JYX
JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Furnell, Steven; Helkala, Kirsi; Woods, Naomi

Title: Accessible authentication : Assessing the applicability for users with disabilities

Year: 2022

Version: Accepted version (Final draft)

Copyright: © 2021 Elsevier Ltd. All rights reserved.

Rights: CC BY-NC-ND 4.0

Rights url: https://creativecommons.org/licenses/by-nc-nd/4.0/

Please cite the original version:

Furnell, S., Helkala, K., & Woods, N. (2022). Accessible authentication : Assessing the applicability for users with disabilities. Computers and Security, 113, Article 102561. https://doi.org/10.1016/j.cose.2021.102561

Accessible authentication: Assessing the applicability for users with disabilities

Steven Furnell[1,4], Kirsi Helkala[2] and Naomi Woods[3]

[1] School of Computer Science, University of Nottingham, United Kingdom
[2] Norwegian Defence University College / Cyber Academy, Lillehammer, Norway
[3] Faculty of Information Technology, University of Jyväskylä, Finland
[4] Centre for Research in Information and Cyber Security, Nelson Mandela University, Gqeberha, South Africa

Steven.Furnell@nottingham.ac.uk, khelkala@mil.no, naomi.woods@jyu.fi

Abstract

Access to the many benefits available from digital technology can often vary depending upon the capabilities and facilities of the individual who is attempting to engage with it. Many digital devices and services require us to be identified and so require some form of user authentication as part of the process. However, the authentication methods that are currently dominant can prove difficult to use and do not meet the needs of users with disabilities. As such, they can constitute an additional barrier that is not faced by other users. This paper presents an assessment of different forms of user authentication (including various forms of secret, token and biometric approaches) against a range of potential disability categories that may affect their suitability for related user communities. The study draws upon disability classification identified by the World Health Organization and analyses how the usability and/or security of current authentication methods fail users with disabilities due to their non-inclusive design. The discussion is based upon a combination of literature review and examination of real-life examples, and identifies aspects of current implementations that can cause problems in different scenarios. The findings suggest that biometric approaches are likely to be more directly applicable without incurring additional overheads, although even here the potential usability impacts are more prominent for some forms of disability. It is further recognised that while some methods can be made more accessible via assistive technologies, the primary aim should be for authentication choices to be as inclusive as possible by default, rather than expecting or requiring that some user groups should face an additional challenge to accessibility.

1. Introduction

Digital technologies have changed our society on many levels. Services and entertainments are available from home coaches; it is possible socialize with multiple friends at the same time without leaving the room; and almost all information is one click away. Some regard this as life getting easier, while others consider it harder. However, the perspective on digital devices can certainly change when a person has an impairment of some kind, and with around 15% of the world's population living with some form of disability (WHO, 2011), technology must consider the needs of all digital users.

Many people have reported that new technology has opened up opportunities and in general helps with their disabilities. Digital technology has made society more equitable as different

services, shopping, information search, education, communication, social life and travelling are better available for everyone. These benefits and issues have been highlighted in previous research. From the positive side, digital technology has been found to give tools to maintain well-being and control in one's own life (Eriksson, 2019; Valjakka, 2017), and to give a new channel for being creative and being able to influence both on an individual level and society level (Eriksson, 2019). Digital media has a main role in both creating new relations and maintaining established ones (Eriksson, 2019; Mainsah et al. 2019; Söderström, 2009; Valjakka, 2017). At the same time, there are also negative aspects to digital technology. For example, being able to use digital tools and online services needs a certain level of technical competence, which is something that not everyone will have.

The challenges and difficulties experienced by those with cognitive, motor and sensory disabilities when engaging with ICT creates a digital divide that has long been recognised (Chadwick and Wesson, 2016). In 2006, the United Nations General Assembly adopted the Convention on the Rights of Persons with Disabilities, defining access to information and communications technologies as a human right (UN, 2006). This convention has been implemented globally and includes a number of articles that promote accessibility and usage of ICT and the online environment for people with diverse disabilities. For example, Article 4 includes the obligations "to promote the availability and use of new technologies, including information and communications technologies, mobility aids, devices and assistive technologies, suitable for persons with disabilities, giving priority to technologies at an affordable cost"; and Article 9 which includes the obligation "to promote access for persons with disabilities to new information and communications technologies and systems, including the Internet". These obligations have led international communities such as the World Wide Web Consortium (W3C) to develop strategies, best practices and standards to meet these commitments. For example, W3C has developed the Web Content Accessibility Guidelines (WCAG), which include several authentication-related criteria (W3C, 2021). For example. Success Criterion 2.2.5 (Re-authenticating) requires that "*when an authenticated session expires, the user can continue the activity without loss of data after re-authenticating*". This recognises that many sites enforce time limits for inactivity and may therefore present difficulties for users with disabilities if tasks take longer for them to complete. Meanwhile, Success Criterion 3.3.7 (Accessible Authentication) specifies that "*for each step in an authentication process that relies on a cognitive function test, at least one other authentication method is available that does not rely on a cognitive function test, or a mechanism is available to assist the user in completing the cognitive function test*". The fact that these criteria both focus upon authentication help to highlight the significance of this issue. Indeed, it is frequently an essential part of accessing digital services that rely upon identifying a known user, and without successful authentication one cannot access to the service. The increasing range of digital devices and services has consequently increased the amount of authentication that users need to carry out on a daily basis. Therefore, it is important that these methods are provided in a manner that is also accessible for people with disabilities, in web contexts and on devices more generally, in order for digital society to be equally available for all. In this paper, we look at the available authentication methods and specifically at authentication from the disability perspective. While some aspects have been examined in prior works (e.g. ten Brink and Scollan (2019) examined PIN-based authentication in comparison to three selected biometrics, and Dosono et al. (2015) have specifically examined the impacts of visual impairments), the current paper provides consideration across a broader range of both authentication methods and disability types.

The discussion in the sections that follow examine the range of user authentication approaches, considering their applicability from the disability perspective. It expands upon an initial

assessment presented in Furnell et al. (2021), which presents an initial review of methods in the context of the International Classification of Functioning, Disability and Health (ICF) checklist and presents an associated validation of user needs. The current paper presents a more substantial exploration of the issues, including a series of illustrative examples that highlight some of characteristic problems facing users with disabilities in the authentication context, supported by an extended discussion of security and usability issues set against the ICF criteria. It then considers the implications of the findings in relation to the wider provision of authentication solutions that are accessible to persons with disabilities. It should be noted throughout the discussion that the users themselves are in no way to blame for the situations being described. The problem is instead that technologies are being presented to them in such a way that they cannot use them, or find themselves having to compensate for unsuitable approaches by adopting behaviours that serve to weaken security.

2. User Authentication and Disability

Methods for user authentication are divided into three widely recognised categories; something you *know*, something you *have*, and something you *are* (NIST, 2017; O'Gorman, 2003). These are briefly summarised in the paragraphs that follow to introduce the categorisation that is then used as a basis for later discussion. It should be noted that the descriptions here are focused upon the different things that the methods will require the user to be able to do (and therefore has potential implications in the context of disability). As such, the details of how the methods work is not relevant unless this impacts what the user is required to do with them (as such, distinctions between aspects such as passive and active tokens – while clearly significant in the implementation of the technology itself - are not directly relevant to this discussion).

- **Something you know**
  In knowledge-based methods a person has a secret. In this paper, we focus on passwords, Personal Identification Numbers (PINs), Challenge-Response methods, Recognition-, recall- and drawing based graphical passwords.

  Textual passwords, that are character strings often referred as passwords or passphrases that are inserted into the login display by typing them either on keyboard or keypad. PINs are similar to passwords but they contain just numbers and would be included in this subcategory.

  Challenge-response methods belong also to the secret category. However, these methods give a hint to remind a person about the secret. Hints can be a list of questions such as what your mother's maiden name is or what your favourite food is. Or, a user is given trigger words to respond to such as what reminds you about blue or what reminds you about summer.

  Graphical passwords include recognition-, recall- and drawing-based techniques. In recognition techniques, the user identifies figures or items that were pre-selected in the registration phase from among several other figure or items. In recall- and drawing-based techniques a user reproduces a pattern or a figure that she created in registration phase, such as recalling a pattern by connecting dots in preselected order or drawing a free hand figure. The drawing and selecting are either done by moving the mouse or by finger on the touch screen.

- **Something you have**
  In these methods, a user possesses an object that is used in authentication process. In this paper, we divide tokens into sub-categories: user-dependent and user-independent. The former is where the user needs to actively interact with the token to use it in the authentication process. By contrast, user-independent tokens are those where the user's actions are not needed.

- **Something you are**
  These methods are biometrics, based upon physiological or behavioural measurements from the user. Biometric authentication compares a sample provided in the authentication session to the sample registered in the enrolment phase. The more unchangeable the measurement is, the better match it will be between enrolment and authentication samples. This is where physiological and behavioural biometrics differs. Physiological measurements (such as fingerprint recognition, face recognition, handprint recognition, iris recognition and retina recognition) tend to stay the same for a longer time period. By contrast, behavioural measurements such as voice, signature, keystroke and gait might have changed even during one day making the behavioural biometrics more inaccurate methods to begin with.

In addition to the use of these categories in isolation, many services now incorporate multi-factor authentication, where two or more methods are used together. Moreover, a further factor - somewhere you are – can potentially use the location of the user's device to strengthen the authentication in a multi-factor context.

Having presented the basic categories of authentication method, it is also relevant to establish a clear understanding of the various disabilities that those using them may be working with. Disabled World (2019) states that "a disability is defined as a condition or function judged to be significantly impaired relative to the usual standard of an individual or group." They divide disabilities into the eight categories of mobility/physical, spinal cord, head injuries, vision, hearing, cognitive/learning, psychological and invisible. The WHO has more detailed categorization for same impairments. Their ICF checklist is used to measure health and disability at both individual and population levels (WHO, 2001).

Within this paper, we selected specific functions from the ICF checklist, to consider whether the impairment would influence the ability to perform and achieve authentication. The ICF checklist is intended to provide "a practical tool to elicit and record information on the functioning and disability of an individual" (WHO, 2003), and the full list is structured into four main sections (body functions, activities and participation, environmental factors, and body structures) which contain more than 100 underlying indicators that can be qualified as a barrier or facilitator for the individual concerned. However, many of the underlying factors are out of scope for the purpose of this study, either because they pertain to health aspects rather than disability, or because they relate to aspects that would not have direct bearing on an individual's ability to use any of the target authentication technologies. As such, we have excluded many items from the list (such as digestive, metabolic and endocrine systems, genitourinary and reproductive functions, and their representative structures, and haematological, immunological and emotional functions), as they are not primary functions or structures needed for carrying out authentication procedures. Similarly, we have excluded impairments relating to the ICF categories for *Non-verbal messages* and *Lifting and carrying objects*, as none of the authentication methods under consideration would be impacted by impairments of these functions (noting that in cases where motoric functions are needed, they

are covered within the *Dexterity* category). As such, the resulting merged ICF function list used in this paper is as follows:

- **Intellectual (I)** relates to a person's intellectual and higher-level cognitive functions, and ability to undertake multiple tasks or a single task and to solve problems
- **Attention (A)** relates to the capability to hold attention and sleep, energy and drive functions, consciousness, orientation, and capability to undertake multiple tasks or a single task
- **Memory (M)** relates to capability to remember
- **Visual (V)** relates to seeing, watching and perceptual functions
- **Hearing (H)** relates to hearing, listening and perceptual functions
- **Competence (C)** relates to a person's capabilities to learn to read, write and calculate
- **Life function (L)** relates to heart, blood pressure, respiration and skin issues
- **Speech (S)** relates to a person's abilities to communicate with spoken messages, to speak, to have a conversation, knowing a language, and having a voice
- **Dexterity (D)** relates to the capability to undertake tasks involving fine hand use, mobility of joints, muscle power and muscle tone in trunk, head and neck region, shoulder region and in upper extremities. The ability to undertake multiple tasks or a single task, involuntary movements, pain, and vestibular issues
- **Walking (W)** relates to the capability to walk, mobility of joints, muscle power and muscle tone in trunk, pelvis, and lower extremities, involuntary movements, pain, and vestibular issues

Given that there are a range of technological approaches and a wide variety of potential disabilities, it is unsurprising to find that some combinations will work less effectively than others. Indeed, some choices of authentication method (or the way in which they are then implemented) could result in users with some classes of disability from being completely locked out of using them. On one level this simply calls for flexibility in the overall approach, and for different routes/options to be made available. At the same time, it also highlights the need to recognise the implications of different decisions from the outset, so that informed technology choices can be made. As such, the next section more specifically explores the issue of accessible authentication, including examples of how current implementations can often fall short in terms of adequately addressing users with different forms of disability.

3. The need for accessible authentication

Accessible (or inclusive) authentication means ensuring that the method provided is usable and equally secure for all users, despite any impairments. There are several variations of guidance for accessible authentication (Still et al. 2017; Wang, 2017), however, they are all based on the principles for Universal Design. The Centre for Excellence in Universal Design describes the seven principles for Universal Design as follows (CEUD, 2017):

1. **Equitable Use**. The design should provide the same means of use for all users. It should be identical whenever possible and equivalent if the identical is not possible. It should provide same privacy, security and safety for all users. It should not stigmatize any users and it should be appealing to all users.
2. **Flexibility in Use**. There should be choice in methods of use so that the design accommodates individual preferences and abilities such as right- of left-handed, accuracy and precision. It should also be adaptable to the user's pace.

3. **Simple and Intuitive Use**. Use of the design should be easy to understand to all regardless their experience, knowledge, language skills, or concentration level. Information should be arranged consistent with its importance.
4. **Perceptible Information**. The design should include different modes such as pictorial, verbal, tactile in addition to written to guarantee information being available for all regardless of ambient conditions or user's sensory abilities. For example, contrast between information and surroundings should be clear. Same applies to describing functions of different element of the design. The design should also be compatible with variety of techniques and aid devices used by people with sensory impairments.
5. **Tolerance for Error**. The design needs to prevent unintended actions. The most used elements should be most accessible and hazardous elements should be shielded. Warnings should be included.
6. **Low Physical Effort**. The use of design should be comfortable and need reasonable operating forces.
7. **Size and Space for Approach and Use**. The design should be able to be used regardless any body size, posture or mobility impairment with or without assistive devices or personal assistance.

In general, people with disabilities are using the same authentication methods as those without. However, usability issues can still be found, especially if there are no alternative methods to choose from. Universal design principles are applied to authentication methods as there exists several services and applications were a user can choose a preferred authentication method. However, that is not the case with all devices, applications and services. To illustrate the sort of problems that can be encountered, we now present a series of examples that illustrate how even baseline approaches to user authentication (e.g. those based around traditional passwords and two-factor enhancements) can easily introduce potential issues in relation to accessibility.

Beginning with basic passwords, the guidance and feedback for users is often complicated and confusing, and therefore may be additionally challenging for those with learning disabilities and dyslexia (Renaud et al. 2020). Indeed, the fact that there is almost a complete lack of consistency over what is accepted from one site to another (and what is therefore considered to be a 'strong' password), can also add a further dimension to the challenge of learning and following good practice. As an example, consider the guidance provided in Figure 1, taken from an online banking website (in this case at the point when the user is required to reset their password). While it is good that password requirements have been explicitly stated upfront (rather than being revealed in a piecemeal manner in response to the user entering passwords that do not qualify), the combination of descriptive paragraphs and the bullet list serves to split the advice into two formats. A single bullet list, or a clearly separated list of Do and Don't points, would arguably make the advice easier to digest and follow.

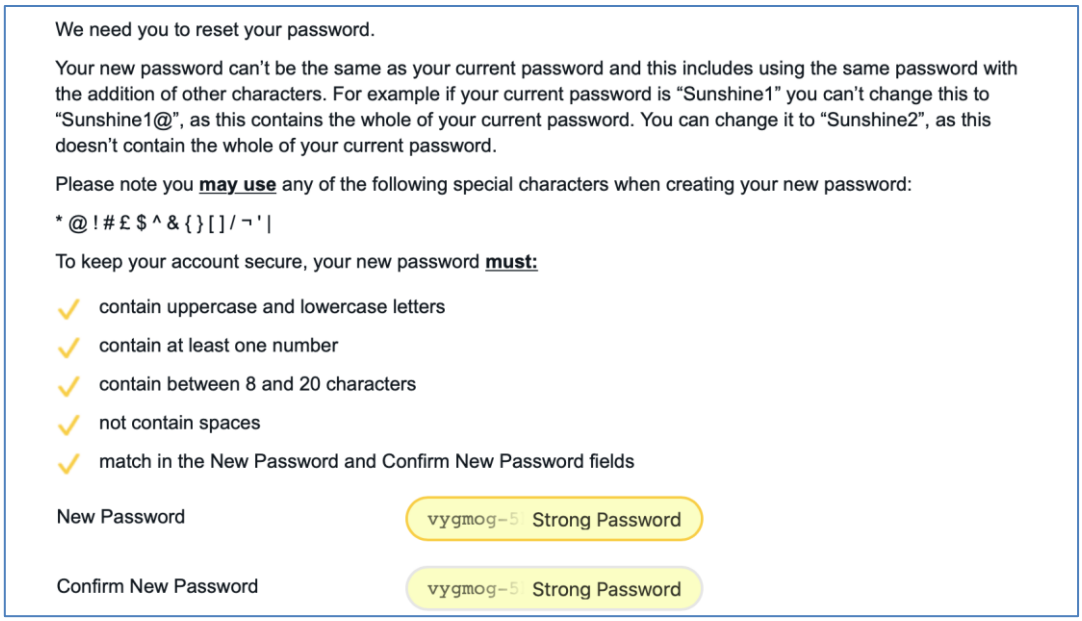


Figure 1 : Example of password reset guidance from an online banking service

We can see from Figure 1 that the browser-generated 'Strong Password' contains a '-' character, and so it is going to be rejected according to the rules on permitted characters. However, the ensuing rejection message (shown in Figure 2) is not particularly helpful in clearly advising the cause of rejection (giving a list of *possible* causes rather than stating the *specific* basis on which it failed, which is clearly known at this point). The fact that the browser is offering the option to generate and save the password automatically is, of course, a potential benefit for our target users – who may otherwise struggle with the tasks of devising the password, committing it to memory, and entering it during subsequent logins. Unfortunately, the problem of such passwords then being rejected by the websites is not unusual, and it is all too easy to find examples of sites that block the usability enhancement that the browser is trying to provide.

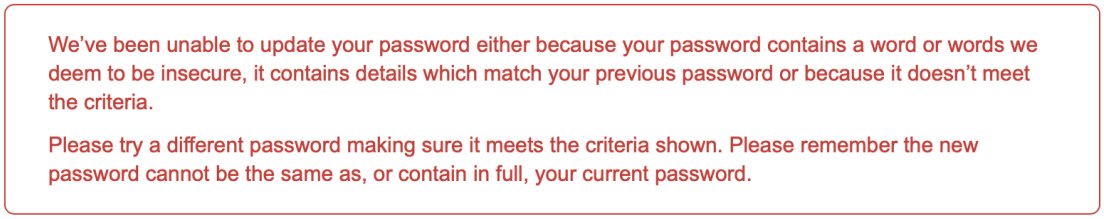


Figure 2 : Notification message to advise that a chosen password was not acceptable

In some cases, website implementations can go even further in terms of frustrating the user's attempts to make use of accessibility shortcuts. Figure 3 illustrates the point, with the browser being prevented form suggesting a password at all, because the website policy does not permit it. So, in this case the user is denied not only the ability to save the password (which the site is apparently seeking to prevent), but also the option to have used the browser to create a strong choice for them to remember by some other means. Such a restriction is in direct contradiction to public advice offered by bodies such as the UK National Cyber Security Centre, whose '6 Top Tips' for individuals to protect themselves online actually includes specific guidance to "Save your passwords in your browser" (NCSC, 2020).



Figure 3 : Site policy prevents the browser from suggesting a password

Meanwhile, some sites seek to assist the user by providing password meters to give feedback on the suitability of their choices. Setting aside the variable quality of the feedback that they actually deliver (Furnell, 2019) there are also comments to be made about the visual clarity of the meters themselves. Looking, for example, at the three examples in Figure 4, one might query the readability of the Dropbox meter for users with a visual impairment (with a less than prominent vertical bar denoting the strength rating, and in this case partly obscured by the browser's 'saved accounts' icon). While the meters from MediaFire and Reddit are more readable, they also appear to be conveying rather contradictory information, with weak ratings (in the red/orange signal colours) nonetheless being accompanied by green ticks to suggest that the passwords (in this case '123456'!) are acceptable. In the absence of further explanation or guidance, this could arguably be cognitively challenging for users in general, regardless of disability status.

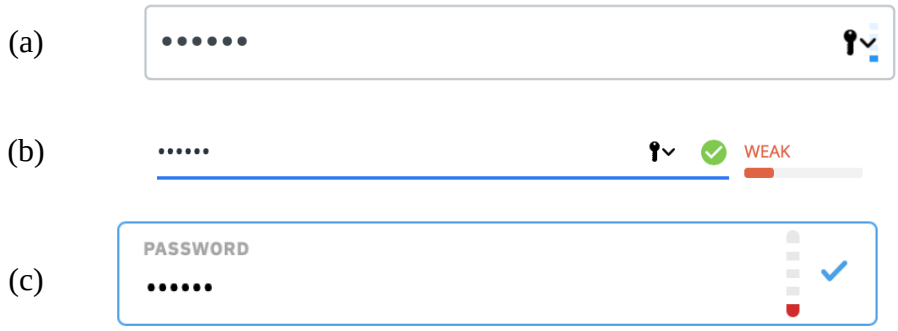


Figure 4 : Password meter examples from (a) Dropbox, (b) MediaFire and (c) Reddit

In some contexts, additional identity verification often takes place to confirm specific sensitive actions or transactions, to confirm that they are being initiated by the legitimate user. Such an example is depicted in Figure 5, in this case taken from an online banking service when the user has elected to create a new payee. The site is invoking an additional step to verify that the actions has been requested by the legitimate account holder, and is calling a pre-stored telephone number associated with their account, which then requires then to speak or type the authorisation code shown on the screen. As can be seen from the screenshot, specific guidance is offered for those that may be hard of hearing, telling them that they need to enter the number 20 seconds after they answer the call. While this is obviously helpful in guiding their response, what it does not tell them is what they are responding *to*. Every other user is clearly listening to *something* for 20 seconds – but a user with a hearing impairment is essentially being advised that they do not need to worry about this and just enter the number when required. Clearly the core instruction (e.g. "Please enter your code") could be said in less than 20 seconds, and so there is presumably some more content to the message that the impaired user is getting no insight into. Although it makes no material difference to the user's ability to complete the security task, it could still leave them feeling at a disadvantage compared to other participants.

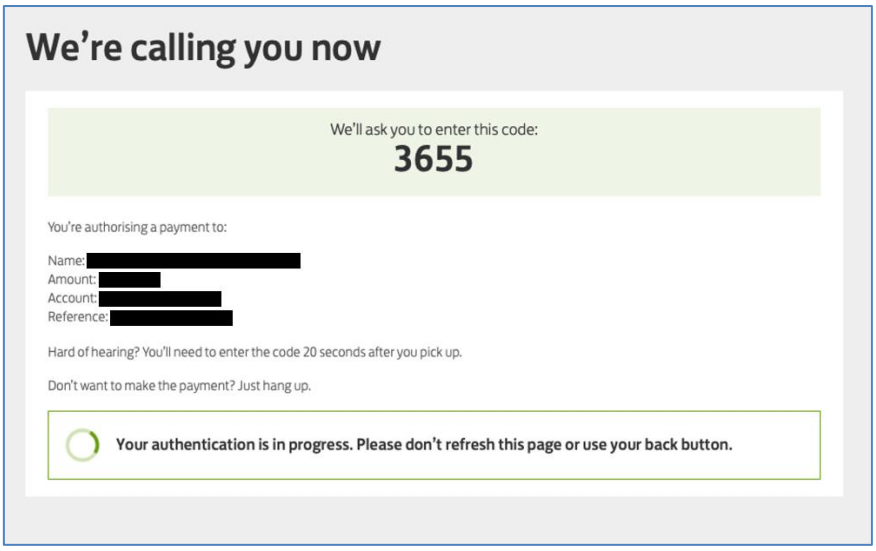


Figure 5 : Online banking transaction verification – example 1

Online banking actually proves to be a rich area for potential criticism, as security-related actions here are rarely as straightforward as they are in other contexts. Illustrating the point, Figure 6 presents an alternative approach to the 'payee creation' activity. In contrast to the previous example, in which the user was verified by phoning them and them confirming the provided code, this example is notably more complicated in terms of both the extent of instructions to be followed and the actions required to follow them. In this case, the payee is being set up on a standard computer via the online banking website. However, to confirm the creation and make the initial payment, the user is also required to generate a 'transaction code' via the banking app on their mobile device. So, the user is required to operate across two devices, initially taking transaction-related details from the website to provide to the app, and then taking the resulting code from the app to provide back to the website. It can be noted from the instructions shown in Figure 6(a) that the user also has a cognitive task to perform in terms of creating the value that they type *into* the banking app, as well as the step of authenticating themselves *to* the app to generate the code. As shown in Figure 6(b), the transaction code has a 30-second validity period, and so this represents a time limit within which the user must then enter it into the website before it times out and they must generate a fresh one. Overall, therefore, this is far from being a straightforward procedure and it is easy to see points at which this could pose additional challenges for users with cognitive impairments (e.g. the ability to interpret and follow the instructions) or physical disability (e.g. particularly having the dexterity to switch between devices and provide the final code within the time limit).

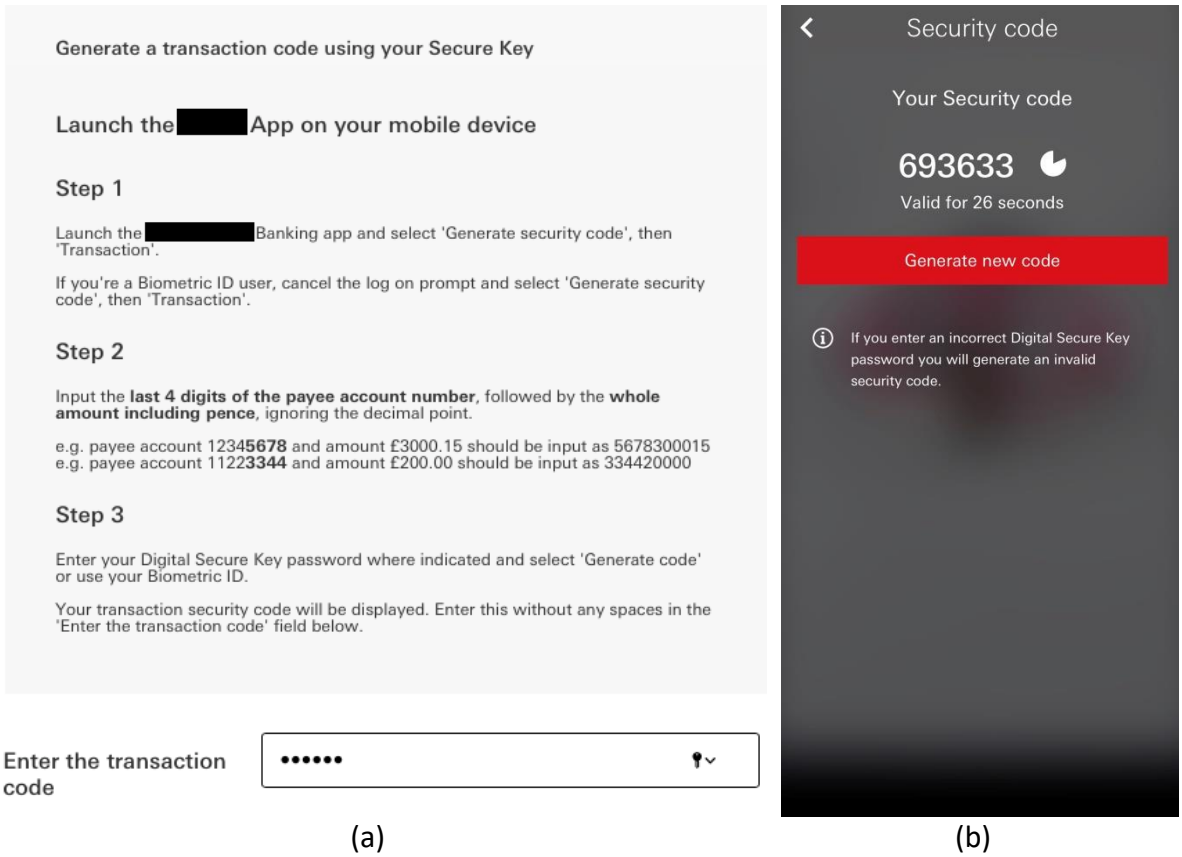


Figure 6 : Online banking transaction verification - example 2

4. Comparison between current methods and ICF-list features

Returning the broader canvas of user authentication methods more generally, the discussion now considers the potential linkage of different impairments to individual authentication methods. Table 1 presents a summary assessment of the potential impacts that the impairment of different ICF functions is likely to introduce in relation to different authentication methods. Specifically, we consider whether a given impairment is likely to affect usability (U) and/or security (S) aspects of a given authentication technique:

- U is entered where a given method may present usability challenges for someone with a particular disability (i.e. they may find it harder to use a given method, or it may be rendered entirely inapplicable).
- S is entered where someone with a particular disability may gain less security from a given method, or use it in such a way that it reduces the level of security that can be achieved.

It should be noted that the assessments presented in the table are not based upon experimental evaluations, but rather upon an informed assessment by the authors based upon a knowledge of both the methods and the impairments, thereby providing a basis to appreciate the potential for usability and security impacts in the related use cases. The work at this stage does not seek to rate the specific *levels* of security and usability impact, and so the entries in the table signify that a given form of impact is present rather but not how severe it may be. So, for example, we can see that memory-related impairment (M) is considered to have a usability-related impact (U) for several methods, but the nature and extent of this impact could differ from method to

method. Moreover, there could still be variations in the context of a single authentication method, depending upon exactly how it has been implemented (e.g. as section 3 has already illustrated, even baseline password methods can be realised differently in practice, which has impacts upon how usable and secure they end up being as a result). As such, the table (and the accompanying discussion in the sub-sections that follow) is therefore considered to offer a top-level view, but further comparative work and assessment would be required to deliver a more detailed assessment. The 'total impacts' column is provided to give a broad overall assessment of how often a given authentication method is likely to be affected by potential impairments

Table 1 : Assessing the potential usability and security impacts of different impairments in relation to different authentication methods

Authentication method		ICF functions impairment impact										Total impacts	
		I	A	M	V	H	C	L	S	D	W	U	S
Memorised Secrets	Passwords	U S	U S	U S	U S		U S			U S		6	6
	PIN	U S	U	U S	U S		U S			U S		6	5
	Challenge – Response	U S	U	U S	U	U	U S			U S		7	4
	Graphical – Recognition	U S	U	U S	U					U		5	2
	Graphical – Recall	U S	U	U S	U					U		5	2
	Graphical – Drawing	U S	U	U S	U					U S		5	3
Tokens	User-dependent	S	U	U S	U					U		4	2
	User-independent	S		U S								1	2
Biometrics	Iris				U			U		U		3	0
	Retina recognition				U			U		U		3	0
	Face recognition				U			U		U		3	0
	Fingerprint recognition				U			U		U		3	0
	Gait							U			U	2	0
	Hand geometry recognition							U		U		2	0
	Typing recognition/Keystroke	S	U	U	U		U S	U		U S		6	3
	Vein recognition							U		U		2	0
	Voice-Speaker recognition		U	U		U		U	U S	U		6	1
	Signature recognition	S	U	U	U		U S	U		U S		6	3

Key:

- ***ICF factors:*** intellectual (I), attention (A), memory (M), visual (V), hearing (H), competence (C), life function (L), speech (S), Dexterity (D) and walking (W)
- ***Impacts:*** usability (U) and security (S)

In general, usability of any of these methods could be complicated by vision and hearing impairments if they are dependent upon the user following audio or visual prompts/instructions. However, unless such prompts are an inherent and unavoidable element of the method, we have not regarded them as primary issues.

The sub-sections that follow expand upon the summary from Table 1, providing further commentary upon each of the ten ICF functions, and considering their potential relevance in the context of the different authentication categories. This discussion is an extended version of the initial assessment presented in Furnell et al. (2021).

4.1 Intellectual

This function relates to a person's ability to think, reflect, transfer knowledge from one context to another, solve problems and carry out intellectual tasks. Authentication procedures are often framed as a series of small tasks, which need to be done in a specific order (e.g., the online banking examples presented earlier are a specific case in point). Depending upon the severity

of a user's cognitive disability (including intelligence, as well as attention and emory), these steps might be difficult to carry out (LoPresti et al. 2008).

Knowledge-based authentication methods can fail to meet the needs of the people with cognitive impairments. For example, passwords need to be created by the user. Strong passwords are long and are often required to contain characters from multiple character sets. If fewer character sets are used, or passwords are just dictionary words, the search space of passwords reduces, making passwords less secure. The same applies to user-selected PIN codes and codes in general. Random codes are more difficult to create and remember than easy ones. Therefore, those with intellectual disabilities, who experience deficits in intellectual functioning such as reasoning, problem solving, judgement, learning, and memory (APA, 2013) could have difficulties with the usability and security of knowledge-based authentication methods.

Challenge-response approaches, whether question-based or association-based, need reflection capabilities. If a person is only able to produce simple and obvious answers, this will impact upon security. The same problematic situation occurs if a person only draws simple sketches in drawing-based methods. Usability issues arise if a person is answering differently each time or drawing different figures due to not understanding the task at hand. Graphical recognition and recall methods are potentially more suitable here, as the user is more likely being prompted with something that may trigger a memory of their secret, compared to the 'blank canvas' that may be encountered in the drawing context.

However, all knowledge-based authentication methods are based on a secret that the person should keep to themselves and not share with anyone. Sharing is a security risk, which is potentially increased with persons of low intellectual level or who are unaware of the consequences of their risky security actions, and could therefore be more easily exploited by others.

As a single factor authenticator, a token holds a secret that a person does not need to know. However, the token itself should be individual and not to be shared. In this context, persons with intellectual disabilities, who can have issues with social judgement, gullibility and a lack of awareness, are at risk of exploitation, victimization and fraud (APA, 2013). This has an effect on security of both token types.

As illustrated in the table, the use of biometrics is generally unaffected by intelligence-related impairments. However, possible exception cases relate to the security aspect of typing and signature recognition approaches. If the enrolled sample is simple, then the security level is affected.

4.2 Attention

Impairments relating to attention may affect a person's capability to keep their focus on a task at hand. Knowledge-based methods are more time consuming than the other authentication methods (Still et al. 2017). Attention is particularly needed when secrets are selected. If the user is not able to pay sufficient attention to the secret during enrolment, then there will be usability issues when later authentication is attempted. From the security point of view, persons with attention difficulties may find it difficult to complete the task oAPA, 2013) and needing to compensate by creating shorter or weaker passwords.

Attention is also needed when the user is required to perform an action, such as authenticating themselves with a user-dependent token. In relation to biometrics, the usability of typing recognition (if implemented in a mode requiring entry of a specific string) and signature recognition also requires a longer transaction time. In addition, with text-dependent voice recognition, the user is needed to pay attention to say the correct passphrase.

4.3 Memory

A person with a memory impairments may experience difficulties with learning, recall, complex attention, and language (APA, 2013). Therefore, they may encounter difficulties with all knowledge-based methods, thereby causing usability issues. A natural compensation in all cases may be to reduce the length or volume of secrets to reduce the memory burden and make things easier to remember (e.g. shorter/simpler passwords; simpler image sequences or fewer points of interest in graphical approaches). However, such adaptations would typically come at the cost of security.

Tokens have a likely advantage over passwords with regards to memory factors. A person only needs to remember to have the token with them, rather than remember a long and complex string. However, due to having to keep track of tokens when they are not in regular use might be harder for some people with memory impairments, therefore potentially affecting the security of the token-dependent authentication.

Biometrics are potentially more suitable for users who have memory impairments , by virtue of using inherent characteristics that are always with the user. Nonetheless, there could still be particular cases (for example, text-dependent modes of voice or typing recognition), where a user is expected to remember a specific passphrase and which may therefore pose difficulties. Also, the typing style and writing style might be affected, as remembering the correct spelling, correct symbol for each letter, and correct sound-letter combination vanishes (Firger, 2013).

4.4 Visual

As with other categories, visual impairments can have different levels of severity. There are assistive technologies (AT) available for the visually impaired, but in this case we compare the inherent nature of the authentication methods when used in a device without ATs to highlight the effect of the impairment.

For the methods relying upon text entry when not using any AT, users with visual impairments might often be presented with difficulties when using a standard keyboard or mobile device (Fuglerud and Dale, 2011), which may leave them little choice but to use shorter strings to maintain usability. A further factor for visually impaired users is that they may be less aware of the threats from adversaries observing their input (Wolf et al. 2017).

Furthermore, those with visual impairment may also find the viability of graphically-oriented methods difficult as these methods place a reliance upon the user having a sufficiently clear impression of what they are expected to be seeing. Issues relating to colour blindness could also have bearing in this context, if the source images are reliant upon the ability to distinguish particular colour combinations.

While tokens are likely to present less of a challenge in relation to visual impairments, a potential issue with user-dependent tokens relates to usability. For example, such tokens may pose difficulties if they rely upon visually displaying a secret (e.g. a one-time code) as part of

the authentication process, as these will often be on small, non-backlit displays. Other usability issues may arise if a token needs to be presented to or inserted into a counterpart device, and such devices are designed or located in such a way that require the user to be able to see clearly to perform the operation.

Biometrics in general should not be an obstacle for users with mild visual impairments , but the usability of certain methods if the user is unable see well enough to interact with the device or perform necessary actions (e.g. positioning themselves or the camera for facial recognition), may pose difficulties. More significant impairments may specifically impact upon iris or retina-based recognition. For example, cataracts can affect iris recognition (Trokielewicz et al. 2014) and macular degeneration will impact upon retinal recognition.

4.5 Hearing

As is evident from the table, many different authentication methods are less likely to cause difficulties for those with hearing impairments.. In certain challenge-response cases, where the challenge is presented in audio form, the usability may be an issue. Furthermore, hearing impairments might impact the usability of voice-speaker recognition. Specifically, a person with a severe hearing impairment, might not be able to control their voice and/or the sound to the extent required by the recognition algorithm, thereby increasing the potential for matching errors (Seladi-Schulman, 2020).

4.6 Competence

In this paper, competence refers to a person not knowing how to read and/or write, and will therefore have an effect on methods that are dependent on textual information, such as passwords, PIN codes, textual challenge-responses, typing recognition and signature recognition. A person who does not know how to read and write can still use passwords and PIN codes as they can be thought to be just a string of items chosen among a keyboard. However, they might be harder to recall as their lack of association as letters and digits might render them as meaningless items, as is the case with young children (Read and Cassidy, 2012). For the same reason, making full use of password and PIN code possibilities is not likely, and the security level of self-selected passcodes may be low. Persons that unable to write may have difficulties with challenge-respond methods that need answers with meaningful words. Whereas, fluent typing is also necessary when typing recognition is used as an authentication method, as the typing style will remain more stable and discernible (Banerjee and Woodard, 2012), and this is more likely to be achieved if the user can associate what they are typing. The same applies with handwritten signatures; either the provided signatures are different (causing false rejection), or the user compensates for the difficulty of writing their name by using a simple curve (lowering the security).

4.7 Life function

This category relates to life-supporting body functions such as heart and blood circulation, respiration and skin, and so associated impairments may specifically affect the usability of biometrics. The usability issues are therefore related to unsteady or inconsistent biometrics samples. For example, cardioid disease or high blood pressure might have an effect a retina vein patterns (Fatima et al. 2019). It might also affect persons walking capabilities (Bloem et al. 2015) and therefore impact upon the effectiveness of gait recognition. In addition, several medical conditions (e.g. tumours) can affect hand vein patterns (Hartung, 2012). Meanwhile, ear, face, finger and hand recognition might be affected if skin injury or skin disease changes

the biometric sample (Drahanský et al. 2017), while respiratory difficulties and ageing can affect voice signal (Vacher et al. 2015).

4.8 Speech

While this impairment has a limited scope in terms of the most authentication methods, there can be issues with regards to voice/speaker recognition, as speech is explicitly required (Lewis et al. 2020). If a user is unable to speak, or unable to do so consistency, then this method will be inaccessible. In less severe cases, false rejection errors could be higher if the spoken voice differs from time to time.

4.9 Dexterity

Fine motoric skills are needed to enable fine hand use. And therefore, the usability of any authentication methods that relies upon moving a mouse, pen or finger steadily, typing on a keyboard, or manipulating a token can cause issues for those with difficulties with fine motoric functioning (Lewis and Venkatasubramanian, 2021). Another issue is how accessible the sensor is. For example, with fingerprint, hand and vein recognitions sensors, the usability depends on the person's capabilities to move and place their fingers and hands, but also upon the design of the device where the sensor is attached.

Users with hand use factors may also find engaging with secret-based approaches difficult. For instance, if users have difficulties in typing stronger/longer passwords they may compensate by using simpler and shorter strings, which will decrease the level of security of passwords(Lewis and Venkatasubramanian, 2021). In addition, the transaction time is slower, increasing the chance for an adversary to observe the process. Similar simplification-based compensations could also be made with challenge-response, drawing methods, and signatures, all of which would have an impact on security.

4.10 Walking

As with speech, walking impairments are less likely to affect the user's engagement with most authentication methods. . However, users with walking impairments may find difficulties with gait recognition as variations in walking style will affect the recognition rate and therefore, the usability of the method in general.

5. Discussion

Table 1 clearly shows that the most of usability issues for the various disability groups are related to the authentication methods belonging to the "Something you know" category (indeed, the most commonly-encountered authentication methods – passwords and PINs – are shown to be the options that present potential usability and security issues most often). It also can be seen that in this category, the security level that authentication method provides is depended on the users' functional capabilities. As this finding is commonly known, it raises a question of why are these methods (especially passwords and PIN codes) are still in such widespread use? Some standard explanations are that they are easy to implement, convertible between different platforms, and cheap to maintain. Additionally, the security level can be raised by demanding longer and/or more complex passwords. Many devices and services also offer the possibility to store passwords locally and to auto-fill password fields, meaning that the burden of both remembering them and typing them can be reduced.

The first examples in Section 3 also concerned passwords and PIN codes, and illustrated usability problems related to the surroundings of the methods (e.g. guidance given when passwords are to be created or warning messages when passwords are not according to the guidelines). While these problems are often related to design and layout, rather than the nature of the method itself, it serves to compound the problem for users with certain types of impairment.

We divided authentication methods within the "Something you have" category into user-dependent and user-independent methods. Based on Table 1, the methods in this category are better suited for persons with disabilities than knowledge-based methods. The few security issues that were identified were related to the misuse of person's disability to steal the authentication item, code or secret. In general, this is a trust issue between the user and the people they are having contact with. User-dependent tokens are to be handled by the users and therefore the usability issues occur if this is difficult for the individual concerned. In addition, as our examples in Section 3 show, the usability issues are not wholly related only to the token itself, but (similarly to passwords and PIN codes) the usage is also affected by the layout of the login page.

Methods in the "Something you are" category have more deviation what it comes usability issues. Behavioural biometrics such as typing, signature or voice-speaker recognition are the methods that cause most of the usability issues for people with disabilities. Security issues with these methods are based upon the same drawbacks as knowledge-based methods; namely a smaller search space. Gait is also a behavioural biometric. As Table 1 shows, it only has few usability issues and no additional security issues related to disabilities. However, based on the overall security that gait can provide, it is not suitable to safeguard systems that need a high level of protection. In addition, the necessary sensors are not commonly available as standard in all devices that may be used, and the fact that the user needs to be moving to be authenticated clearly limits the contexts in which it would be relevant to use the method. Similar comments also apply in relation to hand and vein recognition, the other biometric methods that the table would otherwise suggest pose the fewest additional challenges.

The physiological categories of biometric (such as face, fingerprint, iris, retina, hand and vein recognition) are not having any security issues related to the person's disability. The few usability issues are mostly related to the accessibility of the sensors used for collecting biometric sample. Therefore, these biometrics could be thought to be suitable as authentication methods for both people with and without disabilities. However, while the availability of techniques such as face, fingerprint and (less frequently) iris recognition has become more prominent in recent years, the hardware needed for recognition is not uniformly available across current devices and so they cannot be regarded as a de facto authentication option. Nonetheless, it is notable that the most commonly available biometrics (face and fingerprint) are considered to pose difficulties in the context of far fewer cases than the most common secret-based approaches. As such, the findings concur with prior commentary that biometrics offer the most promising route for accessible authentication (Daltrey, 2020).

Some of the usability issues shown in our examples could have been solved, or made easier to cope with, by assistive technology. The main task of AT is to compensate or substitute impaired functionality. As seen in Table 1 and discussed in Section 4, the usability of many authentication methods is affected by vision and mobility impairment of a person. As touch is found to compensate for vision, Braille keyboards can help the typing process in authentication. To accommodate todays' trends, Alnfiai and Sampalli (2019) have suggested a solution called

BraillePassword to be used for authentication on touch screen devices. Meanwhile, as a means of compensating for hand movement constraints, Chauhan et al. (2017) have suggested BreathPrint, a method that uses audio features from a person breathing via a microphone embedded on a smartphone or wearable device. However, even with an AT-based solution, success would depend upon this being integrated within the system that an individual is using, in place of the traditional, unassisted method. As with smartphones, assistive technology has an associated financial cost, and so it will vary whether would-be users can afford it or not. The potential for discrimination based on such economic differences is one of the concerns of the European Parliamentary Research Service (EPRS, 2018).

Ethical issues are also recognised by the European Parliamentary Research Service (EPRS, 2018). They raise a concern that high-technical solutions are presented as fixes, not holistic solutions for higher inclusivity and acceptability of human diversity. The same concern was previously raised by Söderström (2009), evidencing the long-standing recognition of the issue. However, the advances in the development of assistive technologies raises several ethical issues. EPRS (2018) questions whether there should be limits to the integration of technologies into human bodies, seeing this as an intellectual property right issue. However, there is also a privacy aspect, as a communicative device located under the skin potentially enables 24/7-surveillance of an individual. Privacy legislation should therefore consider the usage of assistive technology by users with disabilities, and should be incorporated into the designing of the systems.

6. Conclusion

Over the last few decades, technology and digital devices have developed, yet authentication has remained somewhat unchanged. With an aging population, and with a growing number of digital users requiring access to their growing number of accounts, meeting the individual needs of users is more imperative than ever before. With the lack of available authentication mechanisms that are usable yet secure, there is a large population of users who are struggling to authenticate themselves. As highlighted at the outset of the paper, this is not a failing of the users themselves, but rather of the technology choices that they can find themselves confronted with.

This paper has reviewed a range of current authentication methods, and examined them from the perspective of users with disabilities. One key contribution of this work is that through identifying the specific aspects of disabilities that cause problems for users when authenticating themselves, this is the first step in finding (or adapting) solutions that will ultimately close the gap in the digital divide. Further to this, it has been acknowledged that the digital divide (exclusion of people with disabilities from the online world), is compounded by social and economic divisions (EPRS, 2018). Lower social and economic status has an impact upon access to assistive technologies that should be supporting users in gaining access to digital services, therefore further increasing the divide. This research identifies the issues that need attention.

One problem area is using authentications methods that are both secure and usable. Users with varying disabilities and severities of disability often find themselves having to compromise on either security or usability when attempting to authenticate themselves. It is notable that all the authentication options can typically be criticised in terms of their potential suitability for some subset of the overall user community. This highlights the desirability of moving away from a reliance upon specific methods and offering flexibility and choice to match users' needs and preferences. Through combining authentication methods and having multifactor alternatives

can provide secure and user-friendly combinations for all users. As disabilities are so varied in symptoms and severity, there should be a variety of multimodal authentication made available so that there are enough alternatives for different needs. Ideally, the choice should be made by the user and not the service provider.

Tokens and biometrics can be combined as they bring only few usability issues for users with disabilities. However, when they are used as a part of the multifactor authentication, the tools needed for the authentication (e.g. fingerprint sensor, code-generator device) should be provided for the users by the service provider. If this cannot be the case, then an equally secure alternative authentication method (e.g. knowledge based) should be made available to guarantee antidiscrimination.

Looking to the future, further research is needed to further investigate the extent of the issues faced by these users based upon empirical and wider data collections. For instance, testing groups of users should be heterogeneous in both age and capability to ensure universal design principles. In terms of more general future focus, developers should be encouraged to more routinely and explicitly consider those who have disabilities, as attempting to meet their needs could potentially lead to improved usability for everyone. Effective options should ideally be available for all user regardless of their devices, and not based on the assistive technology at their disposal.

References

Alnfiai, M. and Sampalli, S. 2019. "BraillePassword: accessible web authentication technique on touchscreen devices", Journal of Ambient Intelligence and Humanized Computing, vol. 10, 2375–2391. https://doi.org/10.1007/s12652-018-0860-x

APA. 2013. *Diagnostic and statistical manual of mental disorders: DSM-5™ (5th ed.)*. American Psychiatric Association, DSM-5 Task Force. American Psychiatric Publishing, Inc. https://doi.org/10.1176/appi.books.9780890425596

Banerjee S.P. and Woodard D.L. 2012. "Biometric Authentication and Identification using Keystroke Dynamics: A Survey", Journal of Pattern Recognition Research 7, 2012, pp116-139. https://doi.org/10.13176/11.427

Bloem BR, Gussekloo J, Lagaay AM,Remarque EJ, Haan J and Westendorp, RGJ. 2015. "Idiopathic Senile Gait Disorders Are Signs of Subclinical Disease", Journal of the American Geriatrics Society, Vol. 48, Issue 9, 2000, pp1098-1101. https://doi.org/10.1111/j.1532-5415.2000.tb04786.x

CEUD. 2017. "The 7 Principles of Universal Design", Centre for Excellence in Universal Design, National Disability Authority. http://universaldesign.ie/What-is-Universal-Design/The-7-Principles/ (accessed 14 May 2021).

Chadwick, D. and Wesson, C. 2016. "Digital inclusion and disability", in *Applied cyberpsychology: Practical Applications of Cyberpsychological Theory and Research*, A.Attrill and C.Fullwood (eds.), Palgrave Macmillan, London, pp1-23. https://doi.org/10.1057/9781137517036_1

Chauhan, J., Hu, Y., Sereviratne, S., Misra, A., Sereviratne, A. and Lee, Y. 2017. "BreathPrint: Breathing acoustics-based user authentication", in Proceedings of the 15th International Conference on Mobile Systems, Applications, and Services (MobiSys '17), pp278-291. Research Collection School of Information Systems. https://doi.org/10.1145/3081333.3081355

Daltrey. 2020. "How biometrics is aiding accessible authentication", Daltrey, 20 July 2020. https://daltrey.com/how-biometrics-is-aiding-accessible-authentication/ (accessed 14 May 2021).

Disabled World. 2019. "Types of disability list", Disability World, 14 December 2019, www.disabled-world.com/disability/types/ (accessed 14 May 2021).

Dosono, B., Hayes, J. and Wang, Y. 2015. ""I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication", Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15). USENIX Association, USA, pp151–168. https://dl.acm.org/doi/10.5555/3235866.3235879

Drahanský M, Kanich O and Březinová E. 2017. "Challenges for Fingerprint Recognition—Spoofing, Skin Diseases, and Environmental Effects", in *Handbook of Biometrics for Forensic Science*, M.Tistarelli and C.Champod (eds.), Advances in Computer Vision and Pattern Recognition. Springer, Cham. https://doi.org/10.1007/978-3-319-50673-9_4

Eriksson, S. 2019. *Vammaisten asema, vaikuttaminen ja digitaalisuus – liikkumisrajoitteisten nuorten kiinnostuksen kohteet ja mielekkäät toimintamuodot yhteiskunnassa*, Invalidiliitton julkaisuja R.29., 2019. https://www.invalidiliitto.fi/sites/default/files/2019-06/Vammaisten_asema_vaikuttaminen_ja_digitaalisuus.pdf (accessed 14 May 2021).

EPRS. 2018. *Assistive technologies for people with disabilities, In-depth analysis*, European Parliamentary Research Service, IP/G/STOA/FWC/2013-001/LOT 6/C3, https://doi.org/doi: 10.2861/422217

Fatima, K., Nawaz, S. and Medrban, S. 2019. "Biometric Authentication in Health Care Sector: A Survey", IEEE International Conference on Innovative Computing, Lahore, Pakistan, 1-2 November 2019. https://doi.org/10.1109/ICIC48496.2019.8966699

Firger, J. 2013. "Handwriting changes can indicate Alzheimer's progression", Everyday Health, 13 November 2013. https://www.everydayhealth.com/alzheimers/handwriting-changes-can-indicate-alzheimers-progression-8042.aspx (accessed 14 May 2021).

Fuglerud, K., & Dale, O. 2011. "Secure and inclusive authentication with a talking mobile one-time-password client", *IEEE Security & Privacy*, *9*(2), pp27-34. https://doi.org/10.1109/MSP.2010.204

Furnell, S. 2019. "Password Meters: Inaccurate advice offered inconsistently?", *Computer Fraud & Security*, November 2019, pp6-14. https://doi.org/10.1016/S1361-3723(19)30116-2

Furnell, S., Helkala, K. and Woods, N. 2021. "Disadvantaged by disability: Examining the accessibility of cyber security", to appear in Proceedings of the Third International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT 21), 24-29 July 2021.

Hartung, D. 2012. *Vascular Pattern Recognition: And its Application in Privacy-Preserving Biometric Online-Banking Systems*, Doctoral dissertations at Gjøvik University College, Norway. http://hdl.handle.net/11250/144366 (accessed 14 May 2021).

Lewis, B., Hebert, J., Venkatasubramanian, K., Provost, M., and Charlebois, K. 2020. "A New Authentication Approach for People with Upper Extremity Impairment", in *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops*, pp1-6. https://doi.org/10.1109/PerComWorkshops48775.2020.9156171

Lewis, B. and Venkatasubramanian. K. 2021. "I...Got my NosePrint. But it Wasn't Accurate: How People with Upper Extremity Impairment Authenticate on their Personal Computing Devices", in Proceedings of the ACM CHI Conference on Human Factors in Computing Systems, (CHI '21), May 28-13, 2021, Yokohama, Japan, pp1-14. https://doi.org/10.1145/3411764.3445070

LoPresti, E.F., Bodine, C. and Lewis, C. 2008. "Assistive technology for cognition [Understanding the Needs of Persons with Disabilities]", in IEEE Engineering in Medicine and Biology Magazine, vol. 27, no. 2, pp29-39. https://doi.org/10.1109/EMB.2007.907396

Mainsah, H., Steinnes, K.K. and Teigen, H.F. 2019. *En undersøkelse av det digitale hverdagslivet til ungdom med nedsatt funksjonsevne*, SIFO rapport nr. 11-2019, Forbruksforskningsinstituttet SIFO, https://hdl.handle.net/20.500.12199/2929 (accessed 14 May 2021).

NCSC. 2020. "Cyber Aware", National Cyber Security Centre. https://www.ncsc.gov.uk/cyberaware#section_3 (accessed 14 May 2021).

NIST. 2017. *Digital Identity Guidelines: Authentication and Lifecycle Management*, Special Publication 800-63B, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

O'Gorman, L. 2003. "Comparing passwords, tokens, and biometrics for user authentication," in Proceedings of the IEEE, vol. 91, no. 12, pp2021-2040. https://doi.org/10.1109/JPROC.2003.819611.

Read, J.C. and Cassidy, B. 2012. "Designing textual password systems for children", in Proceedings of the 11th International Conference on Interaction Design and Children (IDC '12), Association for Computing Machinery, New York, NY, USA, pp200–203. https://doi.org/10.1145/2307096.2307125

Renaud, K., Johnson, G. and Ophoff, J. 2020. "Dyslexia and Password Usage: Accessibility in Authentication Design", in *Human Aspects of Information Security and Assurance*, N.Clarke and S.Furnell (eds.), Springer International Publishing, https://doi.org/10.1007/978-3-030-57404-8_20

Seladi-Schulman, J. 2020. "How people who are deaf learn to talk", Healthline, 2 April 2020. https://www.healthline.com/health/can-deaf-people-talk#nonverbal-communication (accessed 14 May 2021).

Söderström, S. 2009. *Ungdom, teknologi and funksjonshemming: En studie av IKTs betydning i dagliglivet til ungdommer som har en funksjonsnedsettelse*, PhD-thesis, NTNU, Norway. http://hdl.handle.net/11250/267665 (accessed 14 May 2021).

Still, J.D, Cain, A. and Schuster, D. 2017. "Human-centered authentication guidelines", Information and Computer Security, vol. 25, no. 4, pp437-453. https://doi.org/10.1108/ICS-04-2016-0034

ten Brink, R.N. and Scollan, R.I. 2019. *Usability of Biometric Authentication Methods for Citizens with Disabilities*. Mitre Technical Report MTR190511, The MITRE Corporation, September 2019. https://www.mitre.org/sites/default/files/publications/pr19-1396-usability-biometrics-for-disabilities.pdf (accessed 14 May 2021).

Trokielewicz, M., Czajka, A. and Maciejewicz, P. 2014. "Cataract influence on iris recognition performance", in Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments. 929020. 1-14. https://doi.org/10.1117/12.2076040

UN. 2006. *Convention on the Rights of Persons with Disabilities (CRPD)*, United Nations, Department of Economic and Social Affairs. https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html (accessed 14 May 2021).

Vacher, M., Lecouteux, B. and Portet, F. 2015. "On Distant Speech Recognition for Home Automation", in *Smart Health*, A.Holzinger, C.Röcker and M.Ziefle (eds,), Lecture Notes in Computer Science, vol 8700. Springer. https://doi.org/10.1007/978-3-319-16226-3_7

Valjakka, S. 2017. *Näkökulmia vammaisten ihmisten ja mielenterveyskuntotujien tietotekniikan ja digipalvelujen käyttöön*, Digitaalinen arki –selvitysprojekti, ASPA-selvityksiä 1/2017. https://docplayer.fi/46449805-Nakokulmia-vammaisten-ihmisten-ja-mielenterveyskuntoutujien-tietotekniikan-ja-digipalvelujen-kayttoon.html (accessed 14 May 2021).

Wang, Y. 2017. "Universal Authentication: Towards Accessible Authentication for Everyone", Symposium on Usable Privacy and Security (SOUPS) 2014. https://cups.cs.cmu.edu/soups/2014/workshops/papers/accessible_wang_17.pdf (accessed 14 May 2021).

Wolf, F., Kuber, R., & Aviv, A.J. 2017. "Perceptions of mobile device authentication mechanisms by individuals who are blind", in *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, pp. 385-386. https://doi.org/10.1145/3132525.3134793

W3C. 2021. "Web Content Accessibility Guidelines (WCAG) Overview", World Wide Web Consortium, Web Accessibility Initiative (WAI). https://www.w3.org/WAI/standards-guidelines/wcag/ (accessed 14 May 2021).

WHO. 2001. *International Classification of Functioning, Disability and Health*. World Health Organization. https://www.who.int/classifications/icf/en/ (accessed 14 May 2021).

WHO. 2003. “ICF Checklist - Clinician Form for International Classification of Functioning, Disability and Health”, Version 2.1a, World Health Organization, September 2003. https://www.who.int/docs/default-source/classification/icf/icfchecklist.pdf (accessed 14 May 2021).

WHO. 2011. *World Report on Disability 2011*. World Health Organization, 14 December 2011. https://www.who.int/teams/noncommunicable-diseases/sensory-functions-disability-and-rehabilitation/world-report-on-disability (accessed 14 May 2021).