PASSWORDLESS AUTHENTICATION

EVERYTHING YOU WANT TO KNOW

PASSWORDLESS AUTHENTICATION – EVERYTHING YOU WANT TO KNOW

Despite the endless angst over identity theft, the billions in lost assets and productivity due to breaches, the horrific news about ransomware and stolen bank accounts, countless computer users around the globe (and probably the moon) still use – passwords. And as if passwords weren't vulnerable enough themselves, these users employ very *stupid* passwords. Statistics on just how weak passwords are in general continue to amaze us. People complain about being compromised, but they do everything they can to make it possible.

The recent intrusion into Vegas gaming establishments highlighted the weaknesses still posed by social engineering (as in, I called the help desk and pretended to be a guy I found on LinkedIn, then I got his admin credentials), and that barely took any effort. But weak passwords are just as easy to crack.

Most people use the same password across multiple apps, leaving them open to credentials stuffing. More than half of Americans use a birthday or a name as a password. Lots of employees use their employer's name. Almost half never flip their password. A little less than that share their passwords with others. "Password" and "123456" still rank pretty high in usage. Well over half of all major breaches are the result of stolen or weak passwords.

You yell at the dog whenever he gets in the garbage. That works for about, oh, five minutes. Soon as you're not looking, he'll do it again. We created a giant bubble with profligate spending and mindless investment that blew up the economy in 1987. We did it again in 2001. Then again in 2007. It kinda happened again in 2021. The commercial real estate bubble looms even now. We never learn. So it's no surprise that the litany of broken-into accounts and massive breaches doesn't scare us enough past our morning coffee to change our habits.

So how do we keep the dog out of the garbage? Move the garbage can to where he can't reach it. How to keep users from endangering themselves with crummy passwords? Take their passwords away and start using passwordless login.

THE MOVE TO A PASSWORDLESS DIGITAL LIFE

This is what we need to do to take away the attack surface: we need to go passwordless login. We need to do our banking passwordless and wire transfers passwordless. We need to chat passwordless. We need to do our digital onboarding passwordless. Visit our healthcare and hospitals passwordless. Perform or receive our financial services passwordless.

According to Forbes, 80% of Fortune 500 companies are moving to a passwordless platform.

So what does it mean to go passwordless? Security is the obvious benefit. But there are other, very tangible benefits.

- Users love it. Having to think up (and worry about) new passwords with every expiration cycle is stressful. And according to some experts, password reset fatigue leads to the creation of increasingly weaker passwords, or the reuse of old ones after it's allowed.

Remembering multiple passwords across multiple apps is also a hassle ("which one did I use for this lousy site?"). Authenticating with anything other than a password is a blessing.

- Organizational password management is a cost center. Password managers (both people and software), help desk personnel who take endless calls from users who muck up their reset (often because they ignored the multiple warnings that an expiration was imminent), and other IT support are a drain.
- It's also far easier to grow an org if you're not managing passwords out of the gate. User-friendly onboarding does not start with passwords. "Welcome to the company, log in with this phrase to start, then immediately change it." Ouch. Digital user onboarding, passwordlessly, is a much better way to bring new staff into the family.
- Audits. If you want to stay HIPAA, SOC2, ISO, GDPR, and ABCDEFG compliant, you need security. Demonstrating safeguards beyond simple password protection is a great start.

IF NOT PASSWORDS, THEN WHAT?

Too often, "passwordless" doesn't end up meaning "no passwords," but rather "less passwords." They still creep in for initial onboarding, resets, or for enhanced access, or even to register for what is later a no-password approach. In some cases, the passwords are one factor in a two-factor (2FA) scheme. But still there is a password. In this discussion, we are talking about literally no passwords.

But clearly you still need *something* in their place. You don't open up the pool just because there are no lifeguards on duty. So what kind of credential is not just good enough to replace passwords, but can actually surpass them in terms of security and user experience? There are a variety of passwordless solutions on the market, but 1) many of them still involve some version or other of passwords, 2) some of them are expensive, 3) most of them are difficult to implement, 4) most of them are not user-friendly.

Some kind of credential must be asserted on request in order to gain access to a site or application. It might be a biometric (face, voice, fingerprint). Hard tokens or physical keys are still used in extremely secure environments, but these must be provisioned, distributed, maintained, and ultimately retrieved (which often does not happen, which is why they're even more costly in the end) and typically physically plugged in or be otherwise engaged with another piece of hardware.

Alternately, rather than a password, the user may enter a PIN or code or (hopefully not) one-time password, which is still, yes, another password.

PASSKEYS FOR PASSWORDLESS LOGIN

Passkeys are an increasingly common approach to passwordless authentication, although not every vendor has the most elegant design for distributing them.

But let's backtrack. The user needs to retrieve or have access to that credential, which is often retrieved in real time, possibly through email or SMS. If it's a physical key, it must be physically acquired. Backtrack a little more. The user needs to register for that credential. And to make that happen, the user often has to use a password to begin with. So to recap: the user must be granted or otherwise acquire a non-password-based credential, somehow store it, and present in on demand, actively or passively. Is this simple? Not necessarily.

But there is absolutely a path to secure, user-friendly, and efficient passwordless authentication. We'll get there.

THE MAJOR TYPES OF PASSWORDLESS AUTHENTICATION

Let's examine those various approaches to passwordless authentication in more detail. Bear in mind, the purpose of passwordless login is to assert who the user is. If you're really the individual doing the assertion, then the transaction is legit, right?

Leading vendors and thought leaders support various forms of passwordless login, but they still face the age-old challenge of getting users and other vendors onboard. Options are out there, each with its own value, its own risk, its own challenges.

- There's always the (reliable?) Personally Identifiable Number, or PIN. It's not a password, right? Yeah, really it is. What may be different is how it's delivered. As part of a 2FA setup, the user accesses a site which then sends a PIN to their pre-registered phone which they then type into the browser. It's not a terrible solution, but it requires an extra step, and which can still be intercepted. Years ago it was demonstrated at Black Hat how to intercept calls and SMS without forwarding to the original target. Just like a password, or even a device, a PIN demonstrates ownership, not identity.
- One-time password, or OTP. Virtually the same as the PIN. It's more often a random set of characters, or a variation of a real world, maybe with some special characters tagged on. Access the site, receive the OTP on the device, and enter that OTP into the site. Same level of security. Same risk.

MORE ADVANCED PASSWORDLESS AUTHENTICATION

Quick sidebar for these two methods: what happens when the user loses their device?

- Fingerprint. Fairly hard to duplicate and insert into a passwordless login transaction. But the major problem with fingerprint is that many of the hardware vendors no longer support

it. You're not sending a picture of your finger; this requires an adequate scanner, and those went away.

- Voice. It's commonly used for Apple passowrdless logins just to open up phones and get the digital assistant to execute commands. But 1) how often have you said something that the phone innocently picked up as a command? Talked to your own phone only to have your spouse's answer you? And what about deep fakes?

Voice is still a good option, in fact, but a bad actor with a good deep fake *and* the opportunity to attack a specific device with that deep fake could still do a lot of damage. This is not likely a problem for the average consumer, but for key personnel it could be devastating. Like spear phishing attacks that have gone after specific individuals with enhanced access, this kind of assault makes voice a vulnerability in particular circumstances. Apple passwordless login makes this far less likely.

- Strong FIDO2 passwordless authentication. While we're still waiting on broader FIDO2 adoption, it remains a powerful solution, in the form of FIDO2 credentials, known as passkeys. What are passkeys? They are pairs of encrypted keys, public and private, that match up an individual with specific site or application access. Passkeys reside on devices or browsers, and must be asserted by an initial authentication, making them part of 2FA.

The theft of either the public or private key nets the thief nothing useful. And a passkey cannot simply be inserted or guessed or phished. Again, the only weakness with strong FIDO2 passwordless authentication is the lack of widespread use by organizations even as they move toward passwordless login. FIDO2 does provide the potential to allow users to manage how they share identity data via sovereign identity.

Another challenge is in management of passkeys when they reside on a device that is subsequently lost or stolen. If someone steals a device with a passkey, they may not be able to retrieve it from that device, but the legit user needs a way to retrieve their own access. This can be accomplished through biometrics, which we'll cover shortly.

- Knowledge-based authentication (KBA). This was all the rage for a long time, and in fact there have been some large organizations that even won awards for their use of KBA. Annnnnd ... it is largely out of favor, as it involves two types of questions. Either the user has pre-registered their questions and answers, or the identity provider sources data from a broker (such as Experian or Lexis-Nexis) to ask questions about first mortgages, car models, old addresses, etc. All too often, users don't even remember the answers to such random bits, while bad actors can access that information from the dark web.
- Certificates. Digital certificates were also all the rage for years to accomplish passwordless login, and are still in use, but not like in past years. Certificates have to be registered, downloaded, renewed, and eventually revoked. While this process is easier to pull off without physical keys, it still requires a Certificate Authority which in turn enforces that onerous lifecycle of maintenance. An advantage to digital certs is that they cannot be phished or socially engineered.

- Facial biometrics. We already use our faces regularly to open our devices, desktop or handheld. That same face that provides this convenient and secure service can also open up and help assert additional factors on the device, such as passkeys, certificates, or other second methodologies. So while that second factor is app or site specific, it cannot be accessed without the facial biometric being first engaged. This requires the biometric being registered with a simple selfie.

With a proper solution, both registration and subsequent authentication can take seconds, and it is exceedingly difficult for a bad actor to insert a fake. Liveness checks can prevent a hacker utilizing a picture of a picture, or a picture of a screen to spoof an actual, live user.

Multi-factor authentication (MFA) involves combining two or more of the above methods to achieve passwordless login, which can include something you have and something you know (eg. password and device). But this approach assumes that all factors are secure. If one of them still involves a password, then it falls apart. A secure method, if asserted by a password to start with, is still vulnerable. Even better is something you *are,* such as with facial biometrics. I can know what you know, and I can take what you have, but I cannot *be you*. We will dive deeper on that shortly.

THE PROS AND CONS OF PASSWORDLESS AUTHENTICATION

There are clearly benefits to passwordless logins, in terms of security, user experience, and organizational implementation. What's scary about completely switching to passwordless logins is simply change. It's the reason so many orgs still cling to KBA, which was so popular – in 2012. Passwords are just accepted as necessary. But the logic is irrefutable. In terms of security, a passwordless authentication scheme more than passes the smell test when it comes to security. For example, password authentication thwarts a raft of common attacks:

- Brute force. Passwordless authentication can't be broken by simply shoving a pile of passwords down the pipe since, well, *no passwords.*
- Keylogging. There are no keystrokes in the form of passwords to be captured during typing.
- Man in the middle. Passwordless login schemes using keys / secrets are not subject to replay attacks, since secrets are not transmitted.
- Credential stuffing. If you're not sending a password in the first place, there's nothing to replay against all those other sites you might be accessing.

In terms of user experience, the whole hassle of creating, remembering, resetting, recovering, and periodically replacing passwords goes away. And from the perspective of the enterprise, the hassle of maintaining not just password policies, expirations, enforcements, and the help desk infrastructure needed just to handle users who ignore their password reset notifications is a godsend.

So what are the cons of a passwordless authentication environment? Once again, it's scary. Passwords are the universal security blanket, providing the illusion of a firewall, when in fact they provide just as much risk, if not more, than security itself. Users don't like getting codes texted to them. They don't like authenticator apps, which have to be downloaded and pulled up with each login. Physical keys aren't for consumers. The challenges go on and on ... unless you're the beneficiary of a solution that allows you to register easily, and then leverage that registration even more easily day after day. More on that later.

PASSWORDLESS AUTHENTICATION FOR THE ENTERPRISE

As previously mentioned, a majority of Fortune 500 companies are seriously contemplating passwordless login for their employees and even customers. Aiding in this endeavor is the impetus of major vendors in updating their platforms and providing tools to support passwordless login. Even as it dumps on password expiration policies as risky (because each time we have to create a new password, fatigue leads us to create weaker and weaker ones), even Microsoft points the way on passwordless. And development environments catering to a more tech-savvy crowd are also supporting passwordless login, such as with passkeys.

In order to achieve success in a passwordless authentication environment, companies need to decide, as they do with any other project or initiative, what success looks like. Are they shooting for a better user experience, better security, simpler infrastructure? Sure, it's all of those, but since every project has a driver and stakeholder, there is likely one primary goal to start with. This goal will help decide what solution, or combination of solutions, to deploy.

VERTICAL INDUSTRY SUPPORT FOR PASSWORDLESS AUTHENTICATION

Passwordless authentication has universal applications. But there are a number of verticals and their common applications where it has particular value, to protect the enterprise and its employees and customers. Let's have a look at those.

- Consumer banking. Countries where commuting has been tougher and fewer people own cars drove them to large scale online banking even before the USA adopted it. Brazil, for example, saw a large majority of its population move to banking online when in the United States it was still measured in single digits.

That has changed, of course, but what hasn't is the need for tight security, meaning passwordless banking. If your bank account is hacked and drained, good luck proving it wasn't really you, and getting the bank to top your account back off. So the answer to that is securing your online banking life from the start. And passwords are the single biggest threat consumers face in keeping their money safe. It's a very common need for existing banking customers to register for enhanced access when they migrate to online banking services, often meaning multi-factor. Passwordless consumer banking is the killer app for many average citizens.

- Commercial passwordless banking. The volumes may be lower than in consumer banking, but the average transactions are higher dollar amounts. Large scale banking and wire transfers need to be secured with something more than a password. High transactions in general also need more protection.

For example, if someone is sending an unusually large amount, perhaps from a strange device or IP address, to a brand new recipient, and maybe after normal working hours ... this should raise many red flags, necessitating enhanced authentication, such as a method that does not involve a simple password.

Passwordless wire transfers are a key focus of modern banking infrastructure.

- Employee onboarding. While password-free workforces are further along than consumers, there is still a long way to go. Onboarding passwordless will ultimately be easier, since that very first access is often a productivity killer for new hires. All of us have had the experience of being unable to get into our initial applications as fresh employees.
- Workforce / employee passwordless authentication in action. Too numerous to recount, phishing attacks on company employees in general, and spear phishing attacks that target privileged users, have resulted in untold millions in losses, in terms of money and intellectual property. Organizations can protect their staff from their own foolishness by replacing employee passwords with more secure factors like employee passwordless logins.

This includes internal email, calendar, procurement systems, accounting apps, sales tracking, development platforms, and even chat, which is increasingly a channel for even the most sensitive information. In fact, company chat apps are commonly used for sending documents and code, since they require fewer clicks than starting and sending an email, so the ability to chat passwordless while still keeping secure is more important than ever.

- Shared Devices. Another platform used in remote staffing is commonly held devices, for field personnel, cleaning staff, and other employee groups. Using passwords on such a device is problematic for multiple reasons, and can result in people not only sharing passwords, but accessing each other's sensitive information. Gartner suggests that only half of workforce logins will be passwordless by 2025. But that's because of the shortcomings of most available solutions. Better ones do exist.
- Consumer Identity and Access Management (CIAM). Consumer retail, especially for repeat customers, means an opportunity for bad actors to infiltrate sites and send themselves for resale. These kinds of sites are also ripe for credential stuffing attacks, given users' predilection for reusing the same password across similar applications.
- Public Sector. COVID resulted in tens of billions in fraud, in the form of stolen relief funds. Additional costs included the many investigators and security mitigation efforts that were instituted in the wake of that fraud, not to mention the insane costs of having to host millions of additional calls and office visits by those legit claimants whose transactions were impacted by the bad guys who applied in their names. Many states suffered more

fraudulent benefits claims than legit ones. Taxpayers and their potential refunds are regularly targeted via the IRS. The ability to register and subsequently identify oneself using an assertion method other than a password, such as a biometric that can't be faked or inserted, would prevent many such activities.

- Medical Passwordless. Consider these scenarios. The interception of sensitive medical records (under HIPAA). The theft of surgery via the VA (it happens!). The acquisition of prescription drugs that end up resold on the street. Can medical asswords be trusted for these critical situations? Actual, legit users need to assert themselves via a more secure mechanism, to ensure that only the right people receive medical records, pharmacy meds, and a hernia operation. Passwordless login and medical passwordles authentication can greatly help decrease or eliminate this risk at the enterprise level.
- Financial Services / Fintech. If consumer banking accounts are more common and more applicable to the average citizen, financial services accounts often hold more assets. Passwords are wholly inadequate for these types of accounts. Stock traders also need to lock down access that can impact their customers in large fashion. How many passwordless fintech operations are there? Not enough, even though new online banks (which, remember, are only fronting for the larger, actual sponsor banks in the background) are popping up every single day.

Besides the aforementioned Gartner prediction on passwordless corporate logins, they also suggest that fewer than a quarter of consumer logins will be passwordless by 2025. Again, this is based on most existing passwordless solutions, which have good intentions but not the best execution or deployment options.

QUICKIE PASSWORD POLICY REVIEW (HOW DID WE GET HERE?)

As if we needed another reason to dislike passwords, let's remember that it's the entire lifecycle of passwords that cause us so much stress:

You have to acquire that first password to begin with. It needs to conform to requirements, meaning a certain length, the inclusion of numbers and special characters, and you need to remember the darn thing. If the platform you're on is smart enough, it saves you from your own laziness and says, "Don't use that birthday, or your first name, or a common dictionary word." But of course that creates more a burden for you to compose that so-called strong password.

That password is only good for a time, and then it expires, forcing you to create a new one. Don't ignore the notifications, because if you let it expire, you're going to have to make a call to the help desk, and it will be at the most inopportune time possible, such as before that big presentation or demo.

The links for password reset are prime targets for bad actors. They'll click that link all day long and try to create your password for you. Then boom, they're you. Because the password only vouches for who knows it, not that they're actually the person who should.

Bill Gates told a crowd at the venerable RSA conference two decades ago that passwords were dead. And cue the Jeopardy theme. It hasn't happened. Our path to wanting passwordless authentication is a winding one, and the end is only partly in sight.

SO HOW DOES AUTHID ACHIEVE TRUE PASSWORDLESS AUTHENTICATION?

Let's review why we're not already in a fully passwordless login nirvana. First, adoption. FIDO2-based passkeys, while an excellent approach, are not mainstream. Not nearly enough companies have taken them on, even through major vendors such as Apple, Microsoft, Google and others support passkeys.

The difficulty of implementing strong passwordless authentication tools remains a hurdle. Physical keys are hard to provision, distribute, and hand out. Digital certificates have lifecycle issues. Users dislike authenticator apps and OTP, since they require several extra steps, i.e. they are the antithesis of passive. PINS are ultimately no better than passwords.

But passwordless authentication is absolutely possible, and can be accomplished with a maximum of security and user delight. And for the enterprise, a simplified deployment that does not require a massive coding effort.

At authID, we provide the ultimate in strong passwordless authentication. As previously mentioned, the momentum for such a mechanism may stem from a desire for an improved user experience, a simplified deployment, or better security. We strive to support all three of these, which in fact support each other.

FACIAL AUTHENTICATION

Our facial biometrics allow users to register with their face and physical id. We process images of both identity document and selfie incredibly fast (as in 700 milliseconds). Our solution is WASM (web assembly) based, meaning no app to download, so it's lightweight and lightning quick. We determine the viability of that physical id, meaning is it legit, does the data on the front match the barcode on the back, is it tampered with, is it actually issued by the authority it claims to be (such as the DMV), is it a real doc or a picture of a doc, or a printout? Does the picture of the user actually belong, or was it pasted on?

Then, is the selfie a live person, or is it a picture of a picture? And if it that person is live, does that selfie match the picture on the id?

This all takes seconds. The user experience is further enhanced beyond just speed and accuracy. In taking the pictures, the solution provides a digital frame that tells you a face, an id, or the back of an id is actually in focus, and takes the picture for you as soon as it gets a good shot. What makes users abandon this process most commonly? It's just plain hard to do. When the solution

lines up the shot for you, puts it in frame, then snaps the pic, it's doing all the work, and compensating for users who, frankly, don't take pictures of ids for a living.

Once user and physical id are legitimately linked, that facial biometric is registered for all subsequent authentications. Need to log in? Show you face. The process can be started, or even completed, on a desktop. If that login is indeed started on the desktop, the authentication can be taken over by a smartphone, where the user snaps the selfie, and the app recognizes it's them before allowing the desktop to take back over.

The root of trust is *not* the device. It is the user's face that holds the trust. If the user's device is lost or stolen, or needs to be upgraded, there's no call to the help desk to get a new device registered. The user simply invokes their face on the new device, and they're up and running, instantly, with no need for IT intervention, all courtsey of passwordless login.

AUTHID PASSWORDLESS AUTHENTICATION

authID also supports the most robust passkeys option on the market, for those organizations looking to go full FIDO2 authentication for sensitive apps or sites. Passkeys can be generated and stored on the device / browser, and if that device is, again, lost of stolen, authID asks for that lovely face once again and boom, generates a new passkey.

In the case of shared devices, users can assert their own faces to retrieve their own personal access, including their own specific passkeys when such is required. No shared secrets, no shared passwords, no slipping into each other's access.

Nothing is more sensitive (or risky) than one's own digital assets, and nothing is more personal than one's own face. authID lets users use that face to assert control over those assets, easily and quickly and, most importantly, securely.

By having your face registered with authID as your root of trust, your access becomes portable. You're not locked to a particular device. You're not vulnerable to compromised passwords or weak policies. If your passkey expires or walks off with your phone, you can still assert yourself as, well, yourself. You may still leverage your device for access, but the path to unlocking its keys remains *you*. When you walk away, you take your access with you. Walk away from passwords while you're at it. This is why passwordless login will just continue to grow and be implemented by the Fortune 500 and millions of small businesses that are the growth engine of the economy.

Reach out to authid.ai to find out how to achieve the highest level of assurance with the least amount of friction, and leverage the most powerful passwordless authentication solution on the planet. Our secure platform will make your face a happy one.