FIDO Alliance:
FIDO Desktop Authenticator UX Guidelines

Editors:
Prepared by Blink UX
FIDO UX Task Force Members

June 2021- v1

Contents

Figures

Document Purpose

This document provides the user experience (UX) guidelines and best practices for relying parties and implementers of a FIDO desktop authenticator experience, based on a regulated industry (e.g., banking) use case. These guidelines aim to accelerate decision-making during FIDO implementation and specify what information and controls should be given to users.

The principles in this document were developed following multiple (100-plus) sessions of moderated and unmoderated consumer research conducted by Blink, in collaboration with FIDO UX Task Force members. Existing mobile and desktop biometric authentication experiences currently in the market were also reviewed and served as input during the research and evaluation process.

These recommendations represent FIDO's perspective on how to implement FIDO authentication on desktop for consumers and should be used in tandem with other FIDO publications such as FIDO marketing guidelines, FIDO's logo usage guidelines, FIDO Privacy Principles and other technical documentation. A live reference implementation that reflects the guidance in this document can be found at https://digitalbank-test.com.

Device, operating system and browser support for FIDO will change over time. Should you encounter difficulties during your implementation of FIDO Authentication please consider online resources such as the FIDO-dev mailing list, or by simply contacting FIDO Alliance via email.

Intended Audience

The intended audience is anyone responsible for implementing the interface or user experience of FIDO desktop authentication for a browser-based website – noting that these guidelines are based upon a regulated industry use case. This audience includes but is not limited to, user experience designers, product managers and software development teams.

About the FIDO Alliance and the FIDO UX Task Force

The FIDO (Fast Identity Online) Alliance, www.fidoalliance.org, was formed in July 2012 to address the lack of interoperability among strong authentication technologies and remedy the problems users face with creating and remembering multiple usernames and passwords.

The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO Authentication is stronger, private, and easier to use when authenticating to online services.

The Alliance is driven by hundreds of global tech leaders across enterprise, payments, telecom, government, and healthcare that have come together in support of the organization's mission to reduce the world's reliance on passwords. Alliance members contribute to this mission by influencing the development of FIDO specifications, establishing best practices for deployment of FIDO Authentication, and driving global awareness of the Alliance, its mission, and the FIDO specifications.

The FIDO UX Task Force was created by FIDO's Board of Directors to tackle the challenge and develop best UX practices for FIDO implementations. Member volunteers for this project included product leaders from Apple, Bank of America, eBay, Facebook, Google, HYPR, IBM, Intuit, JP Morgan Chase Bank, Microsoft, Trusona, Visa, and Wells Fargo. The FIDO UX Task Force partnered with Blink UX to conduct this first formal usability research of FIDO user journeys and actively works with the FIDO Executive Team to establish FIDO UX best practices and make authentication without passwords more usable for all.

Why FIDO?

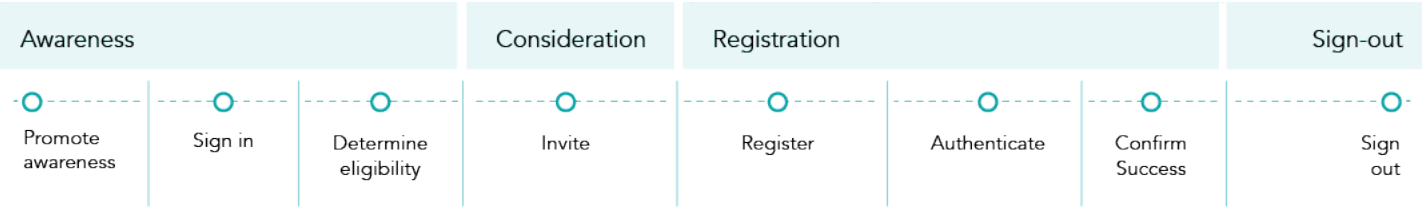
Internet and mobile technologies have revolutionized how we communicate, transact, and deliver services. But these advances also created a problem – an over-reliance on frustrating and risky passwords to authenticate users of online services.

In 2012, several thought-leading organizations and individuals came together to form the FIDO Alliance. The Alliance's mission is to create standards for simpler and stronger modern authentication methods and foster their widespread adoption. Some of the FIDO Alliance's successes since its inception include:

- Published standards for unphishable, strong authentication based on public key cryptography
- Worked with the World Wide Web Consortium (W3C) to establish FIDO technology as an official web standard, which is now built into leading billions of device browsers and platforms
- Established certification tools, processes, and global workshops to facilitate solution development and interoperability testing
- Achieved global endorsement of the FIDO standards-based approach for many of the world's leading consumer electronics manufacturers and web services brands

Given these successes and the growing global recognition of FIDO Authentication, products and services that are marked with FIDO logos are associated with unphishable, interoperable, and user-friendly authentication.

The FIDO registration journey and process steps will appear throughout the document in the following format:

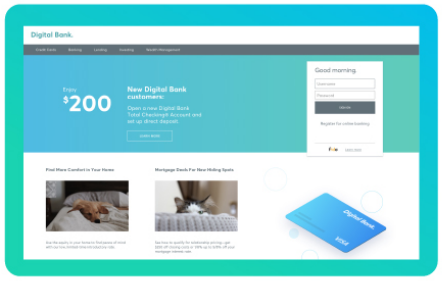


Terminology and Concepts

Three concepts are referenced during the presentation of the UX guidelines. The end-to-end user experience is presented as a **user journey.** Each journey contains **process steps,** and the two journeys presented here were developed with a specific **use case** in mind.

1. **User journey**: This captures the high-level user goals and process steps within the end-to-end FIDO registration and post-registration authentication process on desktop.
2. **Process steps**: Each journey is broken into process steps such as "sign in" and "detect device eligibility", which ladder up to high-level user goals, such as "awareness" or "consideration".
3. **Use Case:** This refers to the specific usage scenario the UX Guidelines are designed to inform — in this case, FIDO desktop authentication on a browser-based website within a regulated industry (e.g., banking).
4. **Biometric sign-in or FIDO sign-in**: This refers to any FIDO-enabled sign-in that leverages the device unlock functionality, including non-biometric modalities on Windows Hello (device PIN) and on MacOS (device password).

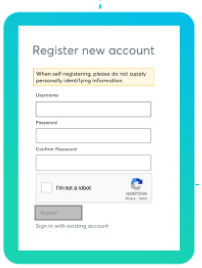
FIDO Registration Journey and Test Site



1

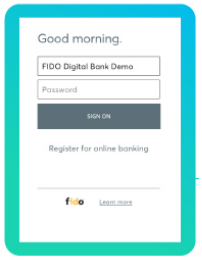
View
https://digitalbank-test.com/simple in Chrome

2



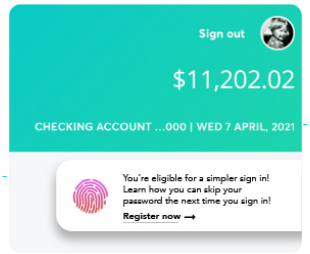
Set up a username and password via the "Register for online banking" link.

3



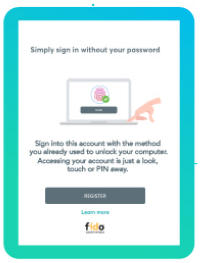
Sign in to Digital Bank with your new username and password.

4



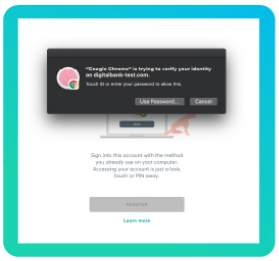
On the Account Transactions page, select "Register now" on the the toast notification with the fingerprint icon.

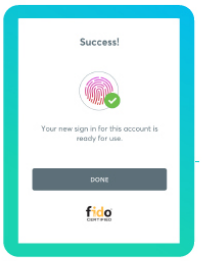
5



Read "Learn more" to view key facts about FIDO.

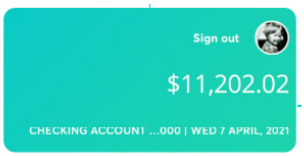
6





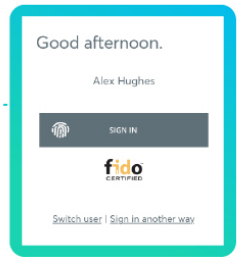
Select "Register." When prompted by the Windows Hello or Apple Touch ID system dialogue, enter the password, PIN, finger scan, face scan or security key you use to unlock your computer. **Now you're registered with FIDO!**

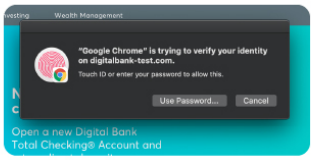
7



After registering with FIDO, sign out of Digital Bank.

8





Sign in to Digital Bank with FIDO.
Easy, Safe, and Private!

Awareness

Purpose: Promote the availability of a FIDO sign-in via multiple strategies

This step provides details about how relying parties can increase customer awareness of FIDO through a combination of persistent and ephemeral messaging strategies aimed at users with devices that support FIDO Authentication. User research indicates that customers may require multiple exposures to the concept of FIDO before taking action to register.

Recommendations

- **Promote biometric awareness at sign-in:** Pre-FIDO registration, indicate the availability of your FIDO sign-in option to users via persistent iconography and text as part of the sign-in UI on your homepage.

- **Differentiate biometric iconography based on user's platform**: Our research indicates the PC and Android phone users find that a generic fingerprint icon most clearly communicates "biometric sign-in" capabilities, whereas Mac and iPhone users find the Apple Touch ID fingerprint icon to be most recognizable.

- **Add FIDO branding at registration:** Because the FIDO brand is not yet familiar to most consumers, promoting the FIDO logo on your homepage pre-FIDO registration is less effective at garnering interest in using a FIDO sign-in than displaying a fingerprint icon and a "call to action" to enable device biometrics.

- **Determine device eligibility:** Once users have signed in with a username and password, detect whether users are visiting your site are on a device that supports FIDO Authentication, and invite only such users to register.

- **Promote FIDO awareness across multiple touch points and a variety of marketing channels**.
  - Offer a Security setting that allows users to initiate (or remove) FIDO registration any time.
  - Utilize tools such as email campaigns, home mailers and/or social media to communicate the availability of enabling device biometrics to sign in on desktop.
    - Digital marketing channels have the advantage of being able to link users directly to the RP site to learn more about why and how to initiate registration of FIDO credentials. Non-digital channels could direct users to visit the relevant Security setting to initiate FIDO registration.
  - Educate Customer Support about FIDO registration, authentication, and value proposition.
    - Include information about which device configurations support FIDO logins as well instructions on how to enable Windows Hello or Apple Touch ID on capable devices.

Awareness: Sign in Pre-FIDO Registration | Sample UI

Pre-FIDO registration, promote awareness of the availability of a FIDO sign-in option by using persistent iconography and text as part of the sign-in UI on your website homepage.

1. **Use a biometric icon (a fingerprint) that users easily recognize** as communicating the availability of "biometric sign-in".
2. Differentiate the icon displayed based on user's desktop platforms (Mac or Windows OS).
3. Include a "call to action" such as, "Enable your device biometrics to access Digital Bank."

   Include a **hover state on the fingerprint icon** to communicate that the user must first sign in with a username and password to enable device biometrics.

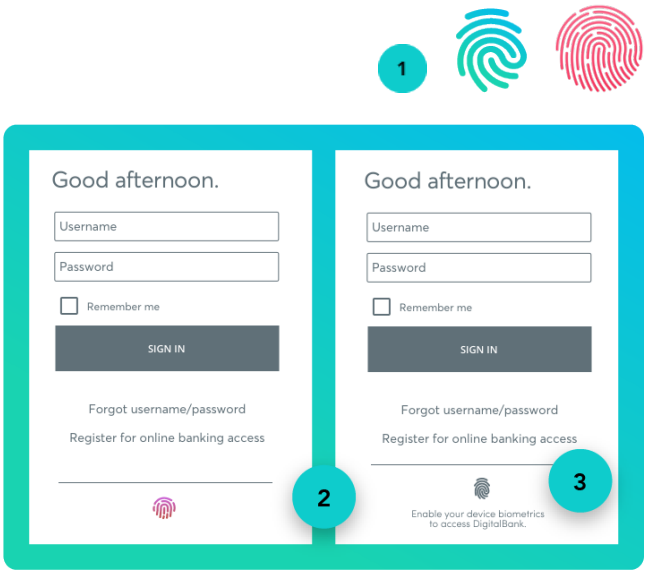
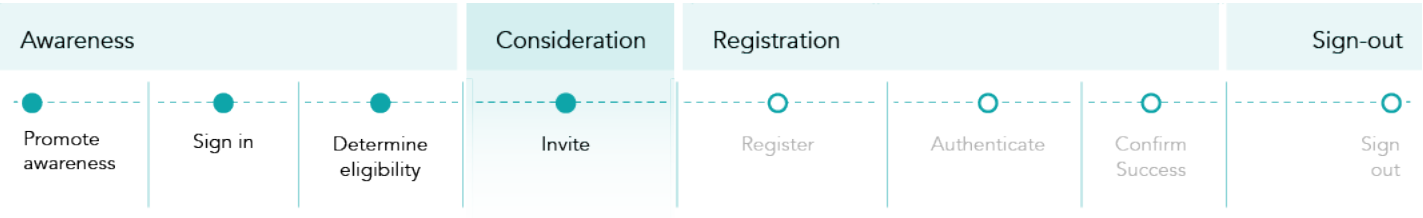


Figure 1 – Pre-FIDO registration sign-in UI examples for Mac (left) and PC (right)

Lead with biometric messaging and iconography at sign-in and add FIDO branding **at registration.** Because the FIDO brand is not yet familiar to most consumers, promoting the FIDO logo on your homepage pre-FIDO registration is less effective at garnering interest in using a FIDO sign-in than displaying a fingerprint icon and a relevant "call to action" to enable device biometrics.



Consideration

Purpose: Invite signed-in users on devices that support FIDO Authentication to register.

Recommendations

- **Invite only users on devices that are capable to support FIDO Authentication, e.g., those where users can utilize Windows Hello or Apple Touch ID:** This targeting is critical to reduce frustration and increase the likelihood of customer success in registering.
    - **Note that some Windows 10 users may not be enrolled in Windows Hello, in which case it may be helpful to point these users to relevant documentation on how to use this functionality.**
- **Focus on the value proposition:** Invitation messages should aim to motivate users by briefly articulating the FIDO value proposition of an "easy and secure sign-in alternative to a password".
    - We recommend the following invitation messages crafted based on user testing. Both effectively communicate the FIDO value proposition and focus on the themes of "Simple" or "Optional":
        - Simple: "*You're eligible for a simpler sign-in! Learn how you can skip your password the next time you sign in. Register now*.
        - Optional: "*Add an easy and safe way to access your account. Register now*."

- **Include biometric images specific to the user's device platform:** Invitation messages should include the biometric fingerprint icon that corresponds to the user's device platform. Our research indicates that the fingerprint image is very effective at helping users to quickly recognize the purpose of the invitation as "enable biometric sign-in."

- **Invite users across multiple sessions:** Display invitation messaging across multiple site visits to ensure users have an opportunity to consider FIDO, research it as needed, and act when convenient. Our research shows users often require multiple exposures to FIDO before taking action to register in the context of other site goals.

- **Strategically employ multiple invitation messaging styles:** To inspire user interest across multiple site visits, utilize more than one invitation format. For example, start with an attention-grabbing "spotlight" page takeover that requires users to respond by dismissing the message or registering for FIDO. For the next few sessions, invite users to register via a more subtle "toast" notification, which doesn't require mandatory interaction.

- **Give users control:** All message invitations should include a way for the user to dismiss the message for the current session. Users expect dismissed messages to re-appear across the next few sessions (e.g., three sessions total).

- **Always link to the FIDO registration page:** Ensure all registration messaging includes an explicit link to a FIDO registration landing page.

Consideration: Targeted invitations | Sample UI

1. Use short and simple invitation messaging that **communicates the FIDO value proposition** of a "simple and secure sign-in without a password."
2. Include an explicit link or button to register or "set up a new sign-in" that navigates to dedicated FIDO registration page.
3. Allow the user to dismiss any invitation messaging for the current session.

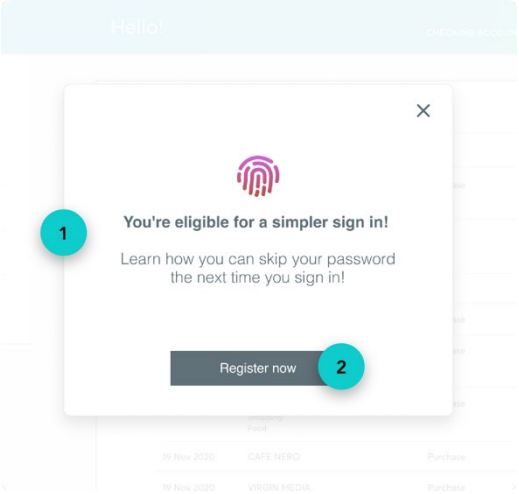


Figure 2 – "Spotlight" page takeover invitation format for Mac users

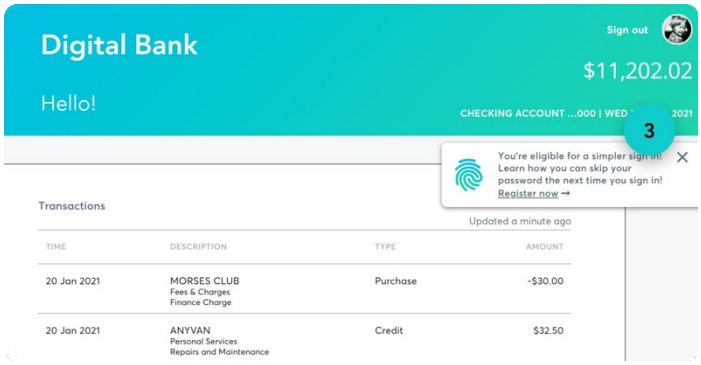


Figure 3 – "Toast" notification invitation format for PC users

Strategically alternate and employ multiple FIDO registration invitation formats to engage users on FIDO-eligible devices, across multiple sessions (Figures 2 and 3).

Display the biometric fingerprint icon relevant to the user's platform. On all registration invitation messaging, display Apple Touch ID fingerprint icon to Mac OS users (Figure 2) the generic fingerprint icon to PC users (Figure 3).

Registration

Purpose: Educate eligible device users about FIDO and allow them to register.

Recommendations

Offer a dedicated registration landing page that meets the following criteria:

- **Provide an explicit affordance to initiate registration** (e.g., a "Register" button).
- **Give users control:** Include a persistent option to leave the registration flow.
- **Include an animation or image to illustrate the process of registering with FIDO** on a desktop computer, using Windows Hello or Apple Touch ID and a biometric (e.g., finger scan).
- **Use simple messaging that describes the process of FIDO registration** *(e.g., "Enter the password, PIN, finger scan, face scan or security key you use to unlock your computer").*
- **Progressively disclose more information about FIDO in a "Learn more" link:** The following statements developed through user testing addressed the top questions and concerns research participants had about FIDO before registering:
    - *FIDO is a technology built into all leading desktop devices (PC and Mac) and browsers, that allows users to sign in securely without a password.*
    - *In the same way your phone uses a biometric, FIDO now enables biometric sign-in on websites viewed on your desktop too.*
    - *FIDO makes sign-in easy, safe, and private!*
    - *FIDO technology uses your computer's built-in authentication method (i.e., Windows Hello or Apple Touch ID) to ensure your sign-in information stays safe from hackers because it never leaves your computer.*
    - *Once you've registered your computer's PIN, facial recognition, fingerprint, or security key, FIDO verifies it's really you and doesn't transmit any of your sign-in information over the internet.*
    - *Registering with FIDO provides you with an additional sign-in option for this device — your password remains valid.*
    - *Leading companies worldwide in retail, telecommunications, finance, and technology are already using FIDO.*
- **Introduce the FIDO brand:** Displaying FIDO-approved branding and explicitly referring to the technology as "FIDO" is appropriate and helpful to users at registration. This additional information in "Learn more" builds trust in FIDO technology and clarifies the registration process.

Registration: Dedicated Landing Page | Sample UI

From the invitation, link users on FIDO-eligible devices
to a dedicated registration page that includes the following:

1. The **ability to exit** the registration process
2. An **animation or image to illustrate registration** or signing in with FIDO using Windows Hello or Apple Touch ID and a finger scan on a laptop computer
3. **Simple instructions about the process of registering** with FIDO (e.g., use the password, PIN, finger scan, face scan or security key you use to unlock your computer)
4. An **explicit affordance to "Register"** or "Set up a new sign-in"
5. **Additional information about FIDO** progressively disclosed via a "Learn more" link, with key facts about the privacy, security, and convenience of FIDO
6. **FIDO-approved branding**

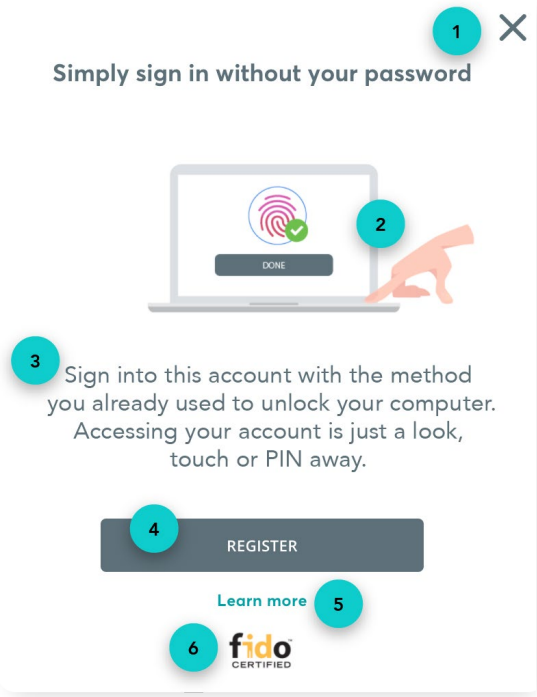
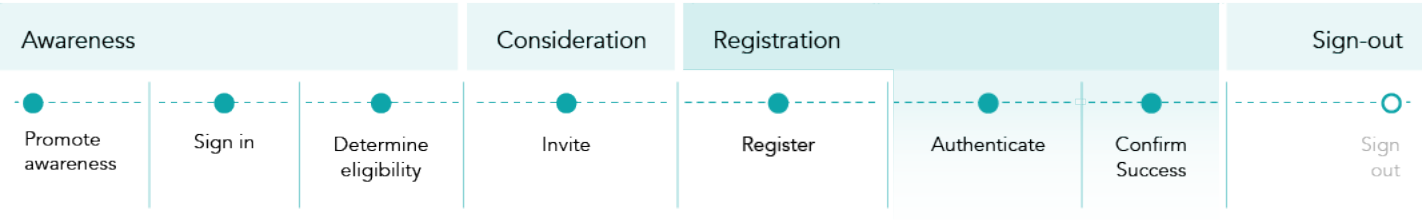


Figure 4 – FIDO registration landing page



Authenticate

Purpose: Allow users to sign into Windows Hello or Apple Touch ID to authenticate and register with FIDO.

Recommendations

- **Prompt authentication with Windows Hello or Apple Touch ID:** After users opt to "Register," prompt them to authenticate by displaying the relevant system dialogue (Windows Hello or Apple Touch ID) on top of the FIDO registration page.

- **Display authentication error messaging on the FIDO registration landing page:** If authentication with Windows Hello or Apple Touch ID fails, display updated messaging on the FIDO registration page to help users succeed in authenticating with Windows Hello or Apple Touch ID.
    - Example: "*FIDO registration failed. Enter the password, PIN, finger scan, face scan or security key you use to unlock this computer. You must have set up Windows Hello or Apple Touch ID on your computer before registering with FIDO.*"

- **Display authentication success messaging on the FIDO registration landing page:** If authentication with Windows Hello or Apple Touch ID is successful, display a success message on the FIDO registration page, with the finger scan icon relevant to the user's platform and a visual indicator of success (such as a green checkmark).

Authenticate: Windows Hello or Apple Touch ID | Sample UI

1. Windows Hello or Apple Touch ID system dialogue: After users opt to register, prompt them to authenticate by displaying the relevant Windows Hello or Apple Touch ID dialogue on top of the FIDO Register page.

2. Error message: If authentication with Windows Hello or Apple Touch ID fails, update the FIDO registration page with an instructional error message.

3. Success message: If authentication is successful, display a success message on the FIDO registration page. Replace the registration animation with the finger scan icon relevant to the user's platform and a green check mark to communicate success.

4. Include FIDO-approved **branding.**

5. Sign-out: Once users sign into your website with FIDO, ensure users can sign out using the same UI they used previously with a username and password.

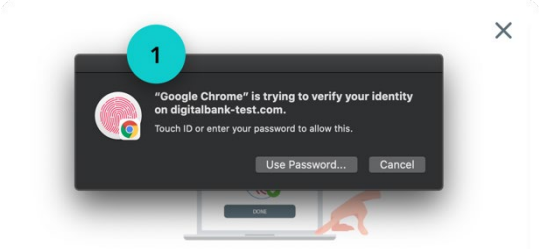


Figure 5 – Apple Touch ID system dialogue in Chrome displayed on FIDO registration page

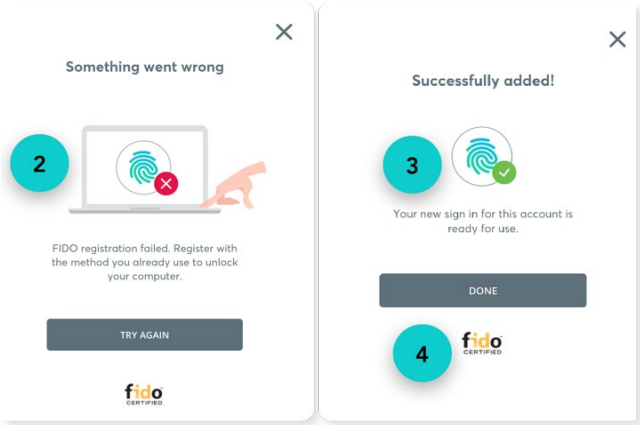


Figure 6 – FIDO registration error page (left) and success page (right) for PC users

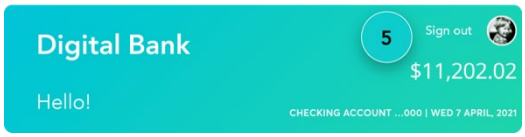
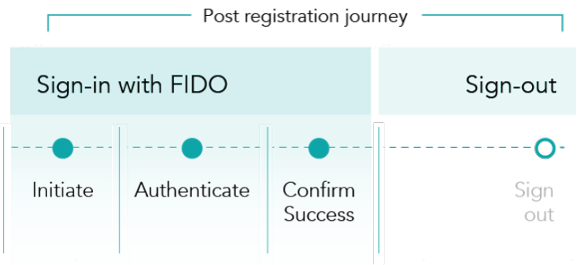


Figure 7 – Sign out using the standard website UI



FIDO Sign-in

Purpose: Allow users on registered devices to sign in with FIDO.

Recommendations

- **Make FIDO the primary sign-in path where possible:** For users on FIDO-registered devices, replace the username and password fields with a single SIGN IN button, along with the biometric image relevant to each user's platform.

- **FIDO Certified:** Display "FIDO Certified" branding beneath the SIGN IN button to communicate that the sign-in experience has been updated and is supported by FIDO.

- **Preserve secondary non-FIDO sign-in paths:** Offer "Switch user" and "Sign in another way" links to preserve username and password sign in functionality.

- **Sign out:** Once users sign into your website with FIDO, ensure users can sign out of your website using the same UI they used previously with their username and password.

FIDO Sign-in | Sample UI

1. **Replace the username and password field with the user's name and a single SIGN IN button,** along with the biometric image relevant to the users' platform.

2. Display **FIDO-approved branding** beneath the SIGN IN button.

3. **Preserve the username and password sign in option** with "Switch user" and "Sign in another way" links.

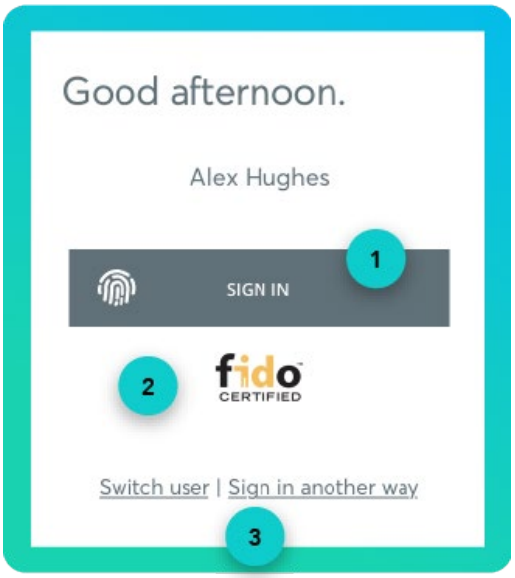


Figure 8 – Post-FIDO registration sign in for Mac users

Optimize Customer Success with FIDO

Purpose: Be aware of helpful strategies for enhancing user success and adoption

- **Promote the partnership between your brand and FIDO:** Customer trust in the new brand of FIDO comes first from FIDO's association with your trusted brand.

- **Lead with biometric language and symbols:** Prior to FIDO registration, promote FIDO login awareness using familiar fingerprint symbols that consumers readily associate with "biometric sign-in" rather than the FIDO brand, which is new to most consumers.

- **Introduce FIDO-approved branding at registration, with educational "Learn more" messaging.**
  - To begin building familiarity and confidence in the brand and the technology, display FIDO-approved branding on the registration page along with other contextual information about FIDO technology.
  - In a "Learn more" section, convey why FIDO is a uniquely safe, secure, and convenient way to sign in.

- **Educate users about how FIDO technology works to instill confidence and trust.**
  - Our research indicates that although many users view biometric sign-in as desirable, convenient, and secure, some users initially express reluctance to share biometric or other computer sign-in information with their bank or with FIDO.
  - In a "Learn more" section on the registration page, reassure users that FIDO uses their computer's existing authentication mechanism (i.e., Windows Hello or Apple Touch ID) to verify their identity; their PIN, password, face scan, finger scan or security key is not shared with FIDO or your website and never leaves their computer.
  - Prepare Customer Support with knowledge about how to register and sign in with FIDO (including information on required configurations for successful utilization and/or settings that would preclude FIDO such as browsing in "Private" or "Incognito" mode), as well as why FIDO is a safe, secure, and convenient alternative for authentication with your website.

Acknowledgments

The authors acknowledge and thank the following people (in alphabetic order) for their valuable feedback and comments:

- Corrine Aberdeen, Content Strategist, Facebook
- Judy Clare, Vice President, Digital Identity and Authentication, JP Morgan Chase
- Kevin Goldman, Chief Experience Officer, Trusona
- Kerry Hebert, Design Director, Visa
- James Hwang, Senior UX Designer, Microsoft
- Megan Shamas, Director of Marketing, FIDO Alliance
- Andrew Shikiar, Executive Director and Chief Marketing Officer, FIDO Alliance
- Jasmine Smith, Team Lead and Developer, IBM
- Rob Warne, Senior UX Designer, Digital Identity & Authentication, JP Morgan Chase
- Shane Weeden, Senior Technical Staff Member, IBM