Deloitte.

Password-less authentication: The next frontier in security

June 2023

Table of contents

Password-less authentication: The next frontier in security

The relevance of passwords through history

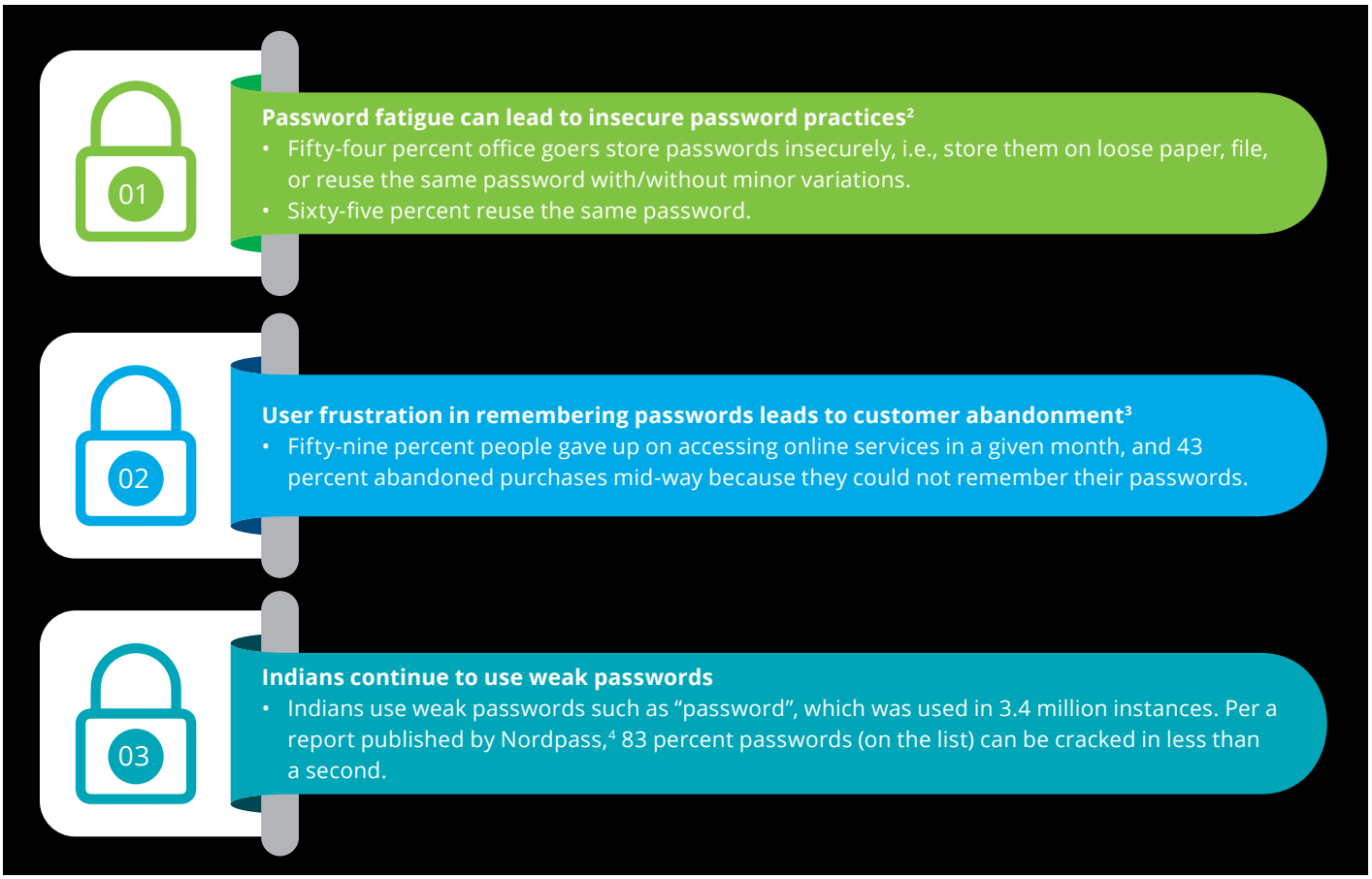
As humans, we have used passwords through time, mainly as a means to grant exclusive access (secret cafés, meeting points, military bases, etc.). The known use of passwords dates as far back as the Old Testament, when two tribes in a conflict used passwords to identify their allies, which effectively screened their rivals as they could not pronounce the password due to differences in dialect. Roman military personnel too used passwords to identify their comrades and provide passage to city gates or secret military facilities. This was also known to have been adopted during the US prohibition when secret cellars or cafes would allow patrons inside only if they knew the password. Such is the history of the ubiquitous password that we adopted into our computing world in the early 1960s.

To date, a set of letters/words familiar to us, i.e., something we know has been our first line of defence to protect our privacy in a connected world. Is it now time to ditch this ancient method of authentication?

The issue with passwords today

Today, passwords are the main gateway to growing online services and the “crown jewels” of any organisation. Passwords are shared secrets that are managed centrally and known to the system as well as the user. Ensuring that passwords are secure is the responsibility of both the user and the system; requiring them to follow complex policies introduced by security teams that take password complexity, expiry, recovery, etc., into account.

For the end user, passwords introduce the added burden of adhering to complex rules with the aim to be unbreachable. It also involves going through complex verification processes if the user forgets the password. An individual user, on average, has 22 accounts and reuses passwords for 16 of them.[1]



User frustration and password fatigue lead to high password reuse and insecure password storage. This has made users vulnerable to credential-based attacks, where attackers steal passwords through phishing or via software programmes in a brute force attack.

Passwords are indeed the weakest link in security and are a major cause of data breach according to Verizon's Data Breach Investigations Report 2022. According to the report, 67 percent of application attacks[5] result from compromised passwords and 82 percent of data breaches involve stolen credentials and phishing.[6]

To help mitigate the risks of passwords being compromised, most organisations implemented multi-factor authentication (MFA) using one-time passwords (OTPs), tokens, push approvals, and authenticator apps. MFA added an extra step of security during authentication; however, it increased friction and user frustration. Hackers now have come up with ingenious ways to bypass MFA through prompt bombing, phishing, SIM swap, account takeovers, etc., which could result in account or data breaches.

Eliminating passwords from the equation while refraining from overwhelming users with multiple levels

[1] Yubico and Ponemon: The 2020 State of Password and Authentication Security Behaviors Report https://www.nass.org/sites/default/files/2020-04/Yubico%20Report%20Ponemon%202020%20State%20of%20Password%20and%20Authentication%20Security%20Behaviors.pdf
[2] Google: https://services.google.com/fh/files/blogs/google_security_infographic.pdf
[3] Verizon: 2022 Data Breach Investigations Report https://www.verizon.com/business/resources/reports/dbir/
[4] https://nordpass.com/most-common-passwords-list/
[5] Verizon: 2022 Data Breach Investigations Report https://www.verizon.com/business/resources/reports/dbir/
[6] FIDO alliance: https://media.fidoalliance.org/wp-content/uploads/2021/10/Online-Authentication-Barometer-Oct-2021.pdf

of authentication is the need of the hour today. While password-less authentication is gaining acceptance in this space, it will still require a paradigm shift.

What is password-less authentication?

Password-less authentication eliminates the root cause of user friction and the weakest link in security. It takes away the frustration of remembering, storing, and transmitting passwords along with adherence to complex rules when setting/resetting passwords. It offers a world without passwords, combined with improved security and a better user experience.

According to Gartner,[7] "By 2025, more than 50 percent of the workforce and more than 20 percent of customer authentication transactions will be password-less".

Thirty-one percent of IT and cybersecurity professionals, responsible for identity and access in their organisations, consider password-less authentication to be the top identity-related activity.[8]

Fast Identity Online (FIDO) Alliance introduced simple and secure ways for password-less authentication and a new standard, FIDO2, which utilises the device that a user normally uses, such as a laptop, desktop, or mobile phone in addition to external authenticators that could be used as a USB attachment or connected over NFC or BLE to authenticate the user.

FIDO Alliance was established in 2013 and now has leading global technology, industry, and government organisations as its members. FIDO's mission is to promote open authentication standards and reduce the world's over-reliance on passwords.[9]

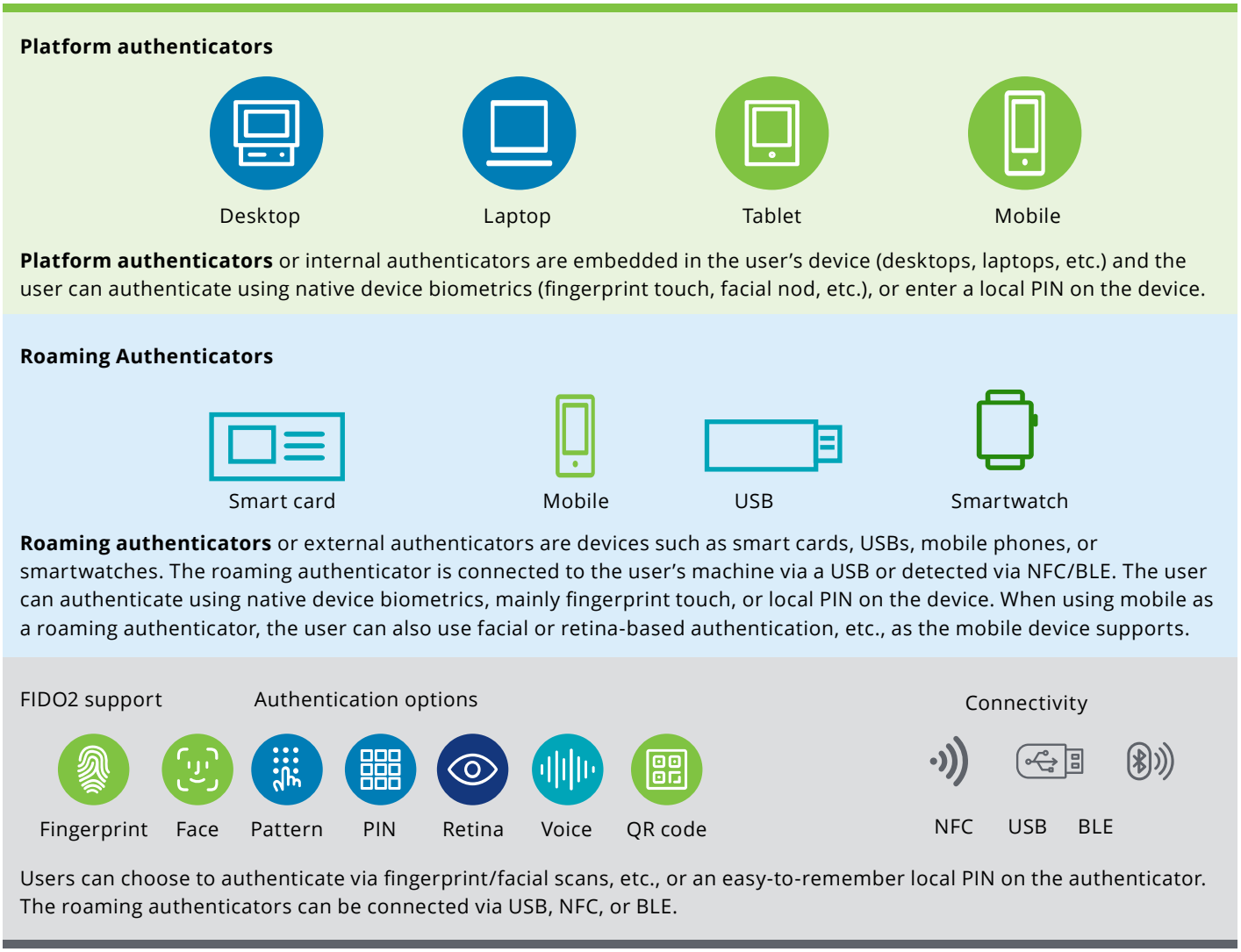
[7] Gartner: You, Too, Can Start Enjoying the Benefits of Password-less Authentication Today
https://www.forbes.com/sites/forbestechcouncil/2023/03/23/embracing-the-end-of-the-password-here-and-now/?sh=a2f93aa30e23

[8] https://www.secureauth.com/resource-center/ebooks/esg-report-2022/

[9] FIDO alliance overview: https://fidoalliance.org/overview/

Figure 1 summarises how FIDO has enabled devices generally used by users as authenticators by utilising local authentication on devices and connectivity over commonly available protocols.

Figure 1: FIDO authenticators - Platform v/s Roaming authenticators



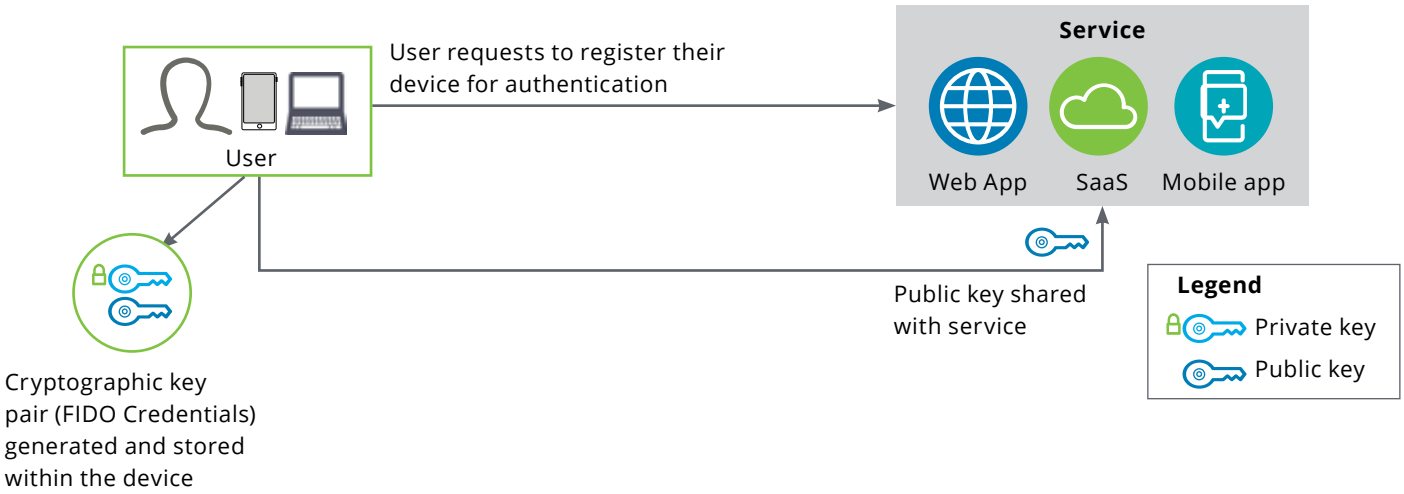
Before FIDO2, smart cards, certificate-based authentication, magic links, etc., offered password-less solutions; however, these were proprietary, not portable across browsers and operating systems, resulted in vendor lock-in, or were not phishing resistant and as secure as FIDO2.

How does it work?

Before a user can log in with a FIDO authenticator, users have to register the authenticator with a service, for instance, a web, SaaS, or mobile application.

The user can register on a platform or a roaming authenticator, based on business and security requirements, with the ability to decide what local authentication option to use, for e.g., PIN, fingerprint scan, or pattern swipe. When a user registers for a service, a cryptographic key pair (public and private key) is generated and stored securely on the user's device. This key pair is referred to as FIDO credentials or simply password-less credentials (Figure 2).

Figure 2: User registration of FIDO2 credentials



Once a user registers a device for password-less authentication, they can log in to the service by using their fingerprint, PIN, or facial scan, etc., as supported by the registered device. In the background, FIDO2 uses standard public key cryptography to authenticate the user, using the stored credentials.

Password-less credentials have to be registered for every device and service. This can be cumbersome and could lead to reliance on insecure recovery processes such as legacy passwords, in a scenario where the user's device gets stolen or misplaced.

To address this issue, FIDO2 introduced passkeys or multi-device, discoverable credentials, which are stored securely in the user's cloud service provider and can be available to the user even if the device is replaced or stolen. If the user has registered their password-less credentials on their mobile phone and accesses the same application from another device, they will be prompted to use the registered credentials from the mobile, if they prefer. The entire process of using passkeys is designed to be easy, user-friendly yet secure, as both mobiles and laptops need to be in physical proximity for the credential discovery to be facilitated over Bluetooth Low Energy (BLE)/ Near Field Communication (NFC).

Passkeys have been adopted by leading multinational technology companies[10] and implemented on their platforms as an alternative to passwords for their users.

[10] https://fidoalliance.org/tech-times-apple-google-and-microsoft-are-pushing-passkeys-password-less-future/

Benefits of going "password-less"

Password-less authentication balances security and privacy along with providing an enhanced user experience and ease of integration/adoption, thus making it a compelling alternative to passwords.

Figure 3: Benefits of FIDO2

Frictionless user experience

Users can choose an authentication method biometric, PIN, or pattern they are comfortable with on their device

Finger touch | Nod on camera | Scan QR code | Swipe a pattern | Enter local PIN | Look into the camera | Speak into micro phone

With discoverable credentials, the user can use the same credentials across devices to access the service

Improved Security

FIDO2 offers multi-factor authentication by default as it combines two authentication factors

1 + 2 OR

Device Something you have

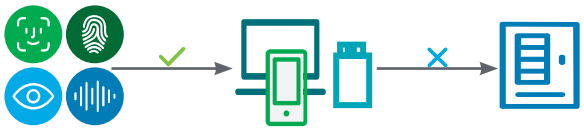
Biometrics Something you are

Local PIN Something you know

Phishing resistant, as there are no shared secrets or passwords that an attacker can steal and it also requires physical proximity of the authenticator during registration and login

Privacy by design

User biometric data is stored on the device locally



User's FIDO credential private key does not leave the device

User activity tracking is not possible as each service has a different FIDO credential

Easy of integration and adoption

FIDO2 is widely supported across leading platforms and browsers

Platforms: Android, IOS, Windows

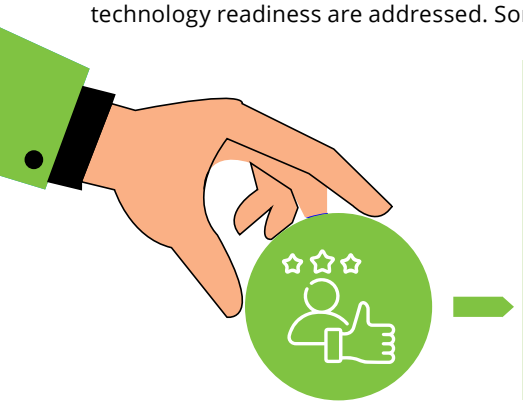
Browsers: Edge, Firefox, Chrome, Safari

A simple JavaScript API call is required for websites/ applications to build FIDO2 support.

FIDO is supported by leading access management and authentication technology vendors.

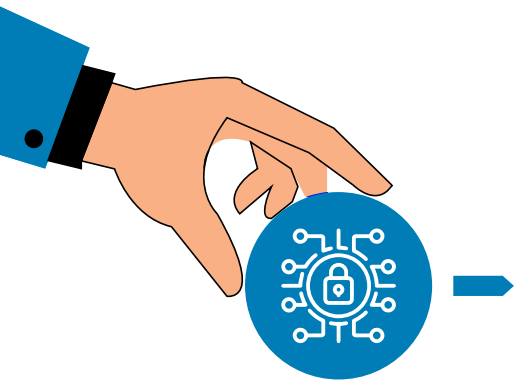
Key considerations as we embark on a password-less journey

As organisations embark on their password-less journey, they need to keep in mind how the user experience, security, and technology readiness are addressed. Some key considerations are as follows:



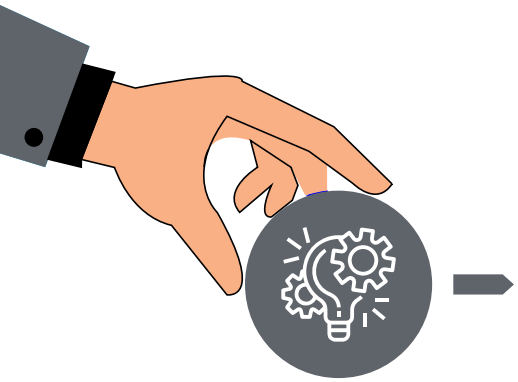
User experience

- User acceptance and adoption will rely on how easy it is for users to move to a new way of authentication. To make the transition easier, users should be allowed to authenticate themselves using options they are familiar with e.g., PIN, fingerprint scan, and facial recognition.
- There will be a learning curve and training will be needed to use biometrics and newer technology including NFC and BLE securely, based on user demographics. Organisations can utilise the FIDO Alliance UX guidelines[11] to enable the design of consistent user experience to help maximise adoption.



Security

- The recovery process in the case of malfunction, loss, or replacement of a device should be well-designed and secure. It should not result in the reliance on passwords or legacy recovery methods that could expose users to credential-based attacks.
- Review of adaptive authentication or behavioural biometrics should be implemented for critical and financial applications. This will help protect against potential bad actors gaining access to the user's authenticator and credentials.
- Staying up to date on new attack vectors and having a proactive mitigation framework/plan in place is crucial. Additionally, planning periodic security reviews to review the overall security posture should also be considered in the overall risk management process.



Technology

- While FIDO2 is supported across most platforms and browsers,[12] it may not necessarily work on older versions. Similarly, passkey[13] implementation varies amongst platform vendors. Organisations need to review the versions of the most-used platforms and browsers in their organisation while planning their password-less journey.
- The organisation's application landscape, both on premise and cloud, should be evaluated to understand if they support password-less authentication, for e.g., a review of password-based legacy applications. It is also possible that modern applications may not support it in their base versions or may require additional costs to enable this feature.

Can FIDO password-less authentication be adopted universally across industries?

FIDO2 password-less authentication has universal applicability and can be adapted for both, the workforce and customers. It needs to be tailored based on the industry, user expectations, security and regulatory requirements.

For the **workforce,** implementing password-less authentication will help reduce friction, enable remote work, reduce helpdesk

[11] FIDO Alliance: https://fidoalliance.org/ux-guidelines/

[12] https://webauthn.me/browser-support

[13] https://passkeys.dev/device-support/

password reset costs, and reduce the time spent on password resets.

- Platform authenticators are best suited for a workforce that has dedicated laptops or desktops, irrespective of whether they work remotely or in office.
- Roaming authenticators can be deployed for a workforce that shares machines, such as call centres/ITES or front-line workers in retail. This can help reduce the lack of accountability that may arise with sharing user ids, a common practice in retail.
- Mobile phones as a roaming authenticator can enable organisations to phase out hard tokens typically used for secure remote login, privileged access, or critical infrastructure access.
- Passkeys or discoverable credentials are stored on the cloud service of the user's device and not managed by the organisation. This may not be acceptable from a security perspective. Hence, these are not recommended for enterprise workforce deployments.

Similarly for **vendors/partners** too, authenticating using their own devices will help reduce the operational costs associated with communicating and resolving login issues.

- For customers, a frictionless experience to access this service from multiple devices is of the highest priority. Organisations aim to offer this experience securely, and going password-less can help enable this.
- For organisations in the B2C space (retail banking, e-commerce, etc.), going password-less will help eliminate exposure to stolen customer credential-related breaches. They can evaluate FIDO2 capabilities relevant for the platform, roaming authenticators, as well as passkeys for a secure and seamless user experience.
- For regulated industries, such as the banking and telecom sector in India, regulatory approvals of the FIDO2 standard as a single factor for customer authentication are not formally available and hence, adoption may be a challenge. Passkey acceptance will also face similar challenges.
- FIDO2 roaming authenticators, i.e., mobile phone as a FIDO authenticator offers better security than SMS OTP and can be considered as a 2FA replacement for SMS OTP[14] in both regulated and non-regulated industries.

Preparing for the journey to a password-less organisation

Moving to password-less authentication is not just a technology change, but also a mindset shift for all stakeholders—user, security, business, and technology teams. Organisations evaluating password-less authentication should consider the following while developing their adoption strategy:

- **Define programme goals and outcomes:** Understand the organisation's vision, business, security, privacy, usability, and regulatory requirements to define programme goals and expected outcomes. For e.g., improved user experience, reduced helpdesk cost, and reduced exposure to cybersecurity threats.
- **Adopt a platform-based approach**: Access management platforms can enable both password-less as well as password-based authentication, thereby providing flexibility for adoption. Access management platforms and specialist authentication vendors provide support for FIDO2 and will enhance their product as the protocols and technology evolve.
- **Start small and build on success:** Identify application(s) with the maximum business impact, best suited for the user demographic and technology fit. Learn and build from the initial success to eventually extend password-less authentication to the rest of the enterprise landscape in a phased manner.
- **Set realistic and achievable goals for adoption:** Moving to password-less authentication is not just a technology change, but also a mindset shift. Start with enabling password-less as an MFA, for desktop login, while keeping an option for users to continue with passwords, and phasing them out as adoption grows and matures.
- **Focus on user experience, communication, and training to maximise adoption:** End user acceptance and adoption of password-less authentication is critical for the success of going password-less. It is important to take the time to build user awareness and rollout guidelines to enable adoption.
- **Measure and review program success:** Seek user feedback and review challenges and learning to bring improvements. Build metrics, for e.g., percentage of password use per application and the number of password-less registration/ logins to measure and report programme success.

Are we ready to go fully password-less?

Support for password-less authentication is evolving as vendors, platforms, and applications continue to build support for FIDO protocols. While factors such as deployment costs, regulatory guidelines, and user readiness will affect full-scale adoption, legacy and modern authentication factors will continue to co-exist as password-less authentication gains acceptance. Organisations should start evaluating password-less login to improve their overall security and user experience. Organisations should also consider utilising frameworks and architecture offered by access management or specialist authentication vendors to enable a smooth transition to a password-less organisation.

[14] FIDO2 Authentication in line with RBI Master Directions: https://media.fidoalliance.org/wp-content/uploads/2022/09/FIDO-White-Paper-_-FIDO-Authentication-in-Digital-Payment.pdf


Cloud

Connect with us

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Tarun Kaura
Leader – Cyber Advisory, Risk Advisory
Deloitte India
tkaura@deloitte.com

Anand Venkataraman
Partner, Risk Advisory
Deloitte India
anandv@deloitte.com

Contributors

Sabiha Hetavkar

Deloitte.