Willow Valley Computer Club

Member of apcug An International Association of Technology & Computer User Groups

Passkeys

Are they the same as passwords?

Are others using them?

Should I use them?

Al Williams

June 6, 2024

This presentation is for the curious.

This presentation provides alternatives to passkeys and an introduction to passkeys.

This presentation is not a how-to.

I will explain why we are being asked to use passkeys by first explaining issues with the alternatives

Then, I will explain what passkeys are and their issues

By the end of this presentation, you will see that there are choices and you should have a basic understanding of the advantages and disadvantages of each choice

Passkeys are the current attempt to solve the authentication problem—to verify that a person is who they say they are.

Websites have tried multiple methods to verify that you are logging into the website and not an imposter. Each method has a problem.

Verifying that you are the user is called authenticating.

Users react to these methods, either accepting or rejecting

A User Who Has Never

- Been scammed, thereby losing money
- Had their IRS information stolen, leading to many months of fighting criminals as they open multiple retail accounts
- Had someone file a false 1040 to the IRS, thereby taking your refund
- Has never had someone take over their email account and send out offensive emails
- Had an online retail account broken into and experienced multiple purchases sent to other people

Is a User Who Thinks Problems are Unlikely

A user who has experienced problems like these is a user who wants to protect themself.

Everyone has a personal threat model.

Your threat model is likely different from my threat model.

Source: *How I learned to stop worrying (mostly) and love my threat model,* Sean Gallagher, 7/8/2017, https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/

thaddeus e. grugq thegrugq@infosec.exchange

@thegrugq · **Follow**

Your threat model is not my threat model.

3:42 AM · May 15, 2017

ARPANET – The Origin of the Internet

- Developed from 1961 through 1983
- Enable computer resource sharing across ARPA sites
- Explore decentralized networks
- Although network security and privacy were considered, the concerns were not implemented

History Source: *The Complete Guide to ARPANet: The Groundbreaking Computer Network that Led to the Internet,* History Tools, November 19, 2023, *https://www.historytools.org/concepts/arpanet-complete-guide*

Privacy and Security Source: *Dark Territory: The Secret History of Cyber War,* Fred Kaplan, Simon & Shuster Paperbacks, 2016, pages 7 - 11

The First Authentication Choice: Passwords

MIT's Compatible Time-Sharing System (CTSS) – an operating system - allowed multiple users to access a single computer simultaneously.

Each user needed to identify themselves to CTSS to protect their files and data.

Professor Fernando Corbato of MIT chose passwords to verify users before granting access. Passwords authenticate authorized users to access the CTSS and its resources.

Source: *The History and Future of Passwords,* Beyond Identity Blog, Sep 23, 2021, https://www.beyondidentity.com/resource/the-history-and-future-of-passwords

The Ongoing Need for Authentication

Reputable websites must accurately identify the user logging in as the “real” user, the authentic user.

The Ongoing Need for Authentication

Examples of why websites must identify the authentic user include:

* Correctly billing the user
* Avoiding inappropriate exposure of personal identifying information such as date of birth, place of birth, address, phone number, date of birth, and more
* Meeting HIPAA requirements imposed on medical providers to protect the privacy of certain health information

How do many users react to using passwords?

U.S.A. Password Use

66% use the same password for more than one account

43% have shared their password

40% say their personal information has been compromised online

47% of those lost money due to the compromise

Source: *The United States of P@ssw0rd$,* Google / Harris Poll, October 2019, *https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf*

Percentage of People With At Least One Account in One or More Data Breaches

United States	31%
United Kingdom	35%
Australia	23%
Germany	19%
Japan	10%

Source: *2022 World Password Day Global Survey Full Report,* https://bitwarden.com/resources/world-password-day-global-survey-full-report/

What Users Can Do

- Do not reuse passwords.

  Hackers won’t be able to log into your other accounts.

- Use long passwords or passphrases with at least 18 characters.

  Hackers also use password lists to attempt to log into accounts. They start with short passwords.

- Use email aliases or relays so that your actual email address is not exposed in a data breach. You’ll need to monitor for data breaches.

  You’ll be able to cancel the account or change the password to prevent loss while not exposing your actual email address.

Have Any of Your Accounts Been Breached?

You can find out if any of your accounts have been breached and if the account password was exposed.

https://HaveIBeenPWNed.com/

If you use more than one email address for your accounts, enter each address.

13,137,301,752 accounts have been compromised

Source: https://haveibeenpwned.com/

Ways to Verify Users

Websites have three ways to verify – to authenticate – users. Each way is called an authentication factor.

Something you know

Something you have

Something you are

Source: *Multi-factor Authentication Guide,* Holly Guevara, October 13, 2020*,* https://auth0.com/blog/multifactor-authentication-mfa/

Something You Know

Password
PIN (Personal Identification Number)
Your mother's maiden name

Example: Windows 11 requires a PIN to log in. The PIN is a number with several digits.

Source: *A review of the evolution of multi-factor authentication (MFA),* Alexandra Daraglu, July 16, 2019, https://blog.typingdna.com/evolution-of-multi-factor-authentication/

Something You Know Summary

The Something You Know authentication factor does not consistently protect users because many users think there is no or little likelihood of a personal threat. This perceived lack of threat leads users to use poor password care and oversight.

Source: *2022 World Password Day Global Survey Full Report,* https://bitwarden.com/resources/world-password-day-global-survey-full-report/

Something You Have

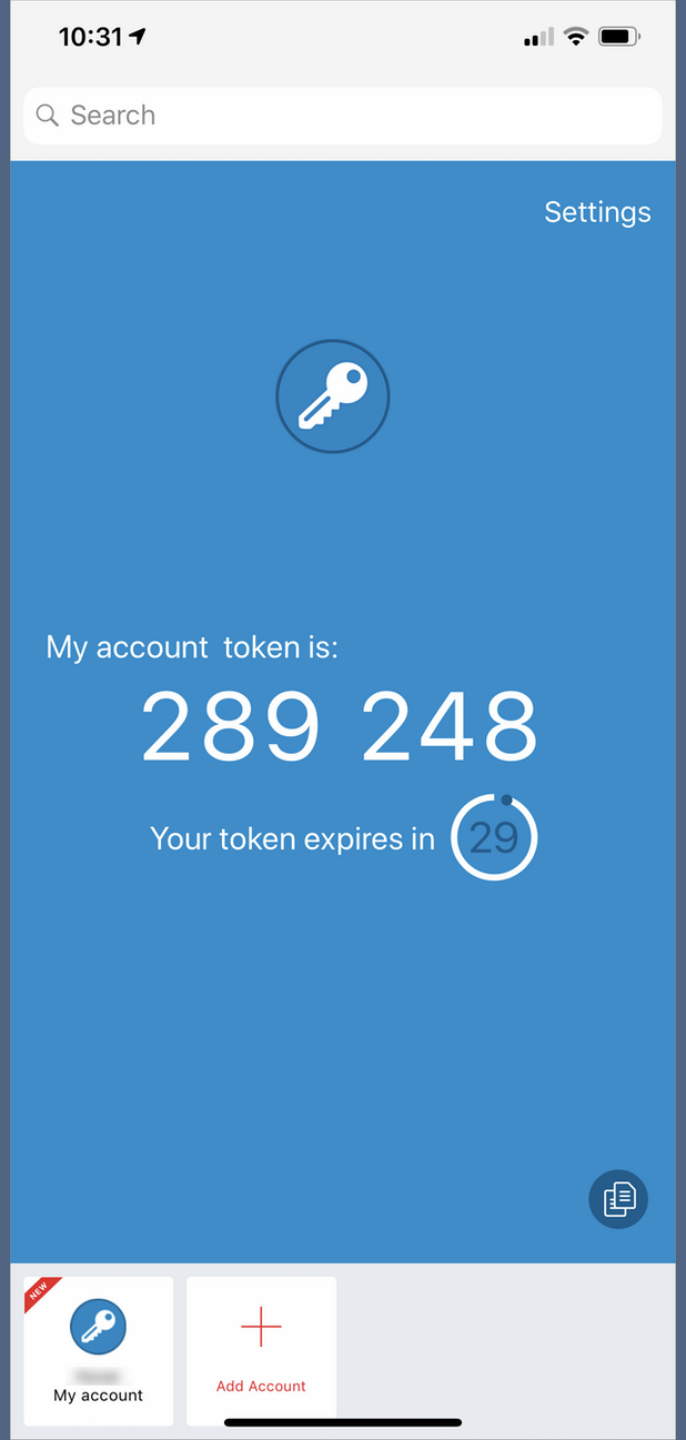
Examples of something you have

- Bank card
- Smartphone
- Authenticator app
- Hardware security key and more

Any device that will verify that you are authentic may be used.

Source: *Multifactor Authentication: User multifactor authentication for local and network …,* https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/level-2/ia-l2-3-5-3/

An image of the Authy authenticator app



User Resistance to Something You Have

Users do not like hardware security keys or security cards such as bank cards

However, smartphones are also something you have, and users have less resistance to using smartphones

Typical Two Factor Authentication (2FA)

You log into you account using your username and password (Something You Know)

The website sends a One-Time Password (a six-or-more-digit code) to your smartphone (Something You Have) via text message or email.

When you enter the code, the website recognizes you as authentic and logs you in.

Text Message Multiple-Digit Code Problem

The hacker convinces the cell phone carrier's representative that the hacker has a new phone and has the representative transfer the phone number to their phone. This is called a SIM swap.

The hacker receives the six-or-more-digit code, logs in, changes the account password and takes over the account.

If you use a second phone number, such as Google Voice, this attack will not work.

Source: *Why you should stop using SMS,* Douglas Crawford, March 9, 2023, https://proton.me/blog/stop-using-sms

Email Multiple-Digit Code Problem (2FA)

Hacker finds password for the email address in a data breach

Hacker logs into email account (let’s assume you’re not currently logged into your email account)

The hacker receives the six-or-more-digit code email, copies the code, deletes the email, and logs into the account before the account owner can. The hacker changes the password and takes over the account.

If you use an email alias and monitor data breaches, you can delete the alias when a breach occurs, preventing this later attack.

Another Two Factor Authentication (2FA)

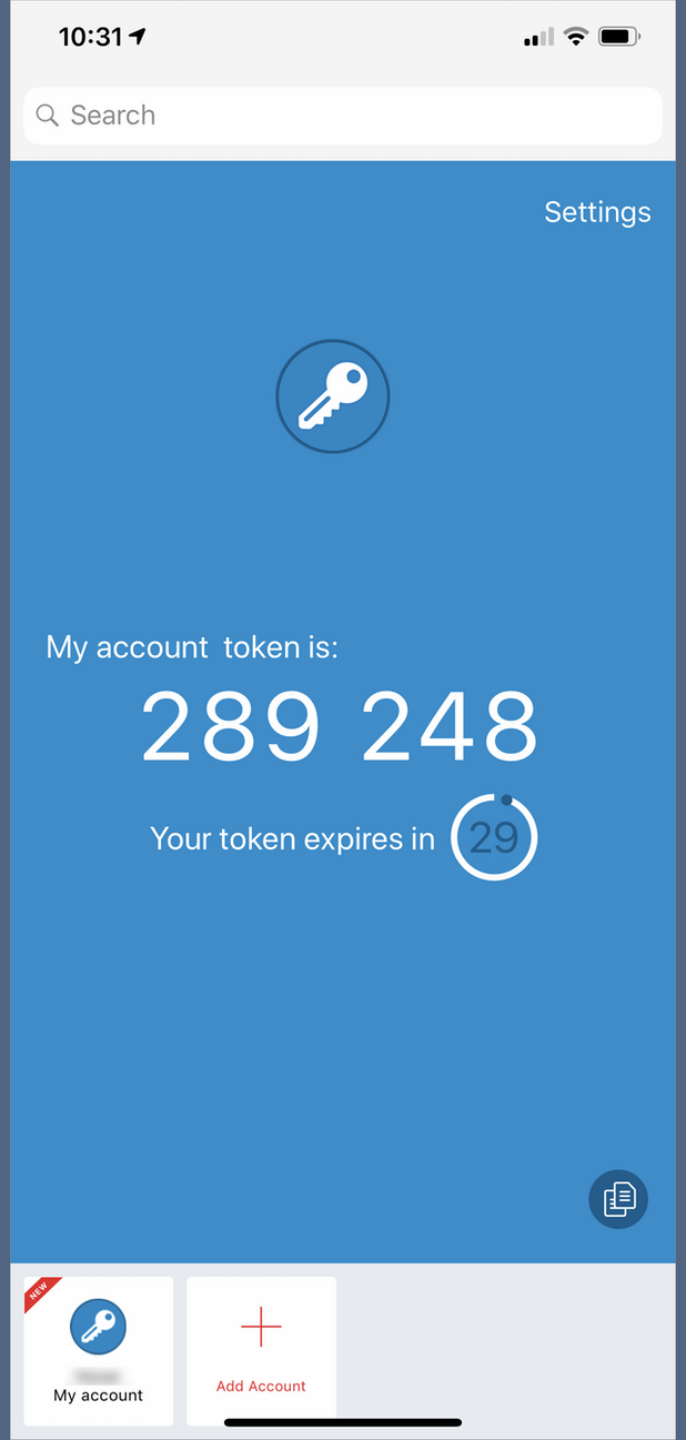
You log into you account using your username and password (Something You Know)

An authenticator app on your phone displays a six-digit code that changes every 30 seconds

When you enter the six-digit code, the website recognizes you as authentic and logs you in.

Source: *Multi-factor Authentication Guide,* Holly Guevara, October 13, 2020*,* https://auth0.com/blog/multifactor-authentication-mfa/

An image of the Authy authenticator app



User Resistance

Many users want to avoid downloading an app like Authy and setting it up for each account they wish to protect.

Source: *Multi-factor Authentication Guide,* Holly Guevara, October 13, 2020*,* https://auth0.com/blog/multifactor-authentication-mfa/

Authenticator Problem (2FA)

The user downloads an app from the Apple Store or Google Play

The app is malicious. It steals the authenticator's keys, enabling the hacker to log into authenticator-protected websites without user knowledge

Do not randomly download apps.

Source: *Most Mobile Authenticator Apps Have a Design Flaw That Can Be Hacked,* October 08, 2021, https://www.businesswire.com/news/home/20211008005015/en/Most-Mobile-Authenticator-Apps-Have-a-Design-Flaw-That-Can-Be-Hacked

Authenticator Six-Digit Code Problem (2FA)

If the smartphone is lost, it is difficult to recover access to accounts unless the user “backups” access to the authenticator app

If the user has “backups” the user can download the authenticator app to a new phone and use the “backups” to restore access to all protected accounts

Source: *Multi-factor Authentication Guide,* Holly Guevara, October 13, 2020*,* https://auth0.com/blog/multifactor-authentication-mfa/

Something You Are

Something you are

- Fingerprint
- Face scan
- Retina scan
- Typing speed, and more

Examples: FaceID and TouchID

Source: *Multi-factor Authentication Guide,* Holly Guevara, October 13, 2020*,* https://auth0.com/blog/multifactor-authentication-mfa/

Something You Are Problems (2FA)

Law enforcement can require you to log into your phone using FaceID, TouchID, or any other biometric, giving them access to your accounts

Criminals can also force you to log into your phone using your biometrics

Source: *Multi-factor Authentication Guide,* Holly Guevara, October 13, 2020*,* https://auth0.com/blog/multifactor-authentication-mfa/

Summary of the Authentication Problems

Users do not want to be inconvenienced

Criminals have found ways to bypass the authentication factors

Source: *Multi-factor Authentication Guide,* Holly Guevara, October 13, 2020*,* https://auth0.com/blog/multifactor-authentication-mfa/

Phishing

Criminals send a false email to trick the recipient into clicking on a link that goes to the trusted website but also allows the criminals to capture your username and password

Some criminals are using compelling but false templates to create phishing emails.

It is becoming harder and harder to recognize phishing emails

Source: *Passkeys: Passwordless logins for beginners,* Dr. Martin Shelton, June 7, 2023, https://freedom.press/training/passkeys-beginners/

Passkeys – the Solution

You do not need any authentication factors to log into a website. For example, username and password are not required

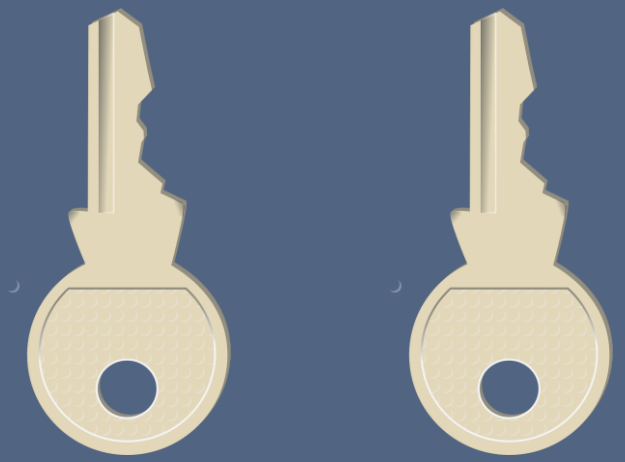
However, you still need to use an authentication factor to access your phone, laptop, or desktop to access the passkeys feature

Any weaknesses in that authentication factor can be a way for criminals to access your passkeys

Source: *Passkeys: Passwordless logins for beginners,* Dr. Martin Shelton, June 7, 2023, https://freedom.press/training/passkeys-beginners/

Why Use Passkeys?

Passwordless authentication cannot be phished

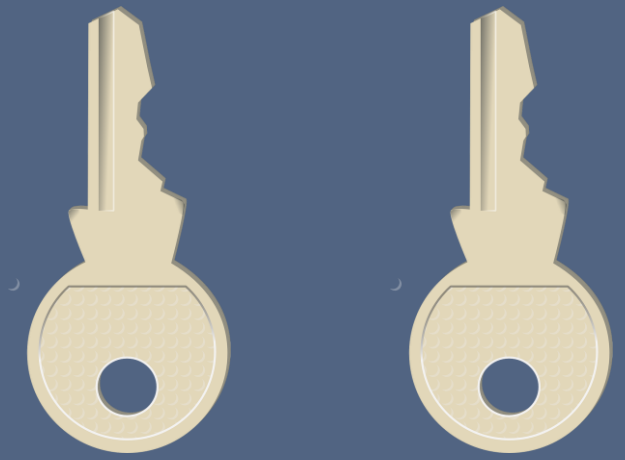


Private Public

What Are Passkeys?

A passkey is two digital keys

Each key is a string of characters



Private Public

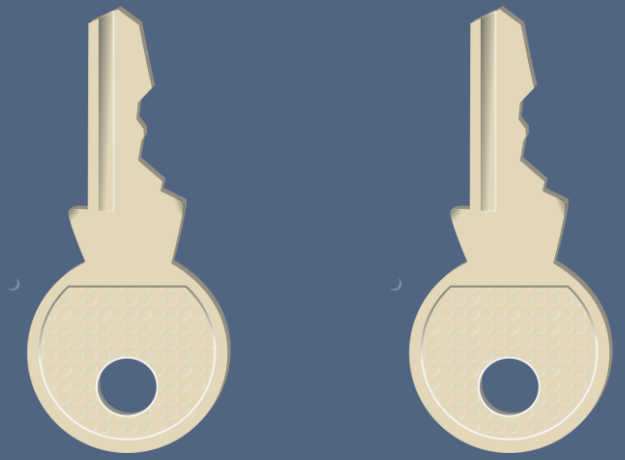
Passkeys

The public key is derived from the private key

An analogy

The private key is the parent

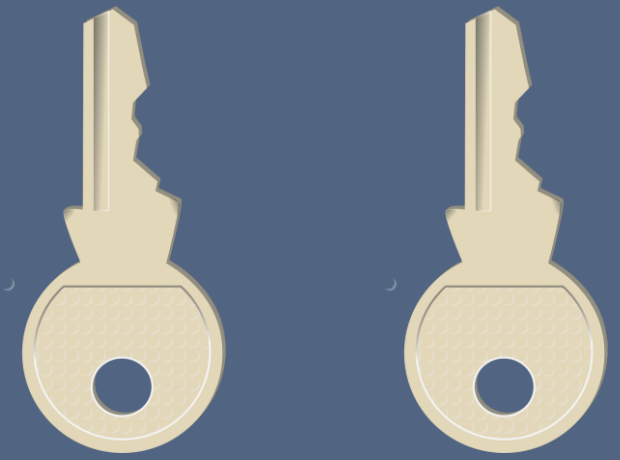
The public key is the child



Private Public

Passkeys

There are at least three ways to implement passkeys. In the following slides I’m going to show the way that is easiest to understand

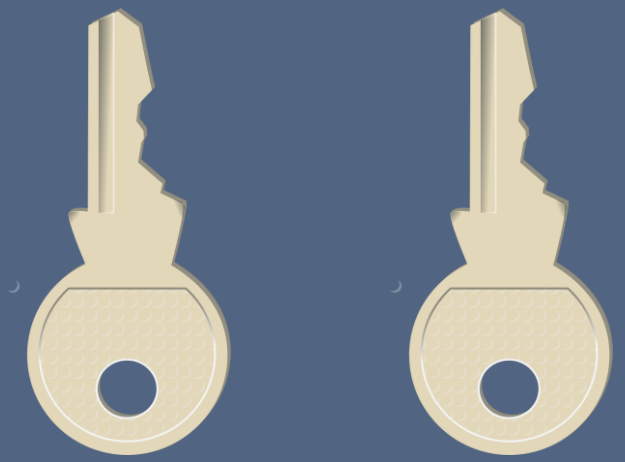


Private Public

Passkeys

The private key is stored on your cell phone, iPad, desktop, or other device

The public key is stored on the service: email, website, etc.

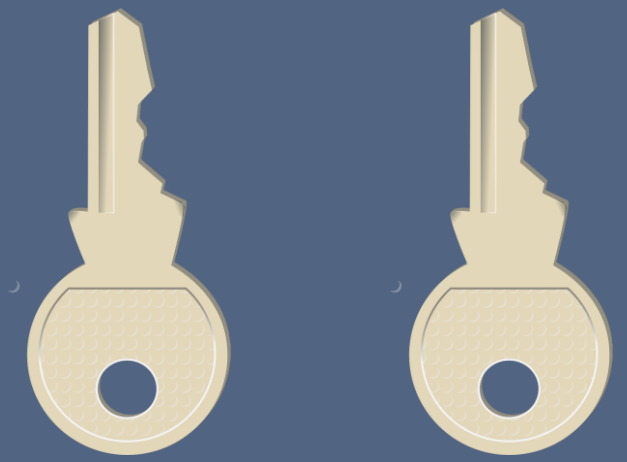


Private Public

Passkeys

When you log into a service, the service's public key verifies that you have the necessary private key on your device

An analogy – the child knows the parent



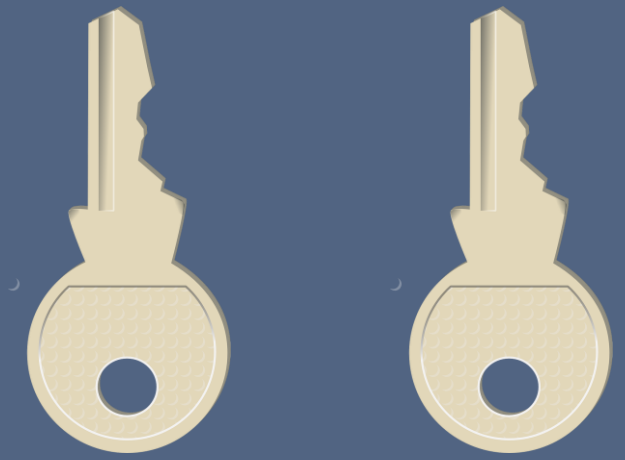
Private Public

Passkeys

The website sends a message to your device

Your device’s software uses your private key to encrypt the message and sends the encrypted message back to the website

The website decrypts the message and compares the decrypted message to the original message. If it matches, you are logged in



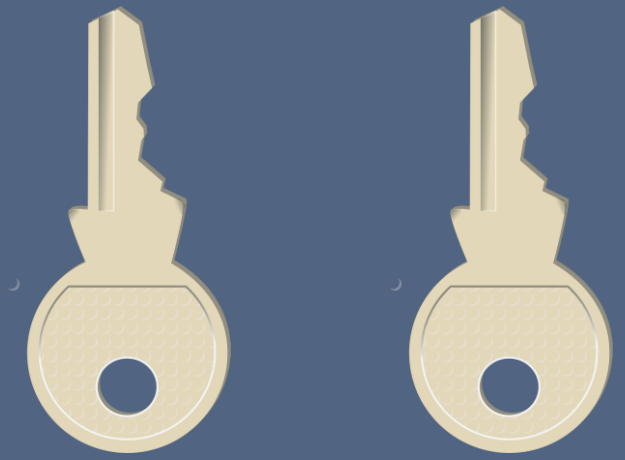
Private Public

Passkeys

Typically in encryption, anyone may have a copy of the public key so that they could have encrypted communications with the holder of the private key

That would allow criminals to claim that their websites were valid sites for the passkey

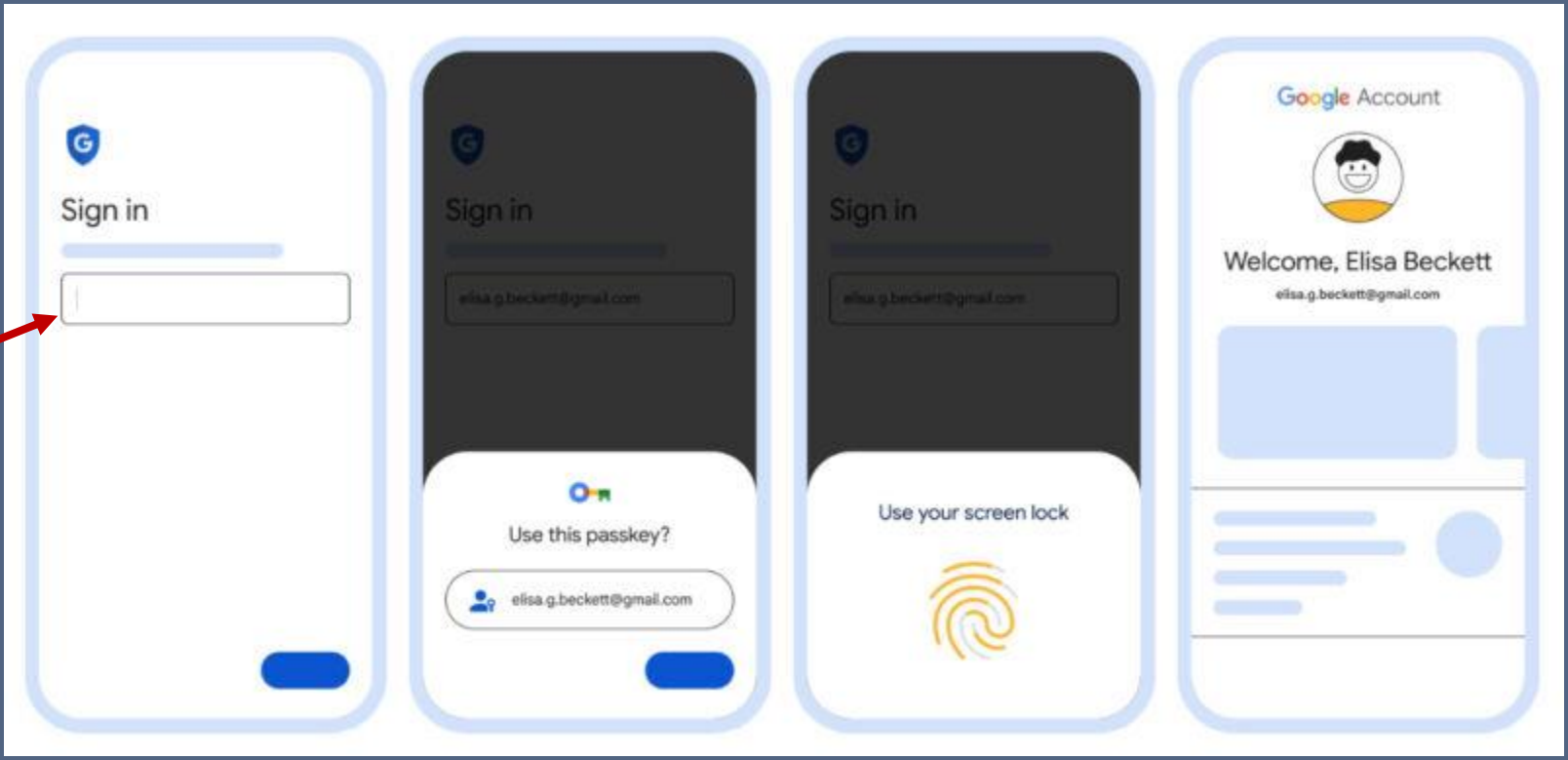
Instead, only one copy of the public key is made. That public key is bound to the website so that it may not be copied and used elsewhere



Private Public

Using Passkeys – According To Google

Username



Source: https://arstechnica.com/gadgets/2023/05/passwordless-google-accounts-are-here-you-can-now-switch-to-passkey-only/

Passkeys and Bitwarden

You may log into your Bitwarden vault (account) using up to 5 different passkeys

Bitwarden supports passkeys for each account stored in your vault

Passkeys Availability on Websites

Support continues to be rolled out

The number of websites supporting passkeys is small but increasing rapidly. To find websites, consult these listings:

Passkeys.directory
Keepersecurity.com/passkeys-directory/
Passkeys.io

Passkeys Availability On Devices

- Android
- Apple products
- Google
- Windows

Passkeys Training

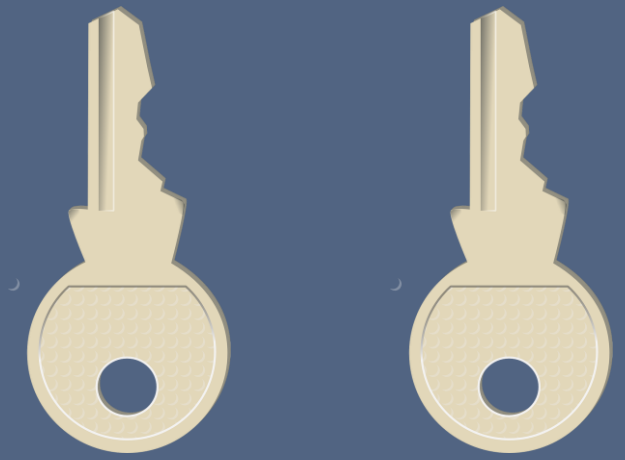
- Apple products
  - Susan Culbertson provides training about using Apple’s implementation of passkeys: culbertson.susan@gmail.com

Passkeys Training

- Bitwarden
  - Jay Shah provides Bitwarden training. He will soon offer training about using passkeys with Bitwarden

Passkeys and Hardware Security Keys

You may also use a hardware security key with passkeys to increase the security on a high risk account



Private Public

Passkeys and Hardware Security Keys

- The YubiKey Series 5 supports Passkeys
- iPhone 7 and newer iPhones support YubiKey 5/NFC
- Android phones that have NFC enabled support YubiKey 5/NFC
- A YubiKey Series 5 key supports up to 25 separate accounts

Passkeys Problem – Device Authentication

If you use FaceID, TouchID, a Passcode, or a PIN to access your Passkeys, it is less work for a hacker to access your passkeys

If you use a password manager (Bitwarden) to store your passkeys and you have a password or passphrase of 18 characters or more to access your vault, storing your passkeys in your password manager will significantly increase the protection of your passkeys.

Passkeys Problem – Syncing

When passkeys are synced across devices, you can use any device to log into a website using passkeys

Apple supports passkey syncing across Apple devices

Syncing is in the early stages for Windows and Android devices

Syncing is not yet supported by Linux distributions

If you store your passkeys in Bitwarden – since Bitwarden syncs across all devices – then your passkeys are available on devices

Passkeys – A Recommendation

If you still need to get more comfortable with Passkeys, use one of the other authentication methods until you've taken some Passkeys training or learned more about Passkeys

Once you are comfortable, I recommend using hardware security keys for high-risk accounts such as financial investment accounts. Store the passkey on two hardware security keys to prevent passkey loss in case a hardware security key is lost.

Summary

Weak and reused passwords encourage criminals

Time-based One Time Passwords can be attacked unless you take steps to prevent the attacker’s access to the TOTP

Hardware Security Keys have not been successfully attacked

Passkeys cannot be successfully phished

Passkeys – Drilling Deeper

Entry level: https://www.howtogeek.com/763503/why-the-future-is-passwordless-how-to-get-started/

Intermediate level: https://duo.com/blog/webauthn-passwordless-fido2-explained-componens-passwordless-architecture

Detailed level: https://duo.com/blog/tags/administrators-guide

Passkeys – Drilling Deeper

Source: *Passkeys – Threat modeling and implementation considerations*, Vincenzo Iozzo, Kasper Mroz, 24 May 2023, https://slashid.com/blog/passkeys-security-implementation/

Advisor: Bill Skelly

Questions?