SWCP Portal

December 2025

Will Passkeys Replace Passwords?

By Mark Costlow

If you believe the hype from the digital punditverse, passwords have run their course and are being replaced. Using passwords to protect computer systems certainly has its problems. To paraphrase Winston Churchill, passwords are the worst way to secure your email, except for all the other ways we have tried.

This month begins a two-part look at a contender that aims to make passwords obsolete: Passkeys. They've been around a while but are gaining momentum. You have probably had your computer or Google prompt you to start using them, so it's time to figure out what they are and how, or if, we use them.

Definitions

Things are confusing right at the start because of the name. Did you say Password or Passkey? Are those the same? And what's a Passphrase? These words all sound the same, and they all refer to limiting access to the person who knows a secret code. But password and passkey have very specific different definitions, and understanding that will get us on the same page as we decide how to proceed.

Password - a "**shared secret**" that grants a person access if they know the secret word.

Passphrase - a fancy, longer password. Usually a phrase made up of many words. Same as a password in every other way.

2-Factor Authentication (2FA), Multi-Factor Authentication (MFA) - a system which requires a password plus at least one other thing to get in. For example, when you log in to your bank with a password, and then they send a text to your phone number on file with an additional one-time code. That texted code is the 2nd factor. The 2nd factor could be other things, like an emailed code or your fingerprint.

Passkey - a special kind of password that uses a mathematical magic trick called "public key cryptography" to make it near impossible to forge or steal. "Passkey" is actually the marketing term to describe a computer standard called "**WebAuthn**" (sic, short for "Web Authentication"). Apple started calling WebAuthn passkeys in 2022, and it stuck.

The most important terms to keep straight are password and passkey:

Password

The defining feature (and biggest weakness) of a password is that it is a **shared secret**, something two people have agreed upon beforehand.

Imagine two spies, Boris and Natasha, are hiding out. They need food and decide Boris will go get it. When he returns, how will Natasha know it's safe to open the door? They agree Boris will say "fruit bat". That is the shared secret. They agreed on it in person and they both know it. There are several problems with shared secrets:

- If either party writes it down, someone can steal it and use it to impersonate Boris.
- If someone was eavesdropping when they arrange the secret, it is compromised.
- If Boris has re-used that same secret for other safe-houses, and the secret is stolen, other spies can now get in to all of them.
- There is no good way to establish a new shared secret over the Internet without the risk of being overheard.

The parallels to our digital lives are apparent. Most sites use a password to secure your data. If your password is stolen, or a fraudster tricks you into giving it up, they can impersonate you and access your account. After a data breach, the thieves may decode customer passwords and use them to unlock users' accounts on other sites.

It's left to end users to solve all these unsolvable problems. The best we can do is mitigate the damages by using long nonsense passwords, unique on every service. Management of these becomes a big headache and people take a lot of shortcuts, with the expected results.

Passkeys

Passkeys overcome these problems using **public key cryptography**. This topic is too involved to explain in detail here so we will just explain what you can do with it, and not worry about how computers make it happen behind the scenes.

The core of the mathematical trick is that a passkey is broken into two parts, the "public key" and "private key". As the names suggest, the private key is an absolute secret and will never be given out to anybody. The public key is truly public and can be given to anybody. It doesn't need to be protected in any way.

There is no shared secret, because you don't share the secret part, and the part you share isn't secret.

The real magic happens when you send a message to someone, mathematically encoding it with the recipient's public key. Let's say you send a message to Acme Corp in this way. Acme (and only Acme) can use their private key to decode it. Conversely, you can encrypt a message using your private key, and anybody can decode it using your public key, but they know the message came from you (and only you). The take-aways are:

- Nobody in the world but you could have sent a message using your private key.
- Nobody in the world but Acme can decode a message sent using Acme's public key.
- Neither party used the other party's private key for these transactions.

This is a great simplification. Entire books and careers are based on this process. But this is really the heart of what makes passkeys a contender to one day replace passwords:

- You can't be tricked into giving a password to a fraudster. Anyone who asks for your private key is either confused or up to no good, **no exceptions**.
- Your private key is not stored on the server. If they have a data breach, they won't get your access credentials.
- Passkeys are too complicated for humans to manage directly, so we must turn over the task to the computer itself. That means things like re-using the same password on every site are not a problem. The computer doesn't care if it has to track a different passkey for every site, it is happy to do that, no short-cuts needed.

What's The Catch?

Passkeys sound pretty great, so why aren't they being used everywhere?

Passkeys have been around for many years, but they require support in everybody's devices and operating systems, and that takes time. But it is starting to come together and we expect passkey adoption to speed up in the next couple of years. The main barriers are Hardware Security Modules and old Internet protocols:

Hardware Security Modules

Passkeys must be stored on your phone or computer. They're too long to memorize or write down. They need to be on your device, available to your web browser, but in a secure way. This requires a "hardware security module", a special part of a computer that provides a high-security vault for the most sensitive information. Apple calls theirs the "**Secure Enclave**", first introduced in 2013. It is where your biometric data is stored (fingerprint for Touch ID and facial features for Face ID). Those biometric features are used to lock secrets away, so they are only accessible by you.

It takes years for new hardware to become ubiquitous, but by now almost every Apple phone, tablet, and computer in use has a Secure Enclave.

Android devices have something similar, although Google Pixel phones and Samsung phones each have separate hardware implementations.

This issue is an unspoken source of strife this year with Windows PCs. On Intel-based computers, this is called the **Trusted Platform Module**, or **TPM**. Windows 10 works with all computers, but Windows 11 REQUIRES TPM 2.0, first added to processors in 2018. This has slowed adoption of Windows 11. Many have balked at the need to buy a new computer for Windows 11. Their older Windows 10 PC is plenty fast enough to run the new software, it just lacks a supported TPM. **Microsoft set a deadline of October 2025** to finally push everyone to upgrade. Windows 10 is no longer supported by Microsoft.

Old Internet Protocols

Passkeys are inherently web-based. Remember that "passkey" is another name for "**web**authn". A web browser is required in the key exchange process. So much software has become web-based that this is OK for most things: social media, shopping, YouTube/TikTok/Vimeo, banking, mapping, job search, AI chatbots. Also phone apps, which almost all use web protocols under the hood.

The biggest category not listed above is **email**. The POP and IMAP email protocols were designed decades ago, before multi-factor-authentication was a consideration. Web-mail interfaces, where email is accessed through a web browser, can make use of passkeys fairly easily. More traditional access methods with a mail client program running on your computer (like Thunderbird, Outlook, or Apple Mail) require more support, which has been slow to come. There is activity in this area though, so hopefully more solutions will appear soon.

Practical Considerations

As with most new technology, there are still a lot of unanswered questions about the way forward. Next month we'll look at how passkeys are being used in practice.

This Month in Ideas & Coffee

- **Dec 10 6pm-7:30pm:** *Phish Proof Founders* - Rick Myers of Caldera Cybersecurity Services hosts a discussion of security issues and solutions for small business owners, nonprofit leaders, and tech-curious folks.
- **Dec 16 6pm-7:30pm –** *WordPress Work Along* - Questions, ideas, and conversation about WordPress. Bring your laptop!

Check the Ideas & Coffee schedule on the SWCP calendar at **https://swcp.com/calendar** and/or the Meetup site at **https://meetup.com** to find out when new events are happening.

Southwest Cyberport - swcp.com
New Mexico's Expert Internet Service Provider since 1994
505-232-7992 | Support: help@swcp.com
5021 Indian School NE, Ste. 600, Albuquerque, NM 87110
Click on bold blue type in browser for links.