laptop, and occasionally a tablet.
Usage of Assistive Technologies	Statements that refer to a participant's assistive technology use	P12: I use a scanner with OCR software at work.
General (*)	General statements	-
Understanding About Authentication	Statements that include the interpretation or definition of authentication	P12: In the context of what we're talking about, identity verification or identity matching.
Understanding About Accessibility	Statements that include the interpretation or definition of accessibility	P4: That certain procedures and web pages are operable with screen readers, for example [...]
Support Needs	A participants names perceived help from others	A2: P2 can operate a computer only with assistance.
Knowledge-based Authentication (*)	Statements that contain information about knowledge-based authentication	-
Experience	A participant describes their general experience	P3: [I use] email address and password for social media.
Challenges	A participant describes difficulties and/or challenges	P8: When setting up an account, I do have problems.
Workarounds	A participant explains developed workarounds	P1: You have points in many systems and don't see the password. I enter the password into another program and copy it into the field.
Accessibility & Usability	A participant evaluates accessibility and usability	P8: Considering my assistive tools, already very good.
Feeling of Security	A participant describes the perceived feeling of security	P3: Very safe. I mean, nobody knows the four-digit code.
Recommendation	A participant makes recommendations and ideas on how to improve	A2: I could imagine an explanatory video that explains the registration step by step.
Concerns & Threats	A participant expresses concerns and describes possible threats	P1: Sometimes it has happened that my password has been cracked.
Token-based Authentication (*)	Statements that contain information about token-based authentication	-
Experience	A participant describes their general experience	P12: Yes, at the university. I have used the Rubicon.
Challenges	A participant describes experienced difficulties and/or challenges	P7: More difficult are the numbers that you get and have to transfer from A to B in a few seconds.
Workarounds	A participant explains developed workarounds	P6: When it comes to technical things, I have my IT buddy who does them for me because I don't understand the instructions.
Accessibility & Usability	A participant evaluates accessibility and usability	P7: It still works out. But there are minimal hurdles in everyday life.
Feeling of Security	A participant describes the perceived feeling of security	P7: Unsafe. [It] is associated with more obstacles for a person with visual impairment.
Recommendation	A participant makes recommendations and ideas on how to improve	P5: A longer time limit would be enough for me.
Concerns & Threats	A participant expresses concerns and describes possible threats	P1: Yes, identity theft again. [Someone] could steal the card and pass it off as me.
Reasons Against the Use	A participant gives reasons against the use	P10: No, I'm hearing about this for the first time today. [I] can't tell you anything about it.
Biometric Authentication (*)	Statements that contain information about biometric-based authentication	-
Experience	A participant describes their general experience	P7: On the iPhone [I] use the fingerprint sensor and facial recognition.
Challenges	A participant describes experienced difficulties and/or challenges	A2: [The] finger [must] be held behind the phone to scan it, [but] the phone is mostly on the table.
Workarounds	A participant explains developed workarounds	A2: Or I can get P2 a cell phone holder. With it could work.
Accessibility & Usability	A participant evaluates accessibility and usability	P5: For me, that always feels very cumbersome. [...] Even in times of Corona. It no longer works with the mask.
Feeling of Security	A participant describes the perceived feeling of security	P6: It's pretty safe. The fingerprint is unique to everyone.
Recommendation	A participant makes recommendations and ideas on how to improve	P4: Set the error sensitivity so that a detection process is not immediately interrupted if the camera is shifted a bit out of the angle.
Concerns & Threats	A participant expresses concerns and describes possible threats	P11: Theoretically, you can hold a photo during face recognition.
Reasons Against the Use	A participant gives reasons against the use	P12: My smartphone doesn't need to know what my face looks like, and it doesn't need to know what my fingerprint looks like.
Comprehension Problems	A participant does not understand the interviewer	P3: [I] didn't understand you very well.
CAPTCHA	A participant makes statements about CAPTCHA	P4: Otherwise, there are [these] CAPTCHA. These with numbers or letters obscured pictures, where you have to enter them.
Context Independent	Statements that are independent of authentication but relevant to accessibility	P1: I wish we would be heard more and [people] would take our wishes to heart and not just implement their ideas.