THE CISO'S GUIDE TO PASSWORDLESS AUTHENTICATION

Bojan Simic - HYPR CTO
Edward Amoroso - TAG Cyber CEO

Introduction

A recent study by Akamai showed that more than 50 billion credential reuse attacks happened in 2019. In fact, 56% of consumer banking traffic were malicious login attempts [1]. Such risk has led enterprise teams to rethink authentication, and the goal of providing a stronger, passwordless, multifactor experience has continued to grow more attractive. Microsoft estimates that the benefits of moving away from passwords can reduce the likelihood of an enterprise being compromised by up to 99.9% [2].

The transition to passwordless security is easier said than done, if only because the use of passwords is so ingrained in the use of applications, devices, systems, and workflows. It persists across virtually every segment and sector of business, government, and personal use. Passwords have the advantage of being easy to explain to users, generally easy to implement in authentication modules, and interoperable across a range of different systems.

Such interoperability, however, might be the greatest security weakness of passwords, because cross-domain use creates spectacular vulnerabilities. An employee of a critical infrastructure company might, for example, select a strong password for work-related tasks such as VPN, but if that password is reused for some Internet-facing eCommerce or video service, then the work-related task is put at significant risk of compromise. Security training thus becomes a primary control in the face of normal password usage.

In this report, we examine the means by which enterprise teams might take steps to actually remove their dependence on passwords through a new method known as "true passwordless" security. The idea is closely aligned with strong, multi-factor authentication (MFA), and derives much of its technical foundation from industry groups such as the FIDO Alliance (Fast Identity Online) and guidance set forth by NIST.

We explore 10 of the most popular use cases for passwordless. These are key areas of focus for you to begin your passwordless initiative. We also evaluate 4 ways to deploy passwordless authentication across a wide population of users and devices.

The goal for buyers should be to reduce risk, lower costs, and enhance the user experience.

Who should read this guide?

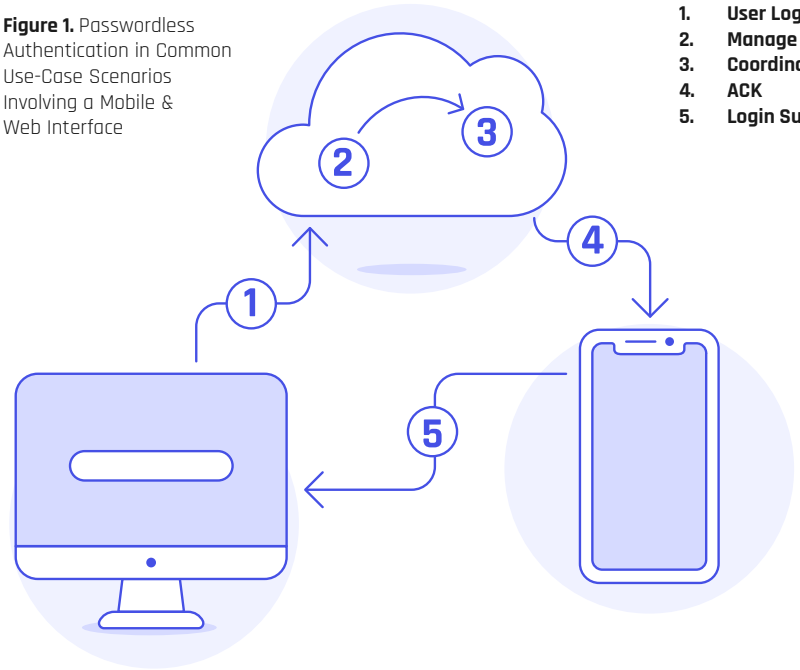
This guide was written for security practitioners, IAM/IT managers and business leaders - folks who deal with password pain on a daily basis - and for whom the pressure to eliminate passwords has never been greater. It is being made available for those seeking a way to stop credential reuse, account takeover, brute force attacks, and lost passwords.

Passwordless Usage

Passwordless authentication is designed to reduce the friction associated with validation of a reported identity, while also reducing the risks and management costs associated with passwords. Generally speaking, passwordless authentication implies a stronger form of security, although presumably if not done properly, it could introduce risk. This underscores the importance of avoiding too much do-it-yourself in lieu of working with an experienced commercial partner.

The schema for passwordless authentication generally involves an identification step to some target asset, system, or resource, followed by a validation step that does not require passwords. It is certainly possible for passwords to be included as an option in the multi-factor layering, but most enterprise teams moving toward passwordless authentication opt for a process that removes passwords entirely. The schema shown in Figure 1 illustrates a common use case.

Figure 1. Passwordless Authentication in Common Use-Case Scenarios Involving a Mobile & Web Interface



1. **User Login**
2. **Manage Identity**
3. **Coordinate Mobile**
4. **ACK**
5. **Login Successful**

A recent analysis by HYPR [3] suggested the following 10 scenarios as being particularly well-suited to benefit from passwordless security. They range from authentication of local devices by individuals to validation of critical transactions in the enterprise, often with the potential consequence of financial loss to the organization. It helps to examine these scenarios closely because they serve to help define the type of functional, security, and assurance requirements for the transition to passwordless.

Workstation Login

The familiar workstation login process for employees and users can benefit from passwordless security in several ways. First, the technology will reduce the aggregate time spent by employees typing passwords. By some estimates, employees might waste as much as 24 hours per year typing passwords each day as part of their normal work activity.[1] Second, the introduction of passwordless workstation login can make the day-to-day experience of using computing devices more comfortable and enjoyable. This helps drive employee productivity and accelerates digital transformation.

Remote VPN

A remote workforce VPN creates a virtual tunnel between the user's endpoint device and the target enterprise. Such remote access by employees, third parties, and even customers is generally done over the Internet with all traffic encrypted end-to-end. A network access server typically terminates VPN requests and authenticates requests based on credentials and passwords. With VPN usage up nearly 54% in 2020 [3], due in part to the pandemic, passwordless support for this process will reduce the massive costs of maintenance tasks such as password resets.

Single-Sign On (SSO)

As a component of the identity and access management (IAM) infrastructure, single sign-on (SSO) capabilities allow users to authenticate once to multiple resources with one set of credentials. The trust relationships required between targeted resource implies the need for high levels of security, so multifactor authentication is desired. Unforutnately SSO implementations have historically relied on passwords. Since SSO addresses the key issue of friction, passwordless support is a natural extension of the function. Passwordless takes SSO to its natural next step by removing passwords from the initial login, binding users to a trusted device and allowing them to extend their authentication thorughout their session.

RDP Access

Enterprise teams often use the remote desktop protocol (RDP), originally developed by Microsoft, to support users connecting remotely to other systems via a simple graphical user interface. It requires that both ends of the connection include special RDP client software for the initiator, and RDP server software for the resource being accessed. Unsurprisingly, RDP attacks are on the rise, reaching an all-time high in mid-2020. RDP requires as much security as possible, and multifactor, passwordless authentication is a desirable option which will support the convenience goal of RDP, while also addressing the obvious risk posed by exposed RDP access ports.

Financial Transaction Approvals

A social engineering attack that businesses must address today involves a fraudster tricking an authorized individual into initiating, approving, or otherwise enabling a financial transfer, often a wire transfer of funds. Such deception might seem unlikely, but empirical data suggests that it is alarmingly common. The use of multifactor proof for authentication and authorization reduce this risk, and passwordless infrastructure decreases the likelihood of the common "password forgotten" excuse that plays an important role in many fraud cases of this type.

---

[1] HYPR recently worked with a major bank that employs 100,000 tellers to study their employee login times. Each successful workstation login averaged approximately 5 seconds. A teller logs onto their computer approx. 60 times each day during a full-time shift. 5s * 60 = 300 seconds * 252 workdays / 3600 = 24.5 hours per employee spent logging in each year. That's approximately 6,575 hours per day spent on typing passwords. Using a 252-day work year, and an average teller pay of $18 per hour, this amounts to nearly $45 million in hourly wages spent on logging in for the entire year.

VDI Usage

Companies employ virtual desktop infrastructure (VDI) to create local desktop views of remote server systems, applications, and software. VDI thus essentially involves hosting desktop environments on a centralized server, where each desktop image runs on a virtual machine (VM). The user accesses the virtual desktop via their PC, tablet, or other device. An important common design consideration for VDI is scaling across a large environment, which implies heavy administrative burdens for password reset functions. The friction of password-based authentication for VDI environments presents a hurdle to its adoption. Passwordless VDI implementation is thus an important time and cost saver in such environments that can accelerate usage across the enterprise.[2]

Banking

The advent of online banking dramatically improved the convenience of personal and business financial management (as was also the case with the introduction of ATMs). While it should be straightforward to log into an online bank website, this is not always the case (as one finds with the dreaded "online services not available at this time" message). Since lost or forgotten passwords are a common root cause for most cases of inability to view online banking information, a passwordless experience should be viewed as an essential requirement in most cases.

Payments and eCommerce

Securing consumer payments for eCommerce transactions has been addressed mostly at the infrastructure level. Secure sockets layer (SSL) and HTTPS secure transport, for example, have secured online shopping and consumer activities. Some friction and transaction velocity issues do remain, however, mostly at the application level – and often with passwords. Businesses have been reluctant to add layers on top of passwords; according to Mary Meeker's 2019 Internet Trends Report, the number of websites supporting Two-Factor Authentication (2FA) had *dropped* to 52% - citing friction as a key driver. A passwordless experience directly addresses these challenges, reducing the likelihood of shopper abandonment during transactions. As such, notable eCommerce giants such as Rakuten and eBay have made passwordless available to millions of users.

Support Authentication

Support centers measure success in two areas: productivity of the support workforce, and satisfaction for customers needing assistance. In each case, the removal of friction in workflow drives high-quality interactions, especially in call centers with traditionally long wait times. When passwords are part of this process, it is clear that passwordless methods such as mobile PUSH should be considered to improve both worker productivity and customer satisfaction.

Personal Login (Of Course!)

According to Microsoft, more than 150 million people are using passwordless methods each month as of 2020. It is a fact of modern life that we authenticate to personal devices many, many times per day – and this process is not always successful. Touch ID and Face ID have helped remove friction, but wherever passwords are used, the aggregate time spent – including time used when the passwords are not working – can be massive. For this reason, passwordless authentication can improve our day-to-day use of technology reduce the frustration that accompanies use of multiple personal devices.

---

[2]HYPR analysis shows that VDI adoption has increased considerably in the financial sector. One large bank, for example, is rolling out more than 90k workstations on VDI in 2020.

Passwordless Options for Buyers

Enterprise buyers have many different commercial options to implement a passwordless experience, each focused on the goal of reducing hard and soft costs, as well as to improve productivity of both users and IT operations teams involved in day-to-day support tasks such as password resets [4]. Below, we analyze the pros and cons of several commercial technology options for buyers to hopefully simplify some of the decisions and source selection tasks inherent in the shift to passwordless authentication.

An important consideration for authentication options is that point-solution emphasis on one-time passwords and legacy SMS is being replaced by more holistic platforms that support a range of passwordless options. Enterprise teams are thus encouraged to seek platform solutions that can build an authentication layer that can be used to match up with the use-cases that matter to the business – recognizing, of course, that these will often be quite different.

FIDO2 Mobile and Web Passwordless Platform

For organizations that prefer a solid vendor partnership to support migration to a passwordless user experience, many good commercial platform options exist. Buyers should seek a commercial partner that includes passwordless MFA, FIDO compliance, SDK support, desktop and mobile apps, convenient management and support tools, and a means for extending passwordless authentication to public cloud-based services.

The most compelling argument for a commercial platform solution lies in its cross-platform functionality. That is, well-designed passwordless support from a vendor will include the ability to integrate all of the options described above, including Windows Hello, Smartphones, FIDO2 tokens, and many more methods such as Active Directory authentication, VDI-based authentication, Passwordless Single Sign-On and identity plugins from commercial vendors.

Advantages of Mobile and Web Passwordless Platform

- Rapid time to value by focusing on devices your users already posess (i.e. smartphones, laptops)
- Excellent commercial vendor options are available for buyers
- Provide integration of common passwordless methods including FIDO2 and biometrics
- Provide SDK support to enable extensibility for local systems and applications
- Interoperable with authentication plugins from commercial identity vendors
- Enable expert support partnership for enterprise authentication teams

FIDO2 Security Tokens

The Fast Identity Online (FIDO) Alliance was created in 2013 to promote authentication standards and reduce reliance on passwords. Its members, now hundreds of companies and groups, publish open specifications that support a range of authentication methods including biometrics, trusted platform modules (TPMs), USB security tokens, and smart cards. FIDO relies on a PKI handshake where clients provide a locally generated public key to a server as the basis for a subsequent authentication challenge.

The FIDO Universal 2nd Factor (U2F) and its extension FIDO2 is a particularly influential open authentication protocol which supports users access many online services without reliance on passwords. It works by services asking users to select one of several available FIDO authenticators, and to then generate a public/private key pair. The public key is shared with the desired service, which then sends an encrypted challenge. The user digital signs that challenge, which verifies its identity.

Advantages of FIDO2 Tokens for Passwordless Authentication

- Hardware-based security keys achieve a higher level of assurance, especially when used in conjunction with MFA
- Defined by open specifications that encourage use of strong authentication
- Open Standards managed by a large community of FIDO consortium vendor participants such as Microsoft, Google, HYPR, and more
- Reliably evolving from FIDO to FIDO2 as computing technology progresses
- Security protection is built on a mature public key technology foundation

Windows Hello

Microsoft has created a biometric authentication method for Windows 10 called Windows Hello that allows users to validate their identity with their fingerprint, iris scan, or facial recognition – thus removing the need for a login password. Users set up the process in the sign-in options under their account settings by registering their facial, iris, or fingerprint scan. Once done, they can access Microsoft accounts and applications with having to enter a password.

The technology works via 3D structured light alongside anti-spoofing methods to reduce the likelihood of impersonation. The system works for users with Microsoft accounts as well as other services (non-Microsoft) that support FIDO. As one would expect, Windows Hello was designed for both enterprise and consumer use – and it appears to be popular in both environments. Apple FaceID offers somewhat comparable support for iPhone X mobile users.

Advantages of Windows Hello for Passwordless Authentication

- Integrated into the Microsoft Windows 10 operating system
- Designed to support FIDO specifications for open authentication
- Supports use of biometric validation with facial, iris, and fingerprint recognition
- Dramatically reduces need for password to access operating system and applications
- Includes anti-spoofing methods to improve accuracy and avoid fraud

Smart Cards

A smart card offers credit-card sized convenience for electronic identification, authentication, and authorization to resources. They are sometimes contactless and can include functions such as data storage and application processing. The most common use of smart cards is for personal identification, national population identification, financial services transaction enablement, and even mobile device processing (SIM cards are a form of smart card).

Smart cards work via an embedded integrated circuit that operates like a small computer with a microprocessor and memory. Most people think of smart cards in the context of their associated readers through with which direct physical contact is made. Many smart cards work through a remote interface with contactless operation via radio signaling. Such design greatly extends the potential use case options for smart cards.

Advantages of Smart Cards for Passwordless Authentication

- Offers credit-card sized convenience for users
- Well-suited for personal identification systems including national databases
- Extensible to support adjunct storage and processing (such as in a SIM card)
- Includes near-field contactless operation through radio interface
- Supports many familiar use cases for business and consumer users

Common Questions

Is OTP a viable alternative to passwordless?
One-time passwords (OTP) are not considered a passwordless solution. While there have been improvements in the overall user experience of OTP-based authentication methods, they inherently rely on passwords and shared secrets. While OTP does not eliminate the use of passwords, one advantage is that it is free. Users adopting an OTP product should consider one of the many free solutions such as Google Authenticator.

What is FIDO Certification?
FIDO Certified products are solutions that have undergone rigorous testing around security, usability, and scalability. Certification by the FIDO standards body, or lack thereof, speaks to a solution's enterprise readiness and deployability. While all FIDO Certified products adhere to similar standards, the solutions vary in speed, usability, and accessibility. Read the FIDO Buyer's Guide to learn more about comparing FIDO products.

What is the difference between FIDO-Certified and FIDO-Supported products?
The official term is "FIDO-Certified." Be cautious of vendors who advertise Passwordless authentication by claiming to be "FIDO-Compliant" or that they "Support FIDO." Using such compliance badges as a marketing gimmick is an old yet effective tactic. Users should ask vendors if both their mobile client and validation server are FIDO-Certified, and can verify their claims with the FIDO Alliance's online registry of Certified technologies.

How can we prepare our help desk?
Your help desk is used to "I forgot my password." In a passwordless environment, the volume of calls goes down as passwordless requests rise. For example, "I lost my phone." is a remark that may come up more often. It's important to have a helpdesk that is trained and ready for any passwordless request that comes their way. Follow the HYPR Help Desk Guide to provide your Help Desk and IT teams a reference to help end users with setup and troubleshooting.

Does NIST provide any guidance for passwordless?
NIST (SP) 1800-17* recommends FIDO as an optimal approach to MFA. This distinguishes what Gartner calls "FIDO-Centric authentication" approach as superior to legacy MFA. Notably, the NSA has recently published guidance recommending passwordless FIDO2 based authenticators such as Yubikey.

References

[1] Akamai Threat Research, 2019
(https://www.akamai.com/us/en/about/news/press/2019-press/state-of-the-internet-security-financial-services-attack-economy.jsp)

[2] Passwordless Protection, Microsoft Research Report, 2018
(https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2KEup)

[3] HYPR Infographic on Passwordless Use Cases
(https://www.hypr.com/top-10-passwordless-use-cases/)

[4] J. Chik, "Go Passwordless to Strengthen Security and Reduce Costs," Microsoft Identity Article, December 11, 2019
(https://www.microsoft.com/security/blog/2019/12/11/go-passwordless-strengthen-security-reduce-costs/)

Bojan Simic is the Chief Technology Officer and Cofounder of HYPR. Previously, he served as an information security consultant for Fortune 500 enterprises in the financial and insurance verticals conducting security architecture reviews, threat modeling, and penetration testing. Bojan also serves as HYPR's delegate to the FIDO Alliance board of directors, empowering the alliance's mission to rid the world of passwords.

Dr. Ed Amoroso is currently Chief Executive Officer of TAG Cyber LLC, a global cyber security advisory, training, consulting, and media services company supporting hundreds of companies across the world. Ed recently retired from AT&T after thirty-one years of service, beginning in Unix security R&D at Bell Labs and culminating as Senior Vice President and Chief Security Officer of AT&T from 2004 to 2016.

About HYPR

HYPR is the Passwordless Company backed by Comcast, Samsung, and Mastercard. Passwords and shared secrets remain the #1 cause of breaches despite billions of dollars invested in cyber security. The HYPR Cloud Platform makes it easy to go Passwordless across the enterprise by combining the security of a smart card with the convenience of a smartphone.

With HYPR, businesses are finally able to solve the desktop MFA gap, eliminate customer passwords, and deliver lightning-fast login experiences their users love.

#EliminateTheTarget at www.HYPR.com

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

1001 Avenue of the Americas, 10th Floor
New York, NY 10011

1-866-GET-HYPR
www.HYPR.com