Challenges with Electronic Identity Authentication: A Qualitative Study with Disabled Participants

David Cropley * , Paul Whittington , Huseyin Dogan

Posted Date: 18 March 2026

doi: 10.20944/preprints202603.1487.v1

Keywords: accessibility; assistive technology (AT); authentication; authorization; disabled users; electronic identification (eID); empirical study; human-computer interaction (HCI); login system

 doi:10.20944/preprints202603.1487.v1

Article

Challenges with Electronic Identity Authentication: A Qualitative Study with Disabled Participants

David Cropley *, Paul Whittington and Huseyin Dogan

Faculty of Media, Science and Technology, Bournemouth University, United Kingdom

* Correspondence: dcropley@bournemouth.ac.uk

Abstract

The background to this research paper approaches why it is that people with disabilities often have extra problems with authentication (i.e., addresses why people with disabilities often have extra problems with authentication (i.e., logging in to online services). While the focus is on authentication, we also explore its relevance to electronic identification and consider the post-authentication authorization (allowing continued use of the service once logged in). While people without disabilities regularly log into websites and applications without too much thought for the process, with an end-goal or task in mind to be achieved with the service that they are accessing. We discover how there is a societal gap in terms of ease-of-use, as previous studies show that people with disabilities can find this step difficult, frustrating, or virtually impossible. For people who have a disability, complications will arise in this process, and we examine the nature of these problems identified by this group. A series of interviews (n=15) is analyzed with Constructivist Grounded Theory methods to discover patterns in the participants' answers and build a theory about why Accessible Authentication is a problem. While aiming to follow constructivist theory methodology, this paper categorizes common traits that participants have revealed in interviews. The key findings reveal that most disabled users say that ability to authenticate effectively is reduced by accessibility barriers; in other words, participants felt hindered when logging in because of their disability. This leads us to conclude, with some degree of confidence, that the data implies a lack of accessibility for users of traditional authentication techniques. A further area of concern for the participants is that maintaining security alongside ease-of-use was important to them (albeit with no clear winner), so future work on improving accessibility should ensure that disabled users' information is not left vulnerable, while maintaining a sufficient level of accessibility for people with disabilities.

Keywords: accessibility; assistive technology (AT); authentication; authorization; disabled users; electronic identification (eID); empirical study; human-computer interaction (HCI); login system

1. Introduction

1.1. Overview

This research aims to elicit empirical evidence to guide the development of a Theoretical Framework (TF) that can be referred to by organizations wishing to implement an Accessible Authentication (AA) system for their clients, i.e., a login system for their application or service, which genuinely considers disabled users' supplementary needs when trying to identify themselves. Therefore, the purpose of this study is to investigate the various difficulties people with disabilities encounter when attempting to authenticate. However, we acknowledge certain limitations which are discussed in Section 5.2.

It is presupposed that this is generally not catered for by mainstream login systems, due to noncompliance with Web Content Accessibility Guidelines (WCAG) [1], which in turn is partially due to a lack of empathic understanding of people without sufficient physical or cognitive ability to conduct the verification process, as a non-disabled person might more easily accomplish. Not only is

 doi:10.20944/preprints202603.1487.v1

it important that reasonable adjustments for disabled users are made under the Equality Act 2010 [2], but it is also a legal requirement for public sector bodies [3].

Following on from this section, we introduce the current state of research in this area with a Literature Review on Accessible Authentication (Chapter 2). Subsequent chapters include our Methods (Chapter 3) for the collection and analysis of data, including abstraction from participants (3.2), Interview Questions (3.3), and Analysis Methodologies (3.4). The Results Chapter (4) disseminates results over multiple sections and sub-sections (too numerous to list here) and constructs the theory. We disseminate aspects of the theory in the Discussion Chapter (5) to appreciate the viability and future possibilities for the research and subsequently culminate with the Conclusion (Chapter 6), which aims to assess the potential impact of this research. Here, we also outline the development of a TF to examine how a lack of accessibility may be hindering our disabled community, and how it can be properly addressed and remedied.

1.2. Hypotheses

The authors propose several research questions that need to be answered in this problem space. Namely:

1. What are the difficulties that people with disabilities face when attempting to authenticate?
2. Is the person's disability the main hindrance to logging onto a system? i.e., is their problem with logging in directly related to their disability?
3. What are the tradeoffs between usability and security? i.e., do we need to make authentication easier for disabled users, or more secure, or both?

From these questions, it should be clear that we believe there will be signs that authentication is often more difficult for people with disabilities than for the average user. This raises concerns for our community about whether this function in the online world is accessible.

2. Literature Review

2.1. Systematic Literature Review

A systematic literature review has been previously published by the authors [4], with respect to the topic of authentication (logging in) for disabled users, which finds limitations in the usability of authentication systems and associated issues regarding security concerns [5] and develops a strong case for the need to improve usability in authentication systems, thus reinforcing this debate. The primary (and focal) search criteria for the review include both the terms 'disabilities' and 'authentication and both had to appear in the reviewed literature for inclusion to be valid. More specifically, it included the category of people with disabilities in the World Health Organization (WHO) Disability Assessment Schedule [6]. and sources included Science Direct, Bournemouth University Research Online (BURO), Sage Publishing, ResearchGate, and Google Scholar for primary criteria searches. Screening for the primary category would limit each reference to books or journals published within the last five years (with some established literature included).

While being mindful about inadequacies, the presented systematic literature review finds that most of the current research is fundamentally theoretical in nature, and those that do present empirical data are focused in specific areas such as biometrics or Special Education Needs and Disability (SEND) in educational testing environments [7], hence they are not necessarily substantiated when considering the empirical goal of our overarching concerns regarding barriers to authentication due to a disability, which will be essential for an all-encompassing Framework to defend the hypothesis that a viable and acceptable solution for Accessible Authentication is currently nebulous.

 doi:10.20944/preprints202603.1487.v1

2.1. Further Literature Review (Conducted at the Time of Writing)

An empirical paper on "Accessible Authentication methods for people with Diverse Cognitive Abilities" [8] reinforces the hypothesis that there are complex issues regarding the accessibility of current authentication techniques. Naturally, though, this paper only accounts for cognitive issues; we are looking at detriments caused by any disability. Not all papers will be this broad in classification. It may also be worth noting that a literature review by Andrew et al. [9] identified "shortfalls and gaps in the literature" in the field of Accessible Authentication, so emerging empirical evidence on this subject is a refreshing discovery.

Additionally, an empirical study conducted in 2017 discusses an alternative for authentication for People Who Are Blind [10], providing evidence for an alternative to traditional authentication. This technique uses a system of long and short taps, or audio entry. This is shown to provide security against eavesdroppers and shoulder surfers minimal detriment to ease of use. It is not known whether this has been implemented in any production environment. Still, it does introduce the idea that authentication can be made more accessible for blind people. It illustrates how scientific research can highlight specific accessibility requirements that need to be met.

A further related study assesses an alternative image-based authentication framework for people with Upper Extremity Impairments (UEIs) [11]. This provides valuable evidence that alternative authentication techniques can benefit disabled users (and potentially the wider community) through a more intuitive system. Although password strength calculations have proved to provide sufficient entropy against shoulder surfing and close-adversary attacks, there could be a scenario in which an online brute-force attack bot scans the first phase stochastically to reduce system integrity, so one might wonder whether it would ever be adopted for public release. Nonetheless, it remains a valid impetus and an important flagbearer for the cause of accessibility rights in authentication. It is also interesting to note that several participants said the application was fun to use, which could help eliminate many pain points when bringing a system like this to market.

The above represents the limited selection of documents available that directly relate to 'Accessible Authentication' (as a unified concept), despite an abundance of topics in either 'Accessibility' or 'Authentication' within their respective domains. Collectively, this paper aims not only to provide further empirical evidence in a relevant context but also to lay the foundations for a derived framework comprising suggestions for existing or new authentication systems, supplemented by a proposal for a prototype application to substantiate the framework's viability and practicality. This framework may eventually recommend a set of categories for AA classification or advise a set of target criteria for production-level implementation.

3. Methods

3.1. Overview

This paper examines a dataset comprising a series of interviews (n=15) with disabled users (with no restrictions on geographical region or gender) that were recorded in audio format and subsequently transcribed and coded using NVivo 20 [12], a qualitative analysis tool. Three stages of coding occurred, each being more refined than its predecessor.

3.2. Participants

The participants that we interviewed (n=15) were sourced from various geographic locations across the United Kingdom (UK), the United States of America (USA), and Europe (EUR); however, the research was open to candidates from all regions from all around the world, and there were no restrictions on this. Age ranges vary considerably from the youngest at 16–19 years through all other age groups (20-29, 30-39, 40-49) up to and including the 50+ age group. No children under the age of 16 were permitted to be included in the study (in line with the granted ethical approval). The ratio of female to male participants is exactly 1:2, with no participants identifying as anything other than these two variants. However, alternative options were provided to state this, if desired. We

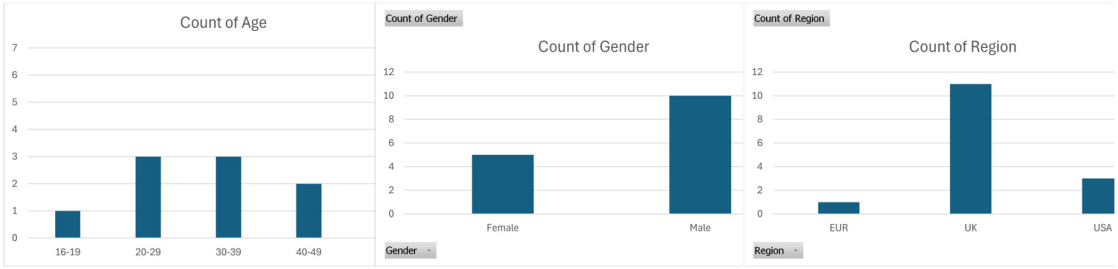
 doi:10.20944/preprints202603.1487.v1

acknowledge that this ratio is not ideally balanced and understand that experiences may vary when gender is considered; nevertheless, we aim to analyze and portray the results without bias, as expected.

Comparatively, the division of impairments between mental and physical disabilities (that were classified as relevant to the research), maintains an appropriate balance, including, but not limited to; Spinal Injury, Quadriplegia, Paraplegia, Facioscapulohumeral Muscular Dystrophy (FSHD), Cerebral Palsy (CP), Dyslexia, Dyspraxia, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorder (ASD) and Schizophrenia.

Bournemouth University (BU) assessed and approved the ethical considerations for this research, in line with their regulatory board. In terms of experience with Assistive Technology (AT), usage ranges from grammar-correction software to gaming AT (including custom switches, paddles, and pen tablets) to eye-tracking technology and wheelchair accessories. Further details of those that are relevant to the paper will be formally discussed in Section 4.

Table A1 depicts the formal demographics of all participants and is situated in Appendix A (A.1). Figure 1 represents this graphically.



(**a**) (**b**) (c)

Figure 1. Demographics showing distribution of (**a**) Age; (**b**) Gender; (**c**) Region.

3.3. Interview Questions

The questions for the interviews were, in general, designed to elicit qualitative results for this paper, and participants would frequently provide extra context when answering, so the majority of reporting for this paper will be qualitative in nature, which allows us to create a verbose theory, which may then hopefully lead on to the development of a Framework for Accessible Authentication. In future work, a refined questionnaire is intended to increase the granularity of the grounded philosophical theory following these first-phase interviews. Vice versa, the questionnaire may also elicit more quantitative results, which could scientifically balance with the constructive theory, and this research could potentially develop into a full mixed-methods analysis by the time it matures.

As an example of questions asked in the interviews, the participant is asked whether they believe that security is an organization's responsibility or their own. Furthermore, previous studies suggest there could be a tradeoff between ease of use and maximum security for logging in; however, literature suggests that people only want security that is "just okay" [13] and will naturally gravitate towards a system that is easier to use, for obvious reasons. Logically, the question then arises: who should take responsibility for a less secure system? Should the organization or the user decide how secure their access to the system is? The results from the interviews will be discussed further in Section 4. They could have a profound impact on the design and implementation of a system that hands over control to one side or the other.

Other questions, as well as preferences for usability over security, include the accessible technology currently used by participants and/or devices they can envisage using or would prefer to use. Later, device preferences can be used to assess and suggest optimal modes for electronic identification (eID) design and build, which may have a variety of other stemming, diversified applications in turn. Note that eID could be regarded as an accessorizing tool for authentication, and if utilized correctly, it can be a vehicle for improving accessibility.

 doi:10.20944/preprints202603.1487.v1

One more difficult question involves assessing their feelings when logging in, whether this is an everyday experience for them or if they have any negative feelings about it. Whilst there is an element of psychological analysis, it is designed to serve as a gauge for assessing the overall need for action and, consequently, to reinforce the validity of developing an Accessible Authentication Framework.

Please note that a complete list of the semi-structured questions asked in the interviews is provided in Table B1 in Appendix B (B.1) at the end of this paper.

3.4. Analysis Methodologies

As we will see in the following section, there was a decision to be made about whether to use inductive or deductive reasoning in our approach to this paradigm, resulting in a dichotomy between the two thought processes. Some questions also present the challenge of "propositional attitudes" [14], which lead to considerations about emotional "hopes, fears, or beliefs" about the predicament. Ultimately, a deductive methodology was chosen, and its justification will now be described in greater detail.

A decision was made to use Grounded Theory (GT) [15] methodologies rather than Thematic Analysis (TA) [16] to analyze the data, and the philosophical rationale for this is duly explained herewith. Initially, the methodological approach for analysis in this research was to use TA, on the basis that some existing themes had already been illuminated by both prior research and the author's own thoughts on this subject. However, on closer inspection, only very few of these themes contain substantial real-world data and consist mainly of early-stage hypotheses about whether usability and security are issues for people with disabilities who wish to authenticate online.

TA can be performed either inductively or deductively, and as a process of deductive reasoning stemming from initial themes it would require that the theory (based on these themes) would need to always be true in all cases [17], and therefore this method had to be discarded (for our purposes) due to the fact we are not trying to prove a tautology (i.e., a consistent truth), yet instead the objective is to provide solutions to various phenomena the occur in the field of AA. Consequently, an alternative derivative analysis method for GT will be needed to provide evidence of credibility, rather than mathematically determined outcomes.

Decisively, even though inductive reasoning can also be used as conjecture for TA, it was felt that there was not a substantial amount of existing research in this topic area to warrant (or support) a full investigation based on the TA thematic principles. Consequently, various GT methodologies were investigated to identify a suitable method for the data set that could yield further knowledge through analytical coding or pattern-based reconciliation.

Expanding more on the qualitative coding method used with Nvivo 20 mentioned above, this particular paper relies on the proven advantages of Grounded Theory [18] methodology to build a focused theory about the results and after careful consideration, Constructivist Theory (CT) [19] was selected as the more specific mode for application of the GT as this enables categorization of the data which in turn leads to the development of our theory, bearing around the key research question of "how can authentication be made accessible?".

This is done via a logical process of primarily generating a set of corresponding (reinforcing) patterns in the 'Initial Coding' phase, then refining and optimizing them in the 'Focusing Coding' phase to highlight commonalities and relational aspects. Finally, a 'Theoretical Coding' phase involves developing a collection of theorems based on qualitative interpretations of the codes that can be extrapolated upon to yield a final set of logical proofs which, in an ideal world, could be empirically replicated from further studies.

We must also consider that the ensuing analysis could be categorized as abductive reasoning, as there will be a temptation to succumb to interpretive guesswork, simply due to the subjective nature of the research. Nevertheless, the findings presented in the following results section are based on real-world empirical evidence, and therefore, we hope they will be acceptable as part of a scientific theory.

 doi:10.20944/preprints202603.1487.v1

4. Results

4.1. Overview

The results aim to answer the research questions posed in the previous section, and we anticipate that our analysis will reveal a wide variety of findings, as everyone is different. Therefore, this is a reason to use GT as a qualitative analysis method, as it allows us to develop a theory grounded in substantive results.

4.1.1. Categorization

Coding was divided into six broad categories during initial Stage 1 coding, including Disability (type and relation to the issue), AT Devices (assistive technology), Usability versus Security (including the tradeoff between the two), Issues (common problems), Desirable Features (ideal solutions), and finally, Responsibility (onus for security). Granularity can be found in a series of subcategories, tallied by the coding process.

4.1.2. Disability

To begin with, we wanted to find out what percentage of users feel their disability hinders their ability to authenticate, and most participants reported issues with authentication due to their disability. In contrast, others considered the problem unrelated to their disability. The results show 29 occasions (72%) in which participants considered authentication more difficult because of a disability, compared with 11 occasions (28%) in which users felt that their disability did not affect their ability to log in. It is worth noting that even users who said they did not have an issue went on to discuss areas where the authentication procedure could be improved, which is not indicative of having no difficulties at all.

According to the coding results, there was an equal balance between those willing to disclose information (about their disabilities) to a third party and those who wanted to keep their details confidential. Finally, a small number were concerned about issues caused by the ongoing deterioration of their disability.

The range of disabilities, either specifically stated by the participants' own personal disabilities or discussed in general conversation during the interview process (several of which were mentioned twice or more), is shown in Table 1, which also categorizes them into physical and cognitive realms:

Table 1. Disabilities were discussed in the interviews.

Disability Category	Nature of Disability
Physical	C6 Tetraplegia (Quadriplegia); Spinal Cord Injury; Muscular Dystrophy; Hand Dexterity[1]; Curved Spine[1]; Asthma; Spinal Problems[1]; Dyspraxia; Cerebral Palsy; Williams Syndrome[2]; Stroke[2].
Cognitive	Dyslexia; Dyspraxia[2]; ADHD; Attention Issues[1]; Obsessive Compulsive Disorder (OCD) [1]; Schizophrenia; Learning Disabilities[1]; Autism; Spectrum Disorder; Depression; Anxiety, Williams Syndrome[2]; Dementia; Stroke[2].

[1] In some cases, these are how the participant refers to the disability. [2] In some cases, a disability could fall into both physical and cognitive categories.

4.2. Coding Results and Resolution of the Theoretical Framework

Table A2 in Appendix A (A.2) records the number of times each topic was referenced in relation to the context of the issue. It is included for the purpose of validating this paper in any given future research opportunities or for use in statistical analyses of the data.

All coding was conducted solely by the first author of this paper, and codes were generated by identifying issues, pain points, and common themes in the transcripts. While the three-stage

 doi:10.20944/preprints202603.1487.v1

refinement helps decide on a final theory, the first-stage coding results remain an important part of the process, as they represent the raw, unrefined data initially discovered by this process. Consequently, the tables presented at the end of this analysis, which describe the beginnings of the proposed Framework, do depend on this raw data.

Three tables have been created that outline the proposed Framework we referred to earlier in this paper. They include mappings of disability against physical and cognitive effects (Table 2), relational connections between authentication challenges and disability types (Table 3), and finally, a table of suggested solutions to authentication issues mapped to both physical and cognitive disabilities (Table 4).

The first Framework table recognizes the different natures of disabilities and differentiates among various forms of physical and cognitive disabilities. It also sets the scene for the second table, which adds weighting to the physical and cognitive disability area in relation to the authentication problems observed in the interviews, and, really, it can be used to inform us as to which disability characteristics are likely to be placed under the most duress during the process of authentication. The third table of the Framework makes an initial attempt to provide solutions as remedies to the problem; it is recognized that this still needs to reference back to the second table to address the areas of greatest concern effectively

Table 2. Disability Types.

Name of Disability	**Degree of effect***			
	Physical	*Cognitive*		
	Physical Disability	Learning Disability	Psychological Disability†	Neurodevelopmental Disorder
ADHD[1]	N/a	N/a	N/a	Major
Anxiety [2]	N/a	N/a	Major	N/a
Asthma[3]	Major	N/a	Minor	N/a
Cerebral Palsy[4]	Major	N/a	N/a	Major
Dementia[5]	N/a	Minor	Minor	N/a
Depression[6]	N/a	N/a	Major	N/a
Dyslexia[7]	N/a	Major	N/a	N/a
Dyspraxia[8]	N/a	N/a	N/a	Major
Muscular Dystrophy[9]	Major	Minor	Minor	Major
Schizophrenia[10]	N/a	N/a	Major	Minor
Autism / Spectrum Disorder[11]	N/a	N/a	Minor	Major
Spinal Cord Injury / Malformation[12]	Major	N/a	Minor	N/a
Stroke[13]	Minor	N/a	N/a	Major
Williams Syndrome[14]	Minor	Major	Minor	N/a

Legend 1

Notes: *: The level of effect may vary from person to person. Includes Major, Minor, and N/a (Not applicable).

†: Also known as a Mental Health Condition. It should be noted that other disabilities can cause psychological difficulties, such as anxiety or depression.

Legend 2

References

1 Is ADHD a Learning Disability -Understanding Neurodiversity. https://www.skillsforhealth.org.uk/article/is-adhd-a-learning-disability-the-differences-and-co-occurrences/ (accessed on 28/02/2026).

 doi:10.20944/preprints202603.1487.v1

2 Your Guide to Anxiety and Disability Benefits. https://www.healthline.com/health/anxiety/is-anxiety-a-disability#qualifications (accessed on 28/02/2026).
3 Is Asthma a Mental Illness? https://biologyinsights.com/is-asthma-a-mental-illness-the-physical-mental-connection/ (accessed on 28/02/2026). Note: Asthma can cause difficulty in traversing to reach the authentication device.
4 Cerebral Palsy. https://www.ninds.nih.gov/health-information/disorders/cerebral-palsy (accessed on 28/02/2026).
5 What is dementia? https://www.alzheimers.org.uk/about-dementia/types-dementia/what-is-dementia (accessed on 28/02/2026). Note: While Dementia technically does not fall into any of the disability characteristics, it does cause cognitive difficulties, and people with learning disabilities are more likely to develop it than others.
6 When a mental health condition becomes a disability. https://www.gov.uk/when-mental-health-condition-becomes-disability (accessed on 28/02/2026).
7 Dyslexia. https://www.nhs.uk/conditions/dyslexia/ (accessed on 28/02/2026).
8 Is Dyspraxia A Disability? https://islts.co.uk/is-dyspraxia-a-disability/ (accessed on 28/02/2026).
9 How Does Muscular Dystrophy Affect the Brain? https://biologyinsights.com/how-does-muscular-dystrophy-affect-the-brain/ (accessed on 28/02/2026). Note: It can cause anxiety and depression.
10 Quadriplegia. https://continentalhospitals.com/diseases/quadriplegia/ (accessed on 28/02/2026). Generally caused by spinal cord injuries, but also by neurological conditions.
11 Schizophrenia. https://www.nhs.uk/mental-health/conditions/schizophrenia/overview/ (accessed on 28/02/2026). Note: Generally accepted to be a psychological disability, but some may question if it is neurodevelopmental: https://psychiatryclinic.org/is-schizophrenia-a-neurodevelopmental-disorder/. (accessed on 28/02/2026).
12 Autism Spectrum Disorder. https://www.nimh.nih.gov/health/publications/autism-spectrum-disorder (accessed on 28/02/2026). Note: Not generally classified as a disability, but more as a developmental disorder, as often symptoms appear in the first 2 years of life
13 Cognitive Effects of Spinal Cord Injury on the Brain. https://biologyinsights.com/cognitive-effects-of-spinal-cord-injury-on-the-brain/ (accessed on 28/02/2026). Note: Generally caused by spinal cord injuries, but also by neurological conditions. Spinal disabilities can also cause psychological issues.
14 Psychological Effects of Stroke. https://www.england.nhs.uk/london/wp-content/uploads/sites/8/2019/09/Psychological-Effects-of-Stroke.pdf (accessed on 28/02/2026). Note: Predominantly a neurological condition that can cause physical disability such as semi-paralysis.
15 What is it? https://williams-syndrome.org.uk/what-is-williams-syndrome-6-2/ (accessed on 28/02/2026).

Table 3. Relational Connections.

Name of Disability	**Degree of effect***			
	Physical	*Cognitive*		
	Physical Disability	Learning Disability	Psychological Disability†	Neurodevelopmental Disorder
Authenticator issues (technical)[1]	6	0	5	1

 doi:10.20944/preprints202603.1487.v1

CAPTCHA issues[2]	2	2	1	4
Character set (not readable)[3]	0	2	0	4
Code retrieval delays[4]	2	2	1	6
Distance from device[5]	8	0	7	3
Environmental distractions[6]	2	0	1	2
Fingerprint scanners[7]	0	2	0	4
Forgotten password[8]	4	5	4	14
Frustrating experience[9]	12	4	9	14
Identification (Authentication)[10]	2	0	2	2
Locked out of service[11]	8	1	3	10
Low difficulty / no issues (control)[12]	11	4	8	13
Number of accounts needed (too many)[13]	3	0	0	4
Password mismatching (on signup)14	2	3	1	8
Privacy concerns[15]	10	3	4	12
Repeated login attempts needed[16]	7	2	2	8
Time based codes[17]	4	2	1	6
Time consuming[18]	3	3	1	10
Two-Factor Authentication (2FA)[19]	8	0	6	1

Legend 3

Notes

*: The level of effect may vary from person to person. Scores + 2 for Major Degrees of Effect and + 1 for Minor (for each participant's disability related to those in Table 2)

†: Also known as a Mental Health Condition. It should be noted that other disabilities can cause psychological difficulties, such as anxiety or depression.

Legend 4

References (Participant / Timestamps | ...)

1 P02 / 34:16.6, 34:36.7 | P05 / 2:40.1 | P15 / 21:39.8

2 P01 / 3:13.7 | P02 / 46:03.1, 46:17.3, 46:33.4, 46:39.4, 47:14.4

3 P01 / 1:00.3, 3:01.4

4 P01 / 10:17.0 | P02 / 16:03.3 | P15 / 21:39.8

5 P02 / 5:29.2, 6:25.2, 16.18.2 | P04 / 4:11:0 | P05 / 1:18.2, 1:40.9, 2:31.9, 2.:40.1, 9:06.3 |P06 / 19.11.7 | P15 / 25.02.3

6 P02 / 6:25.2, 6:40.0 | P15 / 0:54.8

7 P01 / 4:19.9

8 P01 / 10:17.0 | P09 / 10:02.9, 5:19.8 | P10 / 0:54.4, 5:05.1 | P12 / 15:38.5 | P13 / 0:39.5, 4:21.2 | P14 / 0:30.5 | P15 / 0:54.8, 16:08.5

9 P02 / 47:19.1 | P03 / 11:54.1 | P04 / 4:11.0, 19:55.6, 25:04.6 | P09 / 5:09.2 | P10 / 6:58.8 | P11 / 10:06.6, 11:06.1, 11:24.8, 11:54.5, 12:55.1 | P12 / 1:31.2, 5:18.1, 15:38.5 | P13 / 2:26.5, 4:32.7, 5:24.5 | P14 / 1:21.7, 1:29.6 | P15 / 1:32.4, 3:42.8, 22:12.2

10 P02 / 4:58.1, 8:29.1, 9:05.0, 26:42.4, 27:19.8, 32:27.3, 34:04.3, 35:33.8, 49:16.8, 50:56.1, 51:08.4, 51:20.7 | P06 / 10:03.5 | P15 / 8:13.2, 8:53.0, 11:40.8

 doi:10.20944/preprints202603.1487.v1

11 P04 / 23:49.7 | P06 / 15:20.7 | P07 / 10:48.8 | P11 / 0:35.3 | P12 / 1:29.9, 5:02.8, 6:23.4 | P13 / 4:23.7 | P15 / 1:32.4, 2:46.6, 22:12.2

12 P01 / 6:57.4, 9:25.6 | P02 / 3:22.8 | P03 / 10:29.9 | P04 / 17:48.3, 29:44.9, 30:47.2 | P05 / 15:27.1 | P06 / 0:51.4, 19:54.4 | P08 / 12:02.9 | P12 / 15:14.6

13 P11 / 0:54.6 | P13 / 1:16.5, 1:23.5

14 P01 / 1:27.5 | P12 / 6:23.4 | P13 / 2:26.5

15 P01 / 4:27.3, 4:59.2, 5:28.0, 6:17.0, 7:32.7, 12:31.5 | P02 / 29:40.9, 29:46.6, 29:57.6 | P03 / 7:59.9, 10:37.7 | P04 / 11:24.3, 13:45.8, 31:55.4, 36:25.6 | P07 / 6:11.6, 6:42.0 | P13 / 3:28.8, 7:44.9, 8:29.9 | P14 / 6:10.1 | P15 / 8.53.0, 9:55.0, 9:59.4, 10:20.1

16 P01 / 1:45.4 | P02 / 6:54.9, 7:53.2 | P04 / 19:55.6 | P11 / 0:35.3, 11:06.1, 11.37.9, 12:09.8 | P13 / 2:26.5

17 P01 / 7:15.5, 7:18.5, 8:53.2 | P02 / 4:29.2, 4:42.4, 4:58.1, 5:29.2, 15:43.0, 16:03.3, 16:16.2, 47:33.8 | P11 / 11:33.2, 11:37.9, 11:54.5

18 P01 / 4:22.8, 10.36.3 | P03 / 11.05.1 | P11 / 11:06.1 | P13 / 2:26.5 | P15 / 3:42.8, 21:39.8

19 P02 / 47:01.2 | P04 / 4:11.0, 17:48.3 | P05 / 1:18.2, 1:40.9, 2:04.8, 2:31.9, 2:40.1, 15:37.4

Table 4. Suggested Solutions.

Authentication Challenge	**Suggested Solutions**	
	Physical	*Cognitive*
Privacy concerns	Data control/deletion	Data control/deletion
Frustrating experience	Add more support for AT	Add simplified options
Identification (Authentication)	Improve accessibility	Improve accessibility
Forgotten password	Password managers	Password managers
Locked out	Alternative options	Alternative options
Distance from device	On-person device/wheelchair support	eID alternatives
Repeated attempts needed	Provide alternative options	Provide alternative options
Time consuming	Add simplified options	Add simplified options
Password mismatching	Password managers	Password managers
Environmental distractions	Focused experience	Focused experience
Number of accounts	SSO	SSO
Character set	Font and color support	Font and color support
Time-based codes	Extended access support	Extended access support
Two-Factor Authentication (2FA)	Often linked to the distance to the device	Often linked to the distance to the device
CAPTCHA issues	Improve accessibility	Improve accessibility
Authenticator issues	Develop an Accessible Authenticator	Develop an Accessible Authenticator
Code retrieval delays	Linked to time-based codes	Linked to time-based codes
Fingerprints	Provide alternative options	Provide alternative options
Low difficulty / no issues (control)	Increase awareness of alternatives	Increase awareness of alternatives

Legend 5
Abbreviations:
AT—Assistive Technology
eID—Electronic Identification (e.g., electronic cards & keys)
SSO—Single Sign-On
Note:

 doi:10.20944/preprints202603.1487.v1

While some solutions can be tailored to specific Disability Types, several can resolve both physical and cognitive issues; therefore, providing plenty of options in an Accessible Authenticator is the recommended overall solution.

4.2.1. General Findings from Stage 1—Initial Coding

A set of characteristic traits emerged from the participants' answers. Reasoning for this will be deliberated accordingly in our Stage 3 Final Theory Development, later in this section. The list of seven characteristics identified is as follows:

1. **Disability**—There is a wide variety of disabilities that could be addressed by this analysis. Signs of accessibility issues begin to emerge in conversation.
2. **AT Devices**—People tend to prefer authenticating themselves with only one device.
3. **Usability versus Security**—While people prefer a usable platform, security is still a significant concern. Subsequently, this contradicts earlier theoretical research mentioned in the literature review that suggests usability is a larger problem than security; however, it could be accepted that this is more of a problem in the paradigm of an authentication machine's functional capability, which contrasts with the user's value-based and balanced perspective of the situation.
4. **Issues**—Time-based codes present the biggest challenge, specifically, physically being able to reach for a 2FA device.
5. **Desirable Features**—A simplified login is preferred with optional settings.
6. **Responsibility**—The onus for privacy and security should lie with the service provider. A user's own responsibility is also recognized.

Naturally, the very first code produced was for disability type, which in turn led to the first table of the TF, which highlights Disability types versus degrees of effect. This lays out a pattern to distinguish between the physical and cognitive effects of a disability. This is important because it can be used later to see which bands' authentication issues may fall into.

4.2.2. Emerging Characteristics from Stage 2—Focused Coding

During Stage 2 Focused Coding, which involved simplifying and reducing the number of coding topics. This is done by examining all the existing codes we have and reducing them to fewer, similar terms. When we do this, we start to see certain themes emerging, which we later use in our final theory. We also note different helps and hindrances in this phase. There are the following three barriers to analysis:

- It is difficult to reduce the findings without overlooking small but perhaps relevant information.
- Some topics show much greater support from users than others.
- Some topics reveal an almost 50/50 split in opinions, leading to the assumption that there is no right or wrong answer for these questions.

However, on the positive side, we also note the following emerging characteristics, which will enable us to evolve a theory from the data:

- Most users identify problems logging in due to their disability.
- Although the research aims to make logging in easier for users, security is still important to them.
- There is considerable interest in a universal login system.
- There is interest in alternative devices to facilitate the log-in process.
- Forgetting passwords is a common theme.

While there are barriers to be aware of, they do not defy the construction of a theory, simply because several emerging characteristics indicate clear pathways towards it. Hence, in the following stage, we use qualitative analysis (GT) to derive knowledge from the answers.

 doi:10.20944/preprints202603.1487.v1

4.2.3. Formulation of Substantive Theory from Stage 3—Final Theory Development

In this stage, we have developed a final set of categories to explore for our theory. These categories and the resulting theory are described more explicitly in the following two sections, which analyze the data's more meaningful aspects.

To arrive at this theory, annotations and memos from the previous stage of coding were used to progressively move from a numerical to a system of knowledge-based concepts, which will provide structure for our relational-based TF presented later. Naturally, the first two stages were crucial in culminating in this and remain valuable in and of themselves for early-stage raw data.

4.3. Preliminary Analysis for Final Theory

To begin with, we note the most noticeable aspects (characteristics/categories) derived from the coding (please note that these Stage 3 coding categories cross-reference with the following nine subsections, where they are explicitly examined):

1. Most users identify problems logging in as related to their disability.
2. The most desired feature is a simplified login, such as an SSO.
3. Security is of high importance to users and closely matched by the desire for ease of use.
4. The most common issues appear to be with time-based codes (for 2FA) and the CAPTCHA systems.
5. Solutions to accessible authentication problems can be found in the data itself.
6. The option to remain logged in is desirable in certain situations.
7. Many users feel that privacy and security of the login system are the company's responsibility, but several acknowledge their own responsibility too.
8. There is interest in alternative devices to facilitate the log-in process.
9. Forgetting passwords is a common theme.

Next, we discuss the concept of categorization by disability type and why this is not fully analyzed in this study. While it should be understood that although this could lead to meaningful results, it is also true that some login issues can appear as identical for a variety of similar disabilities, for example, dyslexia and ADHD sufferers may both have difficulty reading, due to text jumping around or from lack of the ability to concentrate, whereas those with UEIs, amputation or motor-neuro disabilities (such as Cerebral Palsy) can find inputting difficult for a further variety of reasons.

Therefore, the assumption that a certain type of disability will cause a certain login issue is invalid. That is not to say it could not be used in a highly focused study on just one disability, but this would stray from our intended research objective, which is inclusive of anyone with a disability. For completeness, however, each disability is specified alongside the quotes so that the reader may draw their own conclusions from this research.

There was a wide variety of disabilities exhibited by participants, and there were many people who were reluctant to divulge information to a third party, in contrast with those who would be happy to pass it. There are also several references to problems caused by having a disability, which is undeniably important because it underscores the need for this paper to highlight that there is an existential problem with the level of accessibility in the core systems that we use daily.

Consider the following logical proposition, which defines the issue with today's accessible authentication systems:

Premise 1: Disability ⇒ Difficulty with authentication.

Premise 2: User has a disability

Conclusion: Users with a disability have difficulty with authentication

The subsequent subsections analyze the data with quotations to give context and reference the source in the following format: (Participant Identification, Timestamp, Disability). A link to the full transcripts of the interviews is provided in the Data Availability Statement at the end of this paper.

 doi:10.20944/preprints202603.1487.v1

4.3.1. Most Users Identify Problems Logging in Related to Their Disability

We acknowledge that a control group would have delineated differences between disabled and non-disabled users; this was not a focus of participant selection, and we feel that the results provide an adequate explanation. We also note that several participants do not initially identify it as an issue; however, we will see that this can be with higher functioning neurodiverse participants when perhaps unfairly compared with someone with almost no physical ability in the torso or below. For this reason, we aim to analyze on a case-by-case basis and note any additional problems that may still exist. We also discovered that most users feel they have some extraneous authentication problem they believe is caused by their disability.

Several participants found frustration in not being able to reach their 2FA device with ease too, saying "what if I'm downstairs, and I get tired because of my meds, I try to log in it sends a message to my phone upstairs" (P05, 1:18.2, Schizophrenia/Curved Spine/Asthma), another saying, "so they will text my cell phone with, like, numbers to log in, and sometimes I find that frustrating because I don't have my phone on me, then I have to, like, wheel around to try to find it" (P04, 4:11.0, Spinal Cord Injury), and we might note that tends to an issue surrounding physical disability rather than cognitive ones. One solution is having some sort of attachment to the 2FA device, the participant saying, "I want to have got attached when I'm in that area … a phone charges come [with] that electric wheelchair … it dangles around" (P07, 22:20.6, Spinal Problems).Thus, disabled users generally encounter a range of issues that impede their authentication. There were 12 spoken references in which the user reported few or no issues; although this is encouraging in the current context, it does not equitably compare with the total number of issues reported across all users. This supports our earlier initial hypothesis.

4.3.2. The Most Desired Feature Is a Simplified Login, Such as an SSO

A very desirable feature is a universal and/or simplified login system such a Single Sign-On (SSO) with many wanting an "Easier and faster" (P13, 7:10.6, Stroke) login system with and the majority of participants answering "Yes" to the idea of having a single system to use to login with, similar to systems already provided by Google, Apple and Microsoft, this is expressed by the comment "[it]'d be nice to have one password for everything" (P13, 4:02.3, Stroke), and many would use such a system if it felt secure enough.

However, problems can often occur with systems such as Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) and time-based codes, so a more bespoke Accessible SSO for people with disabilities could be a good idea. A universal login system and simplified login system were the most desirable features, implying a demand for ease of use. Although it does occasionally cause technical problems in favor of security, it reinforces the fact that usability remains imperative to any accessible system, as mentioned earlier, with a focus on Human-Computer Interaction (HCI). The option to remain logged in was the next most desirable. If this can be implemented without any detriment to security, it would be an ideal situation for both the disabled community and organizations seeking to maintain a high degree of customer loyalty.

Some would like to explore the idea of alternative, easier ways to log in as well, such as "just, like, pictures or some pictures" (P10, 2:27.8, Williams Syndrome), which leaves the door open to new, innovative ideas in the world of authentication that could become revolutionary in scope.

While we acknowledge that current perceptions of SSOs tend to be preferential, the reason for probing this area is to determine whether it can be helpful in an accessible way. Reasoning behind this may be the need for fewer distinct accounts for each service, a reduced number of passwords to remember, and a simple, familiar login method that is easier to navigate due to muscle/cognitive memory of how to use it. At this time, this remains unproven from the data but could be a unique area to explore in a future research project.

 doi:10.20944/preprints202603.1487.v1

4.3.3. Security Is of High Importance to Users, but Closely Matched by the Desire for Ease of Use

Initial supposition from the literature reviews suggests the problem leans towards usability. In fact, it turns out that many place a higher value on the security of an authenticator than its usability, especially in vulnerable positions, after "having recently been scammed" (P01, 2:08.6, Dyslexia/Dyspraxia) and "because I did recently just get hacked" (P15, 2:37.5, ADHD).

When comparing usability and security, the coding suggests that ease of use is on par with security in importance to users, who generally want an acceptable level for each, which is entirely understandable. Surprisingly, despite many admitting to making security sacrifices to make things easier, as the interviews progressed, an increasing passion for security was identified. We also discovered debate over whether certain devices, such as fingerprint scanners, could be classified as AT devices at the same time if they are considered to aid login. It is not uncommon for everyday devices to be used in this way, such as Xbox controllers, and a vast number of unheard-of AT devices are available for large Xbox controllers. It is also true that a vast number of unheard-of AT devices remain available for a wide variety of very specific disabilities [20]. Therefore, this is a complex issue due to the practicalities involved in ensuring compatibility with AT for any application to be universally accessible.

Whilst observing at the superficial level of this research, it appears that the simple answer is to make authentication easier for users; however, in many situations, this undermines an essential need for security, which is paramount for any system that can allow access (by an actor) to a user's personal and valuable information. Therefore, contrary to initial speculation, the security of any system suggested by our theory must provide high security guarantees, especially since this group of users can be classified as vulnerable (to breaches) due to factors beyond their control.

While this paper's purpose is not to go into depth on security countermeasures, it acknowledges that application developers are currently waging an ongoing battle against cyber-attacks, with the stakes rising and even household names becoming victims. Many people fear advances from AI attack bots. Still, we must take comfort in the developers community who tireless seek ways to counter these with their own AI advancements such as Deep Neural-Net based Middleware [21] which has its origins in early day neural nets with the invention of the perceptron by Rosenblatt in 1962 [22], something which modern AI moves aways from with today's Natural Language Processing and drifting into multimodal AI which can "seemingly do it all" [23].

While recognize that usability is a problem with Accessible Authentication, and it is challenging to eliminate the importance of usability as this can be a vital ingredient when it comes to accessibility under the perspective of how the HCI is designed for use, especially when it takes into account any difficulties caused disabilities that a user might have, in line with Fitts's law (developed in the 1950's and 1960's) whereby we can actually mathematically quantify processing time with the early psychological perception of what is described as "bits per second" [24].

A participant in one of the interviews saw that people with disabilities are more vulnerable to cyber-attacks, so it would be logical to provide increased security for them. As a reminder, the actual values for the number of references for each characteristic are shown in Table A.2 in Appendix A.

4.3.4. The Most Common Issues Appear to Be with Time-Based Codes (for 2FA) and the CAPTCHA Systems

Initially during the interviews, a common *verification* issue that cropped up was with time-based codes (such as those used by Authenticator Apps), followed by 2FA (codes received via text message) and the CAPTCHA systems, for example, "it comes up with squares … with traffic lights or things, and they're not always clear, I wouldn't say it's down to my disability, but to those just in general, it's like, what quantifies does it have to be all of it in the square with it's just a tiny bit where you get but it still counts that and if you don't count it, not that you win" (P01, 3:13.7, Dyslexia/Dyspraxia), wherein it is interesting to note that the participant feels this is an issue not just related to their personal disability but to everyone, thus raising the question of whether authentication needs to be more accessible for *everyone*.

 doi:10.20944/preprints202603.1487.v1

4.3.5. Solutions to Accessible Authentication Problems Can Be Found in the Data Itself

It was noted that many participants would suggest ideas that could be helpful to users with other forms of disability, in addition to their own. Regrettably, this had to some degree be dismissed for this paper, as they do not necessarily have any direct personal experience of it, for example when talking about passing disability information across to third parties, "say you're low vision … you need larger font. You're able to click a button that says like you know, low vision" (P03, 6:09.1, Quadriplegia) we can see that having enough options available for an assistive authentication system would have to be a prerequisite to try to be fully inclusive to all disability types.

We also acknowledge that a paper open to all disability types may appear too broad (when compared to a paper based on a single disability type); however, we remind ourselves that this is about accessibility issues for authentication, rather than focusing on the ailments of a specific situation.

In relation to the wide variety of disabilities exhibited by participants, they were reluctant to divulge information (about their disability) to a third party, in contrast with those who would be happy to pass it. There are also several references to problems caused by having a disability, which is undeniably important because it underscores the need for this paper to highlight that there is an existential problem with the level of accessibility in the core system that we use daily. We found that, in many cases, participants also offered explicit solutions to problems they had experienced firsthand, which is helpful when brainstorming.

4.3.6. The Option to Remain Logged in Is Desirable in Certain Situations

This concept is as interesting as it is controversial: whether sites should keep you logged in or allow you to access them immediately when you return. For someone with paralysis from the neck down, this would be very helpful, "Yeah … this one" (P08, 13.51.3, Cerebral Palsy).

One opinion is that "there's so much paranoia that security is, um, overwhelming and all the onus id offset onto the user to validate everything … they're offsetting, you know, uh, responsibility, time, efforts and labor and cost onto the customer … they need to find a solution to that themselves" (P05, 19:30.6, Schizophrenia, Curved Spine, Asthma) which follows with the results showing that many participants felt the onus for security should be held by the service or organization.

Another says, "one that annoys me is the connection … every time I log in, "one that annoys me is the connection … every time I log in from there, I have to sign in. It doesn't matter if I'm late, remember me? It never does … Every time. And then. Nothing confidential on their lesson websites" (P07, 15:35.0, Spinal Problems), highlighting inappropriate levels of security for sites which could reasonably be expected to be easier to access.

While this may seem trivial, some participants went into depth about different options and the various ways this could be achieved, suggesting it might be more important than we think.

4.3.7. Many Users Feel That Privacy and Security of the Login System Is the Company's Responsibility, but Several Acknowledge Their Own Responsibility Too

Most users felt that the privacy and security of the login system is an organization's responsibility, not theirs. In the final addition of all issues, it is noted that privacy concerns soon became the greatest concern, possibly reflecting a preference for a secure system over usability. Frustration was the next important concern, based on the only real emotional test question, and it was identified that most disabled users face difficulties due to inaccessible authentication procedures.

Giving way to rationality, several participants agreed that it was both their own responsibility and the organization's, as accidents or negligence could not always be reliably attributed to a third party. While it may remain justified for an organization to be held accountable in certain legal cases, through disclaimers or other legal loopholes, an organization can and will protect itself from a user's own negligence. While some participants have openly acknowledged this, others place the onus

 doi:10.20944/preprints202603.1487.v1

solely on the organization, which may highlight where certain psychological perceptions, expectations, and boundaries lie.

The outcome of this remains to be seen, as it may affect the development of authentication systems when this fact is presented to organizational representatives in future studies.

4.3.8. There Is Interest in Alternative Devices to Facilitate the Login Process

We found that most people would be interested in a general/AT device for authentication, either having some form of preference for a hardware device that can be used in conjunction with authenticating or would like some general form of device that could help with this, many would be willing to try a Universal Serial Bus (USB) key, but most people said they simply used their mobile phone. Consequently, any general device alternative to passwords was the most popular, followed by fingerprint scanners, facial recognition, mobile phones, and then USB keys. Traditional AT devices (i.e., devices that are made for specifically for disabled users) tended not to be desirable unless it is something that a physically disabled user already uses, such as a sip-puff device mentioned by a participant when referring to a friend, and while a mobile phone may not normally be considered as an AT device, it remains the default choice for most disabled users. Furthermore, individuals with Stroke and Alzheimer's disease can benefit from using an eID, such as a USB key or a credit card-sized ID that can be hung around their neck. The ability to remember passwords can be a concern for them, as it is for many other users.

Plenty of participants expressed interest in fingerprint scanners, with many others keen on facial recognition. One participant was particularly excited by the prospect of an eID card which can be kept on a lanyard (that can be kept around the neck) who says "You can see it in my pocket [referring to an ID badge that they show] … so off I have to take responsibility" (P14, 11:39.4, Stroke) as they like the idea of a physical authentication device that you can look after personally. The top five answers (in terms of frequency of references) were:

1. General Device.
2. Fingerprints.
3. Facial recognition.
4. Mobile phone (or tablet).
5. USB key.

4.3.9. Forgetting Passwords Is a Common Theme.

"Forgetting passwords … all the time" (P09, 1:02.9, Anxiety/Depression/ADHD), who said that using "face ID" would make the situation easier, is also a very common theme, mentioned a total of 11 times in the various conversations. With some physical disabilities, "just typing out" (P08, 2:32.1, Cerebral Palsy) is a hard task when their only main method of communication is via eye-tracking, and, as one can appreciate, a lack of manual dexterity would be expected to be a drawback in any situation.

Alternatives to passwords are often welcomed, such that "I would have a harder time remembering passwords, which is why … a fingerprint scanner would kind of be helpful" (P15, 16:08.5, ADHD).

Another cognitive disability related example of this is "when I make passwords up, [I] double up sometimes, or when I do it the second time, the passwords fail to match … and that takes several attempts to do that" (P01, 1:28.5, Dyslexia/Dyspraxia), indicating that dealing with passwords can be a lengthy and unnecessarily time-consuming experience.

Physical disability problems also exist with passwords too, "identification processes that are timed ... timing is too abrupt … with me having to type something … going back onto your web browser and then, you know, trying to do that within the amount of time that was allotted to you" (P02, 4:29.2, Quadriplegia). This is problem is not just limited with passwords either, difficulties with facial recognition can occur "if you have to wear, like, a facial mask … I would have to breathe in at night … it's just airflow right there because your muscles are weaker" (P03, 1:30.3, Muscular

 doi:10.20944/preprints202603.1487.v1

Dystrophy) which reminds us that additional accessibility authentication issues occur in many ways for people with disabilities.

Admittedly, forgetting passwords is something that persons without a disability might be just as likely to do, in some circumstances. One way to test this would be to compare it with a control group, but in this case, we apply the findings to relationships in our TF to see how this problem, and it is a problem, compares to other issues users may experience.

4.3.10. Relating Disability Types to Degrees of Effect for the TF

Now it is time to examine the relational connection between authentication challenges and degrees of effect related to disability as can be seen in Table 3. At this point things become interesting as it really highlights the emerging patterns from this study. For example, the issue with the highest scoring total of all degrees of effect is the problem that generally finds authentication frustrating. Acquiring a total of 39 combined degrees of effect, it indicates that disabled people are not satisfied with the current authentication procedures.

Shortly after identifying 'frustration' as the top issue, the first apparent anomaly appears. It is the total number of participants who initially said that they had no or very few issues with authentication, and with a total of 36 for its degree of effect across all disabilities, it threatens to nullify the research result by implying it was not necessary at all! This is a deceptive result for two reasons. Firstly, any participant who initiated this response from one of the earlier questions in the interview went on to mention several problems that they've encountered with authentication, suggesting that this may be a knee-jerk reaction to the question. Secondly, this is the one (non)issue in a set of 19 and can easily be said to be outweighed by all the others. Controversially, if any organization wished to put forward a case for not making authentication accessible, they could potentially leverage upon this point.

Other points to notice from this table are congregations of higher degrees of effect for both Neurodevelopmental and Physical Disabilities. The former has the highest total at 126 incidents, with 94 for Physical, 56 for Psychological, and 35 for Learning Disabilities.

Some issues also contrast, such as 2FA being much more difficult for physically disabled users than those with cognitive disabilities and forgotten passwords rating highest in users with cognitive disabilities when compared to those who are physically disabled. Certainly, with more theoretical refinement, other, more nuanced patterns can be found in addition to those mentioned so far.

4.4. Final Theory Presented as a Preliminary Framework (TF)

Now that we have a comprehension of the issues that people with disabilities can encounter with authentication, it is time to compile the raw data into a Framework which shows our understanding of disabilities, the participants themselves, and amalgamates this with how it relates to authentication, so that we can achieve an understanding of the areas that will need more work.

We observe that many participants initially reported few or no problems with authentication, then went on to describe specific issues and suggested remedies. Supposedly, this is our control element, which suggests that there may be no problem with the system in its current incarnation, and it scores highly across a variety of disability types in our table C2. In balance, it is not the greatest ranking concern, with the largest implication weighing on frustration with current authentication methods; in reality, if we were to offset it against all the other issues, it would become relatively negligible. This is not to downplay the fact that people generally don't perceive authentication as an accessibility issue, but maybe we can infer from this that there is nothing to compare it to, given the insufficient number of alternatives in the marketplace.

At the final third phase of developing the TF, brainstorming produces a set of ideas for solutions to the problems associated with accessibility in authentication, which are duly explored in Table 4. Repeating solutions can be seen, which simplifies the process of authenticator design for a web developer to achieve an accessible environment, and the table illustrates how the application could respond to the different disabilities that a user has.

 doi:10.20944/preprints202603.1487.v1

4.5. Qualitative Data Summary

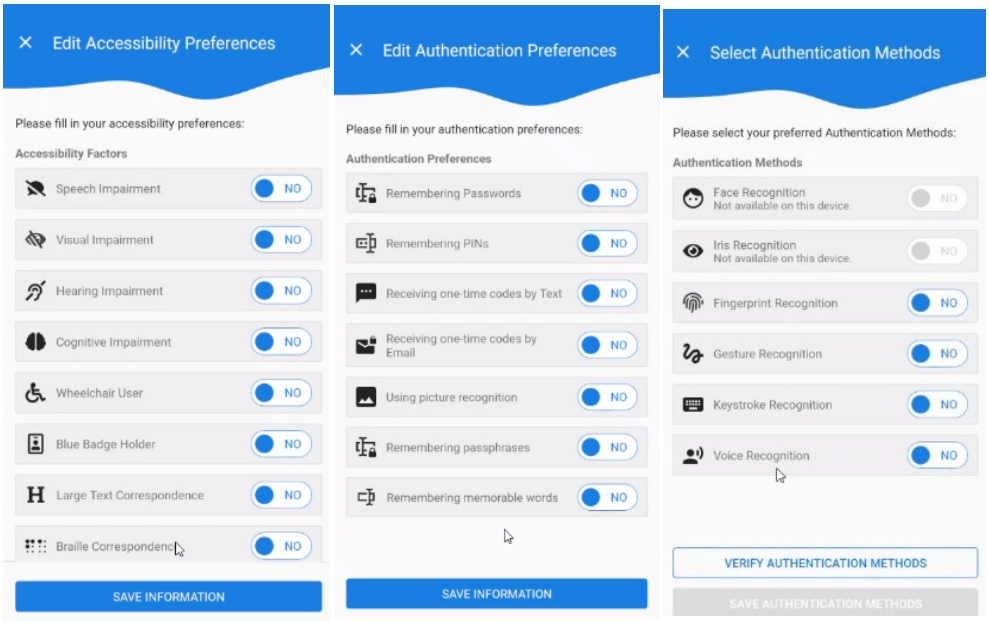
Throughout the interviews, several interesting points were made by the participants, including two who suggested a prominent red button to log in, much like the one you might find on a game show, illustrating a desire for simplicity in authentication. This can be compared to AT devices that use a simple process, such as a paddle or a switch, to trigger an event.

Participants shared several innovative ideas for login systems, showing great creativity and imagination. One mentioned a picture-based system, which, as mentioned, there is already some research into. Another suggested a device connected to her wheelchair that prevents it from going out of reach. One participant was also unaware that USB-based fingerprint keys were already available, which would have been ideal for them. This shows that there is still much scope for authentication, and we should defy anachronistic views of how it should operate. Nevertheless, we embrace the challenge of implementing some of the suggestions in the Suggested Solutions table (C3) to achieve truly accessible authentication.

5. Discussion

5.1. General Discussion

This research acknowledges its origins derive from initial research conducted by Whittington and Dogan [25], and this research included the creation of a prototype application known as Authentibility (see Figure 2), which is designed to accept information about a user's disability to transmit that data to service providers so that they can better cater to their needs. A video explaining this prototype is available at Supplementary Material video link S1. The research now pivots to studying how the user can log in to a more accessible service, although the original idea of passing disability data to the service has not yet been considered for inclusion in future versions of the prototype. For more information and a demonstration of an early-stage second incarnation of the application, please visit the website link S2, which is also provided in the Supplementary Material section. The reader may wish to note that work on this is supplementary to the main research and the resulting Framework and exists solely to demonstrate the Framework's purpose and potential effectiveness.



(**a**) (**b**) (c)

Figure 2. The Authentibility prototype app. The user has the option of specifying (**a**) their disability, (b) their preferences for authentication, and (**c**) the authentication methods they would like to use.

 doi:10.20944/preprints202603.1487.v1

Theoretically, there are two methods of authentication with a service for a user (see Figure 3): either via the authentication app for verification and subsequently to the service, or by accessing the service, which then calls the authentication app for verification. The initial prototype application does not clearly define which of these two methods it intends to use to establish a connection with a service or organization. However, the currently accepted norm for this procedure is the latter of the two, due to reduced complexity [26], in which the service polls the authenticator for identity confirmation. Once the user is logged in, they are then said to be 'authorized,' which can often be confused with 'authentication,' and our focus here is on the authentication aspect of being able to log in with a fair degree of accessibility included.

Development of the application may require further research into Development, Security, and Operations (DevSecOps), along with User Interface (UI) design, and both should be coupled with additional considerations for the disabled. Naturally, this is also a logical method for in-person eID in physical form (e.g., electronic ID cards) when the client is physically located on the service's premises, but again, this digresses slightly from our considerations of accessible authentication in the context of online access.

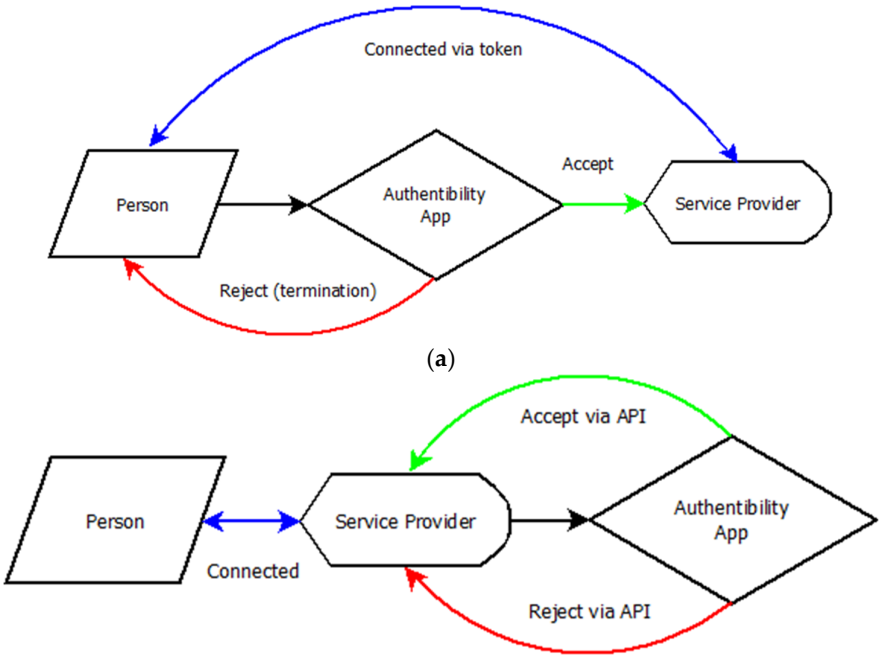


Figure 3. Methods of user access to the service: (**a**) A user goes to the authenticator app first to gain access to the service and is redirected to it with access tokens, such as JSON Web Tokens (JWTs) [27], if identity is confirmed (otherwise known as authorization); (**b**) A user visits the service site to request access and the service checks the users' identity via the authenticator, which replies via a backend API, to authorize the user.

From our results, we found that many users have a serious concern about the security of their personal information, so it is natural to assume that any authentication system should strive to achieve the maximum possible security. The initial idea that making it simpler to use for people with disabilities would be an ideal solution, but it has the disadvantage of reducing security for a vulnerable user group. In addition to using secure hashing algorithms, the bare-metal systems on which an authenticator runs must also be as impenetrable as possible. Note here that the process of authorization, i.e., allowing the user a continuous connection to the service, is distinct and, in some sense, disconnected, and occurs after the authentication process. It is mentioned here to illustrate the continuity of the process of authentication as perceived by a user, although it is in no way central to this paper's research.

 doi:10.20944/preprints202603.1487.v1

We have identified additional problems people experience when logging in that relate to their disability, such as issues with time-based codes and CAPTCHA systems, as well as issues of responsibility. We have discovered a yearning for a simplified system (SSO) and alternative authentication methods, which may be preferable for people with disabilities to improve accessibility. A real need for extra options, such as an increased timespan to remain logged in, along with display, voice, and other accessible assistance features.

We also acknowledge the paradoxical yet significant trade-off between security and usability, which is addressed by adapting these levels to the service being accessed. Suggested security precautions might include hosting software on secure premises with robust security measures, such as Access Control Systems (ACS), physical identification (ID), and Closed-Circuit Television (CCTV), to prevent social engineering or physical access to sensitive hardware [28].

We may also consider defense systems that detect Internet of Things (IoT) attacks that manipulate device firmware, software, and operating systems, such as those found on mobile phones, fingerprint scanners, servers, and other AT hardware. These also include "Intrusion and Anomaly Detection Datasets" [29] such as X-IIoTID, CIC-IDS2017, CICIoT2023, and Edge-IIoTset. Many datasets are open-source and freely available, such as the CIC-IDS2017 dataset from the Canadian Institute for Cybersecurity [30]. These data sets all contain information that can help keep the system secure.

Encouragingly, modern research also suggests that there are also new strategies that we can use to keep the balance between security and performance, without any unfair sacrifice to either side of the scales by using deep learning to adapt defensive strategies on the fly, whereby the system optimizes for maximum performance or security depending on the recognizable characteristics of any given access request [31]. Indeed, advanced ultra-secure and high-performing eID solutions may soon be a common reality with the advent of quantum computing, thereby harnessing the ultra-fast potential of "quantum-enabled data authentication" [32]; pressing onward the boundaries of modern authentication systems that are now fast becoming more deeply interwoven into the general population's daily lives.

Evidently, we will soon encounter many areas for further research that relate to this study of Accessible Authentication, including security in conjunction with UI design, reliability, and operational speed (i.e., Quality of Service, QoS). It would be vital to include the opinions of people with disabilities to determine the applicability of the discussions. The purpose of raising these connections to security is not to highlight the complexity of a secure authenticator, but to illustrate that a highly secure system can execute in parallel with an accessible, user-friendly HCI construct.

While it is true that a substantial body of research already exists in the field of authentication, little remains in the specific area of Accessible Authentication. Nevertheless, with careful assessment of real-world information, we can create a Framework for organizations and program developers to consider incorporating the outlined suggestions into new and existing applications. It is anticipated that once awareness of this Framework is raised, for example, by informing influential entities such as Microsoft, Google, and Apple of the opportunity to be more inclusive with their clients, the research can achieve its full potential impact.

We believe that the results of the analyses in this paper support the substantive theory that there are problems with the level of accessibility available to people with disabilities when they attempt to authenticate.

5.2. Limitations

We acknowledge that this paper is limited by the number of interviews conducted (n=15), and that further diversification of participants is also desirable. We also acknowledge that the focus could be on a specific disability, and that the classification of results by disability is weighed because some disabilities are more prevalent among participants than others. This remains a limitation of the paper as well.

 doi:10.20944/preprints202603.1487.v1

We propose continuing research in this field and planning more interviews with organizational representatives to add additional perspectives on this interesting topic. Following this, a further questionnaire will be released to participants to introduce quantitative analysis into the mixed-methods final report. Objectives will be to increase the sample size and diversity of participants and to use the data with CT's theoretical sampling methodology to refine the data into highly specific, focused observations or key additions to knowledge.

We also recognize that Framework and Prototype Application are yet to reach full maturity, which are two of the final objectives of this research.

6. Conclusions

6.1. Summation

The aim of this introductory empirical paper, situated within this area of specialization, is to promote Accessible Authentication for disabled users. According to the World Health Organization, "an estimated 1.3 billion people—about 16% of the global population currently experience significant disability" [33]. In our increasingly connected digital world, stakeholders must advance to secure more inclusive methods of Electronic Identity Authentication.

We can see from the results that security is important to people with disabilities, so making this a priority in any eID device is essential to fully protect them. It was accepted that any general AT/hardware device would be acceptable as an eID, with fingerprints and face recognition coming out on top, along with the humble mobile phone. Fears over signal-jacking for Radio Frequency (RF) fobs were also expressed, so secure radio channels are needed. However, they can often be based on Remote Keyless Entry (RKE) designs [34], which are easy to replicate at low cost, raising security concerns. Future security system designs should complement any on-board transmissions with Rivest-Shamir-Adleman public-key cryptosystem (RSA) security certificates that ensure the utmost security for users.

6.2. Theoretical Conclusions to the Initial Hypotheses

If we recall the three hypotheses presented in the Introduction, we can objectively assess whether they have succeeded or failed. Our analysis has extracted the problems encountered from the data and sought to understand how, despite many users initially reporting no issues with authentication, there is substantial underlying frustration; when probed further, they reveal not only the real issues they have, but also potential solutions.

For our second hypothesis, we have tabulated relationships between a person's disability type and cross-referenced this to the likelihood of a specific type of authentication problem occurring. This validates that it is possible to resolve relational interconnections between disability types and accessible authentication issues.

The final hypothesis regarding the trade-off between usability and security is, in fact, controversial, not just because of the technical difficulty of achieving it, but also because of the subjective nature of whether users value one aspect over the other. With opinions varying widely, we have not yet been able to determine a firm resolution over this.

6.3. Future Work

We initially considered a further questionnaire (as future work), which supports enhanced questions based on the outcomes of the research so far (which will require a combination of scalar and yes or no answers from the participants) to provide data which may be used with statistical methods such as Multivariate Analysis [35], however after building a case with CT, the idea to continue work with further theoretical sampling (in concordance with CT methodology), as a textually answered questionnaire, is entirely a viable option, which could provide further qualitative focus that is a viable alternative to pursuing quantitative data to complete the research. This decision will require further thought to avoid overloading participants with the burden of writing lengthy

 doi:10.20944/preprints202603.1487.v1

answers. However, alternative routes to further data collection will be considered. Hopefully, then we can address the limitation posed by the relatively small data set (n=15) that has been presented in this paper.

It is envisaged that the Framework or future applications derived from this paper could include physical (on-person) Electronic ID (eID), either as part of a resident Trusted Execution Environment (TEE) for TouchID systems or as an alternative to biometrics. This could be on a more amenable credit card-sized (chip-on-device) ID card or USB memory sticks encrypted with Certificate Authority (CA) or Fast Identity Online 2 (FIDO2) [36] based authenticators. These devices can use passwordless, single-factor authentication, which has been empirically shown to offer advantages over traditional passwords or two-factor (2FA) authentication [35].

To further support this research, the authors also intend to conduct interviews with industry professionals in authentication development. This is to try to establish whether support for disabled users is imperative for them to log in on a fair and equal basis with the rest of the population, and we question whether there is a pattern of atrophy, whereby a satisfactory level of accessibility in today's authentication systems is often overlooked.

To conclude, by examining our Theory, we have discovered multiple issues within the domain of electronic identity authentication, manifesting in various forms. Through an empirical qualitative study, we consider that disabled users are consequently affected by these due to accessibility inefficiencies. It is recommended that solutions be implemented to improve the usability of the user group while maintaining optimal security.

Supplementary Materials: The following supporting information can be downloaded at: https://vimeo.com/513400390?fl=pl&fe=sh, Video S1: Authentibility Demo. https://authentibility.uk/, Website S2: Authentibility Website, including link to prototype application.

Author Contributions: Conceptualization, D. Cropley, P. Whittington and H. Dogan; methodology, D. Cropley; software, Lumivero (NVivo); validation, D. Cropley, P. Whittington and H. Dogan; formal analysis, D. Cropley; investigation, D. Cropley; resources, D. Cropley.; data curation, D. Cropley; writing—original draft preparation, D. Cropley; writing—review and editing, D. Cropley and P. Whittington; visualization, D. Cropley and P. Whittington; supervision, P. Whittington and H. Dogan; project administration, D. Cropley, P. Whittington and H. Dogan; funding acquisition, D. Cropley (self-funded). All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data supporting the findings of this study are available at BORDaR—Bournemouth Online Research Data Repository, under the title "Issues with Electronic Identity Authentication: A Qualitative Study with Disabled Participants".

Acknowledgments: During the preparation of this manuscript/study, the authors used NVivo, version 20, for qualitative coding, cross-comparisons, and graph production. GenAI results were not used in any way for the resultant coding or analysis, as the experimental results proved far too unrelated to be of any practical use. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

2FA	Two Factor Authentication
AA	Accessible Authentication
ACS	Access Control Systems
ADHD	Attention Deficit Hyperactivity Disorder
ASD	Autism Spectrum Disorder
AT	Assistive Technology

 doi:10.20944/preprints202603.1487.v1

BU	Bournemouth University
BURO	Bournemouth University Research Online
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CCTV	Closed Circuit Television
CP	Cerebral Palsy
CT	Constructivist Theory
DevSecOps	Development, Security, and Operations
eID	Electronic Identification
EUR	Europe
FHSD	Facioscapulohumeral Muscular Dystrophy
FIDO2	Fast Identity Online 2
GenAI	Generative Artificial Intelligence
GT	Grounded Theory
HCI	Human Computer Interaction
ID	Identification (physical)
IoT	Internet of Things
JWT	JSON Web Token
OCD	Obsessive Compulsive Disorder
SEND	Special Education Needs and Disability
SSO	Single Sign-On
TA	Thematic Analysis
TEE	Trusted Execution Environment
TF	Theoretical Framework
UEI	Upper Extremity Impairment
UI	User Interface
UK	United Kingdom
USA	United States of America
USB	Universal Serial Bus
WCAG	Web Content Accessibility Guidelines
QoS	Quality of Service

Appendix A

Appendix A.1

Demographic data for the study are depicted in Table A1:

Table A1. Demographic distribution for the study.

Participant	Age Range	Geographic Location	Gender
participant 1	40-49	Southern England, UK	Female
participant 2	30-39	Florida, USA	Male
participant 3	30-39	Mississippi, USA	Male
participant 4	30-39	Philadelphia, USA	Female
participant 5	40-49	Southern England, UK	Male
participant 6	16-19	Southern England, UK	Male
participant 7	50+	Southern England, UK	Female
participant 8	20-29	Midlands, UK	Male
participant 9	20-29	Southern England, UK	Male
participant 10	50+	Southern England, UK	Female
participant 11	50+	Southern England, UK	Male
participant 12	50+	Southern England, UK	Male
participant 13	50+	Southern England, UK	Male
participant 14	50+	Southern England, UK	Male
participant 15	20-29	France, EUR	Female

 doi:10.20944/preprints202603.1487.v1

Appendix A.2

Stage 1 (Initial Coding) data for the study are depicted in Table A2 below:

Table A2. Number of references discovered for each focal topic.

Topic (number of references)	Sub-topic	Description	References
AT devices (132)	General Device	Other or alternative devices	40
	Fingerprints	Preference for fingerprint scanning	17
	Facial recognition	Desirable for login	15
	Mobile phone (or tablet)	User's personal smartphone	14
	USB key	A security key that stores certificates	11
	Voice recognition	The user would like to see voice recognition	7
	Fob	An RF (Radio Frequency) device	6
	Text-to-speech	Text-to-speech conversion to aid login	6
	Speech to text	Closed captioning or text prompts	4
	Font change	Adaptations to font style	4
	Color changes	Adaptations to font color	4
	Eye tracking	Eye tracking device	3
	Sip-Puff Device	A device controlled with the user's mouth	1
Desirable features (89)	Universal login	Would want a universal system	15
	Simplified login	Not too many obstacles or options	15
	Remain logged in	Be logged in when they get back	11
	Something you know	2FA (Two Factor Authentication)	8
	Focused options	Options focused on the disability	7
	Happy with just a password	Would like to see just a password system only	6
	Passcode recording	System records time-based code for you	5
	Easier Recovery	Easier options to recover data	5
	Faster login	Quickest possible login preferred	4
	Delete information	Auto-remove old passcodes	4
	Speak to a person	Would prefer to speak to a real person about login issues	3
	Show password	Option to show password	2
	Use of AI	Use of AI once the info is passed to the organization	2
	Picture-Based Authentication	Selecting pictures to log in	2
Disability (131)	Nature of disability	Name of Disability in question	32
	Due to disability	User feels the issue is due to disability	29
	Pass information	Happy to pass information to third parties	22
	Reluctant to divulge	Reluctance to divulge disability	20
	Not because of disability	User feels the issue is not due to disability	11
	Deterioration	Concerns about a deteriorating or degenerative disability	5
Issues[1] (180, 127 [G], 41 [V], 12 [L])	Privacy concerns [G]	Concerns about information or permissions	27
	Frustrating [G]	Feelings of frustration due to authentication	23

[1] Legend: [G] = General issues. [V] = Verification issues. [L] = Lack of issues.

 doi:10.20944/preprints202603.1487.v1

	Identification [G]	Issues with being identifiable	17
	Forgotten password [G]	Unable to recall password	11
	Locked out [G]	No way to verify own account	11
	Distance from device [G]	Being far away/having to reach a 2FA device.	11
	Repeated attempts needed [G]	Repeated attempts needed to log in or tired from repeatedly having to do it	9
	Time-consuming [G]	Logging in is time-consuming	7
	Password mismatching [G]	Inability to match passwords	3
	Distractions [G]	Environmental disabilities	3
	Number of accounts [G]	Extra complexity caused by the quantity of different logins needed	3
	Character set [G]	Issues with the character set	2
	Time-based codes [V]	Two-step authentication issues	17
	2FA [V]	Two-step authentication issues	9
	CAPTCHA issues [V]	Issues with Google (or other) image recognition test—characterized by the use of traffic lights and stairs	6
	Authenticator issues [V]	Authenticator issues or delays	4
	Code retrieval delays [V]	Issues with biometric	3
	Fingerprints [V]	Time delays in emails or 2FA codes coming through	1
	Low difficulty [L]	Minor or no issues with authentication	12
Responsibility (27)	Companies' responsibility	The company is more responsible	14
	Both responsible	Users and companies are equally responsible	10
	Users' responsibility	The user is more responsible	3
Usability v Security (85)	Security important	User feels security is important	34
	Usability (and speed of access) is important	User feels usability is important	20
	Balanced System	Users need a balance between security and usability	18
	Security Sacrifices	Willing to sacrifice security to make it easier to log in	13

Appendix B

Appendix B.1

The interview questions are listed in Table B1.

Table B1. Questions, their scope, reasoning, and categories.[2].

[2] Questions marked with a * are mandatory, failing to complete this will invalidate your submission. Other questions are optional, but if all are completed this will aid the research more.

Categorization key for the questions is as follows:

DE - Demographics

U - Usability

S - Security

DR - Disability Related

 doi:10.20944/preprints202603.1487.v1

Index	Question	Format	Relevance / Reasoning	Category
01	Name	Text	Indexing/Storage	DE1
02	Age Range *	1. 16-19 2. 20-29 3. 30-39 4. 40-49 5. 50+	Age verification, categorization	DE2
03	Gender	1. Woman 2. Man 3. Transgender 4. Non-binary/non-conforming 5. Prefer to define myself as … Prefer not to say	Demographic	DE3
04	Geographic Location	Text	Classification / Diversity	DE4
05	Disability *	Text	Classification / Relevance / Application options	DR1
06	Do you find authentication (i.e., logging into websites or applications) difficult because of your disability?	Yes / No / Maybe	Perception of an issue	DR2/U2
07	In what ways (if any) does your disability make authentication hard for you to do? What are the main difficulties that you face when you log in to systems that do not take your disability into account?	Text	Context on current issues. Difficulty related to disability.	U3/DR3
08	How important is it for you to get logged in quickly?	Scalar value 1-5 1. Not very important 2. Not important 3. Not fussed 4. Important 5. Very important	Need for speed / ease of use.	U4
09	How highly do you rate the importance of security?	Scalar value 1-5 1. Not very important 2. Not important 3. Not fussed 4. Important	Need for security.	S1

E - Effectiveness (of Authentication System)

P - Privacy

All - All categories

 doi:10.20944/preprints202603.1487.v1

		5. Very important		
10	How often do you sacrifice security to make logging in easier? E.g., easy passwords, password reuse, no 2-Factor Authentication (2FA), etc.	Scalar value 1-5 1. Not very often 2. Not often 3. Occasionally 4. Often 5. Very often	Willingness to sacrifice security.	DR4/S2
11	Do you sacrifice security because it's too difficult to authenticate with your disability? Is there anything that could make this easier?	Text	Does lack of usability bar security?	DR5/S3/U5
12	If you had to choose, would you prefer more security or an easier or faster login?	Scalar value 1-5 1. Much easier 2. Easier 3. Balanced 4. Secure 5. More Secure	Preferences.	S4/U6
13	Would you like to have one system that you could use to log into most of your websites and applications?	Yes / No / Maybe	Is it wanted? Single sign on (SSO) needed?	U7
14	When you log in to a site or service, would you like to have details of your disability passed across so that they can automatically adapt their user experience for you?	Yes / No / Maybe	Need for passing data parameters to third party.	DR6
15	Would you like to have the options to choose which elements of your disability are revealed to each third party that you log into?	Yes / No / Maybe	Level of disclosure to third party.	DR7/P1
16	How do you feel about trusting a company with information about your disability, and what benefits or negative side effects do you think it could have?	Text	Trust, privacy, and confidence.	DR8/P2
17	Would you like to see a login system that could work with a variety of inputs, including paddles, sip/puff, audio/text-to-speech devices, optical/head movement, or other assistive technologies?	Yes / No / Maybe	Application hardware interfacing.	U8
18	In relation to the above question, which alternative or assistive technologies would you like to be able to do this with?	Text	Classify hardware options.	U9
19	Would you like to or currently use assistive technology (AT) such as a paddle or switch to authenticate with? Please specify which AT device you would use.	Text	Use of AT for verification/ 2FA.	U10/DR9
20	Would you say that you are currently happy with the way you have to log in to sites currently?	Text	Overall satisfaction with current technology.	E1
21	Do you find it frustrating or have any reservations when logging into systems (e.g., Loss of data, privacy, access denial, difficulty logging in)?	Text	Negative Emotional States.	P3
22	What strengths do you think a good login system should have, and how would you feel if you could use a system like this?	Text	Positive Emotional states.	E2
23	Do you sometimes think that a company should automatically know who you are, or do you welcome	Text	Security levels, individual	P4/S5

 doi:10.20944/preprints202603.1487.v1

	the fact that there is a layer of security always protecting your data? Do you think authentication systems need to be more intelligent?		recognition, and AI detection.	
24	Do you feel that security is an organization's responsibility, that of the user, or a bit of both?	Text	Placement of responsibilities	S6/P5
25	Would you consider using an on-person device for verification, and if so, which would you prefer? E.g. Key fob, USB key, Bluetooth switch, biometric device, or maybe just a mobile phone	Text	Would they be prepared to carry a device with them for verification?	U11
26	Would you like the opportunity to be included in any future research questions in relation to this PhD?	Yes / No Please fill out the separate contact questionnaire if 'Yes'	Opportunity to participate in further testing systems, reviews or general questionnaires.	DE5
27	Any further comments	Text	Qualitative / vocalization of ideas.	All

References

1. How to Meet WCAG (Quick Reference). Available online: https://www.w3.org/WAI/WCAG22/quickref/ (accessed on 29th May 2025).
2. Meet the requirements of equality and accessibility regulations. Available online: https://www.gov.uk/guidance/meet-the-requirements-of-equality-and-accessibility-regulations (accessed on 29th May 2025).
3. Equality Act 2010. Available online: https://www.legislation.gov.uk/ukpga/2010/15/contents (accessed on 29th May 2025).
4. Cropley, D.; Whittington, P.; Dogan, H. A Systematic Literature Review for Facilitating Authentication for the Disabled. In Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE), Fudan University, Shanghai, China, 11th-13th October 2024, pp. 218-225, DOI: 10.1109/ICEBE62490.2024.00041.
5. Furnell, S.; Helkala, K; Woods, N. Accessible authentication: assessing the applicability for users with disabilities. *Computers & Security* **2022**, *Volume 113*, 102561, ISSN 0167-4048.
6. Üstün, T. B.; Kostanjsek, N.; Chatterji, S.; Rehm, J. Measuring Health and Disability, Manual for WHO Disability Assessment Schedule (WHODAS 2.0), World Health Organization. 2010; p.4. ISBN: 9789241547598.
7. Laamanen, M.; Ladonlahti, T; Uotinen, S; Okada, A.; Bañeres, D.; Koçdar, S. Acceptability of the e-authentication in higher education studies: views of students with special needs and disabilities. *Int J Educ Technol High Educ* **2021**, *Volume 18*, DOI: 10.1186/s41239-020-00236-9.
8. Di Campi, A.M.; Luccio, F.L. Accessible authentication methods for persons with diverse cognitive abilities. *Univ Access Inf Soc* **2025**, DOI: 10.1007/s10209-025-01189-4.
9. Andrew, S.; Watson, D.; Oh, T.; Tigwell, G. W. A review of literature on accessibility and authentication techniques. *ACM Assets '20.* **2020**. Article 55, p. 1–4., DOI: 10.1145/3373625.3418005.
10. Alnfiai, M.; Sampalli, S. BraillePassword: accessible web authentication technique on touchscreen devices. *J Ambient Intell Human Comput* **2019**, Volume 10, 2375–2391. DOI: 10.1007/s12652-018-0860-x.
11. Lewis, B.; Kirupaharan, P.; Ranalli, T-M.; Venkatasubramanian, K. A3C: An Image-Association-Based Computing Device Authentication Framework for People with Upper Extremity Impairments. *ACM Trans. Access. Comput.* **2024**, Volume 17, 2, Article 6. DOI: 10.1145/3652522.
12. NVivo (#1 qualitative analysis software for 30 years). Available online: https://lumivero.com/products/nvivo/ (accessed on 17th June 2025).

 doi:10.20944/preprints202603.1487.v1

13. Grimes, R. Introduction. In *Hacking Multifactor Authentication*; John Wiley & Sons: Indiana, USA, 2021; p. xxvii.
14. Gibson, P. Thought (Chapter 8). In *Philosophy*; Arcturus: London, UK, 2021; p. 126.
15. Mohajan, D; Mohajan, H; Memo Writing Procedures in Grounded Theory Research Methodology. *Studies in Social Science & Humanities* **2022,** Vol. 1, No. 4, pp. 10-18, DOI: 10.56397/SSSH.2022.11.02.
16. Braun V; Clarke V; Can I use TA? Should I use TA? Should I not use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches. *Couns Psychother Res* **2021**, Vol. 21, pp. 37–47, DOI: 10.1002/capr.12360.
17. Mathematical Induction. Available online: https://www.math.wustl.edu/~freiwald/310induction1.pdf (accessed on 1st October 2025).
18. Chun Tie, Y.; Birks, M.; Francis, K. Grounded theory research: A design framework for novice researchers. *SAGE Open Medicine* **2019**, DOI: 10.1177/2050312118822927.
19. Charmaz, K. An Invitation to Grounded Theory (Chapter 1). In *Constructing grounded theory. A practical guide through qualitative analysis*; Sage Publications: London, UK, 2006; pp. 1-12, **ISBN:** 978-0-7619-7353-9.
20. Thompson, G. Products—assistive and accessible technologies. In *Digital Assistive Technology*; Awde, N.; Banes, D.; Banes, K., Eds.; Millennium Community Solutions: King's Lynn, UK, 2022; pp. 74-235.
21. Bhandari, G.; Lyth, A.; Shalaginov, A.; Grønli, T.-M. Distributed Deep Neural-Network-Based Middleware for Cyber-Attacks Detection in Smart IoT Ecosystem: A Novel Framework and Performance Evaluation Approach. *Electronics* **2023**, *12*, 298. DOI: 10.3390/electronics12020298.
22. Rich, E.; Knight, K. Connectionist Models (Chapter 18). In *Artificial Intelligence,* 2nd ed.; Shapiro, D. M.; Murphy, J. F., Eds.; McGraw-Hill: New York, USA, 1991; p. 492.
23. The future of artificial intelligence. Available online: https://www.ibm.com/think/insights/artificial-intelligence-future (accessed on 12th November 2025).
24. MacKenzie, I. S. Modelling Interaction (Chapter 8). In *Human-Computer Interaction*, 1st ed.; Morgan Kaufmann: Massachusetts, USA, 2013; pp. 249-255.
25. Whittington, P.; Dogan, H. Authentibility Pass: An accessible authentication gateway for people with reduced abilities. In Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE), Sydney, Australia, 4th-6th November 2023, pp. 155-162, DOI: 10.1109/ICEBE59045.2023.00043.
26. Schwartz, S.; Maciej, M. SAML (Chapter 3). In *Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software*; Apress: Berkeley, CA, 2020; p. 65. DOI: 10.1007/978-1-4842-2601-8.
27. Dash, S. K. Federated Authentication-II (Chapter 5). In *Web Authentication Handbook*; Orange Education: Delhi, India, 2023; pp. 167-169.
28. Barker, J. Why physical space matters in cybersecurity (Chapter 7). In *Confident Cyber Security*; Kogan Page: London, UK, 2018; pp. 121-130.
29. Firouzi, A.; Dadkhah, S.; Maret, S.A.; Ghorbani, A.A. DataSense: A Real-Time Sensor-Based Benchmark Dataset for Attack Analysis in IIoT with Multi-Objective Feature Selection. *Electronics* **2025**, *14*, 4095. DOI: 10.3390/electronics14204095.
30. Intrusion detection evaluation dataset (CIC-IDS2017). Available online: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on 4th November 2025).
31. Li, Y.; Li, Y.; Wang, G.; Hu, H. An Adaptive Dynamic Defense Strategy for Microservices Based on Deep Reinforcement Learning. *Electronics* **2025**, *14*, 4096. DOI: 10.3390/electronics14204096
32. Zawadzki, P.; Dziwoki, G.; Kucharczyk, M.; Machniewski, J.; Sułek, W.; Izydorczyk, J.; Izydorczyk, W.; Kłosowski, P.; Dustor, A.; Filipowski, W.; et al. Quantum Enabled Data Authentication Without Classical Control Interaction. *Electronics* **2025**, *188*, 104810. DOI: 10.1016/j.jmva.2021.104810.
33. Disability. Available online: https://www.who.int/health-topics/disability#tab=tab_1 (accessed on 6th November 2025).
34. Designing Remote Keyless Entry (RKE) Systems. Available online: https://www.analog.com/en/resources/technical-articles/designing-remote-keyless-entry-rke-systems.html (accessed on 14th November 2025).

 doi:10.20944/preprints202603.1487.v1

35. Battey, H.S.; Cox, D. R. Some aspects of non-standard multivariate analysis. *Journal of Multivariate Analysis* **2022**, *14*, 4096. DOI: 10.3390/electronics14204096.
36. Ghorbani Lyastani, S; Schilling, M.; Neumayr, M.; Backes, M.; Bugiel, S. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. *IEEE Symposium on Security and Privacy (SP)* **2020**, pp. 268-285, DOI: 10.1109/SP40000.2020.00047.