PRIVATE, STRONG & PASSWORDLESS:

A GUIDE TO PASSKEY AUTHENTICATION

WHAT IS A PASSKEY, AND HOW DOES IT CHANGE THE FACE OF ACCESS?

While it almost seems quaint, a rather secure approach to safeguarding one's physical keepsakes is the old-fashioned safety deposit box. It can hold deeds, family heirlooms, passports, or any number of precious items that individuals don't trust to their own homes. Anyone wishing to retrieve these items needs to access the secure part of the bank where the boxes are stored, and bring a personal key. In addition, an authorized staff member of the bank must also produce a key, and together, they can open the box.

This is sometimes called a "two man rule." Some banks require multiple parties to open a larger vault. Various organizations require multiple parties to approve and spend sums over a certain amount. The purpose is to prevent any one individual from creating large scale fraud. And of course the US, along with other countries, physically requires multiple parties acting in concert to enable and launch missiles.

But in the current day and age, a large portion of our most precious assets are digital, and therefore need to be safeguarded accordingly. Increasingly this requires strong defenses and inventive approaches. Dropboxes, photo albums, security videos, documents, and other treasures need to be digitally sealed and made available only to authorized parties. But the traditional, and traditionally unsafe, root to securing these is the most quaint "safeguard" of all, the ubiquitous password. While passwords are certainly a layer of security, there are routes to stealing them passwords, guessing them, or even bypassing them using security questions. The very information brokers who supply the data used in identity proofing also supply that data (through breaches) to the bad actors who use it to take over accounts and reset the passwords, locking out their legitimate owners. And sometime the passwords themselves are simply purloined.

There are many more users than authorized officials to pull off a two man rule in the digital world. We can't all have a twin on the other side of a digital transaction to pair with and ensure secure access. So how to empower this kind of safeguard, so users can achieve access and enact business at the speed of the internet, in way that requires two complementary components, both of which are locked down until they're needed? And preferably do all of this in a passwordless way?

The answer is **passkeys.**

PASSKEYS – BETTER AND SAFER THAN PASSWORDS

So what is a passkey? Let's start with *why* they're needed.

Passwords are still universal, and the world still largely runs on them. But they have so many weaknesses, and bring out the worst in users themselves. Passwords are stored on the server, where they become a honeypot for bad actors who can steal them and use them for not just

break-ins but breaking in on a grand scale. Credentials stuffing works on the premise that users utilize the same password across multiple systems, such as their email, social media, banking accounts, and other assets. The password is the root of access, and is all too often compromised, thereby becoming the root of penetration.

Users not only forget their own passwords (or allow them to expire), they even forget their own security answers which allow them to recover their access, and these answers are often available for bad guys to discover on the dark web. In 2008, a well-known political candidate's mailbox was broken into when a mischief maker clicked her "forgot password" link and answered her security questions, all of which were easily Googled.

The password is typically the baseline of trust, but at a high risk. Hence, many organizations are pushing for alternatives and a future without passwords, or at least a greatly diminished dependence on them. Multi-factor authentication is not a new concept, but too often it requires one-time passwords or PINs, delivered by SMS or email, all of which incur additional risks. Passkeys, coupled with biometrics, are a far more secure version of MFA, bypassing the weaknesses MFA typically entails.

The passkey (sometimes called a FIDO passkey or FIDO2 passkey) is a login credential that serves the same purpose as a password, announcing the user's entry and asserting the right to access. But the passkey takes that high risk out of the equation, and is far more flexible as well. Experts and pundits who cover the tech industry continue to weigh in on the benefits of passkeys.

(And if you're still wondering "what is a passkey" then check out https://www.techtarget.com/whatis/definition/passkey. If you want a definition with opinions, you might prefer What the hell are passkeys and why are they suddenly everywhere?)

Passkeys are not as universally adopted as, of course, passwords, but they are gaining a greater foothold all the time. Even the New York Times has recognized FIDO passkeys as the future although they have written of physical keys which are not trivial when it comes to provisioning, handing out, supporting, and getting back when somebody leaves the company).

Passkeys eliminate the need for passwords and the dangers, as well as the management headaches, that come with them. They are specifically bound to a website or application, and can only be used by those targets. Because of that feature alone, credential stuffing attacks don't work. Any one FIDO passkey is bound to a single entry point, so in the near-impossible event of a stolen passkey, it could not be used across a user's entire portfolio of assets.

Passkeys are sometimes referred to as multi-device FIDO credentials. Originally, FIDO creds were single device only. But now they are portable, meaning they can traverse devices, and they are recoverable, even when the device they originate on is lost or stolen. In addition, the user has no need to register their full identity a second time. Passkey login is flexible, potable, secure.

CISOs forever create unpopular policies for password expiration, as well as password strength. Users are perpetually frustrated by the need to not only devise a new password every sixty to ninety days, but also in a format the satisfies the requirements for complexity: length, alphanumeric, special characters, and with sufficient variation from previous passwords. Passkeys, however, are born strong, without burdening the user with the responsibility for that complexity, making passkey login powerful from birth. They take little time or effort to generate. You don't have to remember them or write them down on a Post-It, since they're stored on your device. And no bad guy will ever send you a phishing email asking you to input your passkey into a fake credential collector. Not that it would do any good anyway, since passkeys require the aforementioned halves to work in unison.

Another important aspect of this design is that neither half of the key pair can be used to reverse-engineer the other.

PASSKEYS - A DIGITAL TWO-PARTY APPROVAL

Two-factor / multi-factor authentication typically includes among those factors the very things that passkeys despise, passwords. Passkeys completely displace 2FA / MFA, such as when a user needs to receive a text with a code or PIN that must be typed into an app. Unfortunately, MFA starts with a username which is more often than not an email address, which is easily found.

Worse than that in terms of user experience is Knowledge-Based Authentication (KBA), requiring a user to answer random questions that they may have set up in advance, or which may be gleaned from a data broker (eg. Lexis-Nexis or Experian) or social engineering. MFA in general produces by its very nature a great deal of friction.

FIDO passkey authentication bypasses that friction, as it does not require an additional step. There is no email stop, no push notification, no text or PIN. However, passkeys do provide even greater security, in tandem with that superior user experience, while leveraging multiple layers of protection, all of which are managed by users themselves. No help desk, extra devices, or additional intervention are required to create achieve or secure the needed access possible through passkey login.

The passkey actually consists of multiple factors, in the form of a public key and a private key. The user keeps the private key, typically on their personal device, laptop, or physical security key. The device can be a hard token that can be inserted into a laptop, but a personal device is infinitely easier, and more economical. Devices can also be locked down with a PIN, but if that PIN is compromised by a thief who also physically acquires the device, the security of the device itself would be at risk. This is why the devices that contain a FIDO credential are best secured by the other aspect of FIDO authentication, a biometric.

All that's stored on the server (as in the service provider) is the public key. When challenged for authentication, the user answers the challenge by providing the private key. Together those keys generate the authentication token necessary for access.

If somebody could actually steal all the public keys of all the users on a server, they couldn't do anything with them, since they're useless without their private counterparts. Likewise, the private keys should be locked down with biometrics, making them equally difficult to leverage.

By storing FIDO passkeys for every target app, a user does not need to track the many credentials they use for their many applications. This eliminates the headaches of managing multiple passwords for multiple apps, or the danger of using that same single password for those apps.

A VARIETY OF USES AND PLATFORMS

Clearly passkey authentication is all about secure access. Passkeys are focused on specific websites or applications. They can also be requested in the case of high risk transactions, or checkouts on e-commerce sites. Because they are used for passwordless login, passkeys reduce the volume of password reset calls, the user's burden of tracking those passwords, and the enterprise's responsibility to manage and expire those passwords.

By using passkeys on personal devices, the expense of distributing, managing, and collecting hard tokens is greatly diminished as well. While hard token security keys represent a whole other level of safety, they are difficult to provision, distribute, and reclaim when a user leaves the organization.

A passkey cannot be used for more than one site. Passkeys are designed specifically to share no information, and therefore cannot be used for tracking users between multiple sites.

Passkeys are not only very simple to use, they are supported by all platforms run by Google, Apple, and Microsoft. As of May 2023, users can create and implement Google passkeys on their personal Google accounts , and it is easy to find instructions for it. No passwords or dual verification are needed, only the passkey. If the Google passkey is secured with a biometric, that data is never shared with Google itself. Google further provides guidance on Android passkeys.

Shortly after Google's announcement of this support, Apple upped their passkey footprint and followed with support in Safari on Mac OS and iOS for sharing passkeys between individuals or groups of trusted contacts via Keychain, meaning the sharing process is encrypted end to end. This option for Apple passkeys is far more secure than Apple's previous option of sharing passkeys and passwords through AirDrop. (For more info on Apple passkeys, check out their support site).

During this same period, Microsoft launched passkey support for users of 365 (although it doesn't appear to like the actual word "passkey"). While at the same time Microsoft is recommending against password expiration policies (saying such policies encourage users to create increasingly weak passwords), it is promoting passwordless login options such as passkeys. Its passkey implementation is integrated with Windows Hello, allowing biometric technology to unlock those passkeys. But as it has often done, Microsoft has gone its own way when it comes to other integrations. It does not support passkeys across platforms. Passkeys cannot be created on other devices, nor synced between Microsoft platforms and smartphones, for example. And signing up for Microsoft 365 still relies on – oh yes – passwords.

A number of well-known sites are leading the way on adoption of passkeys, sites such as PayPal, eBay, Kayak, GoDaddy, and Best Buy. This level of platform and commercial support will help widen this adoption, hopefully starving hackers of opportunities to compromise user accounts and steal digital assets. In the meantime, the viability of this approach is being borne out by Google passkey, Apple passkey, and other major players.

RECOVERY CHALLENGES – ACCOUNTS AND DEVICES

Lost and stolen devices, forgotten or expired passwords, and account takeovers all propagate the costs of remediation, as well as lost productivity. Even the complexities of standard password management are costly. Despite automated password reset tools in place at most established companies, the vast majority of help desk calls are still password-related. This is not just true for consumers, but also for company workforces.

Account recovery beyond even password hiccups is notoriously complex and frustrating. Account lockouts are common, often requiring human intervention, and become bottlenecks to productivity. Even in FIDO implementations, organizations frequently still require or at least make use of passwords, and those very passwords remain a tempting attack vector. In most situations when a user loses their phone, they still need to log into a new one, and the password is still a factor. It may only be a one-time password (OTP), but even that presents an opportunity for bad actors. And with older FIDO credentials, there is still that need for a password to unlock them.

By establishing an identity rooted in a passkey, which in turn is protected by a biometric, the user removes passwords as the root of trust. By presenting a biometric, for example in the form of their face, the user can instantly reclaim their account and generate a new private key without the need for the organization to ship them a new corporate device or intervene via the help desk. The user possesses their own path to recovering that access, and re-enabling passkey authentication without the additional cost or hassle of engaging IT resources.

Crypto consumers tend to be more tech-savvy, as well as more accustomed to authentication schemes that depend on biometrics and other non-standard protocols. Passkeys offer ever

broader and more secure options for these users. Healthcare consumers constitute a wider variety, and a simpler, passwordless approach is of benefit. And while health data is certainly sensitive, financial services customers worry about the security of their accounts for very different and very obvious reasons.

PHISHING FAILURE

By this time, everyone ought to know what phishing is and how to watch for it. Counterfeit emails from seemingly legit sources ask you to visit a site to take care of some urgent matter. When you click the link you're either infected or directed to a place that looks like your bank or social media account, and when you log in, you've just handed your username and password to the bad actor.

But with a passkey, there's nothing to enter. Since the passkey is stored in the browser, a chip, or a physical key (depending on the hardware), and either the browser or OS performs the actual authentication, the user cannot be tricked into entering credentials into a phony site.

Even if someone steals your private key, they still don't have the public one, and vice versa. So personal device or server breaches cannot compromise user access, on either an individual or mass basis. In addition, there are no shared secrets to be compromised.

There are even options for passkeys to operate across all of a user's devices within a certain physical proximity.

Even MFA doesn't necessarily protect against the most sophisticated phishing attempts, nor does it safeguard against SIM swaps. But once again, passkeys can provide that protection.

ARE THERE DRAWBACKS TO PASSKEYS?

Passkeys in themselves are relatively free of weaknesses. The primary concern is not what they can and can't do but rather what they can't do *yet*. Since passkeys are specific to the devices on which they are created and stored, they are not currently, easily synchronized. Microsoft's support for passkeys, like its deployment of Kerberos for example, is more proprietary. It's expected that more platforms, operating systems, browsers, and other web components will be passkey-friendly. Commercial adoption of any standard is the key to cross-platform support, crowd-sourced improvement of delivery, and ultimately the ability of users to achieve portable identity assertion across all their digital objectives.

The fact that some of the largest players on the web have taken the lead, including with their participation in the FIDO Alliance, presents a favorable picture of passkey adoption, not only for the benefit of user security and experience, but also for organizational security and the simplification of infrastructure, as the need for password and KBA management diminishes. Just

as the invention and adoption of SAML exponentially perpetuated the benefits of federated identity, the general advocacy of passkeys has the potential to quickly displace less secure, more frictional solutions.

HOW AUTHID EMPOWERS PASSKEYS TO EMPOWER USERS

Many organizations employ various forms of Multi-Factor Authentication (MFA), meaning multiple methods of authentication, to lock down access to corporate assets. authID empowers a layered approach as well, but in a very passive way that makes for a seamless user experience.

authID's platform is designed to enable users to transact digital business both easily and securely. The easy part is to leave passwords behind, using only biometric to assert one's identity. Enrollment and subsequent logins are all face-based. The secure part is multi-threaded. First, your biometric and your physical id document are required to establish identity. After that, your biometric is yours and yours alone. This not only allows you to access your device, but then allows you to address the desired site or application with the passkey. Your face effectively asserts your passkey for you.

When your device is lost or stolen, you use your username and biometric to reassert your identity, and acquire a new passkey. Since recovery schemes are often exploited for breaking into accounts, it makes sense to secure that as well. Give this one last bit of thought: your smartphone complements the process but you are not tied to that particular device.

The authID solution is based on the FIDO (Fast Identity Online) standard, which is already considered the next stage of MFA, providing for layered security in tandem with a passwordless approach. By leveraging a biometric to safely access the passkey, and leveraging the passkey to safely access the site, the user remains on a secure path to their digital assets. With the biometric the hurdle to unlocking the passkey, even stealing the device does a thief no good in terms of accessing a secured site associated with the passkey on that device.

authID adds further functionality to this kind of implementation. With authID, passkeys can be migrated across ecosystems. For example, an authID passkey can exist on Windows-plus-Android or Windows-plus-iOS, while other passkey deployments are limited to synchronizing within a given ecosystem, such as MacOS-plus-iOS. And authID passkey migration is strictly audited.

The authID passkey recovery process is far more robust than an ecosystem-specific process. Instead of simply migrating FIDO2 keys, authID's secure, audited process creates additional FIDO2 keys after biometric authentication of the user.

Besides a variety of platforms, browsers, applications, and operating systems, many organizations run on multiple identity providers (IdPs), or integrate with partner or customer organizations whose IdP deployments are heterogeneous. authID has the ability to perform the initial

authentication, then federate identity across these various IdPs, including Okta, Ping, ADFS, and others. This capability enables customers to interact more seamlessly, without the need for customized connectors. authID has been used in such scenarios to mitigate issues for clients as they migrated from one IdP environment to another, such that users navigate a varied ecosystem without friction or even the hint of incompatible identity platforms.

authID starts with an industry-standard approach (FIDO2) then layers on additional value to both the user and the organization. The ultimate goal is the speed and accuracy expected by the consumer, and the security and reduced need for infrastructure expected by the provider. In the end, seamless and secure access is a powerful driver to seamless and secure business.

Author: Jeff Scheidel is the Vice-President of Sales at authID, which provides strong, passwordless, biometric authentication, along with powerfully unique passkey support, for delivering trusted digital identities for consumer and workforce environments. Jeff has decades of experience in the security arena, and is the author of a McGraw-Hill book on identity and access management.

For more information on authID, check out our blogs and our library.