January 2026

Auth Lang Syne

By Mark Costlow

Please forgive the horrible title pun. It seemed appropriate if you consider the literal translation of "Auld Lang Syne" as "Old Long Since". Authentication has been a part of computing and networking since shortly after computers were first connected together. The whole point of the Internet is to bring people together into shared spaces. But just as people in cities have to lock their doors, in contrast to those who live in the country with no close neighbors, we must have locked doors on the Internet to keep people safe. So "Auth Long Since" resonates.

Last month we learned what **Passkeys** are and a little bit about how they work. Briefly, they use **public key cryptography** to manage very complicated passwords to reliably verify your identity to a web site. Since they're so much more complicated than simple passwords, we have to let the computer manage them, which ironically can make them a bit more streamlined and quicker to use. One might hope it makes them easier to deal with, but in typical technology fashion, there are several ways to do this, so there is confusion around which method is best for any given situation.

DON'T PANIC

One thing to keep in mind is that Passkeys have not taken over everything yet, and traditional password methods will be around for a long time to come. If there are cases where Passkeys make sense for you, by all means use them. But don't stress about being forced to "convert" to them any time soon. Now let's look at some different real-life Passkey situations.

To Sync Or Not?

Remember that a Passkey confirms your identity on a specific device. Each device has a private key, which is used to create new Passkeys. The private key is stored in the deepest recesses of each device (the **TPM** or **Secure Enclave**).

For convenience, you can synchronize your passkeys across your devices. Your phone and your laptop don't necessarily have a way to talk directly to each other (especially if one is at home and the other is with you out in the world). Doing that kind of sync requires a third-party helper. That means you need some tech giant's cloud service to act as a common meeting place for your devices to trade information. The Big Three are Google, Apple, and Microsoft.

At first glance that might seem scary. How is it safe to store all of your passwords in one place that is out "in the cloud" and under someone else's control? The reason it's considered safe is each device's private key is never given to the cloud. Everything sent out of your computer is first encrypted using the private key, which is stored in your device's secure vault and protected by your biometrics. When a Passkey login flow requests your fingerprint or Face ID to continue, that is how it accesses your private key, under strictly controlled conditions, and only if the computer is convinced *You are You*.

The service-specific keys (i.e. separate ones for Amazon, your bank, Discord, etc) are all encrypted before going to the cloud sync service. It's as if you gave a friend a key ring with your house, car, and gym locker keys for safe keeping. But you give it to them inside a lockbox which is secured with a key that you keep and your friend does not have. If you later lose your housekey, you can visit your friend, unlock the box and take out the key. But your friend can't open the box to use the keys. And if the box is stolen from your friend, the thief can't use them either. (In our analogy, modern cryptography protects your digital keys far more fiercely than any physical lockbox could protect physical keys).

The Silo Problem

If you are a person who mixes computing ecosystems, you probably know what's coming next. The "easy" sync option for each device is to use the cloud service run by the company that sells that device. So if you have a Windows laptop and an iPhone, they don't want to sync at the same place. Even if you use both Chrome and Safari on a Mac, or Chrome and Edge on Windows, each of those browsers will sync to a different cloud.

We have made some progress, in that all of these devices are using the same underlying technology and methods (**WebAuthn**) to manage passkeys. But we still have a balkanized environment because each device only supports its "native" sync service.

It is understandable that we are in this situation, and it is likely a temporary condition in this evolving technology. The foundational promise that makes Passkeys work is that the secret keys are VERY well-protected on your device. That requires super-tight coordination between the hardware and software maker. Every new option or extra compatibility added to a system like that increases complexity. More complexity means more chances for bugs or system flaws that can be exploited by bad actors. So this step, where Passkeys have been

made possible, but not yet perfectly ubiquitous across platforms, is a sensible and expected waypoint for this maturing technology.

In 2025 Apple, Google, and Microsoft all announced plans to improve cross-platform syncing. None of them are fully realized yet, but we expect that to progress over the next couple of years.

If you are suspicious of the Big Three clouds, or use enough different kinds of devices that the silos would be a hindrance, you have two options: third-party password managers, or avoid syncing altogether.

Password Managers

Password managers, or password wallets, have been helping people synchronize passwords across their different devices for many years. Most of them have added support for Passkeys. A few with Passkey support are: 1Password, Bitwarden, Dashlane, Keeper, NordPass, Proton Pass, and RoboForm. If you are already using one of these password managers, you can continue doing so and take advantage of fact that they now also support Passkeys.

Password managers have their own cloud service for your devices to sync through. It's platform-independent, so generally works on all computer, phone, and tablet brands. Most also have web browser extensions so they work in Chrome, Safari, Edge and Firefox. Of course, operating a cloud service costs money so there is usually a monthly or annual fee.

There have been **a few spectacular failures of password wallets**. LastPass, Norton LifeLock, and 1Password have all had security breaches. With traditional passwords, these exploits were devastating. Happily, with Passkeys, such breaches would have much smaller impact. Since the information being synced to these clouds is already encrypted (stored in our metaphorical lockbox), the criminals would just get a big pile of sealed titanium boxes that will never give up the keys inside. The biggest vulnerability is if a new technology like Quantum Computing were to undo all of the fancy math that makes encryption work. (That's a topic for another day).

Blissful Unsyncing

Don't be afraid to skip syncing if you don't want to do it. It's a little less convenient, but you still get all the benefits of Passkeys. Since every Passkey is unique to each person, device, and browser, you might need to create several Passkeys on each web site. For example if you use both Chrome and Safari on your Mac, you'll end up with two Passkeys at Amazon. Add another for your Android phone, and one more for your iPad. Amazon is happy to manage several passkeys for your account.

The biggest inconvenience comes when a device is lost or stolen or replaced. You'll need to login to each service you use to disable the passkeys that were used from that device. It's not hard, just a little tedious and time-consuming.

Practicum

Here are some pointers to access and manage passkeys on different platforms:

- **Apple** – these Apple support articles will help you find and manage passkeys **on your computer**, or **on your iPhone/iPad**, and how to **use iCloud Keychain to sync** among them all.
- **Microsoft Edge and Windows** – **their support article for passkeys** covers the basics, and **this news article talks about emerging support for sync** across devices.
- **Google Chrome and Android** – Passkeys are stored in the **Google Password Manager** built in to Android. You can access it through the system menus or via **https://passwords.google.com**.

Conclusion

First and foremost, Passkeys are a good thing. They will help solve many persistent vulnerabilities of **shared secret** passwords, such as password theft, brute-force guessing, and phishing. They have been a long time coming (the **WebAuthn** protocol first appeared 10 years ago), but are now on the path to becoming ubiquitous. Syncing makes them easier to manage across your devices, but unless you are all-in on a single ecosystem, the syncing process is still irritatingly fragmented.

Is it OK use them now? Sure! Passkeys have matured enough that it's safe to start using them in everyday situations. Do you **have** to use them now? Not at all! For now it's enough to know they exist, and don't be surprised if the landscape is very different a year from now.

This Month in Ideas & Coffee

- **Jan 14 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.
- **Jan 20 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.