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

Paul Whittington
Department of Computing and Informatics
Bournemouth University
Poole, Dorset
whittingtonp@bournemouth.ac.uk

Huseyin Dogan
Department of Computing and Informatics
Bournemouth University
Poole, Dorset
hdogan@bournemouth.ac.uk

***Abstract*— It is important that authentication mechanisms are inclusive to all users including those with reduced abilities. This paper describes our work on Authentibility Pass that allows users with physical and cognitive disabilities to communicate their authentication and accessibility requirements to organizations, including e-businesses, thus ensuring that authentication is accessible. In the initial development phase, a Business Model canvas was created for the Authentibility concept, where the key partners, activities, cost structure and revenue streams were established. This contributed to a value proposition canvas to highlight the customers' tasks, gains, and pains, as well as how Authentibility Pass will mitigate the pains. The second market validation phase is then described consisting of 30 minute interviews (N=9) with key stakeholders, such as higher education institutions, charities and financial institutions. From our findings, it was identified that people with reduced abilities need to repeatedly inform organizations or e-businesses of their requirements. The Authentibility Pass Proof of Concept was subsequently developed comprising of an Android Application, database, web interface and Application Programming Interface (API). User requirements are entered through the Application, including authentication checks for verification. The user's accessibility and authentication requirements are communicated using token-based authentication and stored in organization databases. The API is designed for organizations and e-businesses with existing database systems. The Business Model and Value Proposition canvases, market validation results, user interface designs and preliminary evaluation results are discussed, including suggestions for future work. Authentibility Pass will increase the awareness of organizations to customer requirements with disabilities, resulting in higher levels of satisfaction.**

Keywords— Android, Business Model Canvas, biometrics, multi-factor authentication, security, Value Proposition Canvas.

I. INTRODUCTION

It is important that authentication mechanisms are accessible to users of all abilities, but this user group can encounter barriers due to web security and privacy technologies. This is a larger user community, as worldwide there are one billion people with disabilities, which accounts for 15% of the total population [1], including those who have physical and learning disabilities. Kostanjsek [2] states that a disability should be seen as, "a complex interaction between the person and their environment" and not as a characterization of individuals. Conditions can result in associated impairments, such as reduced finger dexterity, speech, visual and learning impairments. These impairments can cause challenges when interacting with standard technologies and often require the use of assistive technologies that "increase, maintain, or improve the functional capabilities of persons with disabilities" [3]. The authors' previous assistive technology research investigated the recommendations of suitable technologies, based on people's abilities [4] and highlighted that there cannot be a single solution to suit all users. There needs to be a more customised approach that harnesses the actions that individuals can perform independently.

Example challenges with authentication mechanisms include users who have cognitive conditions experiencing challenges following multi-step procedures on websites [5]. Also, people with physical disabilities such as visual impairments, dyslexia and reduced movement in the upper extremities can have challenges using authentication methods such as Personal Identification Number (PIN) codes, textual passwords and one-time codes received by Short Message Service (SMS) [6]. However, there is currently not a solution that enables communication of authentication and accessibility requirements to organizations. 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 organizations. This would be significantly less time consuming than having to inform individual organizations of their requirements. Organizations would know how to best support their customers which would result in a more efficient customer experience and higher satisfaction.

This paper describes the findings from our Authentibility Pass research in terms of creating a business model and value proposition, the designs and implementation of an Android application and the results from an initial market validation phase. This culminates the findings from our previous SmartAbility research, which provides assistive technology recommendations via an Android application, suitable for users with physical disabilities [4]. The disabilities included in SmartAbility were based on the World Health Organization's International Classification of Functioning, Disability and Health (ICF) [7]. The Proof of Concept version is illustrated, as well as preliminary evaluation results and our routes to dissemination and evaluation by the target markets of financial institutions, small medium enterprises (SMEs), non-profit organisations and higher education institutions.

II. 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 3.3.8 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 [4]. It is highlighted that memorising a username and password can be challenging for people with cognitive disabilities and an

alternative authentication method that does not include a cognitive function test should be provided. This could be achieved through 2-factor authentication, allowing multiple options for the second factor, such as a token stored on a Universal Serial Bus device. The W3C also describes common authentication challenges for people with disabilities. This includes users with visual impairments, difficulties with discerning the text required to submit to online forms and users with learning impairments who are unable to follow multi-step procedures and instructions displayed on websites. As a result of these challenges, users can become frustrated and choose to cancel transactions, causing potential financial losses for an organization.

Wang et al. [8] state that it is critical to develop accessible authentication mechanisms that any user can operate in order to make computing inclusive to all, regardless of their disability type. They recommend that the authentication process should be secure and efficient to reduce the risk of attacks such as shoulder surfing, i.e. attempting to observe a password by standing behind the user logging into a system. Bonneau et al. [9] propose a framework to evaluate web authentication mechanisms, with one criteria of the framework being accessibility. Accessible authentication mechanisms have evolved through research from passphrases [10], to tactile authentication methods [11]. A hardware alternative is token-based authentication that consists of devices containing a user's credentials (known as a cryptographic token), providing authentication with an application or service. There are also authentication mechanisms designed specifically for smartphones, which can assist people with physical disabilities who have difficulty with entering passwords on a device.

Five goals of universal authentication have been defined by Wang et al. [8], referred to as the 'SUPER' principles. These are Secure, Usable, Privacy-preserving, Effective and Reachable/accessible. In order to be secure, the authentication mechanisms must be difficult to circumvent to prevent common security attacks. Additionally, the mechanism must be usable for everyone, regardless of their abilities and it should conceal any conditions of the user from the host system. Any mechanism should provide an accurate method of logging users into the system in order to be effective. To maximise accessibility, it should be compatible with public terminals, including common web browsers.

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 organizations, including e-businesses. A competitor analysis was conducted prior to the market validation phase, to establish products in the domain that provide similar features as Authentibility Pass. Table 1 illustrates the competitor analysis where products in both the authentication and accessibility domains were investigated.

Features	iProov	SaveNet	Google Authenticator	Be My Eyes	AccessAble	Moovit	Authentibility
Authentication	●	●	●	○	○	○	●
Accessibility	◗	○	○	●	◖	●	●
Biometric authentication	●	○	○	◗	○	○	●
Hardware based tokens	○	●	●	○	○	○	●
Customisation	◖	◗	◗	◖	○	◗	●

● Fully supported ◖ Mostly supported ◗ Partially supported ○ Not supported

Table 1. Authentibility Pass Competitor Analysis

The features of Authentibility Pass were compared to each of these products and in particular whether accessibility and authentication were both provided in one product. Comparisons were also made considering data transmission via hardware-based tokens and customisation to suit user abilities. Each product was mapped to these features in terms of whether they were fully, mostly, partially or not supported. Overall, it was determined that products either support authentication or accessibility, but not both. The analysis compared the authentication providers of iProov, SaveNet and Google Authenticator, as well as solutions that support accessibility, i.e. Be My Eyes, AccessAble and Moovit. iProov provides online biometric authentication and verification [12] 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 providers. Be My Eyes is a free smartphone application that can connect blind or low vision users with sighted volunteers to provide assistance through a live video call [13]. The AccessAble and Moovit websites provide accessibility information regarding places of interest, restaurants, venues and public transport. Both of these websites can be customised to perform searches based on users' accessibility requirements. The product that contained the most similar features to Authentibility, was iProov, as the main competitor in the market. However, our research highlighted that Authentibility Pass has a competitive advantage by providing both authentication and accessibility features in a single application to support people with physical and cognitive disabilities.

III. Value Proposition

The Authentibility Pass Proof of Concept was developed during the Cyber Security Academic Startup Accelerator Programme (CyberASAP) in the United Kingdom (UK) that consisted of two phases: Value Proposition and Market Validation, followed by Proof of Concept development.

A. Business Model

During the first phase, a Business Model Canvas was created. This is a business tool that is used to visualise the building blocks of a business, including customers, routes to market, value proposition and finance [14]. The Strategyzer Canvas template [15] was used for Authentibility and this contains the blocks: Customer Segments, Value Propositions, Channels, Customer Relationships, Revenue Streams, Key Activities, Key Resources, Key Partners and Cost Structure.

Fig. 1 contains an extract from the Business Model Canvas for Authentibility. The key partners are financial institutions, small medium enterprises, non-profit organisations and higher education institutions. Each of these partners will use the application to obtain the accessibility and/or authentication requirements of their customers. The required resources include semi-structured interviews and surveys which were conducted to contribute to the Proof of Concept designs. It was therefore essential to have access to the market sectors and the customer base for people with disabilities. An initial cost structure was defined, where Authentibility will be provided as an application to

organizations which can be integrated into their current business processes. This will be managed through 'Software as a Service' subscriptions and commercialized by a spinout company from a UK university. There will be three revenue streams: Free, Subscription and Enterprise. The application will be provided free of charge to micro businesses with limited customer support. There will be a subscription plan for SMEs that have high volume of data traffic, where monthly and annual fees will be applied based on the number of transactions. The final tier will be designed for enterprise organizations that provide greater customization features and volume licensing, where Authentibility can be installed on a large number of clients. These revenue streams will be used to maintain the application and provide periodic updates. The outputs for the business model will be to improve customer relationships by increasing the awareness of their requirements, which can easily be retrieved from the application by the organization employees.

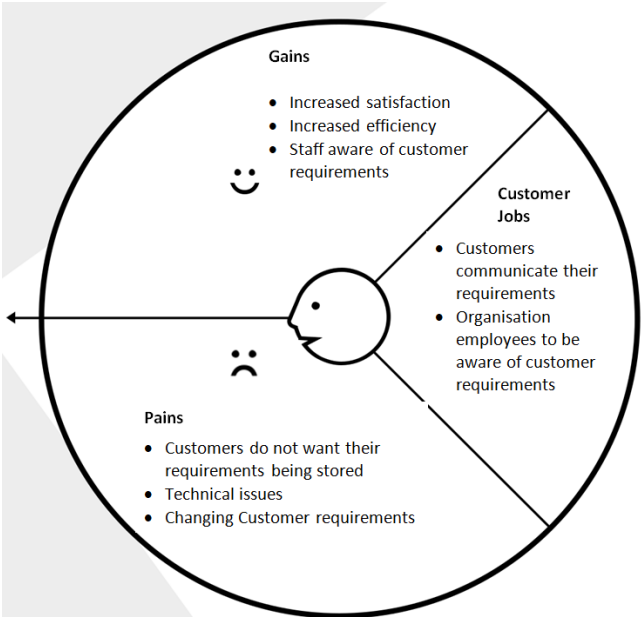


Fig. 1. Extract from the Authentibility Value Proposition Canvas for Customers with Disabilities

B. Value Proposition

The Value Proposition for Authentibility was modelled using the Value Proposition Canvas, a framework developed by Osterwalder, to ensure that a product is positioned around a customer's values and needs [16]. It can be used to determine whether there is a fit between the product and intended market and can be used in conjunction with the Business Model Canvas. There are two main aspects of The Value Proposition Canvas [17], a customer profile and the company's value proposition. The customer profile determines the gains, i.e. the benefits that the customer expects, the pains, i.e. negative experiences and the customer jobs, i.e. tasks the customer is attempting to solve. A customer profile is developed for each customer segment identified in the Business Model Canvas, with individual gains, pains and jobs. The canvas also contains a Value Map that identifies gain creators, pain relievers, as well as products and services that are related to the gains and pains.

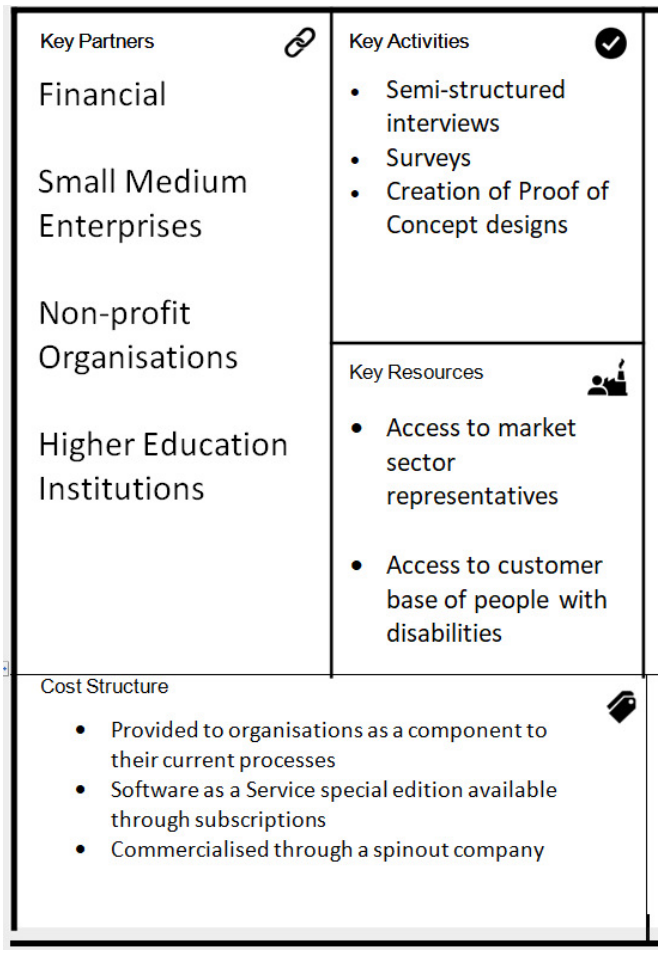


Fig. 2. Extract from the Authentibility Business Model Canvas

Value Proposition canvases were created for each of the customer segments identified in the Authentibility business model: financial institutions, SMEs, non-profit organizations, higher education institutions and customers with disabilities.

Fig. 2 illustrates an extract from The Value Proposition canvas for customers with disabilities when interacting with Authentibility Pass. The gains are increased satisfaction and efficiency with communicating their requirements to organizations and e-businesses. However, there are challenges where customers are concerned about their personal requirements being stored on a system and any technical issues that may occur when retrieving or installing customer data. The main 'job' that is created as a result of Authentibility Pass is organization employees that are aware in advance of their customer requirements. The gains can only be achieved by an efficient system containing a database with customers' authentication and accessibility requirements and the facility for employees to efficiently retrieve customer requirements. To relieve the potential pains for the customers, a database is secured through encryption and password protection and there should be a backup solution in the event of any technical issues with Authentibility Pass, that utilize existing communication methods for customer requirements.

C. Personas

To further understand the type of customer who would use Authentibility Pass, personas were created that describe their interests, personality, skills, dreams and social environments. These also highlighted the reasons why the customer would or would not want to engage with Authentibility Pass. A persona was created for online banking customers with disabilities and specific authentication requirements for an inclusive experience. However, they may not be able to use all authentication methods, e.g. receiving one time codes by SMS due to reduced finger dexterity, but one benefit of the application provides other options they can use. Their 'dream' would be to specify their requirements through an application to enhance their online banking experience. The second persona was created for Receptionists of non-profit organizations who have visitors with accessibility requirements. Receptionists would like to be made aware in advance of any specific requirements of their visitors. Their 'dream' would be to have an application which stores this information for future reference in a database accessed via a web interface. The final persona was created for a customer with a disability who would like to interact with several organizations, communicating their accessibility and authentication requirements. Their 'dream' would be to input these requirements only once into a single application, so that organizations can be informed in advance of their interactions.

.

IV. Market Validation

The Value Proposition for Authentibility was validated with the intended user communities prior to the development of a Proof of Concept Android application, to ascertain any additional functionality that was required to be incorporated.

A. Participants and Procedure

The purpose of the market validation phase was to determine whether there was a need for Authentibility Pass in the domain. The phase included attending an online CyberASAP 'Demo Day' event, which provided the opportunity to obtain preliminary evaluations of Authentibility Pass with industries and potential investors. In addition to this event, separate semi-structured interviews were arranged with the target sectors identified in the Business Model Canvas. It was important to elicit the views from stakeholders in each sector, which covered this range of personas and suitable organizations were identified through our research.

The validation was focused on the UK market, with the view of extending Authentibility Pass to the international market once the Application has been disseminated. Additional target sectors will be considered in future studies, including retail and travel. Table 1 contains details of the organizations involved in this phase. Each was approached with a video call and a semi-structured interview was conducted with the participating employees. The survey questions were centred on the organizations' interaction with customers who have disabilities, including the frequency of interaction, the types of customer requirements recorded, the process of recording requirements, challenges of the current processes and how the organization is informed of changes in customer requirements.

B. Findings

The key results for the target sectors are described below. The participants from semi-structured interviews from each sector highlighted they considered there is a need for Authentibility Pass.

1) 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. One department highlighted that academic staff did not have access to the student record system and are often not aware of specific student needs. A Student Learning Development Manager stated, "The Application could be beneficial to all students with a range of disabilities". Authentibility Pass would provide the benefit of the database being accessible to all university staff, ensuring awareness of specific requirements of students, in order to provide efficient and holistic support. 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.

2) Non-Profit Organizations: 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 customers are currently stored during the registration process for events and the onus is therefore on customers to advise organizations. Regarding accessibility requirements, one organization acknowledged, "It is important should know in advance and it is recognised that this process needs to be improved". Authentibility Pass would be a more efficient solution to communicate requirements, as customers would already have their requirements stored in the Application.

3) Small Medium Enterprises: When organizing events, customers' accessibility requirements are obtained through registration with an event management provider, including their dietary needs. An SME explained "An event is organized and then the delegates' accessibility requirements are checked, but these should be checked beforehand". The requirements are typically held by SMEs until the event has taken place and then deleted. The SMEs stated that Authentibility Pass would be helpful to enable customers to share their accessibility requirements in advance, allowing more efficient planning of events. Authentibility Pass was thought to be a useful addition to their current processes, but as personal data is being stored, it would need to comply with General Data Protection Regulations (GDPR) [18].

4) Financial Institutions: Customers state their accessibility preferences which are tagged to a customer profile by a frontline member of staff. The challenge is that these requirements are selected from a list of options that may not capture individual specific needs. Inconsistencies can be generated when communicating customer requirements between departments of financial institutions due to incompatibility of systems. The Head of Digital Accessibility

at the multi-national bank stated, “There is huge value in standardizing accessibility preferences to drive more inclusive, personalized services”. However, financial institutions would only consider adoption if Authentibility Pass could interact with existing customer databases through an API.

5) User Community: People with disabilities highlighted that there were challenges in communicating their authentication and accessibility requirements to organizations. They often need to repeatedly advise organizations of their requirements when attending events due to their physical and cognitive disabilities, e.g. using a telephone with a speech impairment. The participants saw great benefits in storing their customer requirements only once in the Authentibility Pass application.

V. Design of Concept

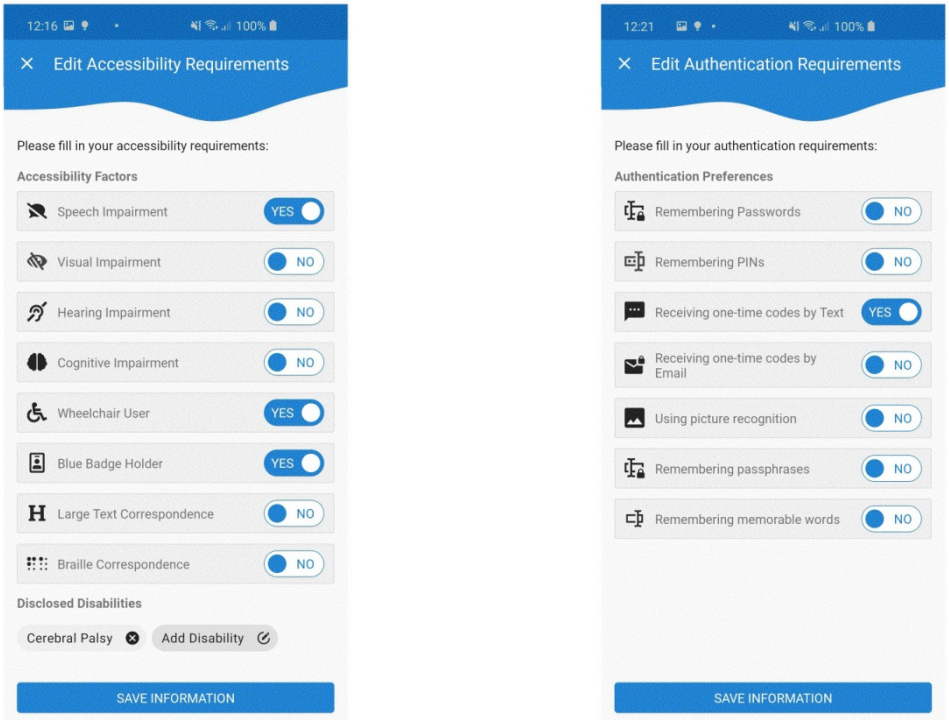
Authentibility Pass is an innovative solution that provides a gateway for people with disabilities, to communicate their authentication and accessibility requirements to organizations and e-businesses. The solution has the following key features:

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

The first stage of the user interface design was to develop storyboard for a user’s journey through the Authentibility Pass application, from inputting their accessibility requirements to sending these to a specific organization. Using the storyboard, wireframe diagrams were subsequently produced illustrating the elements of each user interface. This included input controls, i.e. buttons, checkboxes and text fields, navigational components, i.e. search fields, pagination and breadcrumbs and informational components, i.e. notifications and message boxes. The wireframes highlighted the fields that required validation mechanisms and mandatory fields. The error messages provided to users were also considered in the wireframe diagrams, e.g. if a field is left blank. Best practices of user interface design were followed, including keeping the interface simple to avoid unnecessary errors, maintaining consistency between the interfaces to create efficiency throughout the Application and ensuring the application communicates effectively to the user [18].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 [20].

A. User Interface

The Android Application would be used by people with disabilities, enabling their name and contact details to be entered for the creation of an Authentibility Pass account. Users can enter their accessibility requirements (Fig. 1), including disability type, impairments and specific needs, e.g. Blue Badge holder, through selecting checkboxes with the facility to input additional text information. In the Authentication Requirements section (also shown in Fig. 1), users can state their authentication preferences in terms of the formats to receive one time codes and their abilities to remember passwords and Personal Identification Numbers (PINs). Authentibility Pass will then ascertain the



a Fig. 3. Input of accessibility and authentication requirements through the Authentibility Pass Android application

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 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. Both the authentication and accessibility requirements will be stored in the user's Authentibility Pass account. Users will be able to select organizations from a list to which they can send their accessibility and authentication requirements. Before these are sent, the user enters information for the organization in order to be identified, e.g. account or customer reference number. The benefit of this approach is that the users would be in control of their data and responsible for sending it to the correct organizations of their choice. Token-based authentication transmits the requirements from a user's smartphone to an organization's database, where they are securely stored for future customer interactions. This ensures that the data is encrypted during transmission and only decrypted by the organization with the correct token. The token is created from three components, the header, payload and signature, where the header defines the token type and signing algorithm, the payload consists of the token issuer and expiration details and the signature verifies the authenticity of the transmission. Token-based authentication consists of a five step process: Request, Verification, Token Submission, Storage and Expiration [21]. In step 1, the user's login credentials issues an access request to a server, which is then verified with the login information by using the username and password. The server then generates a signed authentication token, which is valid for a defined period. This is transmitted to the user's application and stored for future visits, when it is decoded and verified. This token remains active until the user logs out or terminates the server connection.

The web interface would be used by organizations to access customer requirements, enabling searches to be performed based on a customer's name or reference number. The web interface would be specific for a particular organization, allowing all customer requirements to be viewed. Organization details can also be updated through the web interface and employees can view specific requirements of customers, in order to determine the most suitable method of interaction.

The private Authentibility Pass API is designed for organizations 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. The key is not publically available to maintain the integrity of Authentibility Pass. The API receives requirements sent from the Authentibility Pass application and transmits these to an organization's database system in a range of compatible file formats, e.g. Comma Separated Variables (CSV) files, which are appended to their existing customer records.

VI. Premliminary Evaluations

Authentibility Pass was presented at the CyberASAP Demo Day event, organized to showcase products to potential investors. The preliminary evaluations highlighted the key areas that will need to be considered during the dissemination of Authentibility Pass.

A. Participants and Procedure

The Proof of Concept was demonstrated live and supported by a pre-recorded video [21]. The virtual event was held on the Zoom platform and attended by approximately 200 investors with a range of backgrounds, including cyber security and finance. The investors were invited to a series of 20 minutes sessions, with each of the teams participating in the CyberASAP programme. During each session, the Proof of Concept was demonstrated live and there were opportunities for discussions with the investors. These discussions were seen as preliminary evaluations of Authentibility Pass that highlighted areas of consideration in the future development.

B. 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 in the financial sector, integration with existing systems would be paramount, as this sector would need to protect 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. This would verify the user and allow access to bank services through Authentibility Pass. The advantage to financial institutions is that customers' data can remain stored on their systems and accessed through the API. The financial institutions suggested that the application could provide authentication and accessibility recommendations to customers with disabilities, based on their requirements.

C. Deployment

A domain expert in cyber security highlighted that organizations responsible for defining standards for cryptographic authentication protocols, should be approached prior to deployment of Authentibility Pass. This would ensure standards are achieved in order for customers' data to be protected. As the Proof of Concept uses token based authentication to transmit user data, Authentibility Pass would only be suitable for organizations that currently use this form of authentication. Other methods of data transmission should be considered as future developments to maximise the number of potential organizations who can use the Application.

D. 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 access rights to the data. To ensure 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 data is being shared with an organization. This statement should include the intended use of information and the maximum storage duration.

GDPR will need to be adhered to, as Authentibility Pass stores personal customer information. For the financial sector, the multi-national bank suggested that a unique identification number would be required to obtain customer requirements. They advised that a customer's account number and sort code should not be used for identification through Authentibility Pass, as transmission of this data is sensitive. An alternative could be to use the customer's online banking number to protect account information.

VII. Discussion

Authentibility Pass will benefit people with disabilities, 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 organizational databases. It is anticipated that the adoption of the solution will increase the awareness of employees of how best to support their customers with disabilities, resulting in higher levels of customer satisfaction. Authentibility Pass will also assist organizations who comply with equality policies, such as the Accessibility Regulations 2018 [23] in the UK.

The first phase of the development involved creating The Business Model and Value Proposition canvases. This was important to determine the target sectors for the application and how each type of customer would benefit from Authentibility, as well as the challenges of adopting the technology. This phase also established an initial revenue model where the application would be provided through tiered licensing. The income generated from the licenses would be used to fund the ongoing maintenance costs of the application, including future updates.

Once the business model and value proposition were established, the Authentibility Pass Proof of Concept was developed based on a market validation phase involving the target market sectors of higher educational institutions, schools, non-profit organizations, SMEs and financial institutions, which informed the creation of the requirements specification. Personas were generated that were used to identify the participants for the market validation. This two-phase approach enabled feedback to be elicited from stakeholders in the potential market sectors. Organizations were approached with a semi-structured interview regarding the current challenges of their customers with disabilities communicating their authentication and accessibility requirements and all expressed positive feedback regarding Authentibility Pass.

It was highlighted by all of the participating organizations that their customers with disabilities had to repeatedly inform them of their requirements, which is time consuming and they acknowledged the need for Authentibility Pass. However, most organizations emphasise that GDPR would need to be followed prior to potential adoption. This has been incorporated into the design of Authentibility Pass by ensuring that users are in control of their own data and responsible for transmitting their authentication and accessibility requirements to the correct organization. There is an additional check before requirements are sent, where users are required to enter their customer ID number for a particular organization. Token-based authentication encrypts the data during transmission and only the recipient organization has the required token to decrypt their customers' requirements. The market validation discovered that there is a need for this type of application to assist customers with communicating requirements.

The Proof of Concept comprises of an Android Application, database, web interface and API that provides a gateway for people with disabilities to communicate their requirements to organizations and e-businesses. An example use case of Authentibility Pass is an event management organization where the application would be useful for visitors who could inform organisers in advance of their accessibility needs, e.g. parking and dietary requirements. The advantage is that users would only be required to enter their information once into the application and select the organizations they would like to share this with. The requirements will then be stored in the organization database enabling employees to access visitors' accessibility requirements through the web interface. The application would also remind customers to check their information is up to date, to maintain an accurate record for organizations.

Presenting Authentibility Pass at the CyberASAP Demo Day highlighted key areas for consideration during the future dissemination of Authentibility Pass to the financial, SME, non-profit and higher education sectors. Integration with financial institutions will be achieved through the API, allowing customer requirements to be exported in various file formats, e.g. text documents and CSV files. Authentibility Pass will adhere to authentication protocols, to maintain security of customer data. To satisfy GDPR principles, the users of Authentibility Pass will be in control of their own data and responsible for sharing this with the appropriate organizations. It is acknowledged that one of the key challenges of Authentibility Pass is the integration with third party systems, such as banking, front of house and event management. During the dissemination of Authentibility Pass, it will be necessary to have discussions with the Information Technology departments of interested organizations, to facilitate integration of the application with their existing systems and infrastructure.

VIII. Conclusions and Future Work

Developing the value proposition and conducting market validation has illustrated there is a significant interest in Authentibility Pass to assist people with disabilities informing organizations and e-businesses 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. Authentibility Pass will improve the satisfaction of customers with disabilities, as organizations will become more aware of their authentication and accessibility requirements. This will be achieved through dissemination to financial institutions, SMEs, non-profit organizations and higher educational institutions.

The feedback received from potential investors at the CyberASAP Demo Day will be addressed in future iterations of the Authentibility Pass development. Potential integration with the open banking platform through the API will be investigated. Open banking provides third party financial service providers open access to consumer banking and transaction data from banks and financial institution. It is becoming one of the major domains for innovation in the banking sector. Usability evaluations will be conducted with the user community involved in the market validation, as well as additional representatives from the market sectors. Authentibility Pass will be disseminated to the participants with the Proof of Concept transmitting data 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) [24] and NASA Task Load Index (TLX) [25]. This will determine whether Authentibility Pass provides an efficient method of communicating customers' authentication and accessibility requirements. Using SUS, participants can rate 10 statements

on a five point scale from ‘Strongly Disagree’ to ‘Strongly Agree’. This allows a single score to be calculated for the overall usability of Authentibility Pass which can be interpreted using the Adjective Rating Scale [26] in terms of ‘Poor’, ‘Good’ or ‘Excellent’ usability. NASA TLX provides measurements of Physical, Mental, Temporal, Performance, Effort and Frustration demands and can be implemented with a minimal amount of training, using a smartphone application developed by NASA. Organizations in the target markets would be approached for potential adoption of Authentibility Pass into their current processes, for interacting with customers who have disabilities. The possibility of integrating the application with existing verification mechanisms and event management platforms would also explored, such as the UK Government Gateway User ID, Eventbrite and TicketMaster. Revenue streams would be established with different licensing packages based on the type of organization. Free trials would initially be provided to organizations with a maximum number of requirements transmissions and full functionality provided through an annual subscription. The API would be provided as a monthly cost to organizations with existing database systems, exporting requirements in a variety of file formats. An iOS implementation of the application will be developed to increase the number of supporting organizations and users with disabilities.

Through dissemination and employment of Authentibility Pass, it is envisaged that Authentibility Pass will become a gateway for people with disabilities to communicate their authentication and accessibility requirements, resulting in increased customer satisfaction.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of Vers Creative UK, to develop and test the Authentibility Pass Android Application, database, web interface and application Programming Interface. would also like to thank the UK Government Department for Digital, Culture Media & Sport (DCMS) in collaboration with Innovate UK for funding this research, through the Cyber Security Academic Startup Accelerator Programme (CyberASAP). also acknowledge the support of the participants involved in the background research.

REFERENCES

[1] The World Bank. “Disability Inclusion”. The World Bank. https://www.worldbank.org/en/topic/disability (accessed Aug. 5, 2023).

[2] N. Kostanjsek, “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, vol. 11, no. 4, pp. 1-6, May 2011.

[3] Assistive Technology Industry Association. “What is AT?”. ATIA. https://www.atia.org/at-resources/what-is-at/ (accessed Aug. 5, 2023).

[4] P. Whittington, H. Dogan, K. Phalp and N. Jiang, N. “Detecting physical abilities through smartphone sensors: an assistive technology application,”, Disability and Rehabilitation: Assistive Technology, vol. 17, no. 8, pp. 974-985, Nov. 2022.

[5] World Wide Web Consortium. “Understanding Success Criterion 3.3.7: Accessible Authentication”. W3C. https://www.w3.org/WAI/WCAG21/Understanding/accessible-authentication (accessed Aug. 5, 2023).

[6] K. Helkala, “Disabilities and Authentication Methods: Usability and Security”, Proc. Int. Conf. Availability, Reliability Security, Prague, 20-24 Aug. 2011.

[7] World Health Organization. “International Classification of Functioning, Disability and Health (ICF)”. WHO. https://www.who.int/standards/classifications/international-classification-of-functioning-disability-and-health (accessed Aug. 5, 2023).

[8] Wang, Y. (2014) Universal Authentication: Towards Accessible Authentication for Everyone. 10th Symposium on Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, 9-11 July 2014. ACM Press, New York, NY

[9] Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F. (2012) The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. 2012 IEEE Symposium on Security and Privacy (SP 2012), San Francisco, CA, 24-25 July 2012, 553–567. IEEE Press, New York, NY.

[10] Porter, S.N. (1982) A password extension for improved human factors. Computers Security, 1, 54-56.

[11] Kuber, R. and Sharma, S. (2010) Toward tactile authentication for blind users. The 12th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS ’10), Orlando, FL, 24-26 October 2010, 289-290. ACM Press, New York.

[12] iProov. “Authenticate & Onboard Online Users Securely”. iProov. https://www.iproov.com/ (accessed Aug. 5, 2023).

[13] Be My Eyes. “Bringing sight to blind and low-vision people”. Be My Eyes. https://www.bemyeyes.com/ (accessed Aug. 5, 2023).

[14] EnSpire Oxford. “Business Model Canvas Explained”. University of Oxford. https://eship.ox.ac.uk/business-model-canvas-explained/ (accessed Aug. 5, 2023).

[15] Strategyzer. “The Business Model Canvas”. Strategyzer AG. https://www.strategyzer.com/canvas/business-model-canvas (accessed Aug. 5, 2023).

[16] B2B International. “What is the Value Proposition Canvas?”. B2B International. https://www.b2binternational.com/research/methods/faq/what-is-the-value-proposition-canvas/ (accessed Aug. 5, 2023).

[17] Strategyzer. “The Value Proposition Canvas”. Strategyzer AG. https://www.strategyzer.com/canvas/value-model-canvas (accessed Aug. 5, 2023).

[18] Intersoft Consulting. “General Data Protection Regulation GDPR”. Intersoft Consulting. https://gdpr-info.eu/ (accessed Aug. 5, 2023).

[19] Usability.gov. “User Interface Design Basics”. Usability.gov https://www.usability.gov/what-and-why/user-interface-design.html (accessed Aug. 5, 2023).

[20] Statcounter. “Mobile Operating System Market Share Worldwide: June 2022 - July 2023”. Statcounter. https://gs.statcounter.com/os-market-share/mobile/worldwide (accessed Aug. 5, 2023).

[21] Fortinet, “Authentication Token”. Fortinet. https://www.fortinet.com/resources/cyberglossary/authentication-token#:~:text=Tokens%20are%20encrypted%20and%20machine,tampered%20with%20and%20block%20it (accessed Oct. 6, 2023).

[22] Knowledge Transfer Network. “Authentibility Pass Demonstration Video”. https://vimeo.com/showcase/8146645/video/513400390 (accessed Aug. 5, 2023).

[23] HM Government. “Understanding accessibility requirements for public sector bodies”. HM Government. https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps (accessed Aug. 5, 2023).

[24] J. Brooke, “SUS: A 'Quick and Dirty' Usability Scale,” in Usability Evaluation In Industry, P. W. Jordan, B. Thomas, I. L. McClelland and B. Weerdmeester, Eds. London: Taylor & Francis, 1996, pp.189– 194.

[25] National Aeronautics and Space Administration. “NASA TLX: Task Load Index”. NASA. https://humansystems.arc.nasa.gov/groups/tlx/ (accessed Aug. 5, 2023).

[26] A. Bangor, P. Kortum and J. Miller, “Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale,”, J. User Experience, vol. 4, no. 3, pp. 114-123, May 2009.