Passkey (Face or Fingerprint Sign-In)

You'r

Passkey (face
sign-in) is se

Co

I Love Pas
They Are N
Every Situa

Roger Grimes
Data-Driven Defense Evangelist at KnowBe4
Published Jun 30, 2023

While passkeys ARE GREAT, there are disadvantages to consider when deciding if you should use and deploy them.

I Love Passkeys

I do love passkeys. I really do. I love anything the FIDO Alliance puts out (**https://fidoalliance.org/**). I talk more about my love of FIDO here: What Is FIDO And Why Is It Good Authentication? **https://www.linkedin.com/pulse/what-fido-why-good-authentication-roger-grimes**.

I like FIDO for dozens of different reasons, but my three primary reasons for loving anything FIDO are because:

· FIDO solutions are phishing-resistant

· It is a well thought out standard

· They are the only authentication vendor I am aware of to publicly publish their threat model, mitigations and vulnerabilities; which makes me trust them more (not less)

I love passkeys themselves. I have been promoting them since last October: You'll Likely Be Using a Passkey Soon **https://www.linkedin.com/pulse/youll-likely-using-passkey-soon-roger-grimes/**.

Passkeys allow you to use strong asymmetric cryptography instead of passwords and their incumbent problems on any software which supports them. Right now, that means on Apple, Google and Windows

devices (with the appropriate newer versions and support). Passkeys are better than passwords.

Problems With Passkeys

But passkeys are not better than every other authentication alternative out there. In general, I like phishing-resistant multifactor authentication (MFA) even more. I think some high-end password managers may even be better, especially when they also support passkeys. Here are some things to think about when considering whether to use passkeys or not.

Not Supported on Most Sites and Services

The biggest negative against using passkeys is they are barely deployed by any site. In order to use passkeys, each site that wants to be passkey-enabled must update its code to understand and utilize passkeys. Right now, I have a hard time finding 10 websites that are

passkey-enabled. Even when I use Internet search engines with the terms ‘passkey-enabled websites’, most of the sites returned are not passkey-enabled. Most of the articles I have read claiming that such and such a site is passkey-enabled are wrong. Usually not even a quarter of their list is accurate. This is a serious chicken and egg problem. So even if you wanted to go all-in passkey, you cannot. You are going to have to use other types of authentication.

Not Cross-Platform Yet

Passkeys created on one platform (e.g., Apple, Google, Microsoft) are not shareable across devices on other platforms. This is a major missing piece that the vendors are working to resolve, but it has not been implemented yet.

Mixed Support on Different Platforms

Passkey is supported by Apple, Google, and Microsoft, which is pretty good support, but it is not equal or consistent across all OS’s or browsers. Each vendor supports different features, does not support others. For example, Microsoft does not yet support cross-device synchronization and neither does Apple on MacOS, but it does on iOS devices. See this for more passkey functionality details: **https://passkeys.dev/device-support/**.

Poor Legacy Support

Passkey basically works on the latest stuff…the latest operating systems and browsers. It does not work on stuff released over a year ago or so. That has very limited support. You may have Windows 11, but your

version might not support passkeys. You may have macOS, but if you do not have the latest, right now that is macOS Ventura, you will not get full passkey support.

Not All Browsers Support Passkeys

Yes, the big three vendors (e.g., Apple, Google, Microsoft) and their current browsers support passkeys, but there is almost no support out there for the many dozens of other browsers, some of them with sizable user bases, including Internet Explorer, Opera, Brave and QQ.

Not Supported on Linux

Right now, there is limited to no support for passkey in the Linux world. If you are using Google Chrome or Microsoft Edge browsers, Ubuntu has limited support, but no other Linux distribution I am aware of does. Ubuntu is the seventh most popular Linux distribution, according to market reports. This means most Linux users do not have the possibility of using passkeys.

1.5 Factor

I am a big believe in multifactor authentication (MFA)…especially the multi part. Every additional authentication factor that an attacker has to overcome makes it less likely they will be successful. That is why I believe phishing-resistant MFA is better (or can be better) than a passkey (when not using MFA modes of it already).

Many passkey supporters will claim that most passkey implementations are already two-factor. Such as they log in using passkey while using their phone and the phone is a second factor. It can be. If you are

logging onto an app on your phone and your passkey is using the same phone for your gesture, then it is not. The whole idea of multifactor authentication is that the factors need to be separate, so that if one of the factors is compromised, the other is not also immediately. If your "second factor" is on the same device as your first factor, then what you really have is something a bit less. I call that 1.5 factor. It is better than single factor, but not as good as a two, solidly, separated factors.

Not Enterprise Ready

Lastly, passkeys, so far, are intended for individual, private use. And that is OK. But passkey is not ready for the enterprise, where centralized control and management is needed. Most enterprise products give admins (and users) a ton of control over various settings (e.g., cryptography used, key size, key life, etc.). You get almost no settings to see, change, or manage with passkeys. And for the consumer market, that's probably the right choice. But the enterprise often needs to see what's going on, how it works, and be able to modify settings appropriate for their own environments. You can't do that with passkeys. How it works is what you get. Hopefully, it meets your required security controls.

Or if someone uses passkey to store and process their enterprise logins, would the enterprise even be OK with them being stored and synchronized across different devices, wherever the user uses their same login ID (e.g., Apple ID, Google/Gmail account, Microsoft account). That would mean the person's enterprise login was connected to and managed by Apple, Google or Microsoft. That could be OK, because many of our enterprise logins are already under the control of

one of those three company's software, but the enterprise login experience is still under the control of that enterprise's IT team. Not so if you are using or allowing passkeys.

In summary, passkeys is a great solution for replacing passwords if you do not have something better, like phishing-resistant MFA, but its lack of current broad support and other issues may not make it the solution for you.

Maxime Massaer 10mo
QA Automation Engineer @ STIB-MIVB

Interesting article! It highlights often overlooked points. I advocate using passkeys as a more secure second factor than TOTP.

Regarding mobile use, this holds true. But many users likely remain logged in across apps with password managers and also fingerprint unlock enabled on those apps.
Some claim having 2FA/MFA, but it often ends up being dual-step login with both codes coming from the same device. Real difference appears when genuine MFA was used.

For me the main advantage is thwarting remote attacks (unless passkey is on hackable cloud). No phishing, brute-force, replay, or rainbow table threats. Key cloning deterred (contingent on site implementing a check for the counter on the passkey).

In a passkey-centric world, an ideal setup involves a hardware authenticator as a passkey that is safeguarding a passkey-loaded password manager.

For the Enterprise part, the only possibility currently available is to force a resident key, a user verification and some attestation.

Like · **Reply**

Ken Palla 12mo

This is a good article by Roger Grimes on passkey usage.

Like · Reply | 1 Reaction

Loren Kohnfelder 12mo
Author of Designing Secure Software: A guide for developers

"1.5 factor" is an interesting term, but I think the key multi-factor question is if the extra factor(s) is worth the effort involved (and that's very context dependent).

Like · Reply | 1 Reaction

See more comments

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

More articles by this author

Epic Rant: Credit Card Companies Are Not...
Jun 25, 2024

Scientific Facts I Know That Still Baffl...
Jun 15, 2024

Here's a Secure by Design Curriculum...
Jun 12, 2024

See all