Guidance for Making FIDO Deployments Accessible to Users with Disabilities

August 2022

Editor:
Yao Ding, Meta

Abstract

In achieving FIDO Alliance's mission of more secure and password-free authentication, we must ensure the needs and preferences of people with disabilities—an estimated 15% of the world's population—are taken into account. This white paper is intended to provide guidance on planning FIDO deployments accessible to users with a wide range of disabilities.

Audience

This white paper is intended for information security executives, product owners, identity and access management, attorneys, accessibility practitioners, and others who are considering deploying FIDO Authenticators across their enterprises. This white paper may also help hardware manufacturers identify opportunities to deliver more accessible external authenticators.

Contents

Figures

1. Introduction

The World Health Organization (WHO) estimates 15% of the world's population, or over one billion people, live with some form of disability[1]. In many countries, laws prohibit discrimination against people with disabilities (PwD) to help ensure PwD fully and equally participate in every aspect of society. For example, 52 constitutions of the 193 United Nations member states explicitly guarantee equality or nondiscrimination on the basis of disability[2]. Digital access has become increasingly important to many aspects of society, including, but not limited to, education, employment, and entertainment. Authentication, allowing private and secure access to these services, has become equally important.

Security codes delivered via text message or email are technically "accessible," but they often require an advanced level of skill and knowledge for PwD using assistive technology to transfer the codes. FIDO technology is best positioned to simplify this process and provide accessible authentication, as it supports a wide range of options that can accommodate vastly diverse needs of PwD.

This white paper provides guidance on planning FIDO deployments accessible to users with a wide range of disabilities. This white paper also helps hardware manufacturers identify opportunities to deliver more accessible external authenticators.

2. Legal Framework for Accessible Authentication

Accessibility practices are often grounded in legal threshold requirements applicable to a company's products. The laws, however, are often intentionally ambiguous as to "how" to achieve accessibility goals—the laws obligate companies to make products accessible to address disability needs, but do not offer specific guidance or technical details. Consequently, legal requirements effectively set baseline principles to guide companies directionally in developing accessible products, rather than offering specific criteria for accessibility development and implementation.

This section provides examples instead of a comprehensive list of laws relevant to accessible authentication. RPs (Relying Parties) are advised to consult legal professionals regarding which requirements apply and how to conform.

[1] "Disability and Health," World Health Organization, November 24, 2021, https://www.who.int/news-room/fact-sheets/detail/disability-and-health.
[2] "Does the constitution explicitly guarantee equality or non-discrimination for persons with disabilities?" World Policy Center, accessed May 5, 2022, https://www.worldpolicycenter.org/policies/does-the-constitution-explicitly-guarantee-equality-or-non-discrimination-for-persons-with-disabilities

2.1 Web Content Accessibility Guidelines (WCAG)

WCAG is an extensive set of accessibility guidelines developed by W3C, an international community that develops open standards to ensure the long-term growth of the web. Although WCAG was originally designed as web content standards, it has become well-recognized and accepted as an appropriate guide for non-web products as well. While WCAG is normative, many obligatory accessibility standards in various countries directly refer to WCAG or mirror WCAG criteria.

WCAG conformance pertaining to authentication is twofold:

1. ***WCAG Conformance of Authentication UI.*** Authentication UI, as part of the product experience, should be created in conformance with WCAG along with other parts of the product. The goal is to ensure authentication UI meets the baseline of being functional to PwD and compatible with assistive technologies. WCAG Level AA is often the conformance level to be fully met. Companies have various ways of achieving WCAG conformance: internal tooling and processes to support accessible design and development, external accessibility audits to identify non-conformance and provide remedial actions, and usability testing with PwD across a spectrum of abilities.

2. ***WCAG 3.3.7 "Accessible Authentication" Conformance.*** There is a proposed "Accessible Authentication" guideline in WCAG version 2.2 Success Criterion 3.3.7[3]. The guideline states:

   > *"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.*
   >
   > *Exception: When the cognitive function test is to recognize objects, or content the user provided to the website.*
   >
   > *NOTE*
   >
   > *Objects and content for the exception may be represented by images, text, video or audio.*
   >
   > *Examples of mechanisms include: 1) support for password entry by password managers to address the memorization cognitive function test, and 2) copy and paste to help address transcription cognitive function test."*

The purpose of this guideline is to ensure there is an alternative to remembering a site-specific password (a cognitive function test). WCAG provides a few examples of ways to follow the guideline, which include FIDO offerings:

[3] Web Content Accessibility Guidelines (WCAG) 2.1 is currently the latest official version of W3C accessibility recommendation. As of the publication date of this white paper, WCAG 2.2 is a working draft, and its content is subject to change before it becomes an official W3C recommendation. RPs should refer to the latest WCAG 2.2 language: https://www.w3.org/TR/WCAG22/

- *Allow for autofill by third-party password managers.* A website uses a properly marked up username (or email) and password fields as the login authentication. The user's browser or integrated third-party password manager extension can identify the purpose of the inputs and automatically complete the username and password.

- *Allow for pasting passwords.* A website does not block paste functionality. The user can use a third-party password manager to store credentials, copy them, and paste them directly into a login form.

- *Use WebAuthn.* A website uses WebAuthn so the user can authenticate with their device instead of a username/password. The user's device could employ any available modality. Common methods on laptops and phones are facial-scan, fingerprint, and PIN. The website is not enforcing any particular use; it is assumed a user will set up a method that suits them.

- *Use OAuth.* A website offers the ability to log in with a third-party provider using the OAuth framework.

- *Use two-factor authentication.* A website requiring two-factor authentication allows multiple options for the second factor, including the following: a USB-based method where the user simply presses a button to enter a time-based token; a QR code display, which can be scanned by an app on a user's device to confirm identity; or a notification sent to a user's device and the user operates their device's authentication mechanism (e.g., user-defined PIN, fingerprint, or facial recognition) to confirm identity.

W3C Accessibility Task Force has clarified[4]:

- Providing any current FIDO Authentication methods in addition to the username/password mechanism as an alternative will automatically pass 3.3.7 (assuming FIDO Authentication does not rely on cognitive function testing).

- When passwordless authentication is provided, as long as the passwordless authentication does not rely on a cognitive function test, it also conforms to WCAG.

2.2 Global Accessibility Laws

While WCAG is normative, many laws from various countries incorporate principles similar to those espoused in WCAG. Below is a non-exhaustive list of accessibility laws that may be applicable to an RP's products, including the products' authentication experiences.

- Americans with Disabilities Act (ADA). Title III of ADA requires places of public accommodation within the U.S. to be accessible to PwD. By its terms, the ADA applies only to physical spaces, but courts have increasingly—though inconsistently—applied the ADA to websites, apps, and online storefronts.

[4] See W3C Accessibility Task Force clarification in this GitHub issue: https://github.com/w3c/wcag/issues/2052.

- Section 504 & Section 508 of the Rehabilitation Act of 1973. Section 504 prohibits discrimination against PwD in any program or activity receiving financial assistance from the U.S. federal government. Section 508 stipulates any electronic or information technology developed, procured, maintained, or used by the federal government must be accessible. Consequently, federal agencies generally require that companies from which they purchase technology must also comply with Section 508. To this end, companies typically provide government customers with a document called an ACR (Accessibility Conformance Report) stating how each product addresses accessibility. Furthermore, technology covered by Section 508 aligns with WCAG compliance.

- 21st Century Communications and Video Accessibility Act (CVAA). The CVAA is a U.S. law enforced by the Federal Communications Commission (FCC) applying to products providing "advanced communications services" such as Voice over Internet Protocol (VoIP, i.e., online calling or multiplayer voice chat), messaging services, video chat or conferencing services, and similar online communications.

- European Accessibility Act (EAA). The EAA became law in 2019, and it is designed to introduce common rules on accessibility across the EU to reduce costs for businesses, facilitate easier cross-border trading, and provide market opportunities for accessible products and services.

- Accessible Canada Act (ACA). The ACA is Canada's federal legislation requiring federal entities and regulated industries (e.g., telecom and banking) to procure and offer accessible information technology and communications technology, and will subject covered entities to new reporting requirements.

- Japanese Industrial Standards (JIS) X 8341-3. JIS X8341-3 provides guidance for both public and private sector organizations on compliance with WCAG in Japan.

3. Current Models of Accessible FIDO Authentication

Current FIDO Authentication deployment of RPs largely follows unique models for both of FIDO's authentication protocols, the WebAuthn model, and the UAF (Universal Authentication Framework) model. A key difference between WebAuthn and UAF is the RP's level of control over authentication modalities. In the context of WebAuthn, RPs are unlikely to, and should not, discriminate based on modalities, even though it is technically possible. While in UAF, RPs are able to define which modalities are available to end users. We discuss the two models separately as they require different considerations with regards to accessible deployment.

3.1 What is WebAuthn?

Web Authentication (WebAuthn) is a core component of FIDO2 and a web standard published by W3C. WebAuthn provides a standardized interface for authenticating users to web-based applications and services using public-key cryptography.

3.2 Responsibility Model & Deploying Accessible WebAuthn

Figure 1 - WebAuthn Model of Accessible Authentication

There are three parties in the WebAuthn model of accessible authentication responsibility:

- End users with disabilities
- User agents: any software or hardware, including assistive technologies, that help in retrieving, rendering, and interacting with RP's applications (e.g., mobile phones, browsers, screen readers, and other non-mouse interactions)
- RP's applications, including the authentication parts of the applications

Each party is partly responsible for an accessible authentication experience.

- **End users** choose user agents most accessible to themselves. The onus is on end users to choose the user agents supporting authenticators they are able to use.
    - End users may buy smart phones that come with face recognition, a fingerprint reader, and similar biometric components. It is assumed end users would choose devices and set up authentication methods suiting their accessibility needs and preferences.
    - End users may buy security keys from the market. Similarly, it is assumed end users would choose security keys that suit them.
- **User agent developers** create UAAG-conforming user agents. By conforming to User Agent Accessibility Guidelines (UAAG), user agent developers make user agents more accessible to PwD and compatible with assistive technologies. WebAuthn rendered on such user agents will be accessible as well.

- **User agent developers** and the **W3C WebAuthn Working Group** ensure compatibility between user agents and WebAuthn.
    - As WebAuthn has become a widely accepted authentication model, it is supported by most popular user agents. If incompatibility is detected, RPs are advised to file an issue to the W3C WebAuthn Working Group and alert user agent developers.
- **Responsibility of RPs**
    - **RPs** ensure their applications are compatible with user agents that support WebAuthn.
    - **RPs** create accessible hardware (ATMs, ticketing kiosks), software (webpages, mobile apps), and training materials (text or multimedia) by practicing widely adopted accessibility guidelines (e.g., WCAG, Section 508, EN 301 549). RPs may be required to produce a completed ACR identifying how the product complies or does not comply with these standards. End-to-end testing with PwD and people using assistive technologies is strongly encouraged to validate interactions leading up to and through the authentication process, which will help ensure the entire user flow is accessible to the widest audience.
    - **RPs** conform to WCAG 3.3.7 by providing at least one method of authentication not relying on cognitive function tests. Supporting WebAuthn automatically meets WCAG 3.3.7 requirements because WebAuthn is a "sufficient technique." See WCAG 3.3.7 "Accessible Authentication" Conformance.
    - When providing hardware directly to end users (e.g., company providing hardware to employees, or financial institutions providing hardware to end users), RPs should provide options for end users to choose those with authenticators accessible to them. If no option is accessible to the user, the RP should provide alternative authentication means.
        - If it is impractical for RPs to solicit user selection, RPs should conform to Section 508 Provision 403, which states, "Where provided, biometrics shall not be the only means for user identification or control. EXCEPTION: Where at least two biometric options that use different biological characteristics are provided, ICT shall be permitted to use biometrics as the only means for user identification or control."

3.3 What is FIDO UAF?

The FIDO UAF protocol allows online services to offer passwordless and multi-factor security. The user registers their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, speaking into the mic, or entering the PIN, for example. The UAF protocol allows the service to select which authenticators are presented to the user (Figure 3) for selection, which is a key difference between this model and the WebAuthn model.

Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows combining multiple authentication mechanisms such as fingerprint + PIN.

3.4 Responsibility Model & Deploying Accessible UAF

Figure 2 – UAF Model of Accessible Authentication

For accessible UAF deployment, RPs should adopt the following recommendations for UAF policy control:

1. Mobile apps should always allow phone-unlocking authentication as an option.

    a. WebAuthn supports phone-unlocking authentication. UAF is a more flexible model and should support phone-unlocking modalities as a fallback. As stated previously in the WebAuthn discussion, the onus is on end users to choose user agents supporting authenticators they are able to use.

2. Mobile apps should allow silent authentication as much as is feasible.

    a. "Silent Authentication" on smart phones and smart watches provides a strong (phishing resistant) possession factor authentication using the standardized FIDO protocol. With this technology, mobile native applications could simply authenticate the user by trusting the device. Some information may be available to users without requiring additional actions (e.g., showing the account balance on the user's device).
    b. We recommend RPs take advantage of silent authentication because it allows smoother UX for all people, including PwD. However, silent authentication should not be offered to PwD as a more accessible but less secure option. Instead, it should be an option equally accessible and equally secure for all users.

3. Phone-unlocking authentication should be allowed as a fallback/substitute for less secure modalities.

4. When the mobile app requires *one* biometric authentication, the mobile app must provide *two or more* biometric options requiring different physiological characteristics.

    a. Example: If voice authentication is required, the mobile app must allow the user to authenticate through another biometric option not requiring voice, such as face recognition or fingerprint.

5. When the mobile app requires *more than one* (N) biometric authentication modality, the mobile app must provide at least N+1 biometric options requiring different physiological characteristics.

    Note: Points 4 and 5 above may be implemented by providing an option to load custom authenticators.

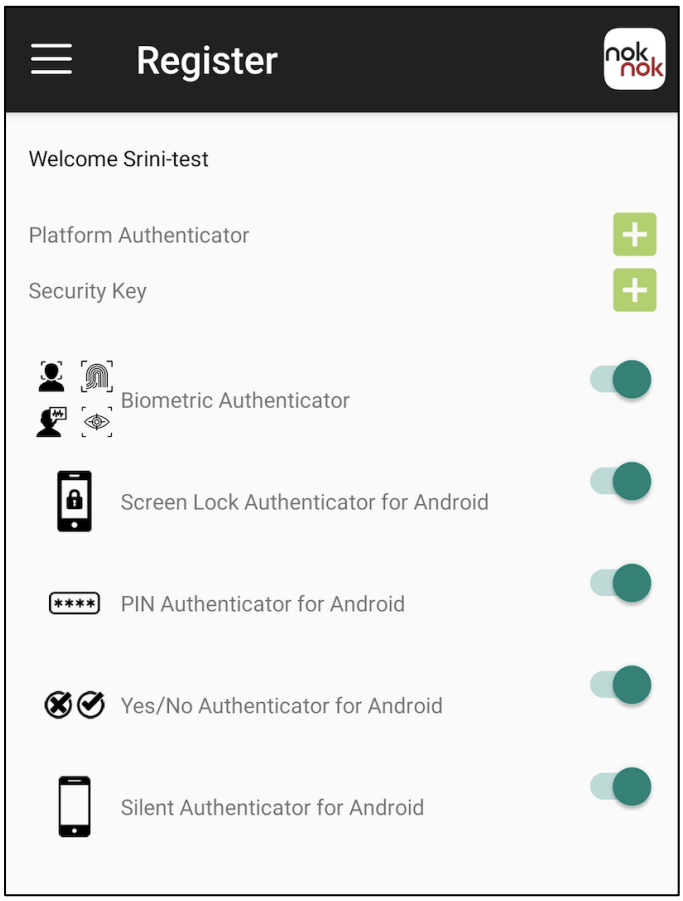

Figure 3 – Mobile App Authentication that uses UAF protocol, allowing the service to select authenticator (example)

4. Unique Aspects of FIDO Authentication Related to Disabilities

Each FIDO Authentication feature may pose barriers to users with certain types of disabilities. We provide a mapping for RPs to understand potential barriers each authentication modality may cause. RPs may use the mapping to identify modality provisionings that are accessible to as many users as is practical. This is a guide and not intended as an exhaustive list of considerations.

4.1 Disabilities Pertaining to FIDO Authentication

Disabilities are vastly diverse. For simplicity in the discussion of FIDO Authentication, we refer to the following five types of disabilities that appear to be most relevant to authentication.

1. **Visual**: blindness, low vision, visual field loss, color blindness, and/or iris loss

2. **Hearing**: profound deafness, hearing muffled sounds, hearing with one ear, and/or other sounds interfering with hearing

3. **Physical**: limb loss, digit loss, limited strength or weakness, limited reach, tremor or palsy, loss of fingerprints, and/or loss of facial features

4. **Speech**: loss of speech, trouble speaking loud enough, and/or trouble being understood

5. **Cognitive and learning**: difficulty reading (dyslexia), difficulty writing, memory loss, low literacy, low digital literacy, and/or difficulty reasoning

4.2 FIDO Authentication Features

From a user experience perspective, FIDO Authentication can be categorized by user interactions:

- Touch
  - Touch security key for user presence check
- Type
  - Type client PIN or screen-unlocking PIN
- Scan
  - Fingerprint scan
  - Vein scan
  - Iris scan (look into camera)
  - Face scan
- Speak
  - Voice recognition

- Move
  - Insert a security key in a USB port
  - Scan security keys via NFC with smart phones
  - Draw a pattern on screen to unlock smart phones
  - Activate buttons for actions
  - Touch screen for selecting actions
  - Use mouse or alternative input devices for selecting actions
  - QR code scan for pairing a device
- Read
  - Instructions on screen
- Timer
  - Complete authentication within limited time

4.3 Potential Access Barriers in FIDO Authentication

This section summarizes the difficulties for PwD for each user interaction. RPs who are deploying FIDO Authentication should understand these difficulties. A mapping between FIDO Authentication methods and disabilities can be found in Table 1.

- Touch
  - People with physical disabilities may have difficulty in reaching or accurately targeting security keys, especially small keys or keys with small, depressed, active touch areas.
- Type
  - Memorizing a username and password (or transcribing either manually) may place a burden on people with certain cognitive disabilities and people using assistive technology.
  - The process of entering passwords, either on a mobile device or on a webpage, can be more accessible by implementing password interfaces meeting WCAG compliance.
- Scan
  - Scan of physiological characteristics may pose barriers to people who do not have these physiological characteristics. For example, people with digit amputations or adermatoglyphia (a genetic disorder preventing the development of fingerprints) may not be able to use fingerprint authentication. People with excessively dry skin are also likely to fail fingerprint scans. Some blind users may not be able to use iris recognition or facial recognition that requires open eyes, or for the users to look at the camera.
  - Users with visual disabilities may also find it difficult to locate a scanner and scan security keys via NFC with smart phones.
- Speak
  - Voice recognition may not work well for people with speech and language disabilities. Some deaf and hard of hearing people who do not use oral communication may not be able to use voice recognition either.

- Move
    - People with physical disabilities may not be able to insert a security key in a USB port, scan a security key on a smart phone, or draw a pattern on a smart phone.
    - People with certain cognitive disabilities may find it difficult to memorize a pattern gesture to perform on a touchscreen.
    - QR code scanning can be challenging for users with visual disabilities. Such users may find it difficult to locate a QR code and position a camera to scan the code. QR code can also be difficult for people with physical disabilities because it requires the user not only to hold a camera, but also to hold it steady.
- Read
    - People with certain learning disabilities, people with low literacy or low digital literacy, or people with memory issues may find instructions about authentication difficult to understand. Instructions can be made more accessible by following the WCAG Cognitive Accessibility Guidelines.
- Timer
    - Some PwD may need more time to complete authentication: they may take longer to physically respond, they may take longer to read things, they may have low vision and take longer to find things or to read them, or they may be accessing content through an assistive technology that requires more time. WCAG provides a set of guidelines on providing users enough time to read and use content. Except in cases where the time limit is essential and extending the time limit would invalidate the authentication, RPs may allow users to turn off, adjust, or extend the time limit. See WCAG Success Criterion 2.2.1 Timing Adjustable for more details.

Table 1 Unique Aspects of FIDO Authentication for People with Disabilities: Potential issues

Note: A narrative version of this table is available on page 20.

User Gesture		Visual	Hearing	Speech and Language	Physical	Cognitive and Learning
Actions	FIDO Feature Examples	Likelihood to encounter barriers	Likelihood to encounter barriers	Likelihood to encounter barriers	Likelihood to encounter barriers	Likelihood to encounter barriers
1. Touch	Touch security key for user presence check	Less	Less	Less	More	Less
	Draw a pattern on screen to unlock smartphones	Less	Less	Less	More	More
2. Type	Type client PIN	Less	Less	Less	Less	More
	Type screen unlock PIN	Less	Less	Less	Less	More
3. Scan	Fingerprint on scanner	Less	Less	Less	More	Less
	Vein	Less	Less	Less	More	Less
	Iris (look into camera)	More	Less	Less	Less	Less
	Face (camera)	More	Less	Less	Less	Less
	QR code (caBLE) screen & camera	More	Less	Less	More	More
4. Speak	Speaker recognition	Less	More	More	Less	Less
5. Move	Insert a security key in a USB port	Less	Less	Less	More	Less
	Scan security keys via NFC with smartphones	More	Less	Less	More	Less
	Click buttons for actions	Less	Less	Less	More	Less
	Touch screen for selecting actions	Less	Less	Less	More	Less
	Use mouse for selecting actions	More	Less	Less	More	Less
6. Read	Instructions on screen	Less	Less	Less	Less	More
7. Timer	Time limits in enrollment, registration, or authentication	More	Less	Less	More	More

5. Principles of Deploying Accessible Authentications

The following principles are guidance for RPs when they deploy FIDO Authentication for PwD.

Principle #1: RPs should design and implement authentication user interfaces and training materials to meet WCAG (Web Content Accessibility Guidelines) Level AA. Conduct user testing with users with various types and degrees of disabilities.

> *Rationale: RPs can make user interfaces before, during, and after the authentication process more accessible by meeting WCAG Level AA and by engaging users with disabilities in user testing.*

Principle #2: When implementing WebAuthn, RPs should not discriminate based on authentication modalities. Non-discriminating WebAuthn would automatically pass WCAG 3.3.7 Accessible Authentication.

> *Rationale: As described in the WebAuthn Responsibility Model, the onus is on end users to choose user agents with authenticators they are able to use, and the onus is on user agent developers and WebAuthn developers to ensure compatibility between user agents and WebAuthn. An RP's responsibility in implementing WebAuthn is to ensure WebAuthn does not discriminate based on authentication modalities.*

Principle #3: When implementing UAF, RPs should comply with the guidelines described in the UAF Responsibility Model.

> *Rationale: RPs are able to choose which authentication modalities are provided via UAF and allow users to choose modalities. Given the extra flexibility, RPs should take some important factors into considerations, including the use of phone-unlocking authenticator as fallback, the use of silent authentication, and requiring one or more than one modalities of biometric authentication.*

6. Acknowledgments

The author acknowledges the following people (in alphabetic order) for their valuable feedback and comments:

John Bradley, Yubico
Elisa Duarte, Visa Inc.
Max Hata, NTT DOCOMO
Srini Kanugovi, Nok Nok
Bill Leddy, LoginID
Rolf Lindemann, Nok Nok
Joyce Oshita, VMware
Marcel van Kleef, ING Group
Jin Wen, JP Morgan Chase Bank

7. Glossary

ACR	Accessibility Conformance Report based on the ITI VPAT®
NFC	Near Field Communication
OAuth	Open Authorization
PwD	People with disabilities
QR	Quick Response
RP	Relying Parties
UAAG	User Agent Accessibility Guidelines
UAF	Universal Authentication Framework
UI	User Interface
VoIP	Voice Over Internet Protocol
WCAG	Web Content Accessibility Guidelines
WebAuthn	Web Authentication

8. References

Campbell, Alastair (@alastc), and Yao Ding (@yao-ding). "WebauthN and passwordless #2052." GitHub, September 23, 2021: https://github.com/w3c/wcag/issues/2052.

"Disability and Health." World Health Organization. November 24, 2021. https://www.who.int/news-room/fact-sheets/detail/disability-and-health.

"Does the constitution explicitly guarantee equality or non-discrimination for persons with disabilities?" World Policy Center. Accessed May 5, 2022. https://www.worldpolicycenter.org/policies/does-the-constitution-explicitly-guarantee-equality-or-non-discrimination-for-persons-with-disabilities.

Employment and Social Development Canada. "Summary of the Accessible Canada Act." November 20, 2021 https://www.canada.ca/en/employment-social-development/programs/accessible-people-disabilities/act-summary.html.

European Commission. "European Accessibility Act." Accessed May 5, 2022. https://ec.europa.eu/social/main.jsp?catId=1202&langId=en.

Federal Communications Commission. "Twenty-First Century Communications and Video Accessibility Act." April 12, 2022. https://www.fcc.gov/general/twenty-first-century-communications-and-video-accessibility-act-0.

"FIDO2: Web Authentication (WebAuthn)." FIDO Alliance. Accessed May 5, 2022. https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/.

U.S. Access Board Information and Communication Technology. "Revised 508 Standards and 255 Guidelines." January 18, 2017. https://www.access-board.gov/ict/#403-biometrics.

U.S. Department of Justice. "Americans with Disabilities Act Title III Regulations." January 17, 2017. https://www.ada.gov/regs2010/titleIII_2010/titleIII_2010_regulations.htm.

U.S. Department of Labor. "Section 504, Rehabilitation Act of 1973." Accessed May 5, 2022. https://www.dol.gov/agencies/oasam/centers-offices/civil-rights-center/statutes/section-504-rehabilitation-act-of-1973.

U.S. Department of Labor. "Section 508, Rehabilitation Act of 1973." Accessed May 5, 2022. https://www.dol.gov/agencies/oasam/regulatory/statutes/section-508-rehabilitation-act-of-1973.

"User Agent Accessibility Guidelines (UAAG) 2.0." World Wide Web Consortium. December 15, 2015. https://www.w3.org/TR/UAAG20/.

"Web Content Accessibility Guidelines (WCAG) 2.1." World Wide Web Consortium. June 5, 2018. https://www.w3.org/TR/WCAG21/.

"Web Content Accessibility Guidelines (WCAG) 2.2." World Wide Web Consortium. May 21, 2021. https://www.w3.org/TR/WCAG22/.

9. Appendix

Narrative Description of Table 1 Unique Aspects of FIDO Authentication for People with Disabilities:

Table 1 describes how specific gestures involved with an authentication flow may be likely to pose more or fewer barriers for people by disability type. The following is a narrative depiction of the table.

People with visual disability may be more likely to have challenges with iris scan, face scan, QR code (caBLE) screen and camera scan, scanning security keys via NFC with smartphones, using a mouse to select actions, and enrollment, registration or authentication where time limits are set.

People with visual disability may be less likely to have challenges with touching a security key for user presence check, drawing a pattern on a screen to unlock smartphones, typing a client PIN, fingerprint or vein scan, voice recognition, inserting a security key into a USB port, clicking buttons for actions, touching a screen to select actions, and following on-screen instructions.

People with hearing, speech and language disabilities may be more likely to encounter barriers with voice recognition. They may be less likely to encounter barriers with all previously listed user gesture examples.

People with physical disabilities may be more likely to encounter barriers with touching a security key for user presence check, drawing a pattern on screen to unlock smartphones, fingerprint or vein scan, QR code (caBLE) screen and camera scan, inserting a security key into a USB port, scanning security keys via NFC with smartphones, clicking buttons for actions, touching screens for selecting actions, using a mouse for selecting actions, and enrollment, registration or authentication where time limits are set.

People with physical disabilities may be less likely to encounter barriers with typing a client PIN or screen unlock PIN, iris or face scan, voice recognition, and following on-screen instructions.

People with cognitive and learning disabilities may be more likely to encounter barriers with drawing a pattern on screen to unlock smartphones, typing a client PIN or screen unlock PIN, QR code (caBLE) screen and camera scan, following on-screen instructions, and enrollment, registration or authentication where time limits are set.

People with cognitive and learning disabilities may be less likely to encounter barriers with touching a security key for user presence check; fingerprint, vein, iris or face scan; voice recognition; inserting a security key into a USB port; scanning security keys via NFC with smartphones; and clicking buttons, touching screens or using a mouse for actions.

End table.