Universal Access in the Information Society
https://doi.org/10.1007/s10209-025-01189-4

LONG PAPER

Accessible authentication methods for persons with diverse cognitive abilities

Alessia Michela Di Campi[1] · **Flaminia L. Luccio**[1]

Accepted: 14 January 2025

Abstract
The technological world offers a plethora of resources that could be potentially engaging for users with diverse cognitive abilities. However, access to these resources is often secured by authentication mechanisms that can pose accessibility barriers. To comprehend how these mechanisms could be better designed to enhance accessibility, we conducted a literature review and subsequently conducted a study, gathering empirical data through online questionnaires administered to 34 users with diverse cognitive abilities. Our investigation and analysis focused on their experiences with various authentication methods, aiming to identify the challenges they commonly encounter. This paper's primary contribution lies in presenting evidence that many conventional authentication approaches lack accessibility. Additionally, we advocate for the adoption of biometric authentication systems as a promising direction, emerging as the most accessible solution based on our study results. Furthermore, drawing insights from existing works, we extracted and synthesized a set of guidelines that we believe IT experts should consider when developing an accessible authentication system. We validated these guidelines through our questionnaire, emphasizing which ones our user group deems most relevant.

Keywords Accessibility · Authentication · Diverse Cognitive Abilities

1 Introduction

There are over one billion persons with disabilities worldwide, constituting approximately 15% of the global population [1]. Despite evolving conditions and efforts to address discrimination, individuals with disabilities still encounter fewer opportunities than the general population. This is more evident than in the realm of digital media. According to Nielsen, American adults dedicate over 11 h daily to listening, watching, reading, or engaging with digital media [2]. While access to any platform is effortlessly available for those without disabilities, requiring only the ability to independently use a smartphone, TV, or computer, individuals with disabilities may face considerable challenges, particularly when authentication methods come into play.

Users with disabilities exhibit a broad spectrum of characteristics, encompassing not only physical limitations like motor, auditory, or visual impairments but also a diverse array of cognitive abilities. This article specifically targets the subset of users with distinct cognitive abilities, constituting approximately 1% of the global population, with 85% falling into the category of mild disabilities [3]. A significant portion of this demographic resides in developing countries [4]. Diverse cognitive abilities encompass a wide range of functional features, including memory, perception, problem-solving, attention, reading, linguistic proficiency, and verbal comprehension. Associated impairments often arise from conditions such as autism, brain damage, cerebral palsy, epilepsy, mental retardation, or neurological deterioration [5].

A prominent objective of our society is to garner increased national and global attention toward expanding the possibilities for individuals with disabilities to access technologies seamlessly, both at home and in educational and professional settings. In pursuit of this goal, the market offers an extensive array of ready-to-use Assistive Technology (AT) tools and devices, as exemplified by ATIA [6], which furnish resources such as screen magnifiers, voice

✉ Flaminia L. Luccio
luccio@unive.it

Alessia Michela Di Campi
alessia.dicampi@unive.it

[1] DAIS, Ca' Foscari University of Venice, via Torino 155, 30170 Venice, Italy

Published online: 27 January 2025

recognition software, and computer mice tracking users' eye movements, among other enhancements to functional capabilities. It is crucial to note, however, that while ATs address various needs, they do not specifically cater to users with diverse cognitive abilities.

Another approach to supporting users with disabilities is to adhere to the principles of Universal Design (UD), which strive to create products accessible to all users. These principles can be applied independently of Assistive Technologies (ATs) or can enhance the design process to align with available ATs [7]. An illustrative example is the Accessify Web accessibility tool [8], designed to enhance web accessibility for everyone, including individuals with disabilities. It aids developers in crafting websites that adhere to Web accessibility standards and guidelines, such as the Web Content Accessibility Guidelines (WCAG). Accessify offers a range of tools and resources, including the Accessibility Checker, which scans web pages and provides suggestions for improving accessibility, and the Color Contrast Analyzer, ensuring readability for visually impaired users by checking the contrast between foreground and background colors. Additionally, developers benefit from tools and plugins like the AccessifyAPI, enabling the integration of accessibility features into web applications, and the AccessifyUI Plugin, furnishing accessibility features for users with disabilities, such as keyboard navigation and high contrast mode.

Another valuable resource is the CAST Figuration [9], an openly licensed, responsive, mobile-first, and accessible framework for developing usable and accessible websites. It aligns with best practices outlined in Section 508 of the "Electronic and Information Technology Accessibility Standards" [10], and in the W3C recommendations [11]. Furthermore, specific guidelines, such as those proposed by the W3C Cognitive Accessibility Task Force [12] (see Sect. 3.3 for more details), offer additional insights and recommendations in this domain.

Despite the available offerings in the market to enhance technology accessibility for individuals with diverse cognitive abilities, there remains substantial work to be done in this domain. A comprehensive understanding of these disabilities and their specific needs is imperative [13]. Many webmasters, software designers, and developers may lack direct interaction or observation of individuals with diverse cognitive abilities, leading to a limited awareness of potential accessibility barriers these users may encounter during the authentication process.

In this endeavor, we aimed to take a progressive stride, substantiating the accessibility of existing authentication methods through real-user interactions with diverse cognitive abilities. Our objective was to propose accessible solutions and compile an exhaustive list of guidelines for accessible authentication systems. We pursued answers to the following research questions:

RQ1: Do users with diverse cognitive abilities find different authentication systems accessible?

RQ2: Which authentication approach do they find the easiest to use?

RQ3: What do they think could improve the accessibility of existing authentication approaches?

To answer these questions we first analyzed the current state of the art of accessible authentication methods (RQ1, RQ2). Subsequently, we conducted a user study by administering an online questionnaire to individuals with diverse cognitive abilities (RQ1, RQ2, RQ3).

Our user study included 34 adult participants.

While we acknowledge that this sample size may not be extensive, as we will elaborate on later, gathering such a number of questionnaires posed a considerable challenge due to the specific type of disability among these users.

Our findings underscore the imperative for enhancements in current authentication methods, encompassing both adherence to existing guidelines and the practical selection of solutions most suited for these users. Notably, biometric systems, intelligent mechanisms that capture an individual's physical attributes such as voice, face, or fingerprints, emerge as a highly promising solution, addressing both accessibility and security concerns. Users with diverse cognitive abilities often opt for passwords considered weak, and employing biometric approaches could fortify system security significantly.

The paper is structured as follows. Section 2 describes the background on the considered disabilities and on authentication mechanisms, and in Sect. 3 the related work and existing accessibility guidelines for authentication. Section 4 introduces the methodology and Sect. 5 the results of our user study. Section 6 discusses limitations and possible improvements to the authentication methods for users with diverse cognitive abilities. Finally, Sect. 7 discusses future work.

2 Background

In this section we first discuss different types of diverse cognitive abilities, and then the authentication mechanisms that we consider in our study.

2.1 Diverse Cognitive Abilities

In this study, we have taken into consideration users with different disorders as described in [14]. Each group includes users with diverse cognitive abilities to ensure

the anonymity of those who filled out the questionnaire. We describe these groups below and summarize them in Table 1.

Difficulty recognising characters. This difficulty impacts an individual's capacity to recognize, differentiate, or recall certain symbols, such as letters, numbers, or other visual cues. It is often linked to learning disorders encompassing impairments in reading, writing, and/or processing mathematical operations [15]. Examples include *dyslexia*, a learning disorder affecting 20% of the population, characterized by challenges in language acquisition and processing, particularly in reading and writing skills. Individuals with dyslexia may exhibit short-term memory issues but often possess a strong sense of visualization, creativity, lateral thinking, and spatial awareness [16]. Another instance is *dysgraphia*, manifesting in difficulties with handwriting, punctuation, grammar, and spelling, while *dyscalculia* involves challenges related to acquiring mathematical skills, such as recognising numbers or symbols, performing calculations, or applying problem-solving techniques [15].

Persons with *Down syndrome (DS)*, a chromosomal disorder involving an extra copy of chromosome 21, may also encounter difficulties in recognising characters. In some cases, individuals with DS may experience compromised abilities in math comprehension, visual comprehension, problem-solving, memory, reading, linguistics, and speech understanding [17]. Generally, those facing character recognition issues may encounter hurdles in activities like reading, writing, and using technology that demands visual text processing, such as typing or web browsing. Hence, they may benefit from assistive technologies like audiobooks, screen readers, or speech recognition software to overcome these challenges.

Difficulty remembering information. Difficulty remembering information occurs when an individual struggles to recall information, past events, or details [18]. This challenge may manifest in various ways, such as, e.g., forgetting important dates, or having difficulty recalling previously learned information. It can be attributed to various factors, including neurological disorders, traumatic brain injuries, psychological stress, and more. This condition can significantly impact an individual's daily life, social interactions, and cognitive abilities. It is often associated to *amnesia* and *Wernicke-Korsakoff syndrome*. Depending on the underlying cause, addressing difficulty remembering information may involve memory exercises, lifestyle adjustments, or medical interventions to enhance overall well-being.

Attention deficit disorders *Attention-deficit/hyperactivity disorder (ADHD)* is a neurodevelopmental disorder that typically begins in childhood and may persist into adulthood [19]. Symptoms of ADHD are categorized into two main groups: inattention and hyperactivity/impulsivity. Individuals with ADHD must exhibit symptoms from either or both of these groups.

Common symptoms of ADHD include difficulty sustaining attention or completing tasks, forgetfulness, frequent mistakes or careless errors, fidgeting or restlessness, and organizational challenges. These symptoms can present difficulties in various aspects of life, including school, work, and social situations.

Pervasive developmental disorders. Pervasive developmental disorder is a broad term encompassing conditions that impact communication, social interaction, and behavior. Typically diagnosed in early childhood, it includes disorders such as *Autism Spectrum Disorder (ASD)*, *Asperger's syndrome*, and *Rett syndrome* [19]. Individuals with ASD exhibit diverse characteristics, often displaying limited social communication and interaction, along with repetitive patterns of behavior, interests, or activities [19]. While impairments in social communication are commonly associated with linguistic delays, individuals with ASD frequently possess strong visual skills and engage in visual thinking, expressing concepts through mental images [20]. They may also experience limited attention and sensory processing disorders, affecting their ability to process information from the five senses. Those with Asperger's Syndrome may struggle with interpreting emotions, thoughts, and body language, although they typically do not experience significant delays in language development and often have above-average or average intelligence [21]. Similarly to ASD, Rett syndrome symptoms may include language loss and coordination impairments, along with repetitive movements. Thus, for both disorders, understanding complex sequences of instructions or memorizing complicated sequences can be challenging.

Table 1 Families of disorders, and the corresponding diverse cognitive abilities

Families of disorders	Diverse cognitive abilities
Difficulty recognising characters (DRC)	Dyslexia, dyscalculia, dysgraphia, Down syndrome, etc
Difficulty remembering information (DRI)	Amnesia, Wernicke-Korsakoff syndrome, etc
Attention deficit disorder (ADD)	ADHD, etc
Pervasive developmental disorder (PDD)	Autistic disorder, Asperger's disorder, Rett syndrome, etc

2.2 Authentication methods

We will now recall some widely used authentication methods, focusing on those discussed in the following sections. Our classification, inspired by the classical approach outlined in [22], includes: i) *Something you know*: This involves checking the user's knowledge of a secret, such as a password, Personal Identification Number (PIN), passphrase, or cryptographic key; ii) *Something you possess*: This verifies the user's possession of a specific device, like a One Time Password (OTP) generator, ATM card, credit card, smartcard, or USB crypto-token; iii) *Something inherent*: This checks biometric features like fingerprints, voice or face recognition, retinal patterns, or a paper signature.

Additionally, systems often incorporate mechanisms to differentiate between humans and robots. Graphical CAPTCHAs, for instance, serve this purpose during the authentication phase.

Let us delve into the details of these authentication methods. While some involve a single step, others are more complex and fall under the category of *Multi-Factor Authentication* (MFA). MFA techniques require users to authenticate themselves using two or more proofs of identity (e.g., a password combined with an OTP or a biometric pattern). In this paper, we will focus on the single-step authentication methods.

2.2.1 Something you know

A **password** is a sequence of characters used, along with a username, to authenticate a user's identity. Passwords are intended to be known exclusively by the user, granting access to devices, applications, or websites. In order to use a password a user first needs to create it, and then to remember it. In the password creation phase, well implemented systems enforce different password policies in order to ensure them to be strong. Typically, the request is to generate long passwords (at least 8/10 characters), containing different types of characters, including uppercase letters, lowercase letters, numbers and characters, and not containing any personal information, and any common word. These types of passwords are **alphanumeric passwords**. Passwords that are randomly generated strings, composed of a mixture of numbers, special characters and both uppercase and lowercase letters are stronger, but harder to remember and thus not so usable. On the other hand, a **mnemonic password** is created by using a memorable phrase, sentence or a combination of words that are easy to remember, and using a character (often the first letter) to represent each word in the phrase. For example, a mnemonic password might be "My first car was a red Toyota Camry" which could be shortened to "MfcwarTC". Mnemonic passwords are often used by individuals have trouble remembering complex alphanumeric passwords, or who prefer a more creative approach to password creation.

A **passphrase** is a password composed of a sequence of different words that make up a phrase or sentence, a **passcode** is a password composed of digits, and a **personal identification number (PIN)** is a short password composed of digits, usually associated with a specific device. A password extension is the **Single sign-on** that allows a user to log into multiple applications and corporate domains using a single set of username and password credentials, thus eliminating the need for multiple passwords.

2.2.2 Something you possess

A **One-Time Password (OTP)** is a string of characters or numbers that a user can use to authenticate for a single login attempt or transaction. It has two fundamental properties: it cannot be reused and expires quickly. A unique value is generated for each one-time password, containing some contextual information like, e.g., time-based data or previous login events. The benefits of using it are: reduced risk when passwords are compromised and resistance to attacks (e.g., replay attacks that assume the reuse of the same intercepted information), difficulty to be guessed (algorithms that generate OTPs often add some randomness), easy of adoption and integration into systems. There are also two types of OTPs: **hard tokens** (physical devices that transmit OTPs), and **soft tokens** (i.e., a push notification or a SMS message containing a code or a link that can be used only once and that must be entered or clicked by the user to prove its identity).

A **security token** is a small portable device that a user plugs into a system to grant access to a network service. Unlike a password, a security token is a physical object that may be in the form of a smart card or may be embedded in a commonly used object such as a key fob which is practical and easy to carry, and thus, easy for the user to protect. Even if the key fob falls into the wrong hands, however, it cannot be used to gain access because the PIN (which only the rightful user knows) is also needed.

2.2.3 Something inherent

Biometric is related to the measurement and analysis of person's unique physical and behavioral characteristics, called biometric traits. It is based on the ratio that every person can be accurately identified by its intrinsic physical or behavioral traits such as fingerprints, voice and face recognition, retinal patterns, paper signature. These traits cannot be forgotten or stolen, and are difficult to counterfeit [23]. There are two types of biometric authentication system approach: classical and Machine Learning (ML) based [23]. Classical biometric authentication assumes that in the *enrollment phase* the image data are first acquired using cameras or optical,

thermal and pressure sensors, and then a mathematical representation of them, called *biometric feature* containing unique patterns, is stored as a template in a secure database for future identification or verification. In the feature extraction phase image enhancement techniques may be applied in case the captured images are of poor quality. During the *authentication phase* a user is identified and verified. The verification consists in checking if a new acquired biometric data belongs to the claimed person by comparing it with the information related to a set of individuals. This is done using pattern-matching algorithms that produce a matching score. The user is accepted if the matching score between the acquired biometric data and the corresponding stored one exceeds a decided threshold. On the other hand, biometric machine learning (ML) approaches are based on machine learning algorithms that analyze biometric data to find correlations between biometric characteristics and a person's identity. Biometric systems require a large amount of training data to work effectively, but may be able to recognize more complex biometric patterns and characteristics than classic biometrics systems. In particular, Deep Learning (DL) techniques, which are a specific ML approach based on neural nets composed of many layers, have been shown to provide reliable authentication models. They can learn the biometric feature representation and at the same time perform classification/regression. This is achieved using multi-layer neural networks, called Deep Neural Networks (DNN). At each layer of the DNN different biometric features are learned, increasing the level of abstraction and the pattern complexity with respect also to classical models. This approach is better suited to uncover underlying patterns of the data, and has been widely used in the last years.

All of these approaches, summarized in Table 2, are used very often, but not all of them have been tested in the literature with users with cognitive disabilities (e.g., passcodes and single sign-on). Moreover, they can be very challenging from different points of view. First, a user is asked to generate something (a password, a voice message, etc.), and this may be a challenging cognitive task. Then, at the authentication time, some techniques may require only one step of authentication, others more than one. A typical scenario is a Two Factor authentication method that first requires the insertion of a password and then of an OTP, thus doubling the cognitive effort of the user.

Table 2 Classification of the different considered authentication methods

Classification	Name
Something you know (knowledge)	Password
	Passphrase
	Passcode
	PIN
	Single sign-on
Something you posses	OTP
	Security token
Something inherent	Biometric (fingerprint, voice, face, iris, signature, etc.)

2.3 CAPTCHAs

In addition to the various authentication methods mentioned above, systems to complete the process often also require users to recognize a *Completely Automated Public Turing test to tell Computers and Humans Apart* (CAPTCHA), i.e., a program that distinguishes a human user from a robot. There are different types of CAPTCHAs, such as: text based, image based, audio based, video based, puzzle based [24]. Text-based CAPTCHAs consist of a sequence of letters and digits that are changed by adding noise, are scattered, rotated, or in a 3D shape to prevent bot programs from reading the file real characters. Image-based CAPTCHAs require a user to recognize a specific image from similar images sometimes mixed with words (e.g., hand lettering, etc.). Audio-based CAPTCHAs require a user to listen to a voice message and type it again. Video-based CAPTCHAs require a user to watch a video and then answer specific questions. Puzzle-based CAPTCHAs assume that the user solves a riddle by introducing blocks of an image and asking the user to combine them or to identify a specific part of the image. Finally, math-based CAPTCHAs assume that the user solves a math problem, such as, for example, product or sum of two numbers.

3 A review of accessible authentication methods for users with diverse cognitive abilities

We initially conducted a literature review with a specific focus on the challenges that individuals with cognitive disabilities might encounter when using authentication systems.

We have thoroughly analyzed the frameworks and empirical studies published in the fields of Cybersecurity, Human-Computer Interaction Psychology, Information Security. Despite our efforts, it was not easy to find papers regarding cognitive disabilities and the use of authentication systems, given that existing studies of user perceptions of authentication schemes have relied primarily on users without cognitive disabilities (see, e.g., [25]). We have synthesized the knowledge extracted from the articles reviewed, summarizing the findings and identifying avenues for future research. During this stage, we were able to derive a set of guidelines and lay the groundwork for the subsequent validation phase, which was carried

out by actual users (as described in the next sections). Here, we outline the various steps involved in the literature review process.

3.1 Papers selection

We divided the literature review selection process in three phases: (1) We selected the most widely used authentication schemes and using specialized databases or reliable sources and relevant keywords, we have searched academic papers or previous research on accessible authentication schemes; (2) we applied predefined eligibility criteria to filter and extract initial search results, selecting only the relevant elements for the evaluation. These criteria included the language of the articles, the date of publication, research methodology or any other relevant factor; (3) we made the final selection of appropriate works on the basis of the results of the previous phases. This selection process involved careful evaluation of the selected items and determination of their suitability for the assessment of authentication schemes.

3.1.1 Phase 1: Search strategy and database selection

For our research we extracted relevant papers using search engines (e.g., Google) and scientific research platforms such as ACM Digital Library, IEEE Xplore and SpringerLink. The selection criteria for these articles was related to the topic of accessible authentication, Web accessibility, cognitive disabilities, biometrics, and usability.

Initially, we used some keywords such as: authentication, accessibility, disabilities, guidelines to search inside the chosen engines and scientific research platforms. We then refined the keywords ending with the following string: (Accessibilit* OR Disabilit* OR ADHD OR dyslexia OR autism OR “down syndrome") AND (passwords OR authentication OR “authentication method" OR Biometrics OR CAPTCHA). Since the search string returned many results we proceeded with the elimination of unnecessary resources by moving on to Phase 2.

3.1.2 Phase 2: Selection criteria

To uphold the relevance and precision of our literature review, we implemented clearly defined inclusion and exclusion criteria throughout the selection process. These criteria were meticulously formulated to encompass research works directly addressing the intersection of disability and accessibility, deliberately excluding studies that did not align with our specific research question.

Firstly, we carefully defined the following inclusion criteria: (1) only papers published in peer-reviewed journals or conferences; (2) the research had to focus on accessible authentication methods for individuals with different types of cognitive disabilities (difficulty recognising characters, difficulty remembering events, attention deficit disorders, pervasive developmental disorders); (3) empirical research, such as user studies or evaluations; (4) studies written in English and published up to 2022 (i.e., before the beginning of the empirical study). As exclusion criteria we removed: (1) non-peer-reviewed papers, abstracts or white papers; (2) studies not related to accessible authentication methods; (3) studies focusing on accessible authentication methods for users without cognitive disabilities; (4) studies with weak methodologies or insufficient details; and (5) duplicate studies. Table 3 provides a summary of the inclusion and exclusion criteria.

3.1.3 Phase 3: Final papers selection

We collected relevant papers and sources for our research subjecting them to a screening process based on abstracts, titles, and keywords. A thorough examination of the full texts led to the selection of 111 items, comprising both papers and websites. From this pool, 31 items were specifically chosen for the literature review, as they proved instrumental in critically analyzing the research questions. The remaining items were deemed more suitable for offering a comprehensive overview of the topic. Within the scrutiny

Table 3 Selection criteria

Inclusion Criteria	Exclusion Criteria
Papers published in peer-reviewed journals or conferences	Non-peer-reviewed sources
Research on accessible authentication methods for individuals with cognitive disabilities	Studies not related to accessible authentication methods
Empirical research, such as user studies or evaluations	Studies focusing on accessible authentication methods for users without cognitive disabilities
Studies published up to 2022	Studies with weak methodologies or insufficient details
Studies written in English	Duplicate publications

Table 4 Number of resulting papers for each phase of the literature review

Main Databases	Amount of papers		
	Phase 1	Phase 2	Phase 3
ACM Digital Library	7.545	823	29
SpringerLink	4.174	146	8
IEEE Xplore	291	80	2
Total	12.010	1.118	39

of these 31 papers, an examination of their references led us to uncover an additional 8 pertinent studies. In total, we scrutinized 39 sources that contributed valuable information. The distribution of papers extracted in each phase is depicted in Table 4.

3.2 Papers Analysis

In this section, we delve into the literature extracted during the selection phase and outlined in Sect. 3.1. In the analysis phase we have distilled the insights from the reviewed articles, summarized the key findings, and identified potential areas for future research. This involved assessing key concepts, relevance to the topic, major trends, differences and similarities.

Numerous studies emphasize the general challenges faced by individuals with diverse cognitive abilities when interacting with computers. For instance, [26] revealed difficulties these users have with keyboard inputs, especially character keys, and recommended exploring voice applications and image-based searches as alternatives. However, studies like this one are very general and not focused on authentication approaches tailored for users with varying cognitive abilities, as our work and the studies described below are.

We now analyze different studies that examine authentication approaches for users with diverse cognitive abilities, focusing first on password and PIN authentication, then progressing to one-time passwords (OTPs), biometric methods, and finally exploring the use of CAPTCHAs. Table 8 and 9 in the Appendix associates for each diverse cognitive ability, and each authentication approach (described in the following sections) the difficulties encountered by users following the division described in Table 1.

3.2.1 Passwords, passphrases, PINs, and accessibility

The creation and use of passwords demand various skills, including attention, creativity, problem-solving, and decision-making. This complexity poses challenges for users with diverse cognitive abilities [27].

Our exploration begins with users facing difficulty recognising characters, followed by those with difficulty remembering information, then by those with attention deficit disorders, and finally by those with pervasive development disorders. We discuss critical points explored in the papers and proposed solutions.

Users with difficulty recognising characters. Numerous studies examining password usage incorporate participants with dyslexia [16, 28]. Challenges faced by these users include difficulties in creating, storing, and entering passwords due to their sequential processing issues and challenges in correct spelling [16, 29]. While general spelling issues can be mitigated with tools like the spell checker proposed in [16], it is important to note that these tools cannot be directly applied to password spelling.

Helkala's study [28] not only addresses individuals with dyslexia but also those with Parkinson's disease, vision impairments, and physical disabilities. The research reveals that individuals with dyslexia encounter challenges in memorizing passwords, leading them to opt for simplistic, non-random passwords with fewer characters, diminishing their entropy and, consequently, compromising security. Additionally, difficulties in spelling may result in delays due to password typos. Conversely, individuals with dyscalculia may face issues with PINs and passwords containing numbers. Potential solutions include incorporating tactile passwords, eye-gaze methods, utilizing songs, and employing graphical passwords.

In [29] the authors investigate the impact of dyslexia on password use, shedding light on the challenges faced by these users. They also discuss the limitations of existing solutions for authentication methods and make some design recommendations. In particular, they suggest having a better understanding of this type of users and running tests with them, bearing in mind that "copying" information could help them. Furthermore, regarding authentication strategies, they recommend, whenever feasible, the adoption of password managers.

In [30] another study was carried out to analyze the challenges faced by individuals with dyslexia in the context of authentication methods. The findings indicate that these users encounter difficulties, particularly when a system mandates the use of "stronger" passwords, leading to frustration during the re-typing process. Conversely, there is a notable interest among users in the potential implementation of graphic, pictorial, and audio/musical "password" approaches.

In the study conducted by [31], the authors guided and observed the authentication processes of seven participants, each presenting distinct cognitive abilities among which also learning disabilities and dyslexia. Those with dyslexia encountered challenges in accurately repeating the spelling of the password, thus the authors emphasize how developers should acknowledge that the challenges faced by users with diverse cognitive abilities may diverge

from those encountered by typical users during system development.

In [32], a survey was conducted among individuals with Down Syndrome (DS), revealing challenges in using passwords, particularly when the system required lengthy ones (at least eight characters). The authors attributed the difficulty in remembering passwords to cognitive limitations and the challenge in entering passwords to physical limitations. To address these issues, the authors suggest the adoption of mnemonic phrases, deemed easier to recall, a proposition that holds benefits for typical users as well [33]. Similarly, in 2012, the authors of [34] investigated the usability of multi-touch tablet devices for individuals with DS. The study identified that children and young adults with DS encountered difficulties in remembering passwords, often relying on a third party for password entry. Notably, their challenges included difficulties in recalling the position of symbols and capital letters.

In [35], the authors conducted an authentication task test with users having Down Syndrome (DS). The study revealed that DS users are more prone to forgetting mnemonic phrases compared to alphanumeric and graphic passwords. This tendency may stem from the abstract nature of mnemonic phrases for this demographic.

In [36], participants (ten users with DS and twenty neurotypical individuals) with prior computer and web browsing experience were tasked with accessing an e-commerce site using an authentication system implementing three methods: traditional alphanumeric passwords, mnemonic passwords, and recognition-based graphic passwords. The study found no significant difference in registration time among the three authentication methods. Users exhibited a lower preference for graphical passwords compared to traditional alphanumeric and mnemonic passwords. Additionally, passwords created by individuals with DS demonstrated similar strength compared to those created by neurotypical individuals. However, users with DS required a longer time for logging into their accounts, although their performance improved with increased experience. In terms of errors, DS users frequently entered passwords with incorrect capitalization or missing characters, and due to the non-visibility of characters, identifying errors proved challenging for them.

Users with difficulty remembering information. In [37] the authors discuss the drawbacks of traditional authentication systems that rely on passwords and PINs. Through an evaluation involving a user group, half of whom faced challenges in remembering their bank's PIN, the authors advocate for the adoption of graphical authentication. This alternative not only enhances security but also addresses memorability issues by utilizing previously learned images. By substituting the need to recall alphanumeric codes with visually memorable images, graphical authentication leverages human visual memory capabilities.

Users with attention deficit disorder. Maintaining focus poses a challenge for individuals contending with attention deficit disorders, particularly when creating secure passwords for authentication. Insufficient attention during the registration process can lead to authentication difficulties in the future, particularly for those with attention-related issues. To enhance the user experience, the authors recommend promptly directing the user's attention to essential authentication elements. Login elements should be easily discernible, aiding users in initiating the authentication process. To mitigate distractions, authentication interfaces should minimize both physical and cognitive efforts required [19, 38].

Pervasive development disorder. In the aforementioned study [31], which involved users with different cognitive abilities, those with Asperger's syndrome struggled with awareness regarding incorrectly entered credentials, highlighting the need for alternative authentication approaches.

3.2.2 One-Time Passwords and accessibility

Users with difficulty recognising characters. Limited research exists on the use of One-Time Passwords (OTPs) by users with diverse cognitive abilities. In [28], the authors suggest the adoption of OTPs generated by a device or received via phone. However, they assert that OTPs may have excessively long transaction times for individuals with disabilities. Due to the temporary nature of the codes, users with disabilities may face challenges in using them effectively. Moreover, individuals with dyslexia may encounter difficulties in reading and reproducing OTPs. Similar issues are highlighted in [39].

3.2.3 Biometrics and Accessibility

Users with difficulty recognising characters. The study [40] presents an evaluation test that demonstrates positive feedback from disabled users with cognitive or learning difficulties regarding the use of biometric systems. The appeal lies in their avoidance of the need for memorizing codes or patterns, addressing instances where users forgot PINs during test executions. The analysis further underscores the significance of minimizing interactions with the system, as excessive interactions tend to induce confusion and frustration.

Users with difficulty remembering information. In [41], the authors highlight the superior performance of biometric authentication over standard password authentication, particularly when using fingerprint scans or voice recognition tools among individuals with memory impairments. Biometric approaches eliminate the need for users to

remember passwords, decipher words or symbols, or engage in puzzle-solving or mathematical tasks.

3.2.4 CAPTCHAs and Accessibility

CAPTCHAs pose diverse challenges for users with disabilities. Individuals with dyscalculia may struggle with CAPTCHAs involving mathematical operations, while those with learning disabilities may face difficulties solving CAPTCHA puzzles or comprehending Google's graphical CAPTCHA requests (reCAPTCHA) [42]. Moreover, audio CAPTCHAs impose a cognitive overload to all users in comparison to the cognitive load necessary to understand normal human speech [43, 44]. In all these cases the risk is that users will be frustrated and soon get bored of navigating into the system.

3.3 Existing Accessibility Guidelines for Authentication

Ensuring that websites and applications are accessible to everyone is of utmost importance, achievable through correct design and coding. However, despite the potential for accessibility, many websites and tools still present barriers, effectively excluding individuals with disabilities from accessing their content and, consequently, the products and services offered online. This challenge extends not only to persons with various disabilities, including physical, neurological, visual, and cognitive impairments but also to older individuals with age-related limitations. Additionally, it impacts those using different devices or facing slower internet connections.

To avoid the barriers of the Web, different guidelines have been developed. Very general guidelines are the Web Content Accessibility Guidelines (WCAG) proposed by the World Wide Web Consortium (W3C) [11].

The focus of this work is on diverse cognitive abilities, and the W3C has also done some work in this direction with the W3C: Cognitive and Learning Disabilities Accessibility Task Force (W3C-COGA) [12]. The W3C Cognitive Accessibility Task Force has indicated how to make content usable for persons with diverse cognitive and learning abilities and has also proposed some design rules to help developers when designing Web pages and applications. Other guidelines for more specific cognitive disabilities are, e.g., [45, 46]. All these guidelines obviously apply.

For what concerns accessibility of authentication methods, few specific indications have been provided by the W3C [47]. The basic ratio is that users with diverse cognitive abilities often struggle to remember a password or solving a puzzle thus, alternative solutions should consider, and should follow, e.g., these rules:

- The use of a password manager;
- The possibility of allowing browsers to fill the login and password fields automatically;
- The possibility to do copy-and-paste;
- CAPTCHAs should not require you to remember previously seen words or images.

Additional guidelines for accessible authentication for user with diverse cognitive abilities have been provided. In [29, 48] the authors claim that for individuals with difficulty recognising characters, such as those with dyslexia or visual impairments, the authentication system should provide options for adjusting the user interface's font type, size, and color contrast. The system should also propose alternative authentication methods, such as voice recognition or biometrics, to reduce the reliance on traditional character-based inputs. Moreover, audio prompts or text-to-speech technology could provide auditory feedback to supplement visual instructions. In cases in which character recognition is necessary, the system should also incorporate features such as predictive text or auto-complete to help reduce spelling errors and to increase accuracy. Additionally, clear and concise instructions should be provided to minimize confusion and ensure successful authentication. In [49, 50], the authors state that for persons with memory difficulties, the authentication system could include biometric approaches and password recovery options such as security questions based on personalized or memorable data information. In [51–53] the authors claim that persons with attention disorders or hyperactivity may have difficulty focusing for extended periods of time. By incorporating a time limit for the authentication task to complete, the system can help ensure that the process remains engaging and does not require extended attention spans, preventing users from fatigue or loss of interest, and leading to better compliance and completion rates. More interaction can also maintain engagement, limit distractions, or limit boredom, so authentication systems could be designed to prompt you click buttons, drag objects or respond to prompts. Finally, authentication systems could incorporate gamification techniques, such as challenges, rewards, levels, or badges, to make the process more pleasant and stimulating. In [54–56] the authors state that for individuals with pervasive developmental disorders, such as ASD, the authentication system could be designed with specific considerations for sensory and cognitive processing differences. For example, the system could offer options for adjusting the user interface's brightness, color, or font size to accommodate sensory sensitivities. It could also use clear and concise language and avoid figurative language or metaphors that may be difficult for them to interpret. Furthermore, the system could allow for alternative input methods, such as voice recognition or touchscreen interfaces, for individuals who struggle with traditional keyboard and mouse

inputs. It may also be beneficial to provide visual aids, such as diagrams or videos, to supplement written instructions.

Other guidelines that consider, in general, persons with diverse cognitive abilities are the following: [52, 53, 57] propose to use alternative authentication methods to the password; [52, 53] suggest to provide for longer times when multi-factor authentication is required, to provide alternatives to CAPTCHAs as persons with different cognitive abilities may not be able to interpret them; Seville et al. [57] emphasize the importance of properly explaining all the steps required to gain access to a system, and allowing you to filter and simplify the content. In [58], the authors propose guidelines for the development of accessible authentication systems. They suggest the use of simple language, avoiding expressing complex or technical ideas, to provide clear and unique automated error messages. Finally, as suggested by [59], a good practice regarding the use of biometrics for authentication is to offer a number of alternatives so that the user can decide which biometric authentication system to use.

3.4 Accessibility Frameworks and Tools

Some works have focused on possible conceptual frameworks and tools that help users with different cognitive abilities navigate the Web by making pages more accessible. These works are not directly related to authentication systems but could still help users in the authentication phase as they simplify navigation and improve the readability of Web pages.

In [60] the authors present a conceptual framework that gives the possibility to analyze some Web pages. The analysis is divided into various phases from the planning process to the testing phase. Several guidelines are given and include that a Web page should be simple, multimodal, delay tolerant, and attention focused. The authors claim that following all these principles is not always an easy task, even for developers, and adhering to accessibility guidelines may not prevent some types of accessibility barriers, therefore, several efforts still need to be made in this direction.

Some tools have also been proposed to simplify navigation for users with cognitive disabilities, in particular with dyslexia. In [61] the authors propose a customization toolbar called Firefixia, designed for persons with dyslexia. The tools allow the user to adapt the presentation of Web content according to their preferences by changing the text size, text alignment and link colors. In [62] the authors introduce a browser extension to help persons with dyslexia navigate the Web by offering customization features such as the ability to change font size, font type, remove text decoration, change foreground and background colors, spacing, etc. From the preliminary evaluations, the feedback has been very positive and users have said that they were able to read the pages more easily.

3.5 Accessibility Guidelines for Users with Diverse Cognitive Abilities

In this section we put together all the various guidelines and recommendations extracted from the literature review of the papers presented in Sect. 3.2, from the existing accessibility guidelines of Sect. 3.3, and from the information extracted from the tools of Sect. 3.4, and we present in Table 5 the comprehensive guidelines that we endorse. These guidelines, in our view, should serve as the foundation for creating an accessible authentication environment. In Sect. 6, we will delve deeper into the guidelines that received affirmation from users who participated in our questionnaire. The guidelines are categorized into four main areas: graphical layout (G1-G2), language (L1-L3), structure (N1-N6), and navigation (U1-U9).

4 Methodology

In the preceding section, we delved into an analysis of the challenges faced by users with diverse cognitive abilities during the authentication process. The primary objective of this study is to gain a deeper understanding of how various cognitive abilities impact the utilization of different authentication methods. Our approach involves conducting a comprehensive study with diverse user groups to validate findings from the literature review, identify key challenges, and gather valuable feedback and suggestions for enhancing the overall authentication experience. In pursuit of this objective, we opted to design a fully anonymous questionnaire aimed at exploring the various ways in which users with diverse cognitive abilities interact with different authentication methods. Ensuring complete anonymity, we refrained from requesting personal information, and we categorized users based on the general cognitive disabilities outlined in Sect. 2.1 and summarized in Table 1.

The questionnaire was crafted in Italian, assuming that all participants were either native Italian speakers or possessed a basic understanding of the language. We employed two primary channels for disseminating the questionnaire: firstly, through pages and groups on major social networks catering to individuals with diverse cognitive abilities, and secondly, via selected associations dedicated to supporting this demographic. Despite challenges in reaching potential participants, including some associations opting not to participate and some users experiencing difficulties with computers or authentication systems, we gathered 34 responses.

Measures. To collect data, we used an online questionnaire. Most of the questions were measured by means of 3

Table 5 Authentication accessibility guidelines

Accessibility guidelines	
G1	Provide options for adjusting font type, size, brightness and color contrast [29, 48, 54–56]
G2	Add visual aid [26, 28, 30, 54–56]
L1	Use a simple and clear language [47, 54–56, 58]
L2	Explain well all the different authentication steps [57]
L3	Provide clear error messages [58]
N1	Allow the use of a password manager [29, 47]
N2	Allow browsers to fill the login and passwords fields automatically [47]
N3	Provide alternatives to CAPTCHAs [47, 52, 53]
N4	Provide a longer response time [52, 53]
N5	Allow to filter the page content to simplify it [57]
N6	Allow to do copy-and-paste [29, 47]
U1	Allow for alternative input methods, such as voice recognition or touchscreen user interfaces [6, 63]
U2	Propose the use of alternative authentication methods [37]
U3	Add gamification techniques to maintain user engagement [51–53]
U4	Do not require to remember previously seen words or images to understand CAPTCHAs [47]
U5	Allow third party authentication [64]
U6	Allow password recovery options such as security questions [31, 49, 50]
U7	Allow the use of the WebAuthn API [64]
U8	Allow the use of biometric authentication [29, 40, 41, 48–50]
U9	Offer alternatives between biometric systems to use (fingerprint, facial recognition, etc.)[59]

options (yes, no, I don't know). There were no open-ended questions. The study was conducted only once, so no new measurements were taken over time.

Ethics. We paid particular attention to protecting the rights of participants in the questionnaire and respecting fundamental ethical principles. On the first page of

Table 6 Questions content divided into three categories

Group	Description
Knowledge	Has the user ever used the required type of authentication?
Behavior	How does the user relate to the proposed authentication system?
Difficulty	Did the user experience any difficulties in using the proposed authentication system?

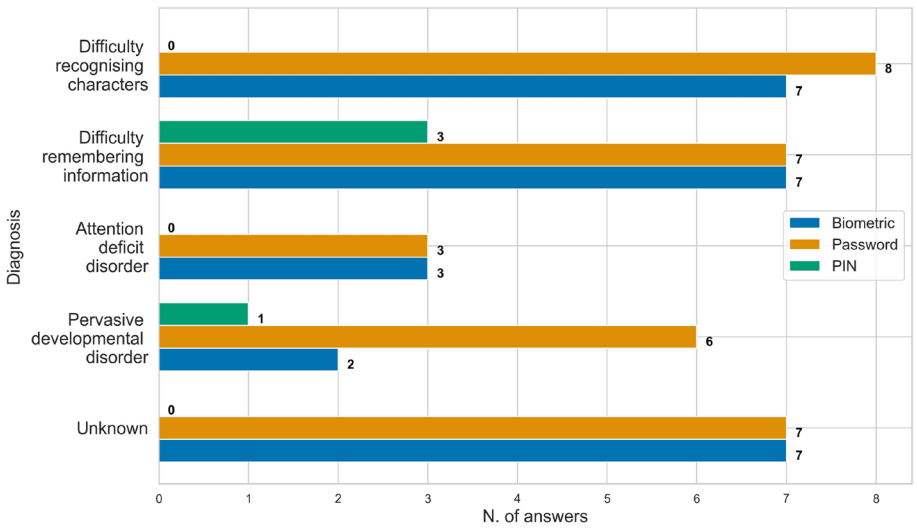


Fig. 1 Knowledge of biometrics (26 users), passwords (31 users), and PIN (6 users) divided by disability

the questionnaire, we provided clear and understandable information to the participants regarding the purpose of the research, participant rights, and the methods of participation. Additionally, the first question of the questionnaire explicitly asked to agree to participate, thus we obtained voluntary and informed consent. To ensure that the questionnaire was accessible to all participants with diverse cognitive abilities, we used simple and clear language, with the addition of images to facilitate the understanding of the questions. We also adapted the duration of the questionnaire based on the participant's abilities, i.e., without posing a time limit. Finally, we ensured the confidentiality and protection of the collected data, using a secure and protected system for data collection and management (in a private Google account not accessible from outside). We did not collect sensitive data, we did not explicitly ask for the type of disability, and none of the questions were mandatory. We indicated to users that search results would only be used for scientific purposes and would be treated with the utmost confidentiality and protection. In conclusion, we did our best to ensure that our questionnaire respected fundamental ethical principles and that its filling could be carried out in a comfortable and accessible way for all participants.

Questionnaire. The questionnaire was crafted using the user-friendly Google Forms platform, allowing respondents to easily access it through their browsers. This feature offered users the flexibility to adjust font sizes and change other settings via browser extensions on their personal computers. As the questionnaire was completed online, we were not physically present during the process, and it is unknown whether someone helped the users answer the questions, though we explicitly asked for independent replies.

Questionnaire content. The questionnaire comprised 14 sections, each containing three to four questions, for a total of 27 multiple-choice questions. The macro-categories of the sections of the questionnaire were:

- **Information**: Questions identified survey population characteristics, including age, gender, diagnosed family of disability;
- **PIN**: Participants were asked about their use of PINs and any difficulties they encountered;
- **Passwords**: This section was similar to the PIN section and focused on password creation, management, and security preferences. We were interested in understanding participants' opinions on the criteria they considered important when choosing passwords, such as ease of recall or security. We wanted to know how often participants reused passwords and the strategies they used to modify them. Additionally, we were curious to learn if participants used password manager applications and

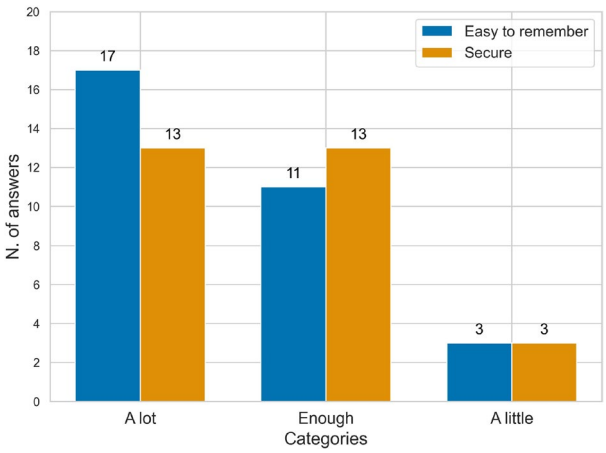


Fig. 3 Comparison of security and ease of passwords: 30 participants answered, multiple answers were allowed

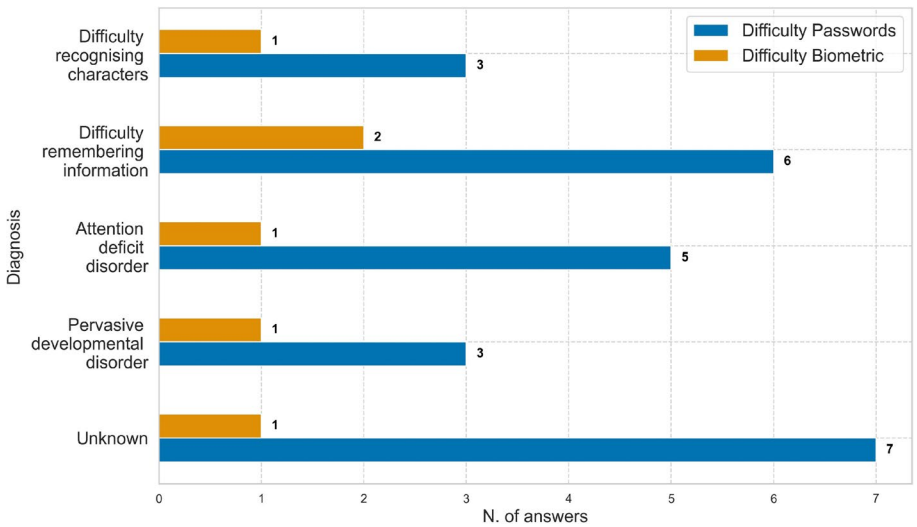


Fig. 2 Difficulties in understanding and using passwords (20 users), biometric authentication (25 users) multiple answers allowed

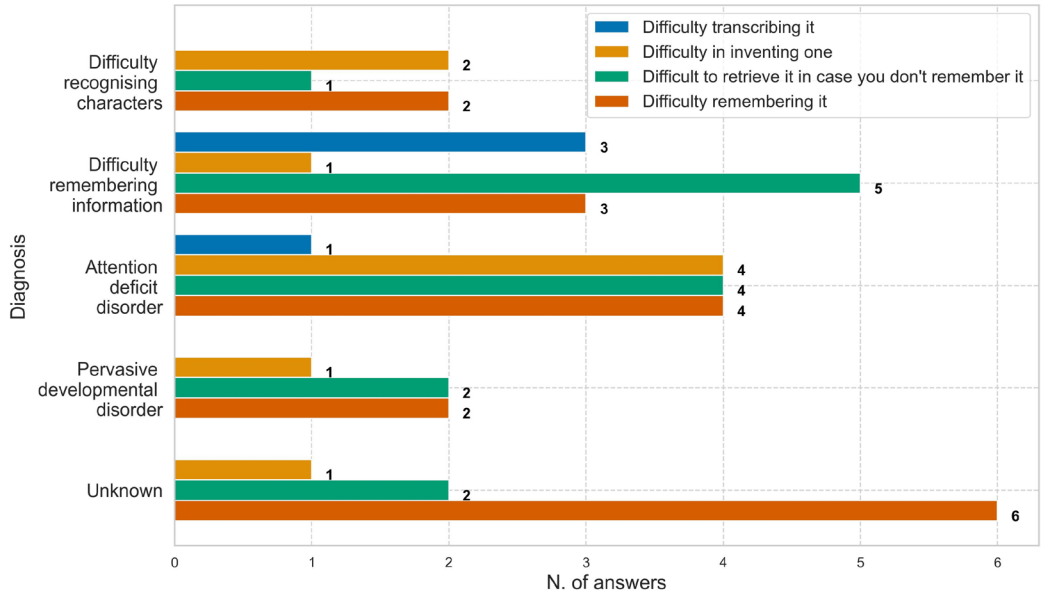


Fig. 4 Passwords difficulties divided by diagnosis: 20 participants answered, multiple answers were allowed

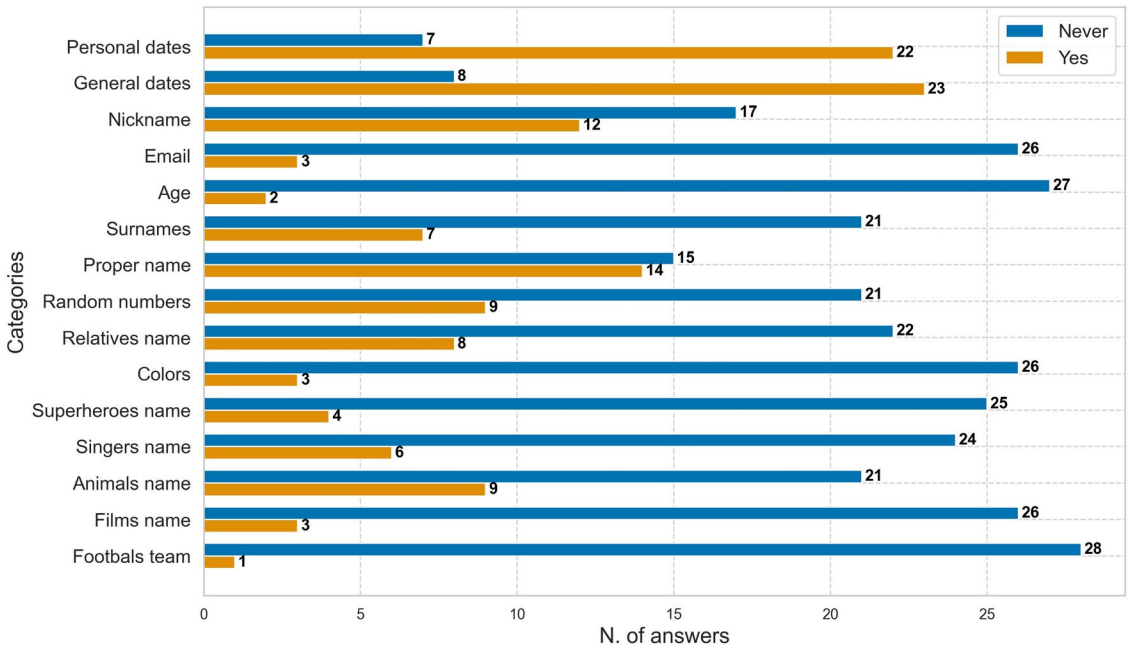


Fig. 5 Categories of words included in passwords: 33 participants answered, multiple answers were allowed

what benefits they perceived from using them. Finally, we explored the patterns participants preferred when creating passwords, such as including uppercase letters, numbers, or symbols;

- **CAPTCHA**: Participants' experiences with and difficulties encountered when interacting with different types of CAPTCHA systems;
- **Biometrics**: We investigated how participants use biometric authentication methods and the eventual challenges they face;
- **Frequently used websites and apps**: we asked to the participants which were the websites and apps they used most frequently, how clear the content was, and the encountered difficulties with website content.

Notice that, for each authentication method, we asked questions that could be analyzed in aggregate form using three categories: knowledge, behavior, and difficulty. Table 6 shows the three groups and their description. In Appendix A, we report in detail the questions of the questionnaire, with the relative proposed answers and the percentages of the answers given.

5 Results

In this section we discuss the results of our questionnaire.

5.1 Participants

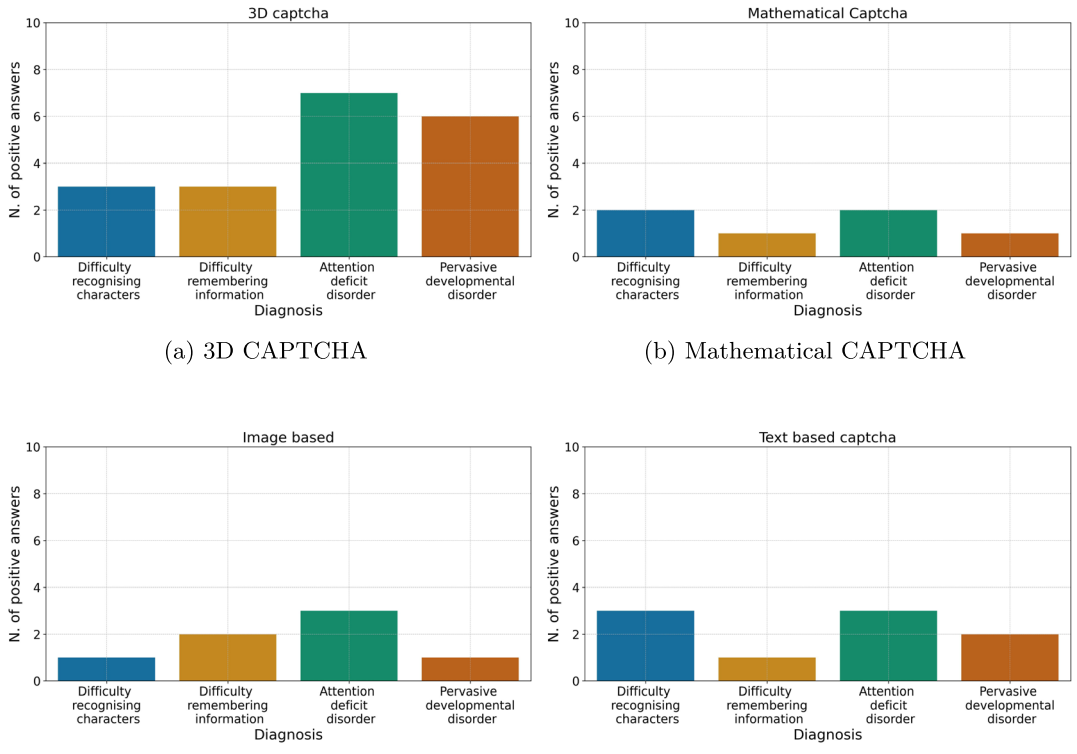
A total of 34 adult participants answered to the questionnaire. All participants were over 18 years old and most were able to use computers on their own. The majority of users were male (Male=17, Female=15, Neutral=1, No answer=1) between the age of 18 and 27. We asked in the most general possible way (to support privacy) what was their certified diagnosis, and most of the participants declared pervasive development disorder ($N = 12$). In fact, a large percentage of users were unaware of their diagnosis ($N = 9$), and that 14.71% of the users had more than one diagnosis. The severity levels of the diagnosis received nearly the same response rate, and most were moderate or mild. Even in this case the answers could be multiple if a user had more than one diagnosis, with a different level of severity. Those who have difficulty recognising characters, and those with attention disorder had a higher severity of the diagnosis than the other groups. Thus, we would expect these two groups to have more difficulty using authentication systems.

5.2 Data analysis

We used Python scripts written by us to analyze data from a Google Forms questionnaire. Our aim was to determine if there were any significant differences in the ratings of the authentication methods used by the participants.

Based on our initial analysis, passwords were found to be the most commonly known and used method ($M = 6.20$, $SD = 1.72$), with biometrics ranking as the second one ($M = 5.20$, $SD = 2.23$), see Fig. 1.

Additionally, our analysis showed that passwords were considered the most difficult ones ($M = 4.80$, $SD = 1.78$),



(a) 3D CAPTCHA

(b) Mathematical CAPTCHA

(c) Image based CAPTCHA

(d) Text based CAPTCHA

Fig. 6 Difficulties with CAPTCHAs divided by diagnosis

while biometric systems were considered the easiest ($M = 1.20$, $SD = 0.45$). We conducted a *binary linear regression analysis* to see if there were significant differences in the difficulty of using passwords and biometric authentication systems for each group of diagnosis. Despite the lack of statistical significance, a trend can be observed, in fact Fig. 2 reveals that individuals with difficulty remembering information, recognising characters and letters, encounter more challenges when using passwords. When it comes to biometrics, there are minimal differences between the groups, and the overall percentage of difficulties is low. We provided participants the opportunity to articulate the challenges they encountered while using the biometric system. The majority of those who experienced difficulties cited initial comprehension barriers, often necessitating assistance from others, as the primary obstacle. Note that, while passwords are a more widely used system, that does not make them any easier for users to understand.

Moving forward with the analysis, we found that most survey participants prefer using a PIN over a password (66.7%). Those who use the PIN as an authentication method (50%) find it difficult to create, write it down and remember it so they tend to reuse the same PIN for different devices and authentication processes (88.3%).

Regarding passwords, it emerges from the questionnaire that 75% of users tend to reuse the same password and prefer passwords that are both secure and easy to remember (see Fig. 3). This is because they have fear of forgetting their passwords (see also Fig. 4). Moreover, 40% of the users find it annoying to click on "recover password" as it slows down the authentication process and increases difficulty.

We proposed a series of password patterns to analyse how these users tend to build them, and it emerged that the most commonly used pattern is the following one: uppercase, lowercase, numbers, and symbol. Moreover, users with diverse cognitive abilities choose important dates (anniversaries, birthdays, etc.), general dates (thus not closely related to particular events), and proper names as the most frequently used categories within passwords (see Fig. 5).

Also these types of patterns and contents make the password sensitive to attacks [65–67]. Moreover, more than 80% of the persons have never used a password manager, and a small number (3.2%) does not know if it has used it or not.

In our survey, 61.8% of participants reported using biometric authentication at least once. The majority (88%) found this type of authentication simple to use. We also asked participants about any difficulties they experienced while using the biometric system. Most respondents stated that they initially had trouble understanding what they needed to do but were able to use it after seeking help.

For the second part of the questionnaire, we aimed to investigate the usability and common issues encountered while using popular websites and applications. The results revealed that Instagram, YouTube, and Instant Messages were the most frequently used apps or websites. However, 20% of users found it challenging to figure out how to use them. Some respondents reported that the text was too small, and there was poor contrast (33.3%). Additionally, 66.7% of participants were unsure of what to do while using these applications.

Analysis of CAPTCHAs. Although CAPTCHAs are not authentication systems, they are often used as a second step after authentication. We wanted to investigate how they affect users, so we presented a selection of CAPTCHAs, and asked participants whether they had used any of them. Out of all participants, 52% reported having used at least one, while the remaining half either had no prior experience or found it difficult to use these types of CAPTCHAs.

We carried out descriptive analyses and estimated *binary logistic regression models* to assess the presence of associations between the diagnosis and the type of CAPTCHA. Although the results of the binary logistic regression were not statistically significant, the following graphs illustrate the trends observed in the data.

From Fig. 6 it can be seen that those who have difficulty with character recognition (i.e., letters, numbers, and symbols) show a higher probability of having difficulties in understanding mathematical and textual CAPTCHAs. For image-based CAPTCHAs, those diagnosed with attention deficit disorder and those who have difficulty remembering information experience more challenges. Finally, 3D CAPTCHAs are the most complicated to understand for all four categories. These findings suggest that 3D

Table 7 Security issues for users with diverse cognitive abilities

Cognitive problem	Possible related security issues
Short-term memory	Difficulty remembering passwords, PINs, temporary codes
Difficulty in data creation	Issues with the creation of security strings
Difficulty in the spelling process	Insertion of incorrect credentials
Attention and concentration difficulties	Insertion of incorrect credentials due to distractions
Nonlinear cognition	Incorrect execution of security sequences
Anxiety or stress	Errors inserting credential due to emotional factors
Analogy and abstraction difficulties	Difficulty using advanced authentication methods

CAPTCHAs pose the greatest challenge for users with various cognitive impairments.

6 Discussion

In this section we answer RQ1 *Do users with diverse cognitive abilities find different authentication systems accessible?* RQ2 *Which authentication approach do they find the easiest to use?* RQ3 *What do they think could improve the accessibility of existing authentication approaches?*

We consider the results derived from the literature review in Sect. 3, and the results of our questionnaire.

We are aware of the fact that our study has some limitations as 34 participants are too few to derive conclusive results. However, we are still confident of the fact that interesting insights could still be drawn from the received answers.

6.1 Accessibility and security of authentication approaches

We first consider the questions RQ1 *Do users with diverse cognitive abilities find different authentication systems accessible?*, and to RQ2 *Which authentication approach do they find the easiest to use?*. From analysis of all the works presented Sect. 3, and of the questionnaires presented in Sect. 4 different interesting issues emerged.

Accessibility of authentication approaches Our study highlights the challenges faced by users with diverse cognitive abilities when using standard authentication methods, such as alphanumeric passwords, PINs, or OTPs. Additionally, two-factor or multi-factor authentication introduces further complexity, requiring users to navigate multiple authentication steps. CAPTCHAs, particularly those with complex images or mathematical puzzles, also present significant difficulties.

We believe that the most promising solutions for users with diverse cognitive abilities involve Intelligent System approaches, particularly those utilizing biometric machine learning (ML) techniques. These techniques have seen widespread adoption in recent decades [23]. As noted in [41] and supported by preliminary empirical studies on users with cognitive or learning difficulties [40], biometric methods effectively address the limitations of traditional authentication approaches by eliminating the need to remember passwords, PINs, or OTPs, and avoiding the challenges of solving puzzles or mathematical problems. The results from our questionnaire, presented in Sect. 5.2, further reinforce the potential of biometric approaches, though additional empirical studies are needed to confirm their feasibility.

Security of authentication approaches. As outlined in Sect. 3.2 and echoed in existing literature (see, e.g., [28, 35, 36]), users with diverse cognitive abilities often opt for simple passwords to avoid memory challenges. Our questionnaire findings, discussed in Sect. 5.2, further support this trend, revealing that 75% of users who rely on passwords consistently reuse the same one. They prioritize creating passwords that are perceived as both reasonably secure and easy to remember. Unfortunately, this tendency leads many users to adopt standard password structures or incorporate easily guessable elements like important dates (anniversaries, birthdays) and general terms, making their passwords vulnerable to various attacks [65–67].

Additionally, Table 7 illustrates the security challenges users with diverse cognitive abilities may encounter with passwords and PINs. Consequently, the substitution of passwords with biometric approaches emerges as a viable strategy to mitigate these vulnerabilities and enhance overall system security.

Limitations of biometric approaches. While embracing the potential of biometric approaches, it is essential to acknowledge certain limitations [68–71]. The initial enrollment phase demands the collection of biometric data, and for systems utilizing biometric machine learning (ML) techniques, training becomes a pivotal step. However, this process can pose challenges for individuals with cognitive disabilities, who may encounter difficulties in comprehending instructions, communicating effectively, and providing accurate and reliable biometric data. Following instructions or maintaining stillness during data collection might prove challenging, resulting in low-quality data unsuitable for training ML systems.

Moreover, addressing the variability in biometric data among individuals with cognitive disabilities is a critical consideration. Unique facial features, for instance, may differ from those of typical individuals, complicating accurate recognition through facial recognition technology. Consequently, the training data must encompass a diverse range of individuals with cognitive disabilities to ensure the system's ability to accurately recognize a broad spectrum of biometric data.

Ethical and legal considerations are paramount when deploying biometric ML systems for individuals with cognitive disabilities. It is imperative to ensure their understanding of the purpose and implications of providing biometric data.

In summary, training biometric ML systems for individuals with cognitive disabilities demands meticulous attention to data quality, variability, and ethical and legal aspects. Involving individuals with cognitive disabilities and their caregivers in the training process is crucial to develop a system that is accurate, respectful of their rights, and preserves privacy.

The response to both RQ1 and RQ2 is clear: users with diverse cognitive abilities encounter challenges in finding various authentication systems accessible, except for biometric approaches, despite the limitations we have highlighted.

6.2 Validation of existing accessibility guidelines for persons with diverse cognitive abilities

We now answer RQ3 *What do users with diverse cognitive abilities think could improve the accessibility of existing authentication approaches?*.

The literature (as discussed in Sect. 3) and our questionnaire findings (outlined in Sect. 4) emphasize the necessity for special attention to users with diverse cognitive abilities. Designing an authentication system that is both accessible and inclusive for them demands careful consideration of their unique needs and challenges, ensuring the implementation of features and options that effectively cater to these requirements.

The questionnaire results support some of the guidelines of Table 5, addressing RQ3. Users highlighted general accessibility concerns related to font adjustments (G1), supporting the need for customizable font type, size, brightness, and color contrast. Additionally, users' tendencies to reuse simple passwords align with guidelines recommending the use of password managers (N1), copy-and-paste functionality (N6), and automatic filling of login credentials by browsers (N2). Third-party authentication options (U5) and the WebAuthn API (U7) are suggested alternatives. Users expressed difficulties with 3D and text-based CAPTCHAs, advocating for alternative solutions (N3). Notably, users prefer biometric authentication over other methods, consistent with findings discussed in the previous section (U8). This empirical study underscores the significance of these guidelines for users with diverse cognitive abilities, emphasizing the importance for IT experts to consider them attentively.

7 Conclusion

This study highlights how users with diverse cognitive abilities face significant challenges when using traditional authentication methods such as passwords or PINs, emphasizing the need for more accessible and inclusive systems. Key improvements include customizable options like adjustable font size, type, brightness, and color contrast to enhance readability. Password management tools such as password managers, copy-and-paste functionality, and automatic login credential filling can simplify the process and reduce security risks. Additionally, third-party authentication options and the WebAuthn API offer more accessible alternatives to traditional methods. Users also expressed difficulties with complex CAPTCHAs, advocating for simpler, more intuitive solutions. A key finding is the strong preference for biometric authentication methods, such as fingerprint or facial recognition, which are seen as more user-friendly and reduce cognitive load. These systems eliminate the need for complex passwords or solving visual puzzles, making them particularly suitable for users with cognitive disabilities.

To make authentication systems more accessible, IT professionals must prioritize these user-centric changes. Implementing customizable features, improving password management tools, and incorporating biometric solutions can significantly enhance both accessibility and security. These improvements will help create a more inclusive online experience for users with diverse cognitive abilities, ensuring they can securely and easily engage with digital environments.

As a future endeavor, conducting an empirical study on the use of biometric and image-based authentication methods with users of varying cognitive abilities could provide valuable insights.

Appendix

The questionnaire

1. I agree to participate in the questionnaire
   - Yes: 100%
2. Age
   - 10-17: 11.8%
   - 18-27: 50%
   - 28-39: 17.6%
   - 40-59: 20.6%
   - 60-79: 0%
   - 80+: 0%
3. Gender
   - Male: 51.5%
   - Female: 45.5%
   - Not specified: 3%
4. What type of cognitive impairment do you have? (Multiple answers allowed)
   - Difficulty recognising characters: 19.51%
   - Difficulty remember information: 7.31%
   - Attention deficit disorder: 21.95%
   - Pervasive Developmental Disorder: 26.26%
   - I dont know: 24.97%

5. Level of cognitive impairment (Multiple answers allowed if more than one answer in the previous question)

   - Mild: 21.2%
   - Moderate: 24.2%
   - Medium: 12.1%
   - High: 15.2%
   - I don't know: 27.2%

6. Have you ever used a PIN to unlock a device or authenticate yourself?

   - Yes: 75%
   - No: 0%
   - I'm not able: 25%

7. If yes, do you find PINs easier or more difficult than passwords?

   - Easier: 66.7%
   - More difficult: 33.3%

8. Are you having difficulty creating, transcribing and/or remembering a PIN?

   - Yes: 50%
   - No: 50%

9. Have you ever reused a PIN for different devices or authentication processes?

   - Yes: 83.3%
   - No: 16.7%

10. Have you ever used a password to unlock a device or authenticate yourself?

    - Yes: 79.4%
    - No: 14.7%
    - I'm not able alone: 5.9%

11. Do you always reuse the same password?

    - Yes: 75%
    - No: 25%

12. When you create a password you think it should be (Multiple answers allowed)

    - Easy to remember, A lot: 54.83%
    - Easy to remember, Enough: 32.50%
    - Easy to remember, A little: 9.67%
    - Secure, A lot: 44.82%
    - Secure, Enough: 44.82%
    - Secure, A ittle: 10.34%

13. What are the reasons for reusing the same password? (Multiple answers allowed)

    - Afraid of forgetting: 66.0%
    - All the sites ask me for the same pattern so I don't want to waste time creating a new password: 43.3%
    - When I think of a new password, I think of one that I use often: 26.7%
    - I have no imagination: 20%
    - Doing "retrieve password" annoys me: 40%

14. Do you often reuse the same password by changing some parts, for example by exchanging letters with numbers or symbols?

    - Yes: 77.4%
    - No: 22.6%

15. Do you use a password manager?

    - Yes: 12.9%
    - No: 83.9%
    - I don't lnow: 3.2%

16. What is the pattern of your password?

    - Uppercase, lowercase, numbers, symbol: 55.8%
    - Only lowercase letters: 13.9%
    - Only numbers: 8.6%
    - Only uppercase letters: 7.6%
    - Other: 14.1%

17. What are the contents of your password? (Multiple answers allowed) (only few options are shown here)

    - Dates: 40.2%
    - First names: 29.5%
    - Nicknames: 22.1%
    - Numbers linked to important events: 17.4%
    - Other: 12.8%

18. Choose what difficulties you have with passwords (Multiple answers allowed)

    - Inventing: 35%
    - Remembering: 60%
    - Writing: 20%
    - Recovering: 50%

Table 8 Description of the difficulties encountered by users during the authentication process

Code	Difficulties	Description
(IP)	Information Processing	Difficulty understanding complex instructions. Long processing times for codes or passwords
(STM)	Short-Term Memory	Difficulty remembering passwords, PINs, temporary codes. Confusion in memories
(SP)	Spelling process	Remembers passwords, PINs, access codes but enters them incorrectly
(DC)	Data Creation	Problems with creating security strings (Password, PIN, etc.)
(MC)	Motor Coordination	Problems entering codes or passwords correctly. Need for alternative or assistive keyboards
(AC)	Attention and Concentration	Difficulty following multiple authentication steps. Potential mistakes due to distraction
(NC)	Nonlinear Cognition	Difficulty following linear sequences of actions. Problems performing specific steps
(SS)	Sensory Sensitivity	Challenges with intense sensory input (light, sound, etc.). Possible adverse reactions to sensory stimuli
(AA)	Analogy and Abstraction	Difficulty in elaborating symbolic or abstract concepts. Problems understanding icons or symbols
(AS)	Anxiety or Stress	Vulnerability to anxiety or stress during authentication. Possible difficulties due to emotional factors

19. Have you ever used a CAPTCHA?

    - Yes: 52.9%
    - No: 26.5%
    - Sometimes: 14.7%
    - Unable to use on my own: 5.9%

20. Which CAPTCHA do you think is more difficult to understand? (Multiple answers allowed)

    - Text-based CAPTCHA: 34.8%
    - Image-based CAPTCHA: 13%
    - 3D CAPTCHA: 69.6%
    - Other: 10.3%

21. What difficulty do you have with CAPTCHAs? (Multiple answers allowed)

    - I can't figure out what's written there: 52.4%
    - I can't enter the correct answer: 19%
    - Other: 28.6%

22. Have you ever used a biometric authentication system?

    - Yes: 61.8%
    - No: 35.3%
    - I am unable to use the systems biometrics on my own: 2.9%

23. Have you ever encountered difficulties with biometric systems?

    - Yes: 12%
    - No: 88%

24. Since you have experienced difficulties with biometric systems, briefly describe what difficulties you have encountered (Multiple answers allowed)

    - They are too complicated: 33.3%
    - Initially I cannot figure out what I need to do but after some help I can: 100%

25. Which websites or apps do you use most frequently?

    - Instagram: 46%
    - YouTube: 44%
    - Instant messaging apps (e.g. WhatsApp, Facebook Messenger): 40%
    - Facebook: 28%
    - Twitter: 16%
    - Other: 26%

26. Is the content of websites you frequently browse clearly displayed?

    - Yes: 82.40%
    - No: 17.60%

27. Briefly describe what the difficulties you encounter and specify the sites

    - I cannot figure out what to do: 66.7%
    - Characters are too small, incorrect colors etc: 33.3%

Table 9 Difficulties encountered by users and related recommendations

Auth. Methods	Diverse cognitive abilities	Difficulties (code)	Recommendation
	General	-	• Provide choices to modify the brightness, color, or font size of the user interface to cater to any sensory sensitivities. Use straightforward and precise language, avoiding figurative language or metaphors that could be challenging to understand. [54–56]. • Include alternative input methods like voice recognition or touchscreen interfaces to replace traditional keyboard and mouse inputs [54–56]. • Use of voice application and the search with images [26]. • Use a simple language, avoiding expressing complex or technical ideas, provide clear and unique automated error messages [58]. • Allow third party authentication and use of the the WebAuthn API [64]. • Explaining properly all the steps required to gain access to a system [57]. • Simplify the content and filter the page content to simplify it [57]. • Use of tools and devices, that provide screen magnifiers, voice recognition software, track the user's eye movement, etc [6, 63]. • Provide visual aids such as diagrams or videos to supplement written instructions[54–56].
	–DRC:	(IP), (SS)	• Allow for font customization and alternative authentication methods such as voice recognition or biometrics [29, 37, 48]. • Add auditory feedback and predictive text to improve the user experience, and clear instructions minimize confusion [29, 48]
	— Dyslexia	(IP), (SS), (DC)	• Add the customization toolbar Firefixia to allow the user to adapt the presentation of Web content by changing the text size, text alignment and link colors [61]. • Add browser extensions with customization features such as the ability to change font size, font type, remove text decoration, change foreground and background colors, spacing, etc [62]
	–DRI:	(IP), (STM)	• Include biometric approaches [49]. • Allow password recovery options such as security questions based on personalized or memorable data information [31, 50]
	–ADD:	(AC), (NC)	• Set a time limit during the authentication process to keep users engaged [51–53]. • To limit distractions and boredom incorporate interactive operations such as button clicking, object dragging, or response prompts [51–53]. • To make the authentication process more enjoyable, use gamification techniques such as challenges, rewards, levels, or badges. [47, 52, 53]
	–PDD:	(SS)	• To accommodate sensory sensitivities, provide options for adjusting brightness, color, and font size [54–56]. • Use clear and concise language, avoiding figurative language or metaphors that may be difficult to understand [54–56]. • For those who struggle with traditional keyboard and mouse inputs, alternative input methods like voice recognition or touchscreen interfaces should be available [54–56]. • Visual aids like diagrams or videos can be provided to supplement written instructions [54–56]
PIN	— Discalculia	(DC)	• Add tactile passwords, eye-gaze methods, songs, and graphical passwords to the authentication process [28]
Passwords	*General:*	(IP), (DC), (STM), (SP)	• (SP) might be solved while browsing, using tools such as the spell checker proposed in [16]
	— Dyslexya	(IP), (AS), (SP)	• Use password managers when possible [29]. • Use web using tools such as the spell checker proposed in [16], however, these tools cannot be used directly for password spelling. • Copy and paste information [29, 47]. • Use of graphic, pictorial and audio/musical password approaches [30]. • Allow the use of biometric systems [40, 41]

Table 9 (continued)

Auth. Methods	Diverse cognitive abilities	Difficulties (code)	Recommendation
	— Down Syndrome	(IP), (DC), (STM), (AA)	• [35] Use mnemonic and graphical passwords. • Use of mnemonic phrases that are easier to remember even for normal users [32, 33]
	–DRI:	(AC), (STM)	• Tokens may be easier to remember than passwords, but for those with memory impairments, keeping track of them can be challenging. Biometrics may be a better option for these users [40, 41]
	–PDD:	(SP), (IP)	• Developers should be aware that the difficulties encountered by users with different cognitive abilities may differ from those of ordinary users [31]
Passphrase	*ADD:*	(AC)	• Make tasks easier and try to make user maintain attention [19, 38]
OTP	*DRC:*	(IP), (AS), (SP)	• Use one-time codes produced by a generator or received by phone so the code does not disappear after some time [28]
Biometric	*General:*	(MC)	• Have few interactions with the system, as many interactions lead to confusion and frustration [40]. • Offer a number of alternatives so that the user can decide which biometric authentication system to use [59]
CAPTCHA	*General:*	(IP), (AC), (NC), (AA), (AS)	• Provide alternatives to CAPTCHAs as persons with different cognitive abilities may not be able to interpret them [52, 53]

Difficulties encountered by users during the authentication process

Comparison between the difficulties encountered by users (divided into the four main categories) and solutions proposed in the literature review. General refers to all the disabilities, specific acronyms are: DRC (Difficulty recognising characters), DRI (Difficulty remembering information), ADD (Attention deficit disorder), PDD (Pervasive developmental disorder). Regarding the difficulties, (IP) = Information Processing, (STM) = Short-Term Memory, (SP) = Spelling process, (DC) = Data Creation, (MC) = Motor Coordination, (AC) = Attention and Concentration, (NC) = Nonlinear Cognition, (SS) = Sensory Sensitivity, (AA) = Analogy and Abstraction, (AS) = Anxiety or Stress.

Acknowledgements The authors would like to take the opportunity to thank all users with different cognitive abilities and all the involved associations who took the time and trouble to respond or help responding to the questionnaire. They also want to thank Prof. Cristiano Varin for his helpful suggestions.

Author Contributions All authors whose names appear on the submission made substantial contributions to the conception and design of the work, drafted the work and revised it critically, approved the version to be published and agreed to be accountable for all aspects of the work.

Funding Work partially supported by projects "SEcurity and RIghts In the CyberSpace - SERICS" (PE00000014 - CUP H73C2200089001), "Interconnected Nord-Est Innovation Ecosystem - iNEST" (ECS00000043 - CUP H43C22000540006), and PRIN/PNRR "Automatic Modelling and $$\forall$$erification of Dedicated sEcUrity deviceS - AM$$\forall$$DEUS" (P2022EPPHM - CUP H53D23008130001), all under the National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

Data Availability Not applicable.

Declarations

Conflict of interest declaration The authors declare that there are no Competing Interests.

Consent Participant data have been completely anonymized, there is no way to relate the results to a person. Participants have been informed that the questionnaires were anonymous and gave the consent to participate. Questionnaires are non-interventional studies, there was no need to have an ethics approval.

References

1. WHO: World report on disability 2011. https://apps.who.int/iris/handle/10665/44575 (Accessed October 2022)
2. Nielsen: Time Flies: U.S. Adults Now Spend Nearly Half a Day Interacting with Media (Accessed October 2022). https://www.

nielsen.com/it/insights/2018/time-flies-us-adults-now-spend-nearly-half-a-day-interacting-with-media
3. Schaepper, M.A.: American Psychiatric Association. Apa Medical Review. https://www.psychiatry.org/patients-families/intellectual-disability/what-is-intellectual-disability (Accessed October 2022)
4. Braddock, D., Jeffery, H., Tanis, S., Ablowitz, E., Haffer, L.: The rights of people with cognitive disabilities to technology and information access. Inclusion **1**(2), 95–102 (2013)
5. Rowland, C.: Cognitive Disabilities Part 2: Conceptualizing Design Considerations. https://webaim.org/articles/cognitive/conceptualize/ (Accessed October 2022)
6. ATIA: Assistive Technology Industry Association. https://www.atia.org (Accessed October 2022)
7. Vanderheiden, G.C., Tobias, J.: Universal design of consumer products: Current industry practice and perceptions. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting (IEA/HFES'00) (2000)
8. Acessify.com: Accessify. https://www.accessify.com/ (Accessed October 2022)
9. Cast: Until learning has no limits. https://www.cast.org/ (Accessed October 2022)
10. Section508.gov: Buy Build Be Accessible. https://www.section508.gov/ (Accessed October 2022)
11. W3C Consortium: Making the Web work. http://www.w3.org (Accessed October 2022)
12. W3C Web Accessibility Initiative: W3C Coga. https://www.w3.org/WAI/GL/task-forces/coga/ (Accessed October 2022)
13. Friedman, M., Bryen, D.: Web accessibility design recommendations for people with cognitive disabilities. Technology and Disability **19**, 205–212 (2007). https://doi.org/10.3233/TAD-2007-19406
14. Diagnostic and Statistical Manual of Mental Disorders: DSM-5, 5th edn. American Psychiatric Publishing, a division of American Psychiatric Association, Washington, DC; (2013)
15. Frolov, L.: What Is Specific Learning Disorder? https://www.psychiatry.org/patients-families/specific-learning-disorder/what-is-specific-learning-disorder (Accessed October 2022)
16. Rello, L., Ballesteros, M., Bigham, J.P.: A spellchecker for dyslexia. Proceedings of the 17th international ACM SIGACCESS conference on Computers and Accessibility (ASSETS'15), pp. 39–47. Association for Computing Machinery, New York, USA (2015)
17. CDC: Data and Statistics on Down Syndrome. https://www.cdc.gov/ncbddd/birthdefects/downsyndrome/data.html (Accessed October 2022)
18. DSM-5: The DSM-5 and the Art of Medicine: Certainly Uncertain. Annals of Internal Medicine 159(5), 360–361 (2013)
19. American Psychiatric Association: The Diagnostic and Statistical Manual of Mental Disorders: DSM 5. American Psychiatric Association Publishing, Washington DC (2022)
20. Grandin, T.: How does visual thinking work in the mind of a person with autism? A personal account. Philosophical Transactions of the Royal Society **364**(1522), 1437–1442 (2009)
21. Child Autism UK: What is Asperger Syndrome? http://www.childautism.org.uk/about-autism/what-is-asperger-syndrome/ (Accessed October 2022)
22. NIST: NIST Password Guidelines 2021: Challenging Traditional Password Management. https://pages.nist.gov/800-63-FAQ/ (Accessed October 2022)
23. Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., Zhang, D.: Biometric recognition using deep learning: A survey. Artificial Intelligence Review, 8647–8695 (2023)
24. Singh, V.P., Pal, P.: Survey of different types of captcha. International Journal of computer science and information technologies **5**(2), 2242–2245 (2014)
25. Zimmermann, V., Gerber, N.: The password is dead, long live the password - a laboratory study on user perceptions of authentication schemes. International Journal of Human-Computer Studies **133**, 26–44 (2020). https://doi.org/10.1016/j.ijhcs.2019.08.006
26. Rocha, T., Bessa, M., Magalhes, L., Cabral, L.: Performing universal tasks on the web: Interaction with digital content by people with intellectual disabilities. In: Proceedings of the XVI International Conference on Human Computer Interaction (HCI'15). Association for Computing Machinery, New York, USA (2015)
27. Prior, S., Renaud, K.: Age-appropriate password "best practice" ontologies for early educators and parents. International Journal of Child-Computer Interaction **23-24** (2020) doi: https://doi.org/10.1016/j.ijcci.2020.100169
28. Helkala, K.: Disabilities and authentication methods: Usability and security. In: Proceedings of the 7th International Conference on Availability, Reliability and Security (ARES'12), pp. 327–334 (2012)
29. Renaud, K., Johnson, G., Ophoff, J.: Dyslexia and password usage: Accessibility in authentication design. In: Clarke, N., Furnell, S. (eds.) International Symposium on Human Aspects of Information Security and Assurance (HAISA'20), pp. 259–268 (2020)
30. Ophoff, J., Johnson, G., Renaud, K.: Cognitive function vs. accessible authentication: Insights from dyslexia research. In: Proceedings of the 18th International Web for All Conference. W4A '21. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3430263.3452427
31. Hayes, J., Li, X., Wang, Y.: I always have to think about it first: Authentication experiences of people with cognitive impairments. In: Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS'17), pp. 357–358. Association for Computing Machinery, New York, USA (2017). https://doi.org/10.1145/3132525.3134788
32. Feng, J., Lazar, J., Kumin, L., Ozok, A.: Computer usage by children with down syndrome: Challenges and future research. ACM Trans. Access. Comput. **2**(3) (2010)
33. Yan, J., Blackwell, A.F., Anderson, R.J., Grant, A.: The memorability and security of passwords - some empirical results. https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf. Technical reports published by the University of Cambridge (2000)
34. Kumin, L., Lazar, J., Feng, J.H., Wentz, B., Ekedebe, N.: A usability evaluation of workplace-related tasks on a multi-touch tablet computer by adults with down syndrome. J. Usability Studies **7**(4), 118–142 (2012)
35. Ma, Y., Feng, J.H., Kumin, L., Lazar, J., Sreeramareddy, L.: Investigating authentication methods used by individuals with down syndrome. Proceedings of the 14th international ACM SIGACCESS conference on Computers and Accessibility (ASSETS'12), pp. 241–242. Association for Computing Machinery, New York, USA (2012). https://doi.org/10.1145/2384916.2384973
36. Ma, Y., Feng, J., Kumin, L., Lazar, J.: Investigating user behavior for authentication methods: A comparison between individuals with down syndrome and neurotypical users. ACM Trans. Access. Comput. **4**(4) (2013)
37. De Angeli, A., Coventry, L., Johnson, G., Renaud, K.: Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies **63**(1), 128–152 (2005). https://doi.org/10.1016/j.ijhcs.2005.04.020
38. Still, J.D., Cain, A., Schuster, D.: Human-centered authentication guidelines, vol. 25, pp. 437–453. Emerald Publishing Limited, (2017). doi: https://doi.org/10.1108/ICS-04-2016-0034
39. Subashini, K., Sumithram, G.: Secure multimodal mobile authentication using one time password. In: 2nd International Conference on Current Trends in Engineering and Technology, pp. 151–155 (2014)

40. Blanco-Gonzalo, R., Lunerti, C., Sanchez-Reillo, R., Guest, R.: Biometrics: Accessibility challenge or opportunity? PLoS One **13**(3) (2018)
41. Daltrey: How biometrics is aiding accessible authentication. Daltrey (Accessed October 2022)
42. Google: reCAPTCHA. https://www.google.com/recaptcha/about (Accessed October 2022)
43. W3C: W3C Captcha. https://www.w3.org/TR/turingtest/ (Accessed October 2022)
44. Moreno, L., González-García, M., Martinez, P.: Captcha and accessibility. is this the best we can do? In: 10th International Conference on Web Information Systems and Technologies (WEBIST'14), vol. 2, pp. 115–122. SCITEPRESS, Barcelona, Spain (2014)
45. Dattolo, A., Luccio, F.L.: A review of websites and mobile applications for people with autism spectrum disorders: Towards shared guidelines. In: Int. Conf. on Smart Objects and Technologies for Social Good, vol. 195, pp. 264–273. Springer, Venice, Italy (2016). https://doi.org/10.1007/978-3-319-61949-1_28
46. Dattolo, A., Luccio, F.L.: Accessible and usablewebsites and mobile applications for people with autism spectrum disorders: a comparative study. EAI Endorsed Trans. **4**(13), 5 (2017)
47. WCAG22: Understanding Success Criterion 3.3.7: Accessible Authentication. https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication (Accessed October 2022)
48. Dosono, B., Hayes, J., Wang, Y.: "i'm stuck!": A contextual inquiry of people with visual impairments in authentication. In: Symposium on Usable Privacy and Security (SOUPS), vol. 15, pp. 151–168 (2015)
49. Farid, F., Ahamed, F.: Biometric authentication for dementia patients with recurrent neural network. In: 2019 International Conference on Electrical Engineering Research and Practice (ICEERP), pp. 1–6 (2019). doi: https://doi.org/10.1109/ICEERP49088.2019.8956981
50. Hogges, J., Shahriar, H., Sneha, S., Ahamed, S.: A two-step password authentication system for alzheimer patients. In: 4th IEEE Annual Computers, Software, and Applications Conference (COMPSAC'20), pp. 1444–1448 (2020)
51. Alqithami, S.: A serious-gamification blueprint towards a normalized attention. Brain Informatics **8**(1), 1–13 (2021)
52. Authority, N.D.: Universal Design. https://universaldesign.ie/technology-ict/web-accessibility-techniques1/developer-s-introduction-and-index/dev-6-%E2%80%93-ensure-custom-widgets-are-accessible/dev-6-4-%E2%80%93-make-sure-login-and-authentication-processes-are-accessible/ (Accessed October 2022)
53. WebUsability: Web Usability Blog - Accessible authentication: logging in made easy. https://info.webusability.co.uk/blog/accessible-authentication-logging-in-made-easy (Accessed October 2022)
54. Bölte, S., Golan, O., Goodwin, M., Zwaigenbaum, L.: What can innovative technologies do for autism spectrum disorders? Autism: the international journal of research and practice **14**(3), 155–9 (2010). https://doi.org/10.1177/1362361310365028
55. Pavlov, N.: User interface for people with autism spectrum disorders. Journal of Software Engineering and Applications **07**, 128–134 (2014). https://doi.org/10.4236/jsea.2014.72014
56. Ramdoss, S., Mulloy, A., Lang, R., O'Reilly, M., Sigafoos, J., Lancioni, G., Didden, R., Zein, F.: Use of computer-based interventions to improve literacy skills in students with autism spectrum disorders: A systematic review. Research in Autism Spectrum Disorders **5**, 1306–1318 (2011)
57. Sevilla, J., Herrera, G., Martinez, B., Alcantud Marín, F.: Web accessibility for individuals with cognitive deficits. ACM Transactions on Computer-Human Interaction **14**, 12 (2007)
58. Australian Banking Association Inc: Guiding Principles for Accessible Authentication. https://www.ausbanking.org.au/wp-content/uploads/2020/05/ABA-Guiding_Principles_for_Accessible_Authentication.pdf (Accessed October 2022)
59. Young-Powell, A.: Ensuring biometrics work for everyone. https://www.raconteur.net/hr/diversity-inclusion/ensuring-biometrics-work-for-everyone (Accessed October 2022)
60. Bohman, P., Anderson, S.: A conceptual framework for accessibility tools to benefit users with cognitive disabilities. In: Harper, S., Yesilada, Y., Goble, C.A. (eds.) Proceedings of the International Cross-Disciplinary Workshop on Web Accessibility, Chiba, Japan, May 10-14, 2005. ACM International Conference Proceeding Series, vol. 88, pp. 85–89. ACM Press, Chiba, Japan (2005). doi: https://doi.org/10.1145/1061811.1061828
61. Avelar, L.O., Rezende, G.C., Freire, A.P.: Webhelpdyslexia: A browser extension to adapt web content for people with dyslexia. In: Science, P.C. (ed.) 6th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Infoexclusion (DSAI 2015), vol. 67, pp. 150–159 (2015)
62. Santana, V., Oliveira, R., Almeida, L., Ito, M.: Firefixia: An accessibility web browser customization toolbar for people with dyslexia. In: International Cross-Disciplinary Conference on Web Accessibility (W4A'13), p. 16 (2013). doi: https://doi.org/10.1145/2461121.2461137
63. Trace RERC: Trace Research Development Center. https://trace.umd.edu (Accessed October 2022)
64. Mozilla, D.: Web Authentication API. https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API (Accessed October 2022)
65. Di Campi, A.M., Focardi, R., Luccio, F.L.: The revenge of password crackers: Automated training of password cracking tools. In: European Symposium on Research in Computer Security (ESORICS'22), pp. 317–336 (2022). Springer
66. Hitaj, B., Gasti, P., Ateniese, G., Perez-Cruz, F.: Passgan: A deep learning approach for password guessing. In: 17th International Conference on Applied Cryptography and Network Security (ACNS'19), pp. 217–237 (2019). Springer
67. Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Lopez, J.: Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In: 2012 IEEE Symposium on Security and Privacy, pp. 523–537 (2012). IEEE
68. Homeland Security: Biometrics Homeland Security. https://www.dhs.gov/biometrics (Accessed October 2022)
69. NIST biometric: Biometric Evaluations Homepage NIST. https://www.nist.gov/itl/iad/image-group/resources/biometrics-evaluations (Accessed October 2022)
70. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology **14**(1), 4–20 (2004). https://doi.org/10.1109/TCSVT.2003.818349
71. Turk, M.A., Pentland, A.P.: Face recognition using eigenfaces. In: Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 586–591 (1991). doi: https://doi.org/10.1109/CVPR.1991.139758