GUIDE

HYPR

Passwordless Security 101

The Basics and Benefits of Passwordless MFA and Passkeys

The Problem With Passwords

Passwords pose one of the most significant security risks for businesses. A recent survey revealed that 65% of people reuse passwords across accounts, and nearly half hadn't changed their passwords in over a year, even after a known breach.[1] Given how cheap and easy it is to deploy credential stuffing and password spraying attacks, passwords are the equivalent of locking a door but leaving the key under the mat.

Growing awareness of this fundamental security flaw has made passwordless authentication, including passkeys, one of the biggest trends in cybersecurity. The vast majority of IT and security professionals (85%) believe that their organization should reduce the number of passwords used by employees.[2] Whether you're a seasoned professional or a newcomer interested in learning more, this guide provides a comprehensive overview of passwordless security. It covers passwordless vocabulary and concepts, passwordless authentication's primary drivers, a high-level look at its architecture, and an exploration of the benefits organizations can expect from passwordless authentication.

Passwordless Authentication: The Basics

Let's look at some of the basic questions surrounding passwordless technology, standards and implementation.

What Is Passwordless Authentication?

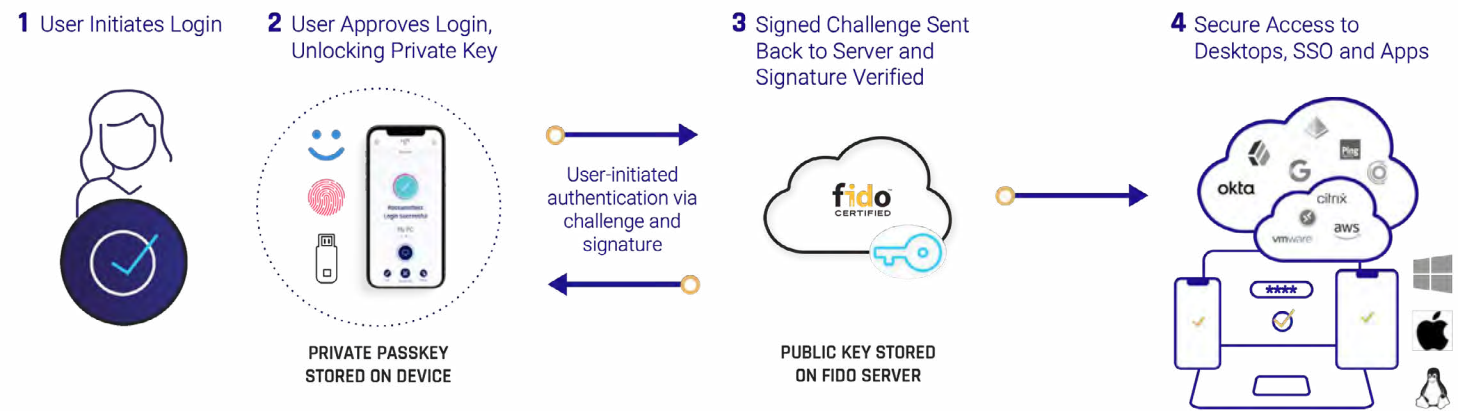
In its most general sense, passwordless authentication is a method of verifying a person's identity without using a password. To log into a computer system or an online service, a person provides a secure form of authentication such as a fingerprint, facial recognition or hardware token/security key. Each of these forms of authentication is considered a "factor." Most passwordless login methods require more than one authentication factor — hence the term "multi-factor authentication" (MFA). Passwordless MFA solutions provide a highly secure form of authentication without the use of a password.

How Does Passwordless Authentication Work?

Leading passwordless authentication is based on public key cryptography. It uses a private-public cryptographic key pair to authenticate a user's identity. The private key is securely generated and stored on the user device — a mobile phone, smart card or security key — while the public key is registered with the authenticating server.

While the specific authentication experience varies based on the login method, most modern passwordless methods approach the problem similarly. In mobile passwordless authentication, for example, users confirm their identity through secure on-device methods such as Touch ID or Face ID. The process is inherently multi-factor as it involves both something you possess (the smartphone) and something you are (the biometric verifier). This, in turn, unlocks the cryptographic keys to use in the authentication flow to access the desktop and web applications.

The following is an example of a user authentication flow without passwords:



Where Can Passwordless Authentication Be Used?

Passwordless technology can be deployed wherever an authentication action takes place, including:

- **Computers (physical or virtual machines):** Passwordless authentication addresses the need for MFA on laptops, desktops, remote login (Remote Desktop Protocol [RDP], Virtual Desktop Infrastructure [VDI]) and servers.
- **SSO-connected applications and resources:** Applications and tools such as VPNs that traditionally have used passwords or password-based MFA can be securely accessed with passwordless authentication.
- **Web and mobile applications:** Passwordless authentication SDKs can integrate with company web and mobile applications for strong customer authentication.

Is Passwordless Authentication Secure?

Fully passwordless authentication — where no password or similar secret is shared between the person and service — is far more secure than password-based authentication. Credentials never leave the user's device and are not stored on a server, so they are not vulnerable to phishing, password theft or replay attacks. Industry leaders are driving forward open standards such as **FIDO** to increase adoption. Passkeys are an example of passwordless technology based on FIDO standards.

Beware, however, of solutions that provide a passwordless experience rather than a truly passwordless product. For example, a solution may use passwordless biometric features such as Touch ID or Face ID to automatically fill in stored password details. The password is still used for the actual authentication. Some solutions send a one-time password (OTP) by SMS or email as part of their MFA flow. However, by definition, an OTP is still a password, and like all other passwords, it is vulnerable to the same phishing and interception threats.

> ***Beware, however, of solutions that provide a passwordless experience rather than a truly passwordless product.***

What Is FIDO and Why Does It Matter?

The FIDO Alliance is the official standards body behind passkeys and created the widely-accepted open authentication protocols for secure, interoperable passwordless authentication. FIDO Board members include Apple, Google, HYPR, Samsung and others and the Alliance works closely with other industry bodies such as ISO, W3C and the World Economic Forum. CISA considers FIDO-based authentication the gold standard for phishing-resistant MFA.

The Alliance also has certification programs that verify quality and interoperability across FIDO Certified products. You can **check a solution's status** on the FIDO Alliance's online registry of certified technologies.

The Benefits of Passwordless Security

Passwordless authentication and passkeys bring a measurable positive impact to an organization's security, IT and business operations.

1

Eliminating Phishing, Password Reuse and Credential Stuffing Attacks

Phishing and its variants account for nearly half of all cybercrimes,[3] with stealing passwords and credentials their primary goal. These are then used to take over accounts or access systems and data. By eliminating passwords or any type of phishable credential, such as OTP codes or SMS tokens, fully passwordless authentication stops up to 99.9% of phishing attempts, password reuse and brute force attacks.

2

Reducing Ransomware and Data Breach Risk

The top two ransomware infection vectors are phishing and RDP attacks. Moreover, 61% of all data breaches are caused by compromised passwords and credentials.[4] Businesses that remove passwords from their authentication process significantly mitigate these risks by reducing their attackable surface.

3

Cutting Password Reset Costs

Businesses spend too many help-desk hours and dollars resetting passwords and assisting employees and customers locked out of their accounts — each password reset costs an average of $70. Passwordless authentication eliminates these costs and lets companies focus their IT and service resources on more productive, value-generating work.

4

Simplifying the User Experience

Usability removes friction and drives adoption. A well-designed passwordless system provides a fast and easy user experience that accommodates various needs. It incorporates multiple authentication factors into one unified login flow.

5

Increasing Workforce Productivity

The average employee wastes nearly 11 hours per year entering or resetting passwords.[5] That figure doesn't take into account any time spent on extra MFA login steps. With passwordless authentication, businesses improve workforce productivity by eliminating time lost on legacy MFA apps and typing in long, complex passwords.

6

Assuring MFA Compliance

Multiple security regulations and many cyber liability insurance carriers require companies to use multi-factor authentication. Many regulations specifically call for phishing-resistant MFA. Passwordless authentication that adheres to FIDO standards in all components generally meets or exceeds these requirements.

Passwordless Authentication Enables Zero Trust

Zero Trust is an approach to IT system design and implementation that mandates no device should be trusted by default. In 2020, the National Institute of Standards and Technology (NIST) published a vendor-neutral set of guidelines for implementing Zero Trust. A 2020 survey by Microsoft Security showed that 76% of global enterprises have at least started implementing a Zero Trust strategy.[6]

The Zero Trust security framework defines how users inside and outside an organization must be authenticated. It effectively abolishes perimeter-based protection schemes by assuming that any user, device or service could be compromised. At a high level, this means continuously taking measures to assess when and how users can access applications and data.

Zero Trust is more than a concept — it works. The average cost of a data breach at organizations with a Zero Trust approach was $1.76 million less than those without it.[7] The Zero Trust approach is not only gaining widespread traction; the recent Executive Order on Cybersecurity mandates it for federal agencies and companies in their supply chains.

> ***Passwordless authentication allows organizations to enact Zero Trust principles without a negative impact on user experience.***

Phishing-Resistant MFA Critical to Zero Trust

A cornerstone of any Zero Trust initiative is phishing-resistant multi-factor authentication. Under Zero Trust, MFA becomes the gatekeeper, and the strength of that gatekeeper affects the security of the entire Zero Trust architecture. Unfortunately, organizations often find gaps in employee MFA adoption, especially among those who work remotely or travel often. The friction of forcing employees to juggle multiple authentication steps creates adoption hurdles that slow down the Zero Trust initiative as a whole.

FIDO Certified passwordless authentication allows organizations to enact Zero Trust principles without a negative impact on user experience. It builds trust into the user's identity, ensuring that authentication processes align with the highest level of assurance (NIST 800-63B AAL3) for Zero Trust initiatives.

How To Get Started

The security threats and business challenges facing companies of all sizes make clear the need to move away from passwords.

Organizations considering passwordless authentication should first clarify their particular use cases and business challenges by answering the following:

- Do you need passwordless desktop MFA for your workforce? What operating systems or platforms are used?
- Do you want or need integration with your single sign-on (SSO) provider?
- Does your business require risk monitoring and adaptive authentication capabilities?
- Are you looking to enable your digital transformation initiatives?
- How quickly do you need to deploy MFA to meet cyber insurance or regulatory requirements?
- Are you looking to deploy synced or device-bound passkeys for your customers?

When you start looking for a passwordless solution, make sure that it not only aligns with your needs today but will also be able to evolve to meet future requirements.

It's critical that you also take into account factors that could affect deployment and adoption:

- What level of support is required and do you have the necessary resources?
- Is the solution easy to use?
- What level of expertise do you need to manage the software?
- Will the solution scale as your business grows?

With an understanding of the basic concepts and a clearer idea of your authentication needs, you will be well prepared to take the next steps in adopting passwordless security.

Sources

1 Psychology of Passwords, LogMeIn, August, 2021

2 From Passwords to Passwordless, Vanson Bourne and LastPass, October, 2020

3 Internet Crime Report 2020, Federal Bureau of Investigation, March, 2021

4 2021 Data Breach Investigations Report, Verizon, May, 2021

5 State of Password and Authentication Security Behaviors Report, Ponemon Institute and Yubico, January, 2019

6 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha

7 Cost of a Data Breach Report 2021, IBM Corporation, July, 2021

See passwordless authentication in action.

Visit: hypr.com/demo

HYPR

About HYPR

HYPR creates trust in the identity lifecycle. The HYPR solution provides the strongest end-to-end identity security, combining modern passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. With a third-party validated ROI of 324%, HYPR easily integrates with existing identity and security tools and can be rapidly deployed at scale in the most complex environments.