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

David Cropley * , Paul Whittington , Huseyin Dogan

Posted Date: 10 February 2026

doi: 10.20944/preprints202512.0371.v2

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

 doi:10.20944/preprints202512.0371.v2

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

This research paper address why it is that disabled people 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 stage of authorization (allowing continued use of the service once logged in). While 'normal' people 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 disabled people 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. identifying patterns in the A series of interviews (n=15) are analyzed with Constructivist Grounded Theory methods to discover patterns in the participant's answers and build a theory about why Accessible Authentication is a problem. By way of inductive theorem building, this paper categorizes common traits that participants have revealed during interviews. The key findings reveal that most disabled users say that their capability to authenticate effectively is effectively 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 there is a lack of accessibility for those using traditional authentication techniques. A further area of concern for the participants suggests that maintaining security alongside ease-of-use was found to be important to them, so future work on improving accessibility should find ways to ensure that disabled users' information is not left vulnerable.

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

1. Introduction

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. This is generally not catered for by mainstream login systems, due to disconformity with Web Content Accessibility Guidelines (WCAG) [1], which in turn is partially due to a lack of empathic understanding for people without sufficient physical or cognitive to conduct the verification process as a non-disabled person might more easily accomplish. Not only is it important for reasonable adjustments for disabled users to be made under The Equality Act 2010 [2], it is actually 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), Analysis Methodologies (3.4) and Data Science Modelling: Trends

 doi:10.20944/preprints202512.0371.v2

(3.5), where we philosophize over advanced analytical methods. 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 culminates with the Conclusion (Chapter 6), which aims to assess the potential impact of this research. Here, we also outline the development of a TF wherein accessibility complications causing hinderance to our disabled community can be properly addressed and remedied.

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 that 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' 'authentication and both had to appear in the reviewed literature for inclusion to be valid. More specifically, it included the category of disabled people listed in the World Health Organization (WHO) Disability Assessment Schedule [6]. Secondary criteria research investigated individual cases of the terms 'disability' and 'authentication' and 'Application Programming Interface (API)'. Tertiary search criteria included philosophical paradigms, business, Assistive Technology (AT) and other authentication concepts. Repositories, databases and sources included Science Direct, Bournemouth University Research Online (BURO), Sage Publishing, Research Gate and Google Scholar for the primary criteria searches. Various other sources were used for secondary and tertiary criteria and are listed in more detail in the literature review itself. Screening for the primary category would see each reference limited to being a book or journal published within the last five years (with inclusion of some established literature) and saw the exclusion of matter that did not meet the exact search terms specified previously, and any non-academic material (e.g. news and general websites).

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.

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

An empirical paper about "Accessible Authentication methods for people with Diverse Cognitive Abilities" [8] does reinforce the hypothesis that there are compound issues concerning the accessibility of current authentication techniques. Naturally though, this paper only accounts for cognitive issues whereas we are looking at detriments caused by any type of disability and not all papers will be this broad in classification. It may also again be worth noting that a literature review by Andrew et al. did note "shortfalls and gaps in the literature" [9] in the field of Accessible Authentication, so emerging empirical evidence on this subject is a refreshing discovery to make.

Additionally, an empirical study conducted in 2017 discusses an alternative method of authentication for People Who Are Blind [10], which provides evidence to support an alternative technique to traditional authentication. This technique uses a system of long and short taps, as opposed to keyboard and audio entry. This is shown to provide security against eavesdroppers and shoulder surfers, with minimum detriment to ease of use. It is not known whether this has been implemented in any production environment, but it does introduce the idea that authentication can

 doi:10.20944/preprints202512.0371.v2

be made more accessible for blind people and illustrates how scientific research can highlight specific areas of accessibility 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 provide benefits for disabled users (and potentially the wider community) through a system that is more intuitive. Although password strength calculations have proved to provide sufficient entropy against shoulder surfing and close-adversary attacks, there could be a scenario where an online brute force attack bot could scan the first phase stochastically to reduce the integrity of the system, so one might wonder if it would ever be adopted as a public release. Nonetheless, it remains a valid instigation and important flag bearer for the cause of accessibility rights in the realm of authentication. It is also interesting to note that several participants said the application was fun to use, which could potentially eliminate many pain points when it comes to bringing a system like this to market.

The above represents the limited selection of documents available that directly relate specifically to 'Accessible Authentication' (as a unified concept), despite an abundance of topics in either 'Accessibility' or 'Authentication' in their individual 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 of suggestions for existing or new authentication systems, supplemented along with a proposal for a prototype application to substantiate the viability and practicality of the framework. 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 created from a series of interviews (n=15) with disabled users (with no restrictions on geographical region or gender) that were recorded in audio format and then transcribed and coded using the NVivo 20 [12] 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 the 16–19-year-old range, through all other age ranges (20-29, 30-39, 40-49) up to and including people in the 50+ age dimension. No children under the age of 16 were permitted to be included in the study (in line with allowances of the ethical approval that were granted). The ratio of female to male participants is exactly one third female to two thirds male, with no participants declaring their gender as anything other than these two variants, although alternative options were provided to state this, if desired. We acknowledge that this ratio is not ideally balanced and understand that experiences may vary when gender is considered, and we have nevertheless aimed to analyze and portray the results without bias, as would be expected.

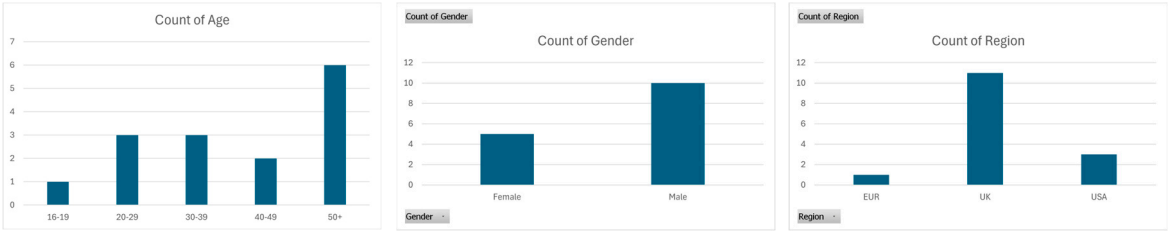
Comparatively, the division of impairments between mental and physical disabilities (that were classified as relevant to the research), maintains an appropriate balance, including, but not limited to; Spinal Injury, Quadriplegia, Paraplegia, Facioscapulohumeral Muscular Dystrophy (FSHD), Cerebral Palsy (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 and

 doi:10.20944/preprints202512.0371.v2

paddles and pen tablets), 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 below 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 illicit qualitative results for this paper and participants would frequently provide extra context when answering, so therefore 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 developmentof a Framework for Accessible Authentication. In future work, a refined questionnaire is intended to be created which will aim increase the granularity of the grounded philosophical theory after these first-phase interviews. Vice versa, the questionnaire possibly may also illicit more in the way of quantitative results, which may scientifically balance with the constructive theory and this research could potentially stem into a full mixed-methods analysis by the time of its maturation.

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 as to who should take responsibility for a less secure system? Should it be the organization or the user who decides how secure their own system access is? The results from the interviews will be discussed further in Section 4 and could have a profound impact on Framework design and implementation for a system that hands over more or less control to one side or another.

Other questions as well as preferences for usability over security include accessible technology currently used by participants and/or devices that 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.

One more difficult question includes loosely assessing the feelings experienced 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 be 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 all the semi-structured questions asked in the interviews can be found in Table B1 within 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 for our approach in this paradigm resulted in a dichotomy over which thought process should be used.Some questions also present the challenge of "propositional attitudes" [14], which lead to considerations about emotional "hopes, fears or beliefs" about the

 doi:10.20944/preprints202512.0371.v2

predicament. Ultimately, a methodology focused on deduction was chosen, and the justification for this will now be described in further detail.

A decision was made to harness Grounded Theory (GT) [15] methodologies instead of Thematic Analysis (TA) [16] to analyze the data, and the philosophical reasoning behind this is duly explained herewith. Initially, the methodological approach for analysis to be used in this research was intended to have used TA as its method on the basis that some existing themes had already been illuminated upon by both previously conducted 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 disabled people 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 of GT will be needed to provide evidence of credibility, as opposed to 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, this is why various GT methodologies were investigated to find a suitable GT method to apply to the data set, which can consequently build theorems from 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 contruction 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 also must consider the fact that the ensuing analysis could be categorized as abductive reasoning, as it can be appreciated that there will be a temptation to succumb to interpretive guesswork, simply due to the subjective nature of the research. Nevertheless, the findings given in the results section coming up next are based on real-world empirically induced findings and therefore we would hope that they would be acceptable as part of a scientific theory.

3.5. Data Science Modelling Trends (for Future Analysis Methods)

These methods of analysis can also be applicable in the field of Data Science, as it co-aligns with theoretical data modelling to identify opportunities and statistical prediction for "forecasting of short and long-term outcomes" [20], rather than trying to produce a single law, which could ultimately prove to be refutable. Increasingly, Generative AI (GenAI) is currently taking on a more predominant role in data science analysis and could also lend itself to the dynamic modelling of a *heuristic framework* (using experimental rules to test hypotheses) that creates new suggestions for developmental standards or categories for AA, provided that a collection of appropriate, pre-existing datasets are properly fed into an automaton that has been formulated with GenAI at its core.

 doi:10.20944/preprints202512.0371.v2

3.6. Hypotheses

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

1. How often do people with disabilities encounter problems when they try to log in to systems?
   - What are the issues people with disabilities face when they try to authenticate?
2. Is the person's disability the main hindrance for 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 that of the average user. This raises concerns for our community about whether this particular function in the online world is accessible, or not.

4. Results

4.1. Overview

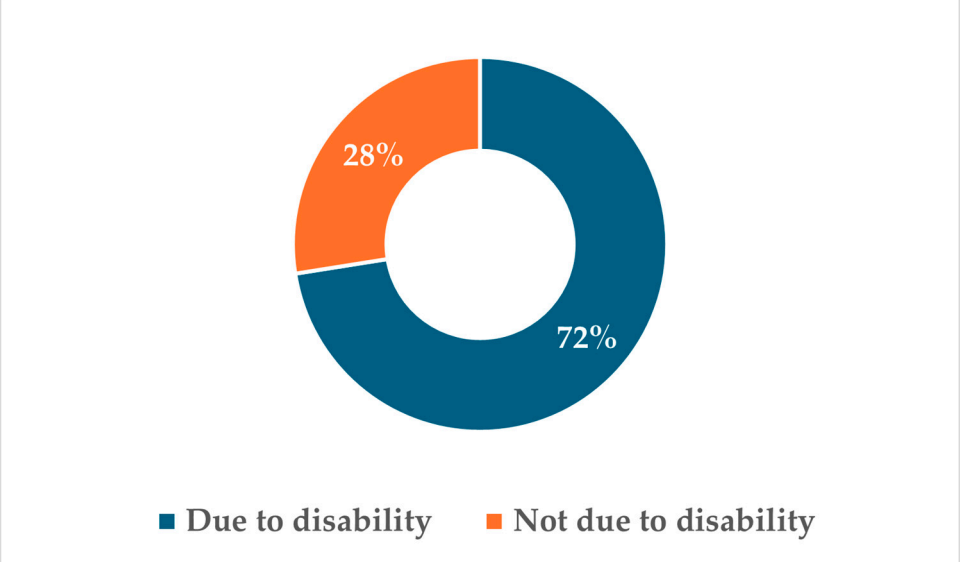
The results aim to answer the research questions stated in the previous section and we anticipate a our analysis will show a wide variety of results, because everyone is different. Therefore, this becomes a reason for utilizing GT as a method of qualitative analysis, because from this we can deduce a theory with 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 sub-categories, which have been talliedby 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 it was found that most users find that authentication is made more difficult due to their disability, as illustrated in Figure 2 below.



 doi:10.20944/preprints202512.0371.v2

Figure 2. Disability affecting Authentication (n=15). This figure illustrates a perceived disparity between difficulty and ease of use when a particpant was asked if they think it is due to their disability or not.

As we can see from the pie chart in Figure 2, more people had issues with authentication due to their disability as opposed to the problem being unrelated to it in their opinion. The results show 29 occasions (72%) where participants consider authentication to be more difficult because they have a disability as opposed to 11 occasions (28%) whereby users felt that their disability did not really affect their ability to login with relative ease. 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 improve, and it is not indicative of the fact that they were not without any difficulties altogether.

There was an equal balance between being willing to reveal information (about their disabilities) to a third party, and about as many of those who wanted to guard their details, according to the coding results. Finally, a small number were concerned about issues caused by the ongoing deterioration caused by 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 below, which also categorizes them into physical and cognitive realms:

Table 1. Disabilities 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 disability is referred to by the participant; [2] In some cases a disability could fall into both physical and cognitive categories.

4.2. Coding Results

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.

4.2.1. General Findings from Stage 1 - Initial Coding

A set of characteristic traits were seen to emerge from the participants' answers. Reasoning for this will be deliberated accordingly in our Stage 3 Inductive Theorems, 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 analyisis. 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.
    - **Issues** – Time-based codes present the biggest challenge, specifically physically being able to reach for a 2FA device.
4. **Desirable Features** – A simplified login is preferred with optional settings.

 doi:10.20944/preprints202512.0371.v2

5. **Responsibility** – The onus for privacy and security should lie with the service provider. A user's own responsibility is also recognized.

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 looking at all the existing codes that we have and reducing them down to fewer terms, which can be terms which are similar. 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 hinderances 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 construct a theory from the answers.

4.2.3. Formulation of Substantive Theory from Stage 3 – Contructivist Theory

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

Remark 1.

4.3. Formal 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):

- Most users identify problems logging in relation to their disability.
    1. The most desired feature is a simplified login such as an SSO.
    2. Security is of high importance to users but closely matched by the desire for ease of use.
    3. The most common issues appear to be with time-based codes (for 2FA) and the CAPTCHA systems.
    4. We have covered a wide spectrum of disabilities in our study.
    5. The option to remain logged in is desirable in certain situations.
    6. Many users feel that privacy and security of the login system is the company's responsibility, but several acknowledge their own responsibility too.
- There is interest in alternative devices to facilitate the log-in process.
    7. 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

 doi:10.20944/preprints202512.0371.v2

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 that it could not be used in a highly focused study into just one disability, but this would stray from our intended research objective, which is inclusive for anybody 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 because of having a disability, and this is undeniably important because it verifies the need for this paper to highlight that there is an existential problem with the level of accessibility in a core system that has repeated daily use in our lives.

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 can be found in the Data Availability Statement at the end of this paper.

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

We acknowledge that a control group would delineate differences between disabled and non-disabled users, however this was not a focus for participant selection, and we feel that the results provide adequate explanation. We also note that several participants do not initially identify it has 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, noting any extra problems that may still exist and it was discovered that most users feel that they have some form of extraneous problem with authentication that 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, Schizophenia/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, we see that disabled users generally have a variety of issues that they find detrimental to the authentication process for them. There were 12 spoken references where the user claimed to have few or no issues, and although this is encouraging for the current situation, it does not equitably compare to the total of all other issues found to be experienced by all the users.

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

 doi:10.20944/preprints202512.0371.v2

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, as 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 disabled people 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 with a preference for security, it reinforces the fact that usability is still imperative to any accessible system, as was 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, this would be an ideal situation, both for the disabled community and organizations wishing to maintain a high degree of customer loyalty.

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

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 regarding accessible authentication points the problem leans towards usability. In fact, it turns out that many place a higher value is 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 versus security, the coding suggests that ease of use matches security in importance to users, where users would generally like some kind of acceptable level for each, which is entirely understandable. Surprisingly, despite many admitting to making security sacrifices to make things easier, as the interviews progressed, increasing passion for security was identified. We also discovered some debate over whether certain devices, such as fingerprint scanners for example, could be classified in some way as AT devices at the same time if they can be considered to aid the ability to login. It is not uncommon for everyday devices to be used in this way, such as X-Box controllers, and while it is also true that there remains a vast quantity of much unheard-of AT devices available for a large variety of very specific disabilities [21]. 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 which 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 have a high level of security guarantees, especially so as 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 any depth in security counter-measure steps which can be taken, it is acknowledged that application developers do have an ongoing battle against cyber-attacks, currently, where the stakes are becoming higher and even household names are becoming victims. Many people fear advances from AI attack bots, but 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 [22] which has its origins in early day neural nets with the invention of the perceptron by Rosenblatt in 1962 [23], something which modern AI moves aways from with today's Natural Language Processing and drifting into multimodal AI which can "seemingly do it all" [24].

While recognize that usability is a problem with Accessible Authentication, and it is challenging to eliminate the importance of usability altogether as this can be a vital ingredient when it comes to

 doi:10.20944/preprints202512.0371.v2

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' 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" [25].

An observation was made by a participant in one of the interviews that disabled people are technically 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.

To conclude the analysis, we define these with Lemmas (sub-Theorems), as they are particularly subjective in nature and would not necessarily require defined proof for them to still be useful as weighted opinions (or suggestions) that can be added to the proposed Framework for Authentication Applications.

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*.

4.3.5. We Have Covered a Wide Spectrum of Disabilities in Our Study

It was noted that many participants would come up with ideas that could be helpful to users with other forms of disability to their own, and 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 based open to all disability types may appear too broad (when compared to a paper based on a single type of disability), 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, there were many people who 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 because of having a disability, and this is undeniably important because it verifies the need for this paper to highlight that there is an existential problem with the level of accessibility in a core system that has repeated daily use in our lives.

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

This concept is as interesting as it is controversial as to whether sites should keep you logged in or allow access immediately when you return to them. 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,

 doi:10.20944/preprints202512.0371.v2

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 … everytime I login from there I have to sign in. It doesn't matter if I'm late, remember me? It never does … Everytime. 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.

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. On final addition of all issues, it is noted that the general issue over privacy concerns soon become the highest concern, which could be relationally linked to preferences 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 have difficulties due to a lack of accessibility integrated into authentication procedures.

Giving way to rationality, several participants agreed that it was both their own responsibility as well as the organizations, as accident or negligence could not always be reliably blamed on the 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 solely on the organization, so it may highlight where certain psychological perceptions, expectations and boundaries lie.

4.3.8. There Is Interest in Alternative Devices to Facilitate the Log in 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.Resultantly, any form of general device alternative to passwords was the most popular, followed by fingerprint scanners, facial recognition, a mobile phone 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 condition can see the benefits of using an eID, such as a USB key or credit card-sized ID that can be hung around their neck. The ability to remember passwords can be a concern for them, which can also be the case for many other users as well.

Plenty of participants expressed interest in using fingerprint scanners, with many others expressing keenly interested in 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.

 doi:10.20944/preprints202512.0371.v2

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 mechanical ability 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 password[s], which is why … 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 … its just airflow right there because your muscles are weaker" (P03, 1:30.3, Muscular Dystrophy) which reminds us that additional accessibility authentication issues occur in many ways for disabled people.

4.4. Qualitative Summary

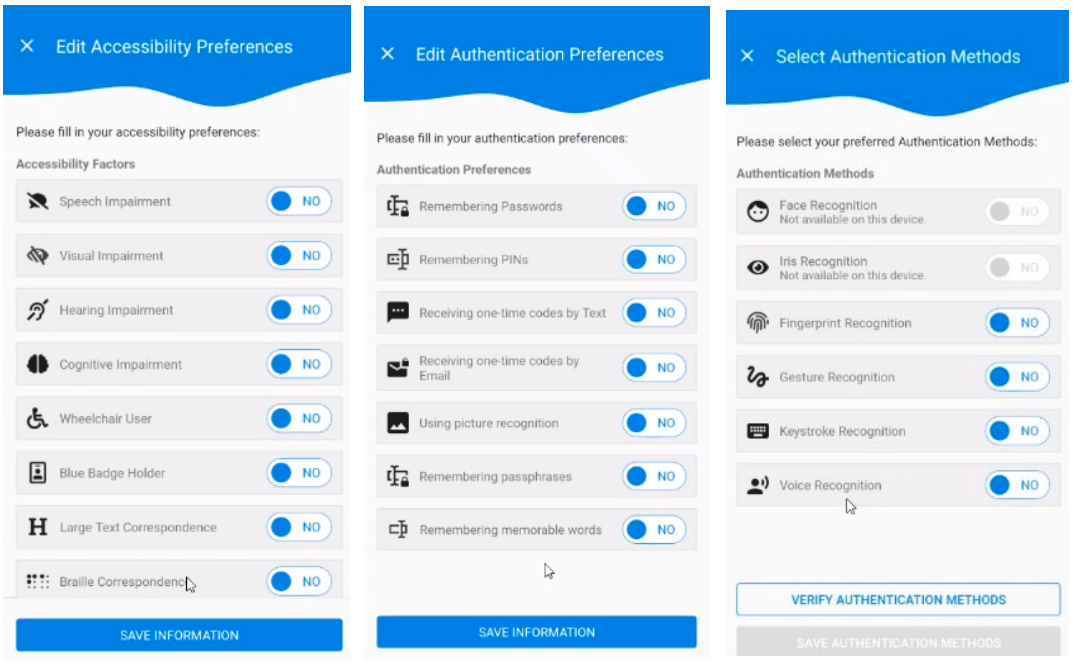
Throughout the interviews several interesting points were made by the participants, including two who mentioned the idea of a prominent red button to log in with, much like the type you might find in a game show, thus illustrating a desire for simplicity when authenticating. This can be compared to AT devices that have a simple process of 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 which prevents it from going out-of-reach. One participant was also unaware that USB-based fingerprint keys were already available, as this would be ideal for them. This shows that there is still much scope for authentication, and there is no need to adhere to anachronic views of how it should be.

5. Discussion

This research acknowledges that its origins derive from initial research conducted by Whittington and Dogan [26]; that included the creation of a prototype application known as Authentibility (see Figure 3), which is designed to accept information about a user's disability in order to transmit that data to service providers so that they can better cater for their needs. A video explaining this prototype can be found in the Supplementary Material video link S1. The research now pivots to adapt to study the way that the user can log in to a service that is more accessible to them, although the original idea of passing disability data to a service is something yet to be considered for inclusion in future versions of the prototype.

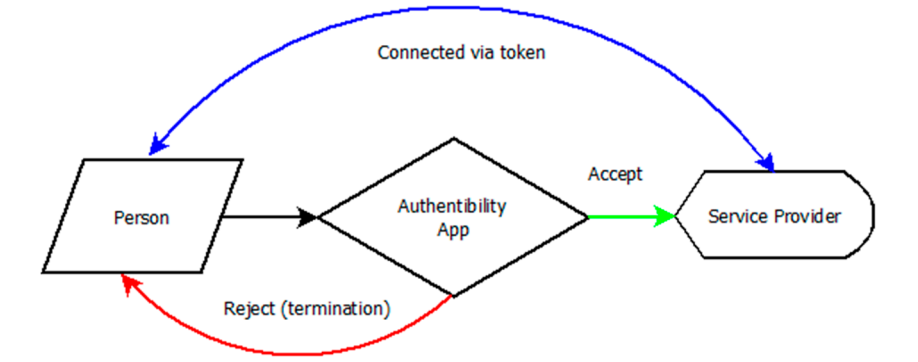
 doi:10.20944/preprints202512.0371.v2



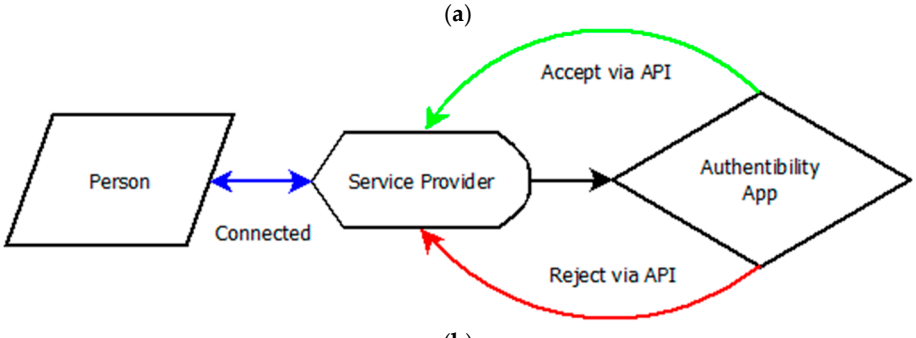
(**a**) (**b**) (c)

Figure 3. The Authentibility prototype app. The user has the option of specifying (**a**) Their disability; (**b**) Their preferences for authentication; (**c**) Authentication methods they would like to use.

Theorectically, there are two methods of authentication with a service for a user (see Figure 4), either via the authentication app for verification and subsequently on 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 these two, due to reduced complexity [27], whereby the service polls the authenticator for eID confirmation. Development of the application may require further research into Development, Security and Operations (DevSecOps), along with User Interface (UI) design, both coupled with extra considerations for the disabled. Naturally, this is also a logical method for in-person eID utilization, in the event that the client is physically located at the service's premises.



(**a**)



(**b**)

 doi:10.20944/preprints202512.0371.v2

Figure 4. 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) [28], if identity is confirmed; (**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.

From our results, we have found that many users have a serious concern for the security of their personal information, so it is natural to assume that any authentication system should strive to achieve the maximum security possible. The initial idea that making it simpler to use for disabled people would be an ideal solution but has the disadvantage of reducing security to a vulnerable user group. As well as using secure hashing algorithms, the bare-metal systems that an authenticator runs on will also have to be as impenetrable as possible.

We have identified extra problems that people suffer when logging in that are related to their disability, such as those found with time-based codes and CAPTCH systems, as well as issues with responsibility. We have uncovered a yearning for a simplified system or SSO along with alternative authentication methods which may be preferable for disabled people 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 can perhaps be solved by adapting these levels dependent on the service that is being accessed. Suggested precautions for security might include software hosting at secure premises with good security such as Access Control Systems (ACS), physical identification (ID), Closed Circuit Television (CCTV) to prevent social engineering or physical access to sensitive hardware [29].

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" [30] such as X-IIoTID, CIC-IDS2017, CICIoT2023 and Edge-IIoTset. Many datasets are open-source and so freely available to use without cost, such as the CIC-IDS2017 dataset that is provided by the Canadian Institute for Cybersecurity [31]. These data sets all contain information that can help keep a system secure.

More 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 [32]. 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" [33]; 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 of further research that can be linked to this study of Accessible Authentication, both in terms of security in balanced conjunction with UI design, reliability and speed of operation, i.e., Quality of Service (QoS). It would be vital to include the opinions of disabled people to determine the applicability of the discussed theories.

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 exercised, for example, by informing influential stakeholders(such as Microsoft, Google and Apple), of the opportunity to be additionally inclusive to their clients, the research can achieve its full potential impact.

 doi:10.20944/preprints202512.0371.v2

We believe that the results from the analyses in this paper sustain the substantive theory that problems exist with the level of accessibility available for disabled people when they attempt to authenticate.

We acknowledge that this paper is limited by the number of interviews conducted, with further diversification of participants being desirable and a limit on how much of the quoted text could be included. We also acknowledge that focus could be on one specific disability, or that we could classify results by disability, and this remains as a limitation to the paper as well.

6. Conclusions

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" [36], and in our increasingly more connected digital world, stakeholders must make advances to secure more inclusive methods of Electronic Identity Authentication.

We can see from the results that security is important to disabled people, so making this a priority on any eID is a must to protect them fully. It was accepted that any general AT/hardware device would be acceptable as an eID, with preferences for fingerprints and face recognition coming out 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 [37], which can be replicated at low cost, which raises 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.

6.1. 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 [34], 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 so as not to overload the participants with the burden of writing out lengthy answers. However, alternative routes to further data collection will be considered.

It is envisaged that the Framework or future applications devised from this paper could foreseeably include physical (on person) Electronic ID (eID), either as part of a resident Trusted Executions Environment (TEE) for TouchID systems or alternative 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) based authenticators. These devices have the strength to utilize passwordless, single-factor authentication devices, which have been empirically proven to have advantages over traditional passwords or two-factor (2FA) authentication [35].

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

To conclude, by looking at our Theorems, we have discovered the existence of multiple issues within the domain of electronic identity authentication, manifesting themselves in various forms. Through the process of an empirical qualitative study, we consider that disabled users are consequently affected by these, due to a lack of accessibility inefficiencies. It is recommended that

 doi:10.20944/preprints202512.0371.v2

solutions should be implemented to improve the usability for 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.

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 that supports the findings of this study is available at BORDaR – Bournemouth Online Research Data Repository - 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 the purposes of qualitative coding, cross comparisons and graph production. GenAI results were not utilized in any way for resultant coding or analysis, as experimental results proved far too unrelated to be of any purposeful 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
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-OnSSO

 doi:10.20944/preprints202512.0371.v2

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 is depicted in Table A1 below:

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

Appendix A.2

Stage 1 (Initial Coding) data for the study is 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' personal smartphone	14
	USB key	A security key that store certificates	11
	Voice recognition	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

 doi:10.20944/preprints202512.0371.v2

	Sip-Puff Device	A device controlled with the users' 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 real person about login issues	3
	Show password	Option to show password	2
	Use of AI	Use of AI once info passed to organization	2
	Picture based authentication	Selecting pictures to login	2
Disability (131)	Nature of disability	Name of Disability in question	32
	Due to disability	User feels 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 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
	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 login 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 quantity of different logins needed	3
	Character set G	Issues with 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 use of traffic lights and stairs	6

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

 doi:10.20944/preprints202512.0371.v2

	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) 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 login	13

Appendix B

Appendix B.1

The interview questions are listed shown in Table B1.

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

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, categorisation	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

[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

E - Effectiveness (of Authentication System)

P - Privacy

All - All categories

 doi:10.20944/preprints202512.0371.v2

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 5. Very important	Need for security.	S1
10	How often do you sacrifice security to make logging in easier? E.g. easy passwords, reuse passwords, 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

 doi:10.20944/preprints202512.0371.v2

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 technology devices?	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 that you are currently happy with the way you have to login 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 the fact that there is a layer of security always protecting your data? Do you think authentication systems need to be more intelligent?	Text	Security levels, individual recognition, AI detection.	P4/S5
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),

 doi:10.20944/preprints202512.0371.v2

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.; Venkatasubramanianl, 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).
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. Data science vs data analytics: Unpacking the differences. Available online: https://www.ibm.com/think/topics/data-science-vs-data-analytics (accessed on 14th June 2025).
21. Thompson, G. Products – assistive and accessible technologies. In *Digital Assistive Technology*; Awde, N.; Banes, D.; Banes, K., Eds.; Millenium Community Solutions: King's Lynn, UK, 2022; pp. 74-235.
22. 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.
23. 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.
24. The future of artificial intelligence. Available online: https://www.ibm.com/think/insights/artificial-intelligence-future (accessed on 12th November 2025).
25. MacKenzie, I. S. Modelling Interaction (Chapter 8). In *Human-Computer Interaction*, 1st ed.; Morgan Kaufmann: Massachusetts, USA, 2013; pp. 249-255.
26. 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.

 doi:10.20944/preprints202512.0371.v2

27. 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.
28. Dash, S. K. Federated Authentication-II (Chapter 5). In *Web Authentication Handbook*; Orange Education: Delhi, India, 2023; pp. 167-169.
29. Barker, J. Why physical space matters in cybersecurity (Chapter 7). In *Confident Cyber Security*; Kogan Page: London, UK, 2018; pp. 121-130.
30. 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.
31. Intrusion detection evaluation dataset (CIC-IDS2017). Available online: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on 4th November 2025).
32. 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
33. 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.
34. Battey, H.S.; Cox, D. R. Some aspects of non-standard multivariate analysis. *Journal of Multivariate Analysis* **2022**, *14*, 4096. DOI: 10.3390/electronics14204096.
35. 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.
36. Disability. Available online: https://www.who.int/health-topics/disability#tab=tab_1 (accessed on 6th November 2025).
37. 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).