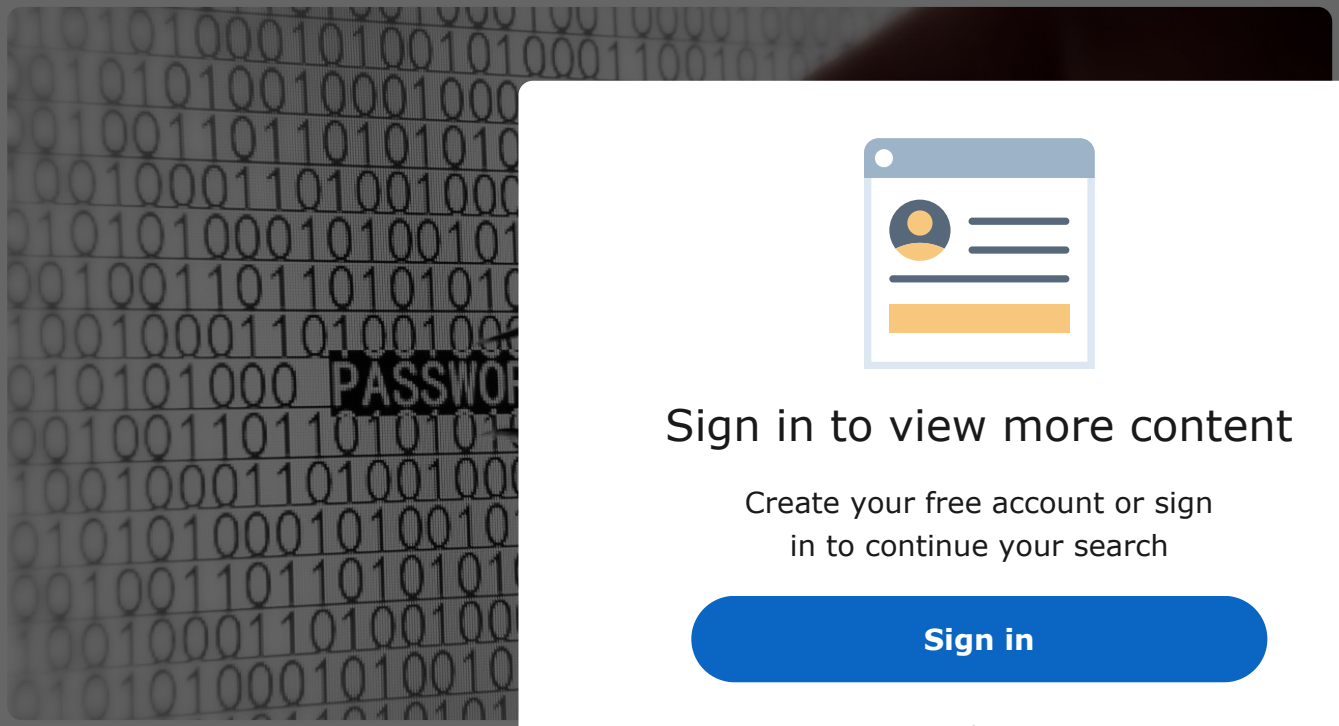

Psyomjesus, CC BY-SA 4.0 <https:/

What you s about Appl and WebAu

David Carns
Passionate about the intersection of law and technology

Intro

Apple Passkeys and WebAuthn are exciting passwordless technologies that will likely change the way you and I interact with the internet on a daily basis. (A bit of background might help and then the rest is pretty short, so read on!)

Background

There is a big movement in developer circles around Web3, decentralization, and blockchain everything. 🙄 …I am actually in support of a lot of the concepts behind these buzzwords, but they are overhyped and overused.

Today's web is heavily centralized. Most websites completely rely on Google, Amazon Web Services, Microsoft, or Meta for their backend. A significant part of the web would stop working if not for those service providers. Throw Cloudflare or other CDNs into the mix and suddenly you just covered 95% of the modern web. Think I'm exaggerating? Watch how much stuff breaks on the internet when any of those services go down for even 15 minutes.

Web3 is supposed to fix all of that eventually, but while we are holding our collective breaths for Web3 to fulfill its promises (and while I write a longer article about Web3), I wanted to share one exciting change that will begin the process of marching toward a more decentralized web: Apple Passkeys and WebAuthn.

Apple Passkeys and WebAuthn

Apple just announced the release of "**Passkeys**" in their newest version of Apple's mobile and desktop operating systems (iOS 16 and MacOS Ventura) due out this fall. Passkeys is Apple's implementation of the **WebAuthn** authentication standard release by the FIDO alliance, which has broad industry support. (Apple's not the only one delivering on WebAuthn, so stay tuned for support from Google, Microsoft, Amazon, and almost everyone.)

Passkeys and WebAuthn basically represents an end to using username and passwords pairs on most apps and websites. If successful, this will end a nightmare of phishing attempts, password data breaches, and more. Here's how it works:

1. When you sign up for a web service or online app, the service will create an account using your selected username, but it will **not** have you create a password.

2. Your computer or mobile device, instead, will create a unique secret key for the service and provide the service with a public key that it can use to verify you.

3. Each time you log in to the service, the service will ask *your* computer or mobile device for authentication based on that secret/public key pair.

4. No passwords will be exchanged when logging in and authentication happens on *your* device, not the service.

Robert Black (Blacky) · 1y

Is Your SSL Server Vulnerable to a FREAK Attack?

Bruce Morton · 9y

HONEYPOD: BRINGING SANITY TO THE INTERNET VIA AD BLOCKING, TRACK BLOCKING, AUTHENTICATION, FULL DATA MONITORING, SECURITY VIA BLOCKCHAIN AMONG OTHERS

Jannyh Obomanu · 5y

CryptoSmarts 2: Best Encrypted Messaging Apps

Mint Dice · 3y

WWDC 2016: Apple to require HTTPS encryption on all iOS apps by 2017

Michel Landenbergue · 8y

Show more

Explore topics

Sales

This all happens with a sophisticated dance of public key cryptography infrastructure (PKI) but as far as you are concerned it will feel like magic. Feel free to read the WebAuthn link above for more technical information. Your computer or mobile device will use your device's authentication system (often based on face authentication or fingerprint authentication) to verify that you are indeed the person logging in.

A Move to Decentralization

Passkeys and WebAuthn is probably one of the most important shifts to decentralization of the modern web. Each user account will use its own device for authentication, instead of storing password information at each service. For all of the Web3 decentralization hype that hasn't *really* materialized yet, WebAuthn will deliver an important aspect of decentralization ***this fall***…and possibly will be a harbinger of things to come for what Web3 promises.

Amy Bowser-Rollins 1y

Hey David - I was reading about Web3 last Fall and how it will impact my WordPress site. I look forward to your future article on that. Since I personally own multiple devices, mostly Apple with one Windows machine tossed in, do they anticipate Passkeys and WebAuthn to work seamlessly across all the devices I would use to access the same product/site/service? Is the local secret key the same or different across devices? Just curious. Thanks for sharing your knowledge, these short easy-to-read articles are interesting and quite helpful.

Like · Reply | 1 Reaction

See more comments

Marketing

Business Administration

HR Management

Content Management

Engineering

Soft Skills

See All

To view or add a comment, **sign in**

More articles by this author

Prompt Engineering Basics - #2
Dec 20, 2023

Prompt Engineering Basics - #1
Dec 16, 2023

Containers vs Virtual Machines
Jun 30, 2022

See all