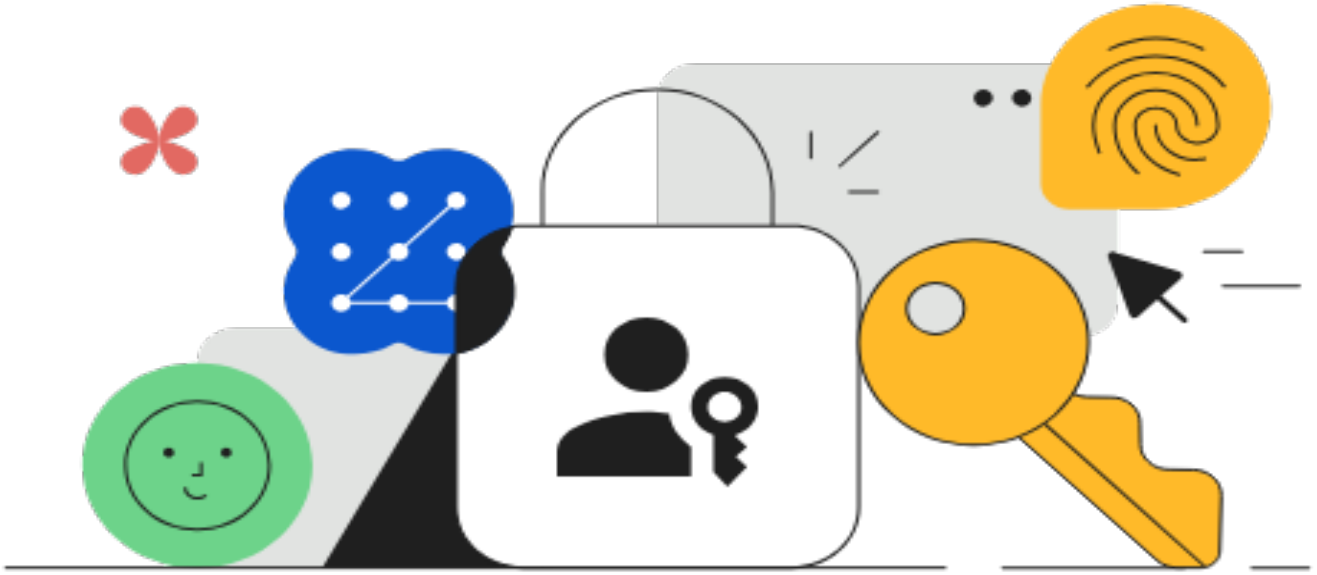
Passkey Sign on



mdlug 2025

Pat Baker

Pat Baker

Information Assurance (CyberSecurity), Intelligence Analyst, Technology Analyst, Linux/Unix Knowledge

OtakuSystems LLC
otakusystems.com

Technologist, Futurist, Philosopher, Geek

- Seeker of wisdom and knowledge

Disclaimer

Not responsible for any damage done to you, your friends, your accounts, your pet goldfish, etc. All information is for educational or general knowledge purposes.
Information held within may or may not be legal by your country, state or business.

If it's not legal then you should do it?

“Passkey” what is it?

A kind of quick explanation, sorta.

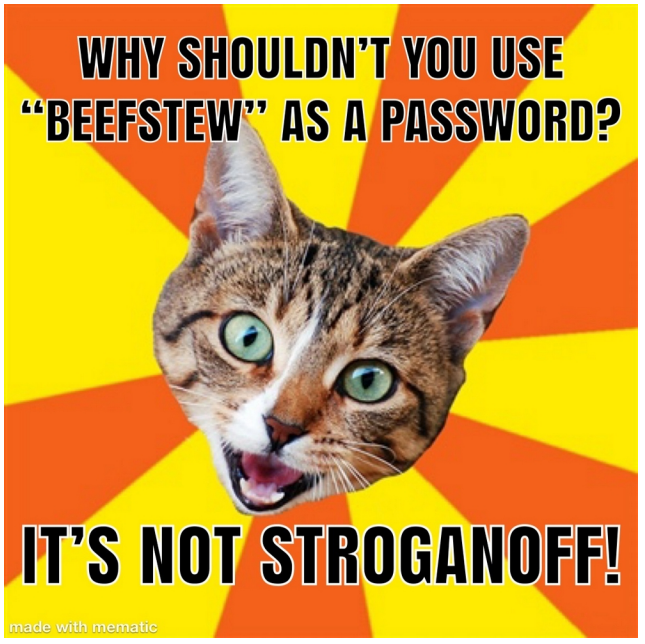
HealthEquity

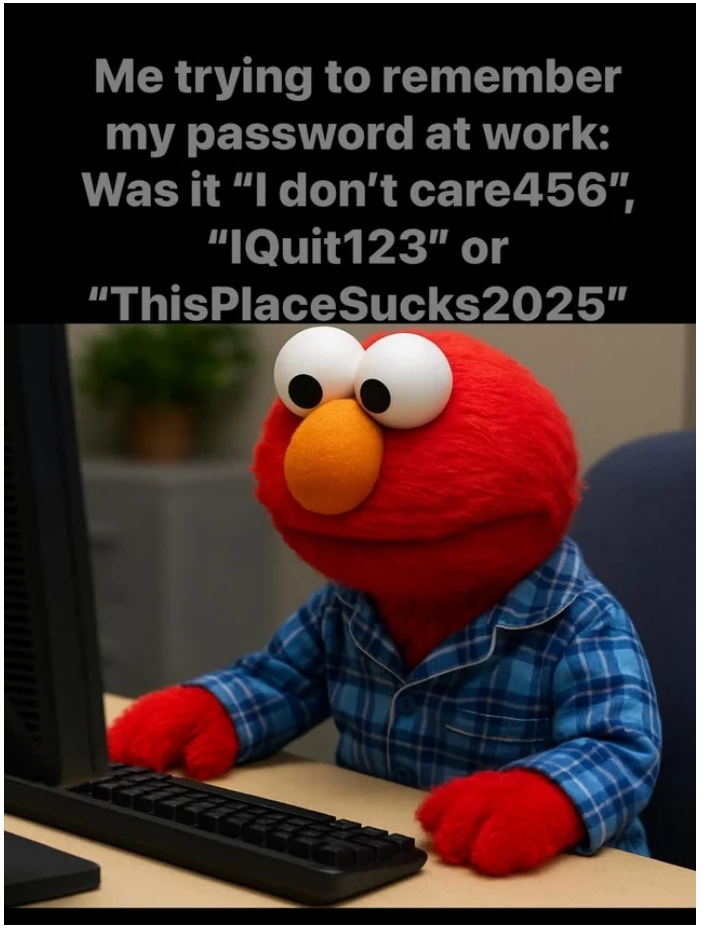
Get the HealthEquity Mobile app ➔

Passwords are out. Passkeys are in.

Coming soon: You'll need to create a passkey with the mobile app to access your benefits—even online or when calling us. The app's also an easier way to stay on top of everything.[1]

Learn about passkey





What is PassKey?

A passkey is like a digital house key stored on device you trust, like your computer or phone.

It lets you sign in to websites just by using your fingerprint, face scan, or PIN—no typing long passwords.

Why use them?

1. They’re easier
- No password to remember, No need to type anything. At times never prompted to enter a password or login credentials.

2. They’re more secure
- Passkeys can’t be guessed, They can’t be stolen in a data leak, Hackers can’t “phish” them with fake websites.

3. Stored in central location
-Passkey data is stored in a ‘central’ location, in a ‘secure’ place.

Reason not to use them, ‘yet?’

- New implementation of old idea, like 2FA.

- No full standard, multiple groups (Google, Microsoft, Apple) want you to use their definitions.

- Not usable on all devices, conflicting ‘standards’ problem.

- May be locked to a single device or system.

The old ways?

Account / Password – been around for near ever, most people understand what is is and how it works.

Two Factor Authentication, key or device – a challenge given and response returned. Something I have or something I am.

Issues with old ways

Account / Password – Account / Password database can be stolen, site phishing issues from hackers, reuse of passwords on multi sites.

Two Factor Authentication, key or device – Lose the device, some sites not use 2FA.

How do passkeys work?

In order for passkeys to work, an authenticator, such as a mobile device (some refer to TPM Trusted Platform Module) or password manager that supports passkeys, generates two cryptographic keys for each account you create. One key is public and stored on the site where you create the account, and the other is private and stored in your authenticator. When you sign in to your passkey-enabled account, your authenticator and the website communicate to authenticate your login without exchanging any actual secrets that a hacker could exploit.

How do passkeys work?

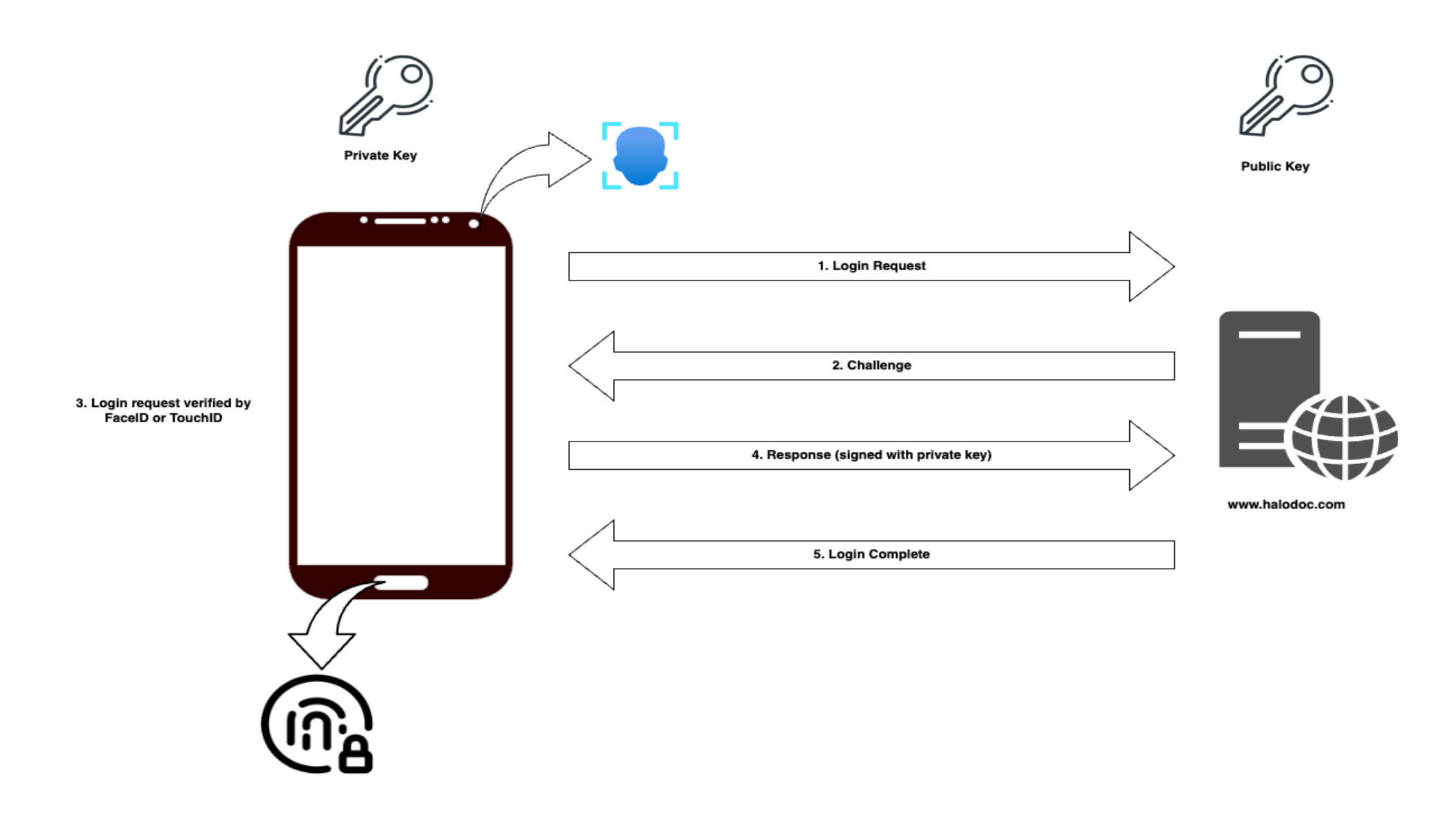
Passkeys are created using the WebAuthn API that’s widely implemented in all modern browsers and operating systems. Most of the complexity is hidden in the software. The user only needs to approve the creation or use of the passkey. User approval can take the form of an on-device biometric check using a fingerprint sensor or facial recognition or a local device password or PIN.

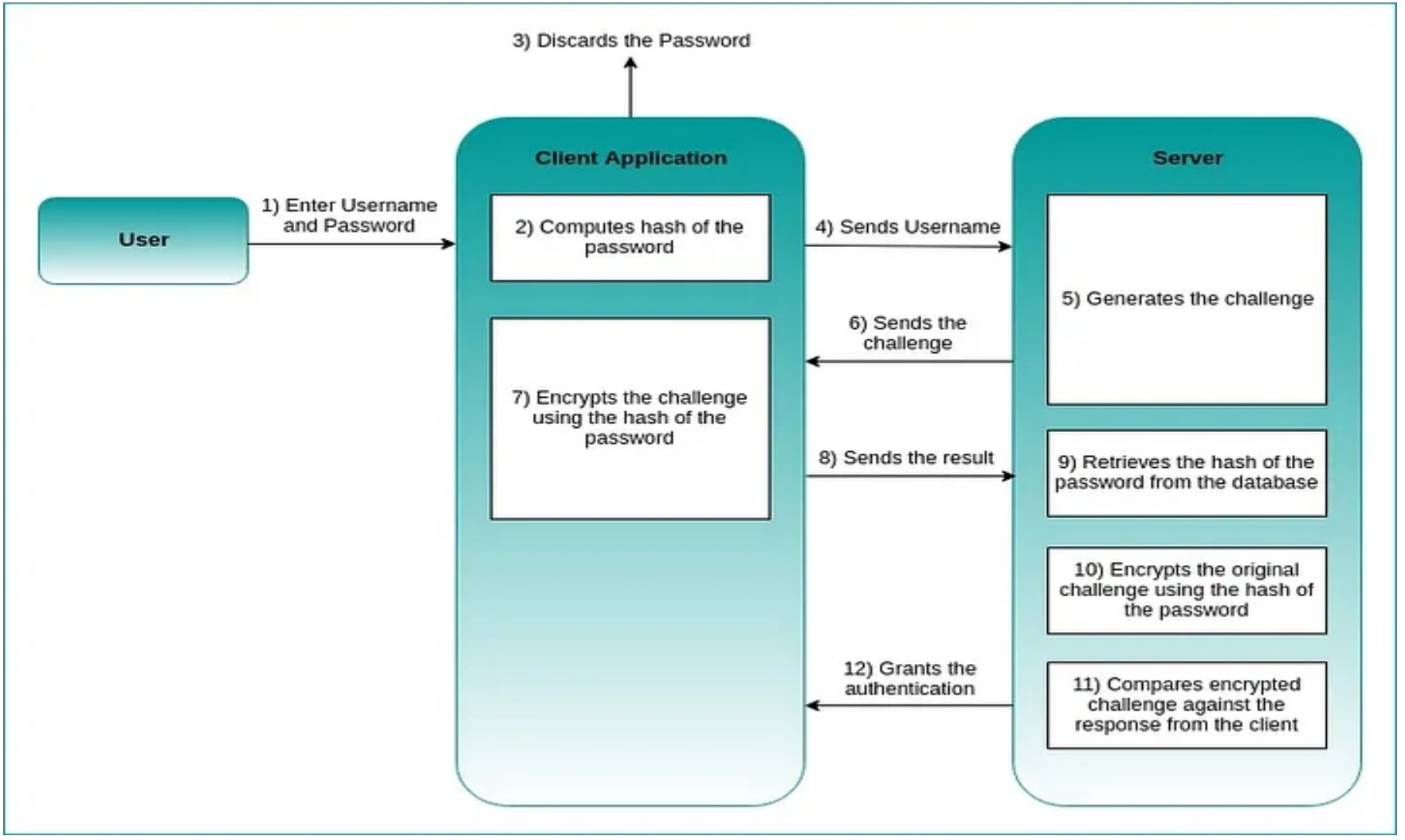
How do passkeys work?

Passkeys can be either device-bound or synced between devices. Device-bound passkeys are typically ones that are created on a hardware key, such as a YubiKey or a Titan Security Key, while synced passkeys are typically managed by a password manager—either one that's built into your device's operating system or a standalone/ site vault password manager such as 1password, lastpass, dashlane. Synced passkeys have the advantage of being available on any of your devices where the password manager is available.

A bit deeper

Using cryptographic key pairs (public/private) instead of passwords, allowing passwordless sign-ins that are phishing-resistant and secure, relying on biometrics (face/fingerprint) or device PINs for local device verification instead of sharing secrets. When you log in, the service sends a random challenge, your device uses its stored private key to sign it (after biometric confirmation, or other way), and the server verifies that signature with the corresponding public key, proving it's you without ever sending a password.


Private Key
Public Key
1. Login Request
2. Challenge
3. Login request verified by FaceID or TouchID
4. Response (signed with private key)
5. Login Complete
www.halodoc.com


3) Discards the Password
Client Application
Server
User
1) Enter Username and Password
2) Computes hash of the password
4) Sends Username
5) Generates the challenge
6) Sends the challenge
7) Encrypts the challenge using the hash of the password
8) Sends the result
9) Retrieves the hash of the password from the database
10) Encrypts the original challenge using the hash of the password
12) Grants the authentication
11) Compares encrypted challenge against the response from the client


User
IT system
on the Internet
Challenge/Response Process
Registration
Private
Key
Challenge
eb9695b23
Response
48d6a0f48
Public
Key
eb9695b23
48d6a0f48

Registration Process

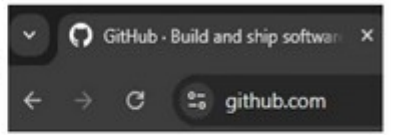
How the Registration Process Works:

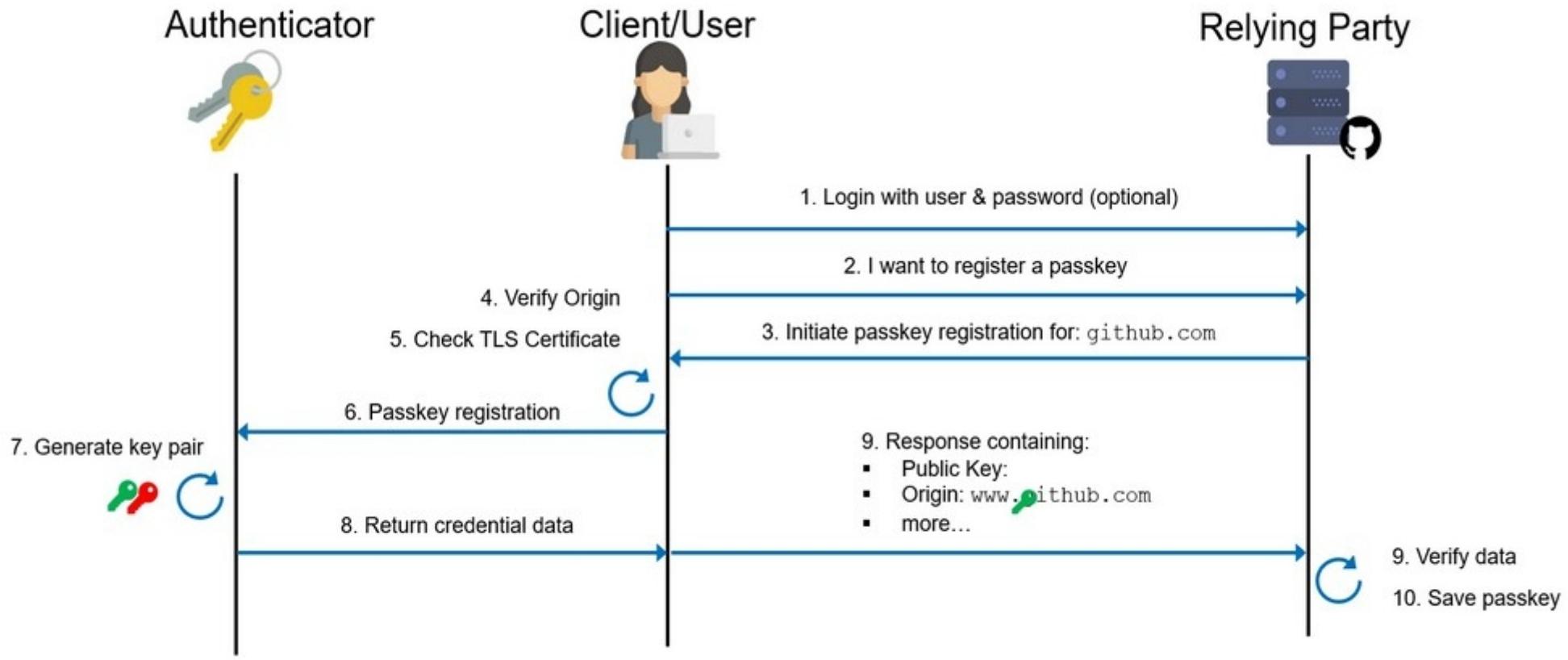
Registration: When you first set up a passkey, a unique key pair is generated: a private key (stays on your device) and a public key (sent to the website's server).

1 - Login Request: You click "Sign in with a passkey" on a service.
2 - Challenge: The server sends a random "challenge" to your device.
3 - Device Verification: Your device prompts you for a biometric (Face ID, fingerprint) or PIN to confirm it's you.
4 - Cryptographic Signature: Your device uses the private key to create a unique digital signature for that challenge.
5 - Verification: The signed challenge is sent back to the server, which uses the stored public key to verify the signature.

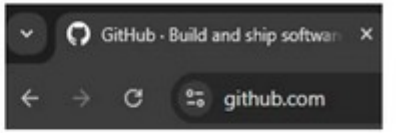
6 - Access Granted: If the signature is valid, you're logged in instantly and securely.

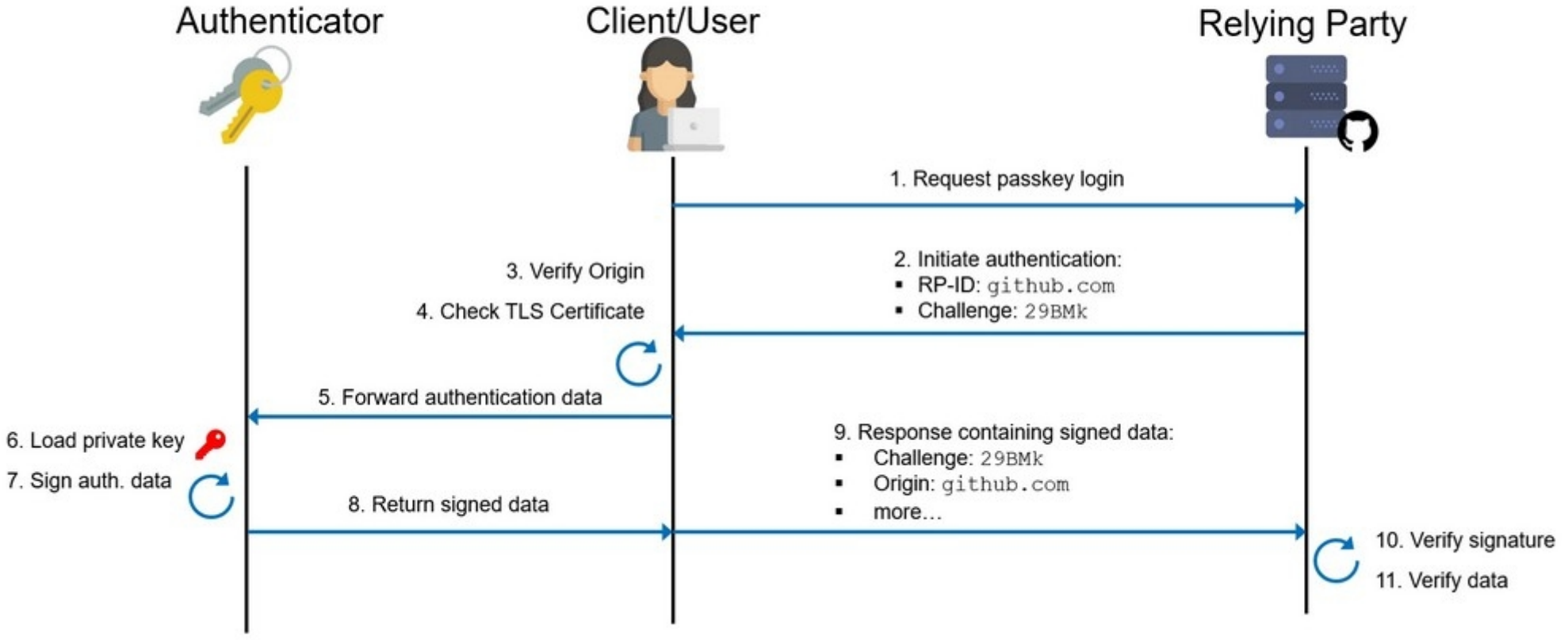
Passkey Registration Ceremony (simplified)





Passkey Authentication Ceremony (simplified)

Origin: 



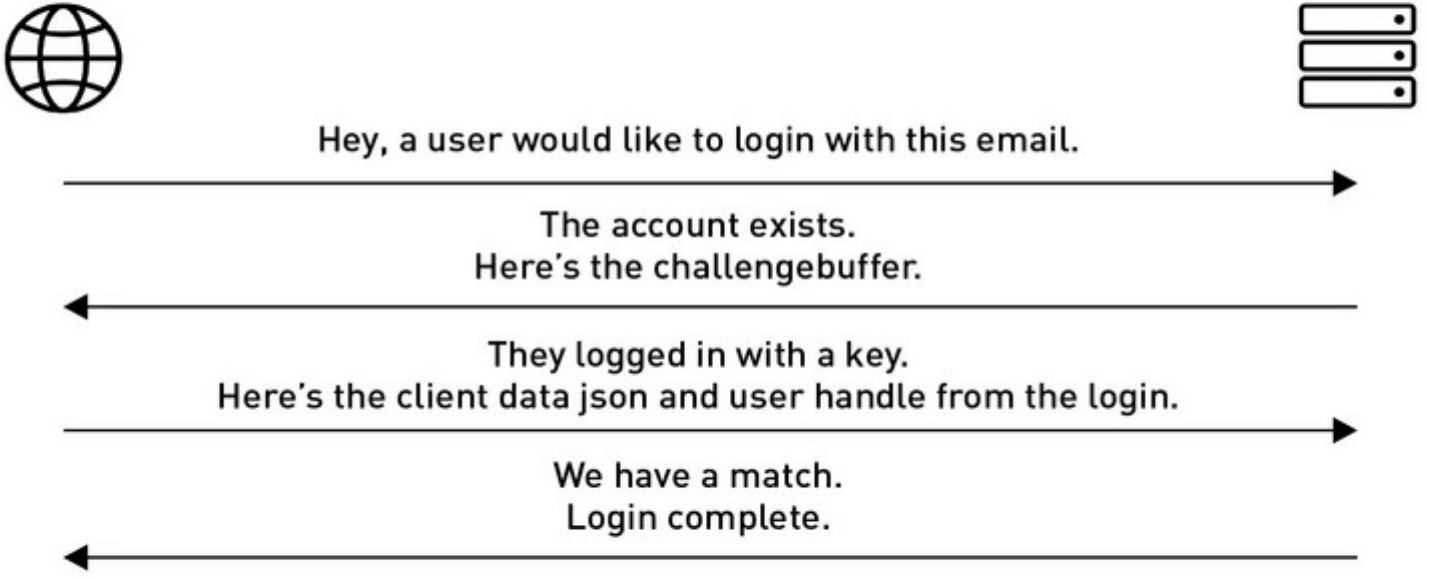
Some quick links

https://www.youtube.com/watch?v=2xdV-xut7EQ&pp=ygUfcGFzc2tleXMgZXhwbGFpbmVkIGluIDUgbWludXRlcw%3D%3D

https://www.youtube.com/watchv=UfdZJsWitFc&t=315
https://www.youtube.com/watch?v=bdp8RdjV6PU&t=48
https://www.youtube.com/watch?v=BMM98e6QYSI&t=12

Passkey

Authentication



Public Private key encryption

Public key vs. Private key (super simple)

- Private key = your secret password
  - You never share it.
  - It proves you are you.
- Public key = your public address
  - You can share it with anyone.
  - Others use it to send you encrypted stuff or verify your signature.

Public Private key encryption

How they work together

You keep your private key safe.

You give people your public key.

If someone wants to send you something securely, they encrypt it with your public key.

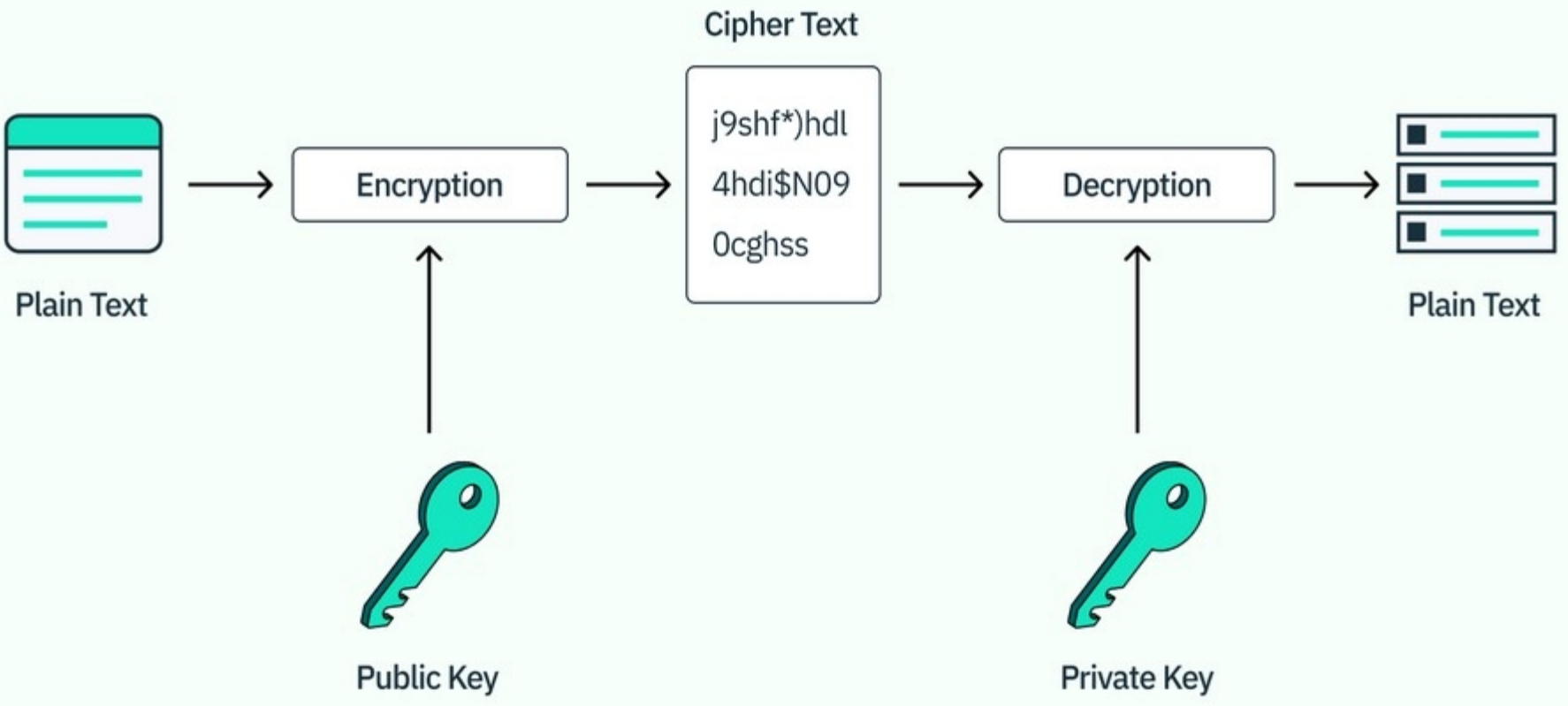
Only your private key can unlock it.

If you want to prove something is from you, you sign it with your private key.

Anyone can verify the signature using your public key.

Public Private key encryption

One-sentence summary
Public key = shareable lock; private key = the only key that unlocks it.


Cipher Text
j9shf*)hdl
4hdi$N09
0cghss
Plain Text
Encryption
Decryption
Plain Text
Public Key
Private Key

Public Private key encryption

Sites to learn more

https://en.wikipedia.org/wiki/Public-key_cryptography
https://preveil.com/blog/public-and-private-key/

Passkey Services

Small list of sites

- 1password
- Lastpass
- Bitwarden
- NordPass
- Keeper
- Dashlane
- Others…(google, microsoft, apple, amazon)...

Standalone passkey managers

- Some I found or have used

- KeepassXC – (2.7.x and newer)
- Proton pass

Links of note

https://www.passkeys.com/passkey-manager
https://fidoalliance.org/passkeys/
https://www.dashlane.com/blog/what-is-a-passkey-and-how-does-it-work
https://preveil.com/blog/public-and-private-key/
https://blog.compass-security.com/2025/02/passkeys/
https://blogs.halodoc.io/passkey-authentication/
https://www.twilio.com/docs/verify/passkeys/technical-overview
https://youtu.be/QYdHm7zoF_M
https://youtu.be/bdp8RdjV6PU
https://youtu.be/3BmYR--3z8M

Questions?