http://dx.doi.org/10.14236/ewic/HCI2022.42

Authentibility Pass: An Accessible Authentication Gateway for People with Reduced Abilities

Paul Whittington
Bournemouth University
Fern Barrow, Poole, Dorset, BH12 5BB
whittingtonp@bournemouth.ac.uk

Huseyin Dogan
Bournemouth University
Fern Barrow, Poole, Dorset, BH12 5BB
hdogan@bournemouth.ac.uk

Authentication is a key component of modern web interfaces. As such, it is important that these authentication mechanisms are inclusive to all users including those with reduced abilities. In this paper, we describe our work on Authentibility Pass that allows users with reduced abilities to communicate their authentication and accessibility requirements to organisations, thus ensuring that authentication is accessible. We first, describe a market validation phase of 30 minute interviews (N=9) with key stakeholders, such as higher education institutions, charities and financial institutions. From our findings, we identified that people with reduced abilities need to repeatedly inform organisations of their requirements. The Authentibility Pass Proof of Concept was then developed comprising of an Android application, database, web interface and Application Programming Interface (API). The market validation results, requirements specification, user interface designs and preliminary evaluation results are discussed, including suggestions for future work. Authentibility Pass will increase the awareness of organisations to customer requirements with reduced abilities, resulting in higher levels of satisfaction.

Accessibility. Android. Biometrics. Multi-factor authentication. Security.

1. INTRODUCTION

Worldwide there are 500 million people with reduced abilities, which accounts for 15% of the total population (The World Bank, 2022) and includes those who have physical and learning conditions. Kostanjsek (2011) states that a disability should be seen as, “a complex interaction between the person and their environment” and not as a characterisation of individuals. Conditions can result in associated impairments, such as reduced finger dexterity, speech, visual and learning impairments. It has been identified that people with reduced abilities encounter barriers due to web security and privacy technologies. Example challenges include users who have learning conditions experiencing challenges following multi-step procedures on websites (World Wide Web Consortium, 2022).

It is important that authentication mechanisms are accessible to users of all physical and learning abilities and there is currently not a solution that enables communication of authentication and accessibility requirements to organisations. The benefit of such an approach would be a user would be required to enter their requirements once, which can then be used by a number of organisations.

We believe that Authentibility Pass is the solution and this paper describes the findings from a market validation phase conducted prior to the development and discusses the designs of an Android application database, web interface and API, which combine to create Authentibility Pass. The Proof of Concept version is illustrated, as well as preliminary evaluation results and our routes to dissemination and evaluation.

2. BACKGROUND

The World Wide Web Consortium (W3C) highlights the importance of ensuring that there is an easy, accessible and secure method to access online content for users who have reduced abilities.

However, the W3C Web Content Accessibility Guidelines (WCAG) 2.1 does not recommend compliant authentication methods. Success Criterion 3.3.7 of WCAG 2.1 does provide guidance on accessible authentication in terms of ensuring that websites have an easy to use and secure method to log in and access content (World Wide Web Consortium, 2022). It is highlighted that memorising a username and password can be challenging for people with reduced learning abilities and an alternative authentication method that does not include a cognitive function test should be provided.

The aim of Authentibility Pass is to provide accessible authentication to users with a wide range of abilities who currently have challenges with communicating their requirements to organisations. The intended user community for Authentibility Pass are people with reduced physical or cognitive abilities who find traditional methods of communicating with organisations challenging. A competitor analysis was conducted prior to the market validation phase, to establish products in the domain that provide similar features as Authentibility Pass. Products in both the authentication and accessibility domains were investigated and it was determined that products either support authentication or accessibility. Authentication providers include iProov, SaveNet and Google Authenticator and solutions that support accessibility include Be My Eyes, AccessAble and Moovit. iProov provides online biometric authentication and verification that can be useful for people who are not able to enter passwords due to their disability, whereas SafeNet and Google Authenticator are general authentication mechanisms.

3. MARKET VALIDATION

The Authentibility Pass Proof of Concept was developed during the Cyber Security Academic Startup Accelerator Programme (CyberASAP) that consisted of a market validation phase and a development phase. A ‘Demo Day’ event was then held and provided the opportunity for industries to evaluate Authentibility Pass.

3.1 Participants and Procedure

The purpose of the market validation phase was to determine whether there was a need for Authentibility Pass in the domain. Prior to the validation, the following target sectors were identified; higher educational institutions, schools, non-profit organisations, SMEs and financial institutions. It was important to elicit the views from stakeholders in each sector and suitable organisations were identified through our research. Each was approached with a video call and a semi-structured interview was conducted with the participating employees. During the interview, the participants were asked about the current processes for obtaining customers accessibility and authentication requirements, as well as any challenges that can be encountered. The responses were used to determine the types of requirements that would need to be captured by Authentibility Pass.

3.2 Findings

The key results for each domain are described below.

Higher Education: Authentibility Pass would be beneficial to students with a range of reduced abilities. Learning Support departments currently update a student record system with information on conditions, exam adjustments, Disabled Students’ Allowance requirements and personal contact details. It was acknowledged that students may express concern over large numbers of staff having access to their accessibility requirements, but this would be offset by the students receiving a higher level of support.

Non-Profit Organisations: Authentibility Pass would be a valuable solution for Front of House teams and Duty Managers, but it would need to be compatible with existing event management systems. Accessibility requirements for their customers are currently stored during the registration process for events and the onus is therefore on customers to advise organisations.

Small Medium Enterprises: When organising events, customers’ accessibility requirements are obtained through registration with an event management provider, including their dietary needs. SMEs stated that Authentibility Pass would be helpful, to enable customers to share their accessibility requirements in advance, allowing more efficient planning of events.

Financial Institutions: The Head of Digital Accessibility at the multi-national bank stated, “There is huge value in standardising accessibility preferences to drive more inclusive, personalised services”. However, financial institutions would only consider adoption if Authentibility Pass could interact with existing customer databases through an API.

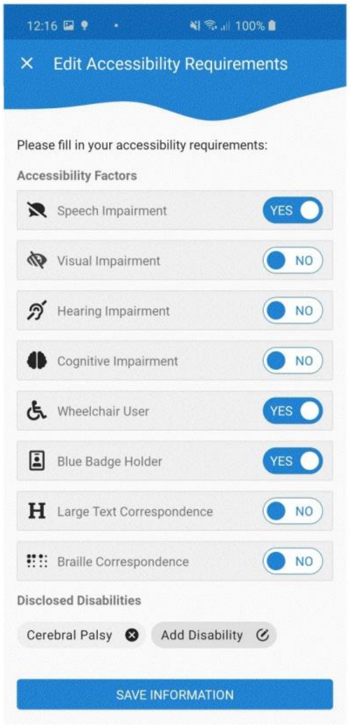
User Community: People with reduced abilities highlighted that there were challenges with communicating their requirements to organisations and they often need to repeatedly inform individual organisations.

4. DESIGN OF CONCEPT

Authentibility Pass is an innovative solution that provides a gateway for people with reduced abilities, to communicate their authentication and accessibility requirements to organisations. The solution has the following key features:

- Customers only need to enter their requirements once, which can be sent to multiple organisations.
- Customers are in control of their own data, deciding which organisations can have access.
- Organisations are provided with a service that records customers' authentication and accessibility requirements.
- Organisations with existing databases can use an Application Programming Interface (API) to receive requirements that are sent via the Authentibility Pass application.

The Authentibility Pass Android application, web interface, database and API were developed simultaneously to provide a gateway for people with reduced abilities to communicate their authentication and accessibility requirements. The Android platform was chosen, as this has 71% of the worldwide market share for mobile operating systems (Statcounter, 2022).



Please fill in your accessibility requirements:

Accessibility Factors

Speech Impairment	YES
Visual Impairment	NO
Hearing Impairment	NO
Cognitive Impairment	NO
Wheelchair User	YES
Blue Badge Holder	YES
Large Text Correspondence	NO
Braille Correspondence	NO

Disclosed Disabilities

Cerebral Palsy

Figure 1: *Input of accessibility requirements through the Android application*

4.1 User Interface

The Android application would be used by people with reduced abilities to enter their accessibility requirements (Figure 1) including disability type, impairments and specific needs, e.g. Blue Badge holder, through selecting checkboxes with the facility to input additional text information. The Authentication Requirements section of the application has a similar interface where users can state their authentication preferences. Authentibility will then ascertain the authentication methods that are compatible with their device and allow users to verify each of the available methods. The Application will conduct a series of short checks to verify whether the user can operate each authentication method. If the user is unable to complete the check, the relevant authentication method will automatically be deselected from their requirements. Users will be able to select from a list, which organisations they choose to send their accessibility and authentication requirements. Token-based authentication was implemented to transmit the requirements from a user's smartphone to an organisation's database. The web interface would be used by organisations to access customer requirements, enabling searches to be performed for requirements based on the customer ID or name. The private Authentibility Pass API is designed for organisations that have existing database systems and once registered, they will be provided with a unique API key to facilitate integration with their existing database systems. Authentibility Pass can either be used by people with disabilities or through the support of a parent/carer if they are unable to operate the smartphone interface.

5. PRELIMINARY EVALUATIONS

Authentibility Pass was presented at the CyberASAP Demo Day event and the preliminary evaluations highlighted the key areas that will need to be considered during the dissemination of Authentibility Pass.

5.2 Integration

The user interface of Authentibility Pass received positive feedback from a multi-national financial institution, which emphasised that customers' accessibility needs are an important consideration. For Authentibility Pass to benefit the financial sector, integration with existing systems would be paramount, as this sector would need to ensure the integrity of their customers' data. Open banking was suggested as a potential solution, where

Authentibility Pass would interface with customers' existing online banking accounts.

5.3 Deployment

A domain expert in cyber security highlighted that organisations responsible for defining standards for cryptographic authentication protocols, should be approached prior to deployment of Authentibility Pass. It would be beneficial to approach Single Sign-on (SSO) providers to determine new feasibility of incorporating Authentibility Pass. This would ensure that the necessary standards are achieved in order for customers' data to be protected.

5.4 Data Privacy

Data privacy and security for Authentibility Pass is an important consideration in terms of where the customer data is stored, the duration and which users are granted access to the data. To ensure that users are in control of their own data, a domain expert in data privacy recommended that a data protection statement be incorporated into the Application that informs the user when data is shared with an organisation.

6. DISCUSSION

Authentibility Pass will benefit people with reduced abilities, as well as developers and system integrators to adapt websites and/or systems to the specific access and authentication requirements of their customers. It will enable customers to enter their requirements into a smartphone application, which can then be sent to secure organisational databases. It is anticipated that the adoption of the solution will increase the awareness of employees of how best to support their customers with reduced abilities, resulting in higher levels of customer satisfaction. he Authentibility Pass Proof of Concept was developed based on a market validation phase which informed the creation of the requirements specification. This two-phased approach enabled feedback to be elicited from stakeholders in the potential market sectors to understand the current challenges.

It was highlighted by all of the participating organisations that their customers with reduced abilities had to repeatedly inform them of their requirements, which is time consuming and they acknowledged the need for Authentibility Pass. However, most organisations emphasise that GDPR would need to be followed prior to potential adoption. Token-based authentication encrypts the data during transmission and only the recipient organisation has the required token to decrypt their customers' requirements.

7. CONCLUSIONS AND FUTURE WORK

Conducting market validation has illustrated that there is a significant interest in Authentibility Pass to assist people with reduced abilities informing organisations of their authentication and accessibility requirements. The findings identified the features of the Proof of Concept, consisting of an Android application, database, web interface and API. The validation also highlighted data privacy and security issues that will need to be addressed. As Authentibility Pass communicates personal data, a balance will need to be achieved so that organisations are informed of the necessary requirements, whilst ensuring data privacy through token-based authentication and data encryption. The main lesson learnt from the development is that there is people with disabilities often have to repeatedly inform organisations of their requirements and Authentibility Pass provides a solution to this.

The Proof of Concept will be disseminated to the participants of the market validation, where data will be transmitted to a single database, using token-based authentication. The usability of Authentibility Pass will be assessed by a questionnaire consisting of System Usability Scale (SUS) (Brooke, 1996) and NASA Task Load Index (TLX) (National Aeronautics and Space Administration, 2022). Organisations in the target markets would be approached for potential adoption of Authentibility Pass into their current processes, for interacting with customers who have reduced abilities. The possibility of integrating the application with existing verification mechanisms and event management platforms would also explored. Revenue streams would be established with different licensing packages, based on the type of organisation. An iOS implementation of the application will be developed to increase the number of supporting organisations and users with reduced abilities. This will result in Authentibility Pass becoming a gateway for people with reduced abilities to communicate their authentication and accessibility requirements.

ACKNOWLEDGMENTS

The authors would like to acknowledge the support of Vers Creative UK, to develop and test the Authentibility Pass. We would also like to thank DCMS in collaboration with Innovate UK for funding this research.

REFERENCES

Brooke, J. (1996) SUS: A “quick and dirty” usability scale. In Jordon, P.W., Thomas, B., McClelland, I.L. and Weerdmeester, B. (eds), Usability Evaluation in Industry. Taylor and Francis, London.

Kostanjsek, N. (2011) Use of The International Classification of Functioning, Disability and Health (ICF) as a conceptual Framework and common language for disability statistics and health information systems, BMC Public Health, 11, 4, 1-6.

National Aeronautics and Space Administration. (2022) NASA TLX: Task Load Index. https://humansystems.arc.nasa.gov/groups/tlx/ (Retrieved 19th June 2022).

Statcounter. (2022) Mobile Operating System Market Share Worldwide – December 2020. https://gs.statcounter.com/os-market-share/mobile/worldwide (Retrieved 19th June 2022).

The World Bank. (2022) Disability Inclusion. https://www.worldbank.org/en/topic/disability (Retrieved 19th June 2022).

World Health Organization. (2001) International Classification of Functioning, Disability and Health (ICF). https://www.who.int/standards/classifications/international-classification-of-functioning-disability-and-health (Retrieved 19th June 2022).

World Wide Web Consortium. (2022) Understanding Success Criterion 3.3.7: Accessible Authentication. https://www.w3.org/WAI/WCAG21/Understanding/accessible-authentication (Retrieved 19th June 2022).