

FIDO Alliance: FIDO Security Key UX Guidelines

Editors:
Prepared by Blink UX
FIDO UX Task Force Members

June 2022

Document Purpose

This document provides the user experience (UX) guidelines and best practices for relying parties and implementers seeking to enable multi-factor authentication (MFA) with FIDO security keys as a second factor, based on a regulated industry (e.g., banking or healthcare) use case. These guidelines aim to accelerate decision-making during FIDO implementation and specify what information and controls should be given to users. Note that these UX recommendations are optimized for browser-based sites accessed on desktop/laptop computers, rather than mobile apps or mobile web. The guidelines do not, however, include recommendations about security policies or account recovery.

The principles in this document were developed following multiple (N = 68) sessions of moderated and unmoderated consumer research conducted by Blink, in collaboration with FIDO UX Task Force members. User research participants included consumers who owned and used security keys, primarily for work, as well as prospective security key users, who used two-factor authentication for personal online banking but had no experience with security keys prior to their research session. Note that our research scope did not include strategies to entice prospective users to purchase keys. In addition to user research, security key second-factor authentication experiences currently in the market were reviewed by the FIDO UX Taskforce and served as input during the research and evaluation process.

These recommendations represent perspectives from the FIDO Alliance's UX Task Force on how to implement MFA for FIDO security keys as a second factor on desktop/laptop for prosumers. For this document, a "prosumer" refers to a security- and privacy-conscious consumer who is an early adopter of security and privacy technologies and services in their personal lives.

These guidelines should be used in tandem with other FIDO publications such as FIDO's logo usage guidelines, FIDO Privacy Principles, Guidance for Making FIDO Deployments Accessible to Users with Disabilities (to be released in Summer 2022), FIDO UX Guidelines for Desktop Authenticators 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 Security Key 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 the interface or user experience elements of an MFA deployment that leverages FIDO security keys, 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, is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords.

The FIDO Alliance is working to change the nature of authentication with open standards that provide sign-in experiences that are more secure than passwords and SMS OTPS, simpler for consumers to use, and easier for service providers to deploy and manage. FIDO Authentication is stronger, more 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 for this project was created by the FIDO Alliance Board of Directors to tackle the challenge and develop best UX practices for implementing MFA with FIDO security keys for consumer web-based sites, on desktop/laptop across platforms. Member volunteers for this project included product leaders from Feitan, Google, IBM, Idemia, JP Morgan Chase Bank, Meta, Microsoft, NIST, OneSpan North America, Onfido, Trusona, Trustkey, Visa, VMware, and Yubico. The aim of the guidelines is to help RPs design a better, more consistent user experience for the consumer security key audience, and ultimately, maximize adoption.

Why FIDO?

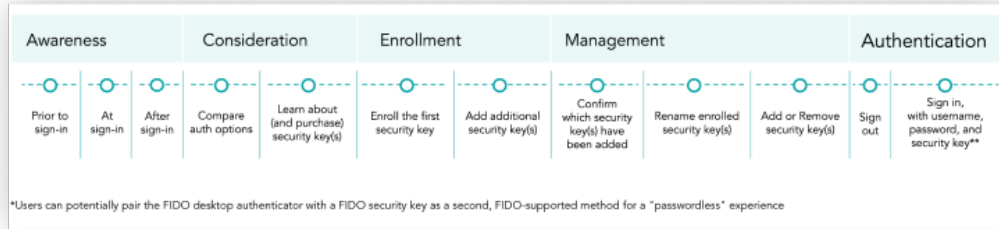
Internet and mobile technologies have revolutionized how we communicate, transact, and deliver services. But these advances also created a problem — an over-reliance on frustrating and risky passwords to authenticate users of online services.

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 include:

- Published standards for phishing-resistant, 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 phishing-resistant, interoperable, and user-friendly authentication.

FIDO Security Key Enrollment User Journey: User Goals and Process Steps



The end-to-end user experience is presented as a user journey. The FIDO security key enrollment and authentication user journey contains up to 12 process steps and was developed with a specific use case in mind (i.e., consumers on a regulated industry website, seeking to enable MFA with a FIDO security key as a second factor). Four concepts are referenced throughout the UX guidelines are noted below.

1. **User journey:** This captures the high-level user goals and process steps within the end-to-end security key enrollment and authentication process on desktop/laptop.
2. **Process steps:** Each journey is broken into process steps such as "awareness at sign-in" and "compare auth options," which fall under high-level user goals such as "awareness" or "consideration."
3. **Use Case:** This refers to the specific usage scenario the UX Security Key Guidelines are designed to inform — consumers enabling MFA with FIDO security keys as a second factor on a browser-based website within a regulated industry (e.g., banking or healthcare).
4. **MFA sign-in with security keys as a second factor:** This refers to any MFA sign-in that includes a FIDO security key as a second factor on Windows or Mac OS desktop/laptop.

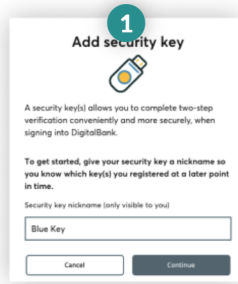
FIDO Security Key Enrollment User Journey and Test Site

View digitalbank-test.com in Chrome

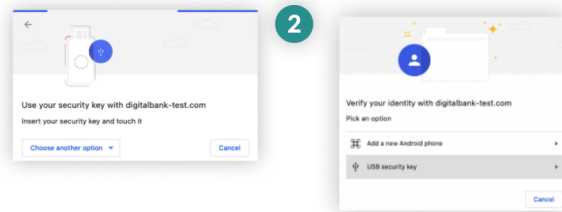
Set up a username and password via the "Register for online banking" link.

Sign in to Digital Bank with your username and password.

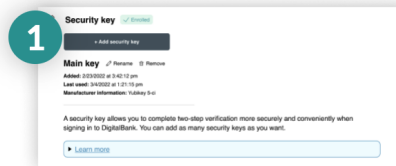
On the Account Transactions page, select "Security and Privacy" settings on the main navigation or under Profile. Alternatively, click a Security and Privacy link within a toast notification.



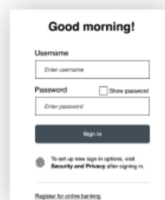
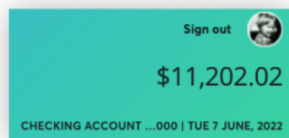
Scroll to the bottom of Security and Privacy Settings page and read "Learn more" to view facts about security keys.



When prompted, by your browser, pick "USB key" as the option for verifying your identity. Connect your key (via USB or bluetooth) and touch it (if using a biometric key).



Now your FIDO key is enrolled as a second authentication factor! **If you have another key, add it now, as a backup.**

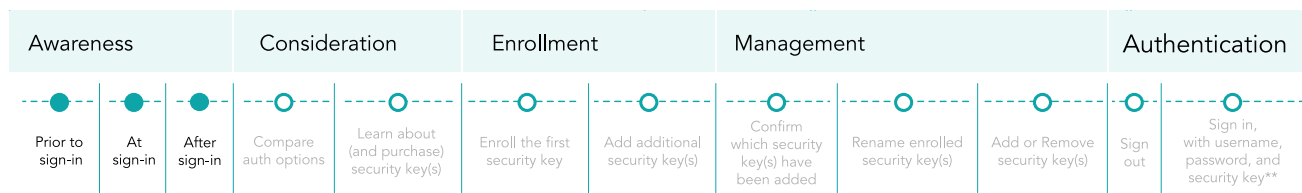


After enrolling a FIDO security key as a second factor, sign out of Digital Bank. Sign in to Digital Bank by entering your username and password and connecting your key. Simple, Fast and Secure!

Let's Get Started

Now we're going to do a deep dive into the FIDO deployment recommendations and sample UI for each user goal in the security key enrollment and authentication journey.

Awareness



*Users can potentially pair the FIDO desktop authenticator with a FIDO security key as a second, FIDO-supported method for a "passwordless" experience

Purpose: Promote user awareness of available alternatives to password-only authentication, and direct users to Security and Privacy settings to manage new sign-in options, including security keys.

This step provides details on how RPs can increase customer awareness of available alternatives to password-only authentication (i.e., FIDO security keys and platform desktop authenticators) through a combination of messaging strategies and site information architecture updates. RPs may choose to promote platform authenticators and/or security keys to their customers, depending upon the customer segments or lines of business they are targeting. Our user research indicates that customers may require multiple exposures to new authentication options before taking action to set up new sign-in method(s).

Recommendations

Prior to sign-in:

- Outside of your website, strategically utilize multiple channels to promote Security and Privacy settings as a destination to optimize account security.
 - Outside of the site, utilize email campaigns, home mailers, and/or social media to recommend that users visit Security and Privacy settings to learn about and enhance account security and set up MFA, including using security keys.
 - Within online communications to customers about privacy and security recommendations, always link to the Security and Privacy settings page.
 - Consider targeting specific customer profiles who might benefit the most from using security keys (e.g., high net worth banking customers) by sending educational material about authentication options, including the benefits of security keys.

At sign-in:

- Promote general awareness of the availability of an alternative to password-only authentication, rather than specifically promoting what is likely to be an unfamiliar method of security keys:
 - For RPs who offer biometrics on desktop web, indicate the availability of an alternative to password-only authentication on the sign-in UI by displaying the familiar biometric icon (i.e., a fingerprint), which users widely recognize as indicating the availability of biometric sign-in or touch unlock
 - Our research demonstrated that even though users were not using a biometric login, a fingerprint icon triggered them to consider a non-password login.
 - The familiar fingerprint icon was more effective at garnering user interest in updating sign-in options than specifically referring to the unknown concept of security keys.
 - RPs who do not offer biometrics on desktop web should consider using an icon on the sign-in UI to represent the broader category of authentication (e.g., a user outline and a checkmark or a lock with asterisks to indicate a PIN code).
 - Next to the authentication icon on the sign-in UI, include brief, static messaging as a call to action to direct users to Security and Privacy settings after sign-in, to set up new sign-in options.

After sign-in:

- Within your website, make Security and Privacy settings a discoverable destination for managing account security by updating your site architecture and/or strategically promoting this settings link on your site.
 - Make Security and Privacy settings more discoverable within your site. Promote a Security and Privacy settings link within the main site navigation, or add it as a unique destination under Profile (i.e., outside of the more general Settings menu item).
- Within your website, strategically utilize multiple messaging strategies to promote Security and Privacy as a destination to optimize account security.
 - To inspire interest across multiple site visits, utilize more than one messaging format. For example, utilize temporary messaging strategies such as banner ads or “toast” notifications to invite users to visit Security and Privacy to update their sign-in method.
 - Multiple message exposures are often necessary to inspire new sign-in method enrollment, especially for security key adoption.
 - Enrolling a security key is a multi-step process, and it requires an investment of time and effort to learn about, purchase, and enroll a security key.
 - Our research shows that, in the context of other site goals, users often require multiple exposures to the idea of setting up new sign-in options before taking action. Give users several opportunities to notice relevant messages and take action when it is convenient for them.
 - For example, display toast notifications across multiple site visits, inviting users to visit Security and Privacy settings to update their sign-in method.

Awareness: Promote Security and Privacy Settings to Enhance Account Security

Sample UI

Promote users' active management of their account security and sign-in options by making Security and Privacy settings a more discoverable destination.

At sign-in:

1. For sites that offer biometric authentication, use a biometric icon (a fingerprint) within the sign-in UI to communicate that a biometric sign-in (i.e., an alternative to password-only authentication) is available.
 - Our research demonstrated that even though users were not using a biometric sign-in, a fingerprint icon triggered them to consider an alternative to password only sign-in.
2. Include a persistent call to action to update sign-in options (e.g., "To set up new sign-in options, visit Security and Privacy after signing in.").

After sign-in:

3. Employ a toast notification to direct users to Security and Privacy to add new sign-in options.
4. Add authentication iconography on the toast notification (i.e., a fingerprint for RPs that offer biometric sign-in).
5. Add a "Security and Privacy" link as a destination on the main account navigation or as a peer to Settings, in the user Profile menu.

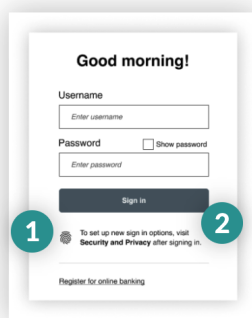


Figure 1 – Sign-in UI example with fingerprint icon and call to action text

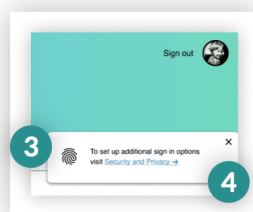


Figure 2 – Toast notification with biometric icon and link to Security and Privacy settings

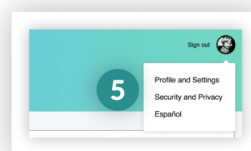
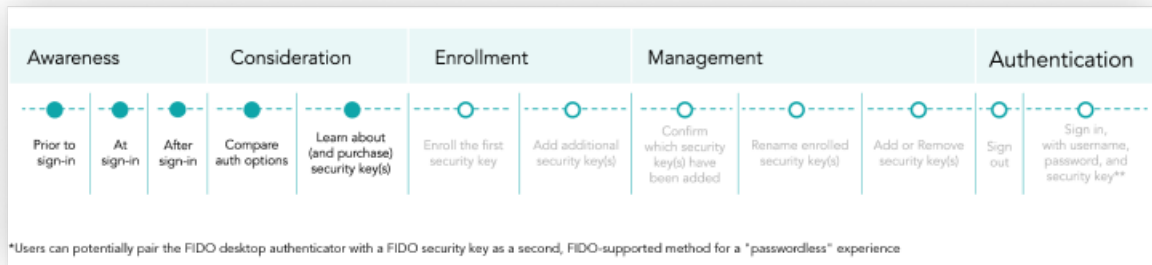


Figure 3 – Security and Privacy settings link on the main navigation or under user Profile

Consideration



Purpose:

- **Empower users to take an active role in protecting their accounts by designing the Security and Privacy settings page to help users learn about and compare available authentication options, including security keys.**

More and more companies are offering security keys as a stronger way for customers to authenticate and protect their accounts. Yet, our research shows that most consumers are not familiar with security keys as an option for consumer website authentication.


Educating customers about the advantages of security keys, how to purchase a FIDO security key, and how to prepare for account recovery by enrolling multiple keys can help your customers overcome barriers to consumer adoption.

Recommendations

Help users compare and learn about authentication options available on your site, including security keys, by offering a Security and Privacy settings page that meets the following criteria:

- Display an explicit recommendation that users increase the security of their account(s) by adding a second authentication method in addition to a password.
 - Make sure this recommendation message is dismissible by the user.
- Use icons to tell stories. Stories are easy for users to remember and icons tell stories.
 - Add iconography to the recommendation message on Security and Privacy settings to increase its visibility and visual interest and to signify recommended methods to add, such as platform authenticators (e.g., fingerprint icon) and security keys.
 - Use icons next to authentication method names as well, to distinguish each method and enhance the scannability of the page.
- Provide clear visual indicators to mark the sign-in method(s) in which the user is currently enrolled.
- Provide a brief description of the authentication process and/or unique value proposition of each method.
 - Because more consumer awareness about security keys is needed, we recommend emphasizing that a security key is a second factor (i.e., used in addition to a password) and that multiple security keys can be used and are recommended.
 - Example text: “A security key allows you to complete two-step verification more securely and conveniently when signing in to Digital Bank. You can add as many security keys as you want.”
- Progressively disclose more information about security keys and platform authenticators in a “Learn more” link.
 - Ensure the “Learn more” link is visible before and after security key registration, as both are relevant touchpoints when users have questions or concerns about using security keys.
 - Through user research, we’ve identified topics that addressed the top questions and concerns participants had about security keys, which served as potential barriers to adoption.

▼ Show less

- **What is a security key?**
A security key is a small, physical device that works in addition to your password on sites that support it. A single key can be used with multiple accounts or sites.
- **Why should I use a security key?**
Security keys protect you against imposter websites that try to steal login credentials (like usernames and passwords). Other forms of 2-factor authentication (including text, email, messages, authenticator apps, and push notifications) do not give you the same level of protection as a security key.
- **How security keys work**
You must first add security keys using the button above. Once added, you'll be required to use them after signing in with your username and password. Doing this creates one of the strongest forms of authentication available to protect your account.
 - **What security technology do security keys use?**
Most keys use an authentication "standard" called FIDO® which allows for secure authentication without drivers or software. When a user signs in a website with a key, FIDO® cryptographically signs a challenge from the browser that verifies the website's actual domain name, which provides strong protection against phishing (e.g., when a fake website is used to trick users into sharing personal information). An attacker would need to control the website domain name or the browser to get a usable signature from the key.
- **Why do security keys look like thumb drives?**
Although hardware security keys may resemble thumb drives and are sometimes inserted into your computer's USB port, they are not storage devices. Your personal information is not trackable or linkable across sites or online accounts when using a security key.
- **What happens if my security key gets stolen?**
The key works in addition to your password, not as a replacement for it. If someone steals the key, they still can't get into your bank account without knowing your password (or which sites are registered with your key). You can sign in with a backup method and remove the stolen key from your account.
- **Add more than one security key**
Adding multiple security keys is highly recommended. If your security key is lost or stolen and you do not have a registered backup security key (or other backup authentication method), access to your account could be interrupted while we verify your identity. We recommend keeping one key easily accessible and another stored separately in a safe space.
- **Purchase security keys**
Security keys vary by manufacturer and can be purchased from mainly online retailers. We recommend FIDO certified keys. See a [list of FIDO® certified keys](#).
- **Name your security keys**
Give your security key a friendly "nickname" that only you can see, so you know which key you registered with this account at a later point in time.

Consideration: Security and Privacy Settings Page

Sample UI

From within a toast notification, on the main site navigation, and/or within the user profile, link users to a Security and Privacy settings page that includes the following:

1. Recommendation message to add an additional sign-in method, with biometric and security key icons, that is dismissible by the user
2. Enrolled status indicator or tag, to help users quickly identify which methods they are currently using, and which are still available to them
3. A security key section that features an icon and a brief description of the value of security keys and their role as a second authentication factor; include recommending the use of multiple keys
4. “Learn more” link which is visible before and after security key enrollment

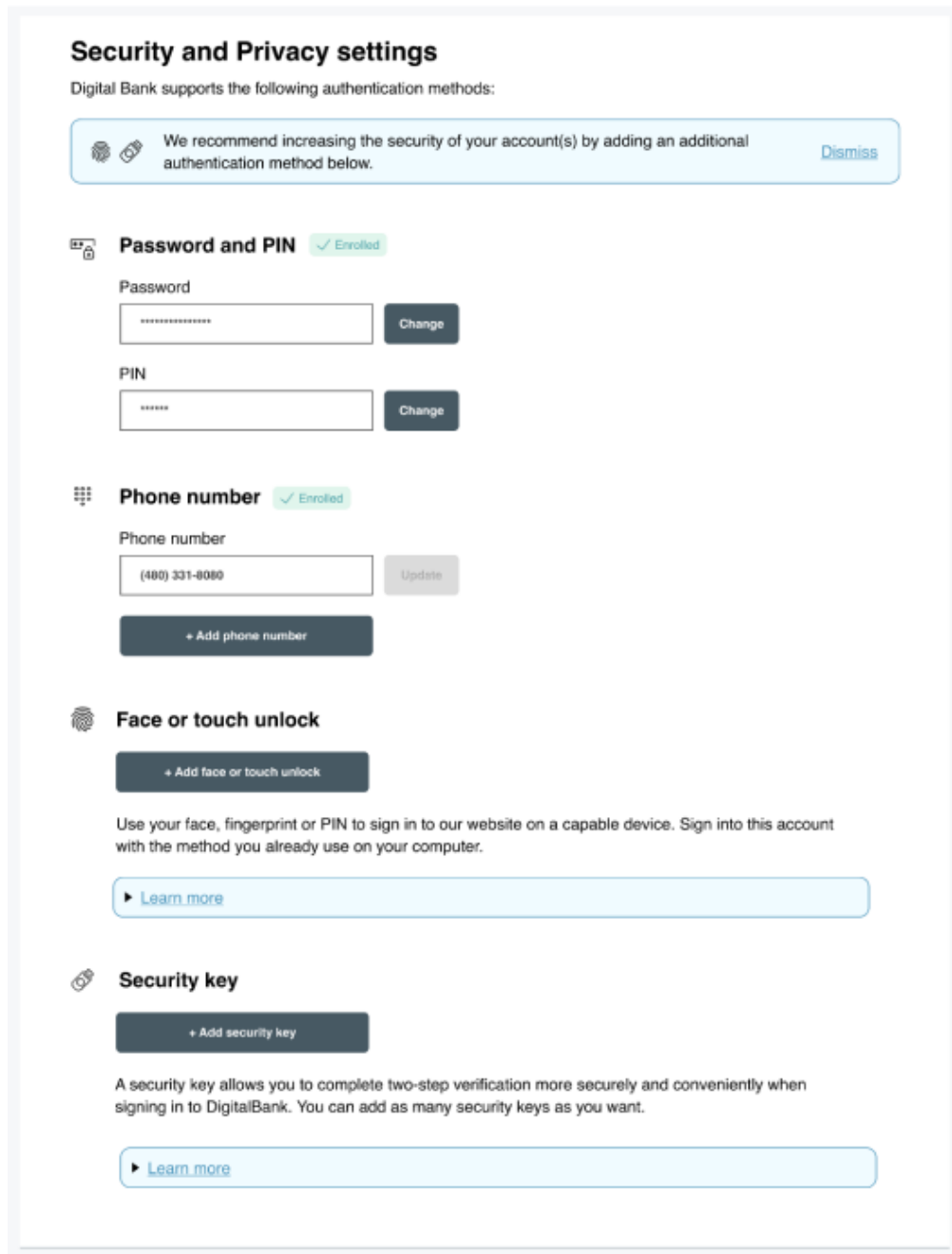
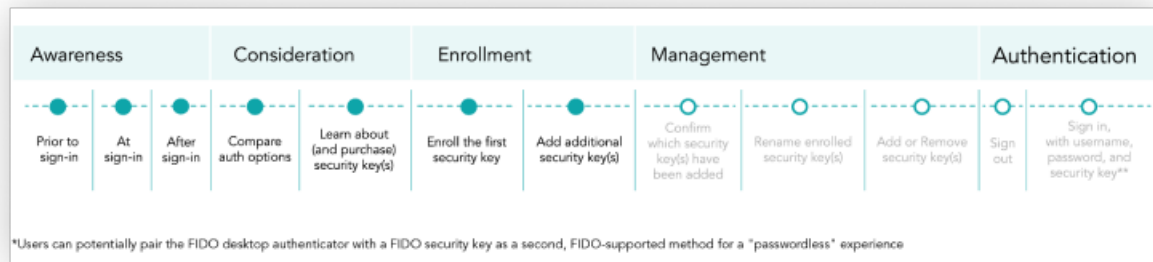


Figure 5 — Security and Privacy settings page (before security key enrollment)

Enrollment



Purpose: Allow users to authenticate with a FIDO security key as a second factor and enroll additional keys (immediately or at a later time), for account recovery.

Recommendations

- Encourage the use of multiple keys: At multiple touchpoints, strongly encourage users to add more than one key for account recovery and backup.
- Support updating, adding, and the removal of keys: For every authentication method, including security keys, provide an explicit affordance for updating existing authentication information (e.g., a "change" or "update" button), for removing authentication methods currently in use (e.g., a "remove" button), or adding new authentication methods to the user's profile (e.g., an "add" button).
- Reiterate the value proposition of using a security key: e.g., "A security key allows you to complete two-step verification conveniently and more securely when signing into DigitalBank."
- Add the ability for the user to add a nickname: To begin enrollment, require users to enter a nickname of their choice that can be used to recognize the registered key at a later point in time.
 - Specify that the nickname is only visible to the user (i.e., is not equivalent to a password that needs to be secure) and serves as a future reminder to the user of which keys they have registered.
- Make the FIDO API call and allow the browser and/or OS to handle the remaining security key enrollment UI.
- Optional attestation step: As part of the security key enrollment process, your organization may configure your site to require attestation (i.e., asking the user's permission to share manufacturer information with your site, such as make and model of their security key). If details are available from the security key manufacturer, requiring attestation will allow for the make and model to be displayed to the user after a security key is enrolled with their account.
 - FIDO Alliance does not recommend adding this attestation step for consumer user cases, because it requires a user to grant permission to your site via an extra dialogue during the security key enrollment process.
 - If your organization opts for a simpler registration process, attestation can be turned off, bypassing the permission dialogue. With this option, details around the make and model of the key would be unavailable to the customer at a later date. Adding this additional attestation step may be valuable for security key enrollment for workforce scenarios.
- Optional user verification step: As a part of the security key enrollment process, your organization may also choose to configure your site to require user verification, meaning asking the user to add a PIN or fingerprint to authenticate with a security key. This optional verification step was out of scope for the research related to these UX Guidelines.
- Display enrollment success or error messaging on the security key enrollment landing page.
 - If security key enrollment is successful, display a success message, with a security key icon and a visual indicator of success (such as a checkmark next to the security key icon).
 - If security key enrollment fails, display an error message to help users understand that enrollment failed and allow them to reinitiate the enrollment process.
- At multiple touch points, inspire users to add a second security key for account recovery and backup.
 - Prior to security key enrollment, provide messaging on the Security and Privacy settings page, encouraging users to add multiple keys.
 - Immediately after security key enrollment, strongly recommend and offer an opportunity to add a second security key, in a manner that requires the user to pause and consider this recommendation.
 - On the "Key successfully added" screen, use multiple strategies for emphasizing that two or more security keys should be used:
 - Headlines: Create a headline emphasizing in bold that "Only one security key is registered."
 - Text: Explicitly recommend adding at least two security keys in the event that one security key is lost or stolen.
 - Illustrations: Use illustrations to emphasize the state of only one security key being registered and the desired state of two security keys being registered.
 - "Add a second key" option: Offer two action buttons ("done" vs. "add a second key") that are equally visible and accessible, with "done" as the default action, as most participants likely won't be ready to add another security key immediately.

Enrollment: Authenticate with a FIDO Security Key as a Second Factor and Add Additional Keys

Sample UI

“Add security key” enrollment page should include the following:

1. The ability to exit the enrollment process
2. A security key icon or image
3. Messaging that describes security keys as a second-factor authentication method
4. A requirement to add security key nickname
5. Specify that the security key is only visible to the user (i.e., is not equivalent to a password that needs to be secure)
6. Messaging that specifies that the nickname serves the purpose of reminding the user which security keys they have registered at a later point in time

“Successfully added” screen should include the following:

1. A security key icon to visually indicate successful enrollment (e.g., a checkmark)
2. The user-defined, security key nickname
3. A reminder to keep the security key easily accessible for sign-in
4. A reminder that only one key is registered and a recommendation that users add more than one security key in case one is lost or stolen
5. A directive to keep one security key easily accessible and another stored in a safe place
6. Primary action buttons that should be binary responses to the question, “Would you like to add another security key?” Include two equally prominent action buttons, including the option (Yes, add another).
7. A “Done” action button as the default, as most users are unlikely to have another security key handy to enroll
8. A security key enrollment error screen (e.g., “Something went wrong”) should include the following: Iconography and text to indicate enrollment was not successful
9. Explicit action buttons to re-initiate the security key enrollment or cancel

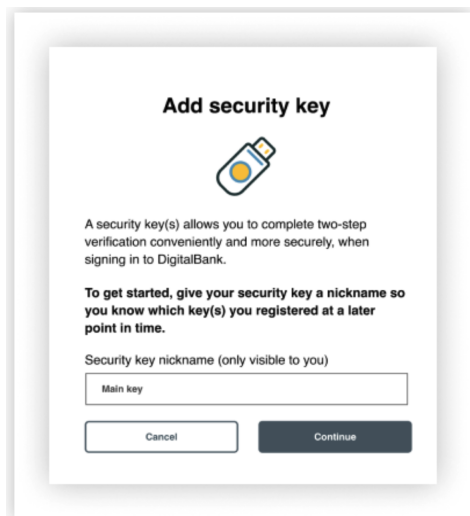


Figure 6 – Add security key page

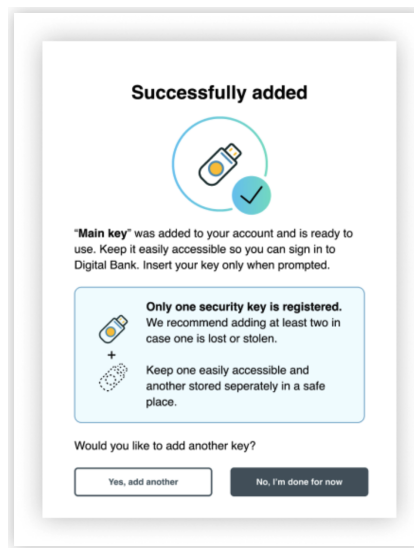


Figure 7 – Successfully added page

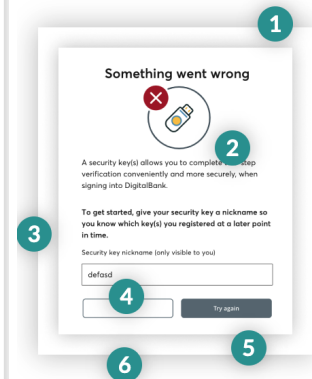


Figure 8 – Post-FIDO registration sign in for Mac users

Management

Purpose: Aid users in confirming which security key(s) have been enrolled, when the security key was enrolled, and when it was last used. Offer clear, discoverable options to rename and remove enrolled security keys, and to add additional security keys.

Recommendations

- After enrollment, return to Security and Privacy settings (unless the user is adding a new security key). Display relevant security key data on the page, without requiring the user to drill down.
 - Include the following security key information:
 - Key nickname
 - Added date
 - Last used date
 - Security key manufacturer information (if attestation is turned on and the user opted to share)
- Display an “Add key” button as the primary call to action in the “Security key” section of Security and Privacy settings
- Offer users a visible option to rename the security key with a new nickname.
- Offer users a visible option to remove a security key from the account.
 - Confirm whether the user wants to remove < security key nickname >.
 - Display an icon to visually indicate “remove,” such as a red minus symbol above a security key.

Sample UI

Immediately after enrollment, unless the user opts to add a second security key, return the user to Security and Privacy settings.

On the Security and Settings page, display security key data to help users confirm enrollment was successful and that no unauthorized security key use has occurred. Empower users to update the security key nickname or unenroll the security key, including:

1. Key nickname
2. Date added and last used
3. Attestation security key manufacturer information (optional)
4. Persistent “Add key” option as the primary call to action
5. “Rename” and “Remove” options

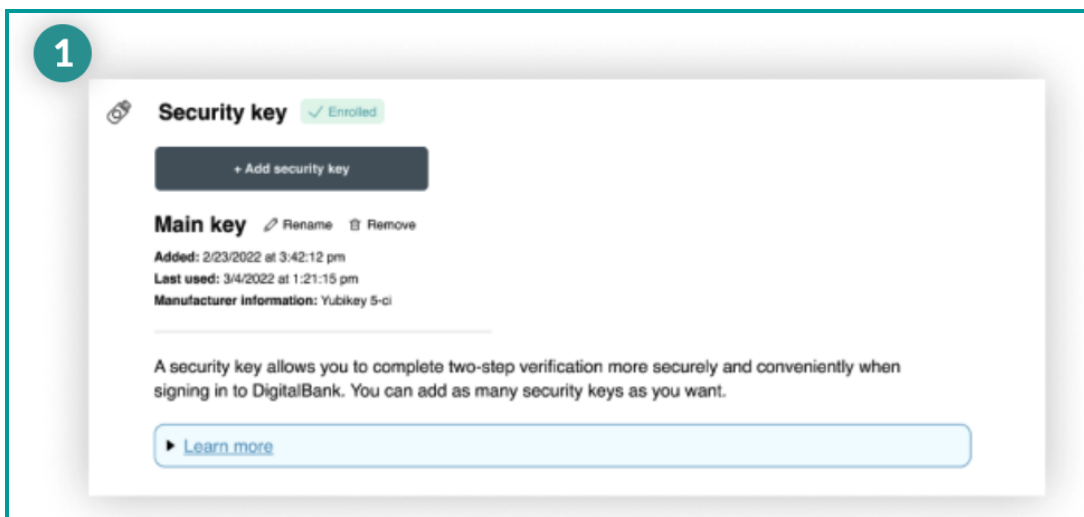
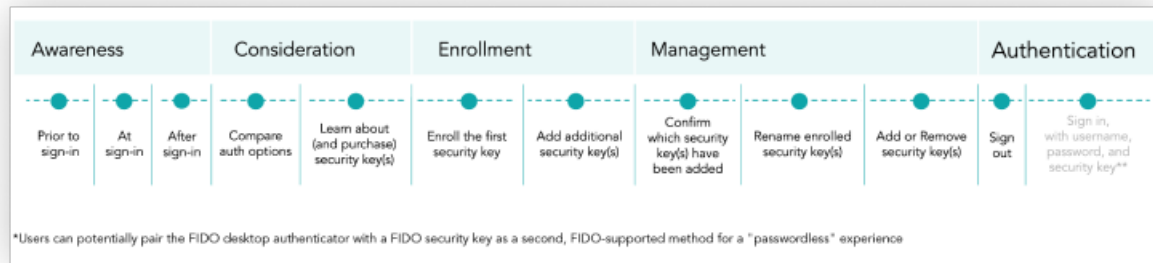


Figure 9 — Security and Privacy settings page (after security key enrollment)

Authenticate



Purpose:

Allow users with enrolled FIDO security keys to sign in with their security key as a second factor after entering a username and password.

Recommendations

- After security key enrollment, do not alter the first factor (i.e., username and password) sign-in experience
 - User research suggests that updating the homepage to communicate that a security key has been added to the account was viewed as a privacy and security violation.
- Preserve secondary non-FIDO security key sign-in paths
 - Offer "Switch user" and "Sign in another way" links to preserve multi-user access and other secondary authentication methods the user has registered with the account.
- After username and password is entered, prompt the user to connect their security key when ready.
 - Offer an option (e.g., a "use a security key" button) for the user to initiate connecting the security key rather than automatically launching the browser dialogue for connecting a security key.
 - User initiation of connecting a security key does introduce an additional click but it helps ensure that the browser dialogue doesn't time-out if the user doesn't have their security key handy.
 - Our research suggested that launching directly into the OS/browser dialogues created some anxiety for users who might not have their security key within reach. Users also felt frustrated when retrieving their security key caused the browser dialogue to time out and required the user to restart the enrollment process.
- Sign out Once users have enrolled a FIDO security key, ensure they can sign out of your website using the same UI they used previously with only their username and password.

Sample UI

- After security key enrollment, the sign-in UI for username and password entry should be consistent with pre-enrollment.
- At sign-in, after the user has entered their username and password, display a “Connect your security key” page with a security key icon.
- Allow the user to initiate connecting their key with a “Use security key” button.
- Include a cancel option.
- Include a “Sign in another way” option to ensure the user can utilize a back-up method if their key is unavailable.
- After security key enrollment, the sign-out UI should be consistent with pre-enrollment.

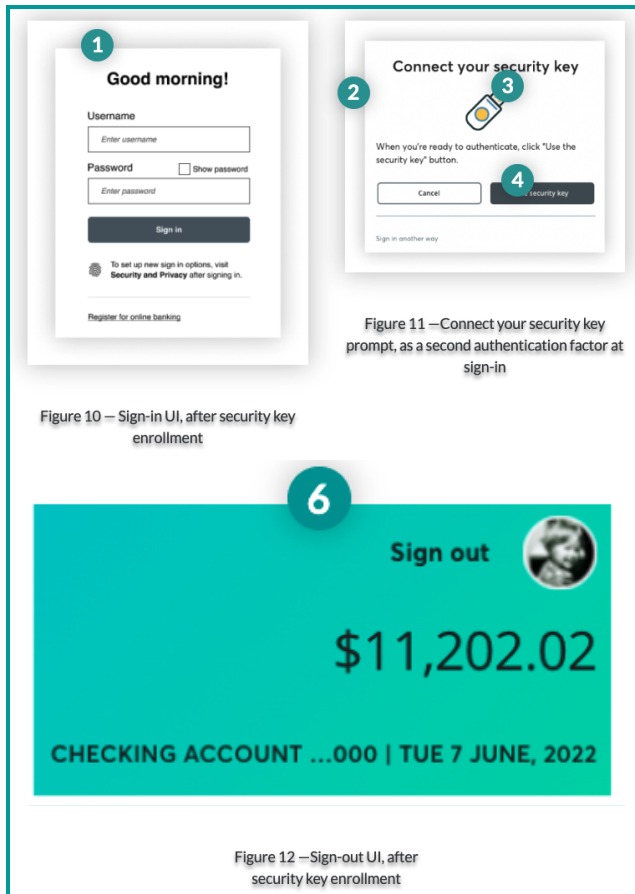


Figure 10 – Sign-in UI, after security key enrollment

Figure 11 –Connect your security key prompt, as a second authentication factor at sign-in

Figure 12 –Sign-out UI, after security key enrollment

Optimize Customer Success with FIDO Security Keys

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

Recommendations

- Lead with familiar authentication language and symbols
 - Rather than explicitly promoting the unfamiliar concept of security keys, promote the availability of alternatives to password-only sign in using the familiar fingerprint icon (if biometrics are supported) or other imagery that represents authentication, such as a lock and asterisks for a PIN.
- Promote the Security and Privacy settings page as the on-site hub for managing and learning about account security in general and security keys specifically
 - Encourage users to visit the Security and Privacy settings page to facilitate the discovery of security keys as a sign-in option. Create a context where users can learn about the nature and advantages of security keys and take action to identify a security key to purchase and/or enroll a security key.
- Educate users about how security keys work to instill confidence and trust.
 - More and more sites are offering security keys for authentication but our research indicates that lack of user education is a barrier to adoption.
 - Our research indicates that the resemblance of a security key to a USB drive leads some prospective users to worry that security keys could contain malware or a virus that might automatically infect a machine when the user inserts the security key into it. Demystifying how security keys work and distinguishing them from USB drives in the “Learn more” text can reassure users and remove that barrier to adoption.
 - Our research indicates that the resemblance of a security key to a USB drive leads some prospective users to worry that security keys could contain malware or a virus that might automatically infect a machine when the user inserts the security key into it. Demystifying how security keys work and distinguishing them from USB drives in the “Learn more” text can reassure users and remove that barrier to adoption.
 - Prepare customer support with knowledge about:
 - How to enroll and authenticate with FIDO security keys
 - Which security keys are FIDO Certified and compatible for use with your site
 - Why FIDO security keys are a safe, secure, and convenient alternative for authentication with your website
- Strongly encourage users to enroll multiple security keys, to help ensure users are not blocked from accessing their account if a security key is lost or stolen.
- Promote the partnership between your brand and the FIDO Alliance.
 - Customer trust in the relatively unknown FIDO branding elements comes first from FIDO’s association with your trusted brand.
 - Additionally, security-aware consumers are more likely to be aware of the FIDO standards, and will be more likely to use their security key.

FIDO Security Key UX Guidelines Terminology

Persistent messaging: Messaging text that is consistently visible within a UI, in a consistent location. Persistent messaging helps ensure that if a user misses a message on a particular visit, the message will still be there, in the original location, to be comprehended or acted upon at a later time, if desired.

Temporary messaging: A brief message that appears onscreen for a certain duration and then disappears, which can be utilized to attract user attention. For example, the novelty and movement of a “toast” notification can attract user attention more effectively than persistent messaging. This type of notification should not obscure user data, should be dismissable by the user, and should not be used for errors that block the user in continuing the task flow.

Progressive disclosure: An interaction design technique that sequences information and options across more than one screen to reduce feelings of overwhelm for users. Progressive disclosure keeps important information within reach, without bombarding the user with all relevant information, actions, or tasks at one time.

Security key: We recommend using “security key” terminology (rather than USB key or key) throughout the UI.

Prosumer: For this document, a “prosumer” refers to a security and privacy-conscious consumer who is an early adopter of security and privacy technologies and services in their personal lives.

Acknowledgments

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

- Dirk Balfanz, Software Engineer, Google
- Julia Elman, Security Experience Supervisor, Login.gov
- Kevin Goldman, Chief Experience Officer, Truona
- George Huszar, Director of User Experience Design, Idemia
- Arthur Law, Head of UX, Yubico
- Pablo Matos, Global UX Strategy and Research Lead, OneSpan North America Inc.
- Joyce Oshita, Certified Professional in Web Accessibility, VMware
- Daria Salice, Product Manager, Identity and Security, Meta
- Megan Shamas, Senior Director of Marketing, 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