Passkeys are here!

What now?

- Co-chair of FIDO2-TWG
- Product lead for platform (Chrome/Android) passkey implementation
- Work on Google Account passkey implementation

Christiaan Brand

Group Product Manager

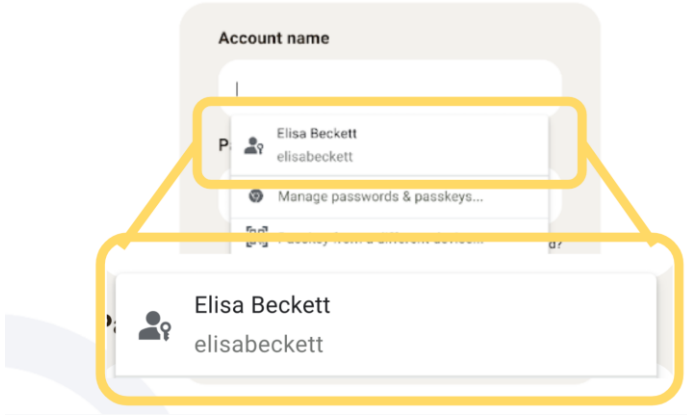
Google

identiverse

@christiaanbrand

#identiverse

Passkey overview



Syncing

Passkeys aren't only stored on a single device, but synchronize to your (Google) account and is available on your other devices too

Cross-device

Passkeys on *one* device, can be used on a *different* device using FIDO's standardized cross-device flow

Discoverable

Passkeys contain metadata which allows your system (browser, autofill, etc) to present passkeys to you, even if you didn't know you had one

Passkeys are available everywhere (well... almost)

How do they work?

Passkeys enable signing in to a site using the same method you use to unlock your device (FaceID, TouchID, etc).

The biometric unlocks your “passkey” to generate a signature that enables you to sign in.

They don't only replace passwords

Passkeys are inherently *two-factors-in-one;* meant to replace **both** the user's password **and** traditional multi-factor authentication step.

Communicating the value proposition to users

Confidentiality
(Security)

My sensitive information should be **protected from unauthorized access**

Security needs

Integrity

My sensitive information should not be changed or deleted by others

Availability
(ease of access)

I want **easy access** to my sensitive information when I need it

Ease of use and safety is most important

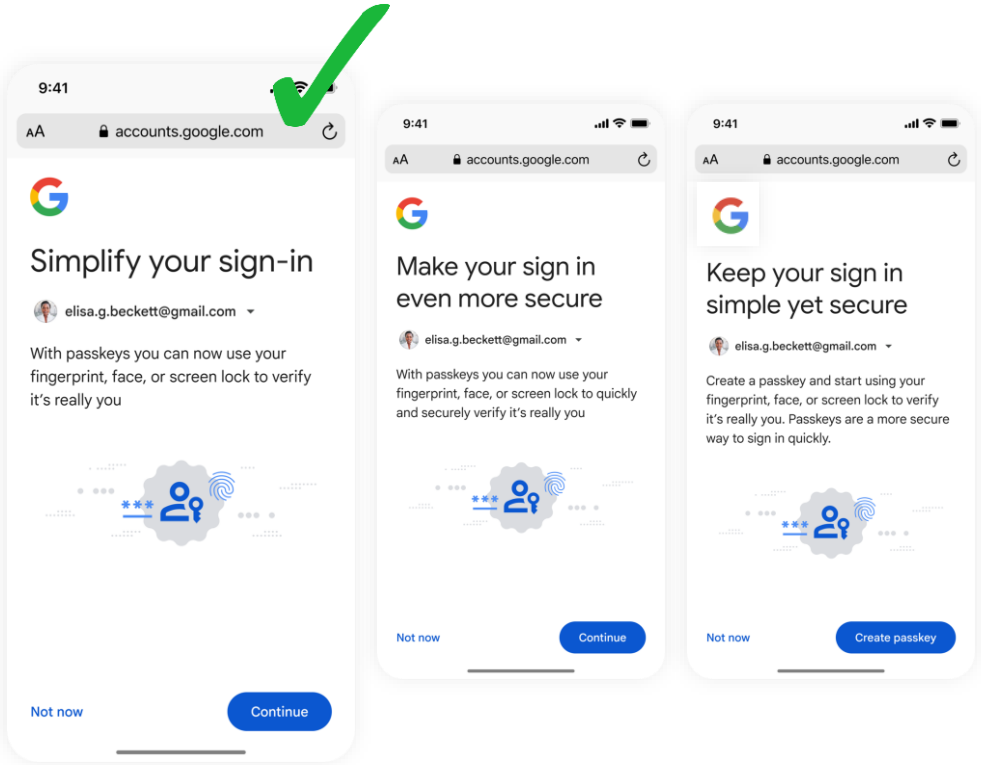
	Passkeys are faster and safer than passwords	Passkeys will work across all operating systems and platforms (computers, apps, phones)	Passkeys are protected even if you lose your phone	Passkeys can't be guessed, stolen, or duplicated	Passwords are going away, passkeys will replace them
Interested in using Passwordless based on statement	**Majority interested or very interested**	Mostly 'Likely'	Many 'likely', some 'unlikely'	Many 'likely', some 'unlikely'	Mixed responses
Why?	The speed, simplicity and efficiency of passkeys makes them persuasive as a concept	The versatility of this one-stop-shop' solution is appealing	Dispenses with need to recall passwords	Some find the messaging about security reassuring	Some see passkeys as an inevitable progression – others would like more information
Confusion or Concern About Statement	Some have lingering concerns about security. Others are unsure how 'passkeys' actually work	So much reliance on a single device is troubling	Implies surrendering responsibility for security	Some are skeptical about this claim	How can we be sure passkeys are safe?

Ease of use and safety is most important

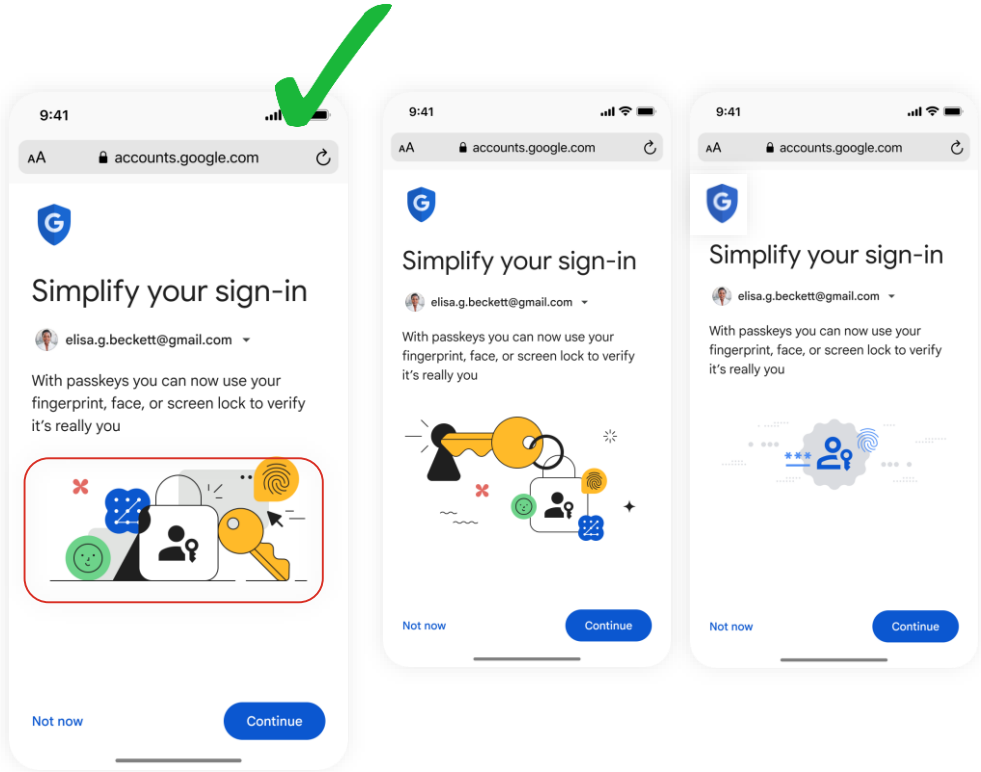
	Passkeys are faster and safer than passwords	Passkeys will work across all operating systems and platforms (computers, apps, phones)	Passkeys are protected even if you lose your phone	Passkeys can't be guessed, stolen, or duplicated	Passwords are going away, passkeys will replace them
Interested in using Passwordless based on statement	Majority interested or very interested	Mostly 'Likely'	Many 'likely', some 'unlikely'	Many 'likely', some 'unlikely'	Mixed responses
Why?	The speed, simplicity and efficiency of passkeys makes them persuasive as a concept	The versatility of this one-stop-shop' solution is appealing	Dispenses with need to recall passwords	Some find the messaging about security reassuring	Some see passkeys as an inevitable progression – others would like more information
Confusion or Concern About Statement	Some have lingering concerns about security. Others are unsure how 'passkeys' actually work	So much reliance on a single device is troubling	Implies surrendering responsibility for security	Some are skeptical about this claim	How can we be sure passkeys are safe?

The speed, simplicity and efficiency of passkeys makes them persuasive as a concept

Making it practical



Participants confirmed preference for a simple and clear title that speaks for the simplicity of passkey.



Most participants chose the first icon variation because the images were colorful and provided specific details on how passkey could be used, such as fingerprint and face ID

We want users to remember...

UX

Simplify authentication

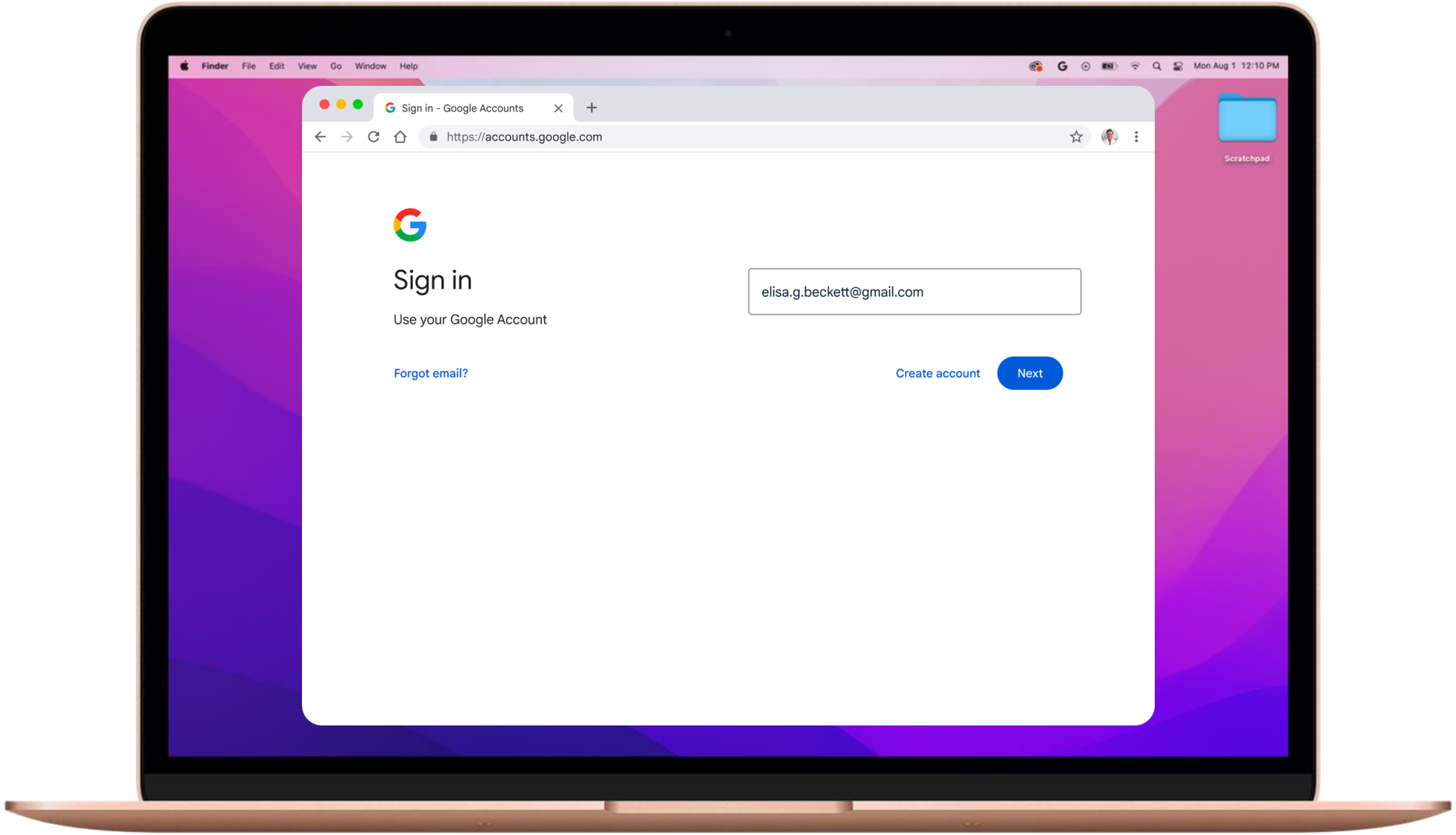
Use screen lock to create and use passkeys and are a standalone alternative to passwords

Improve security

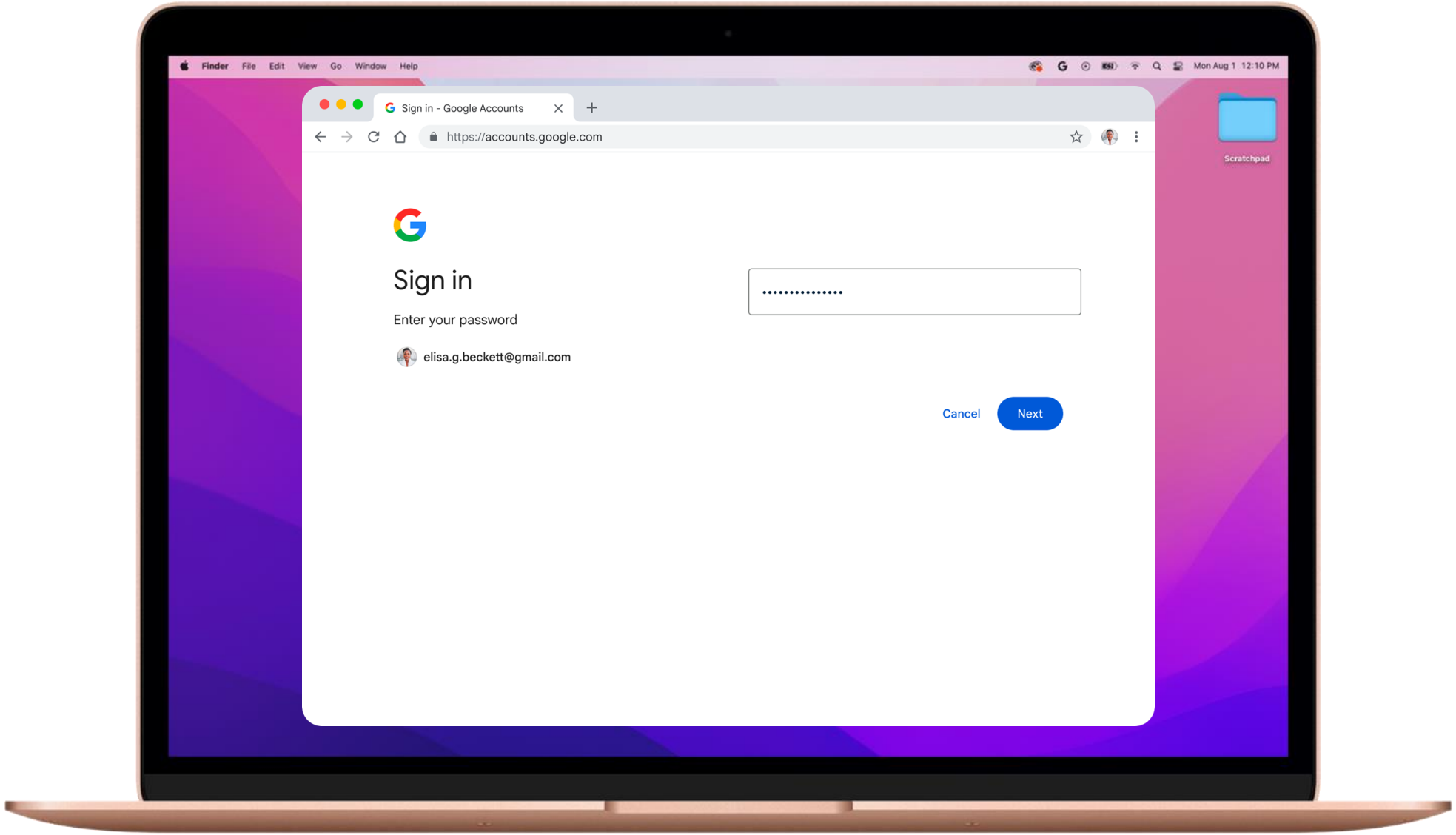
Server leak resistant, phishing resistant, and end-to-end encrypted

Let’s look at some user journeys

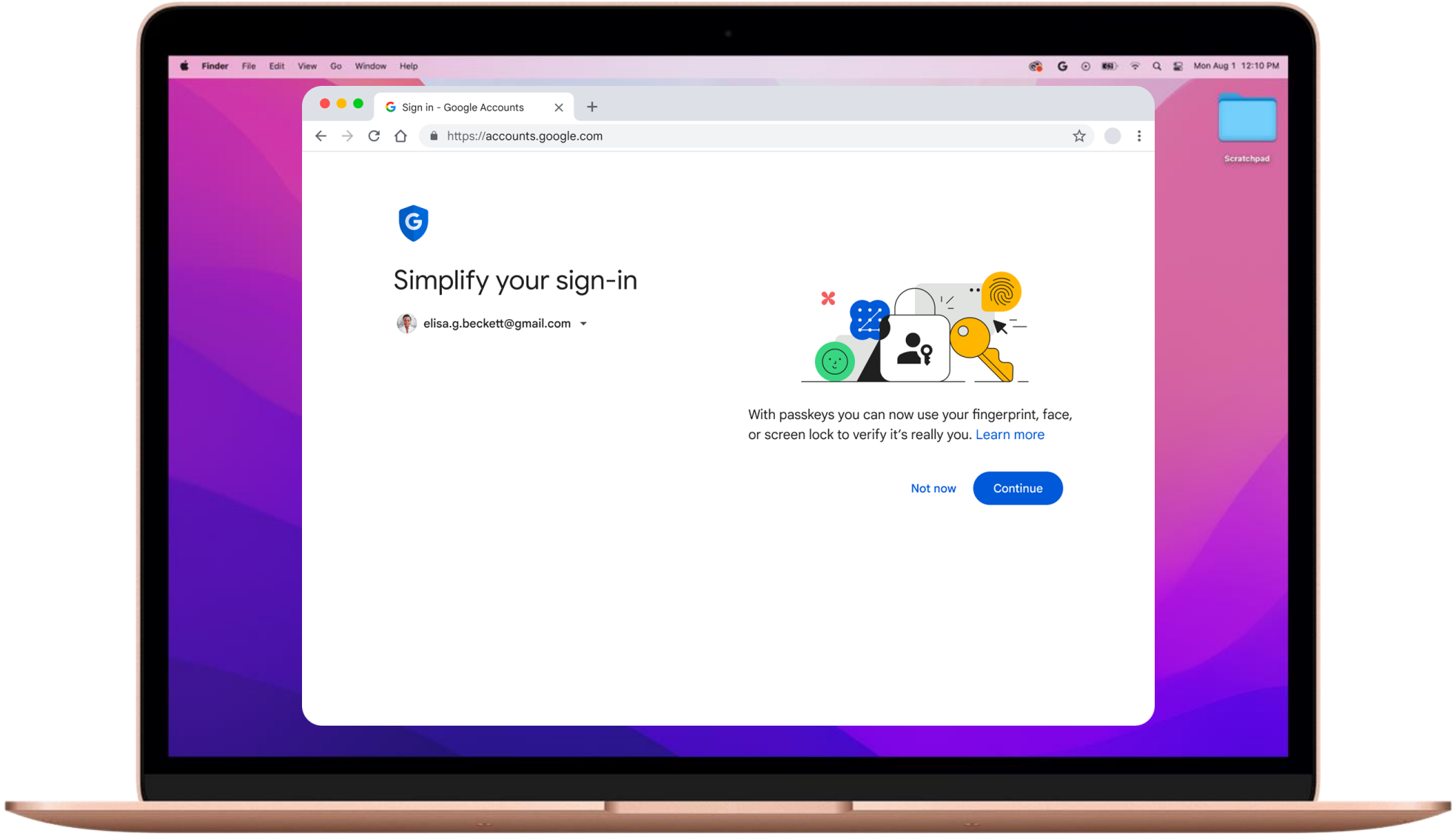
Creating a passkey



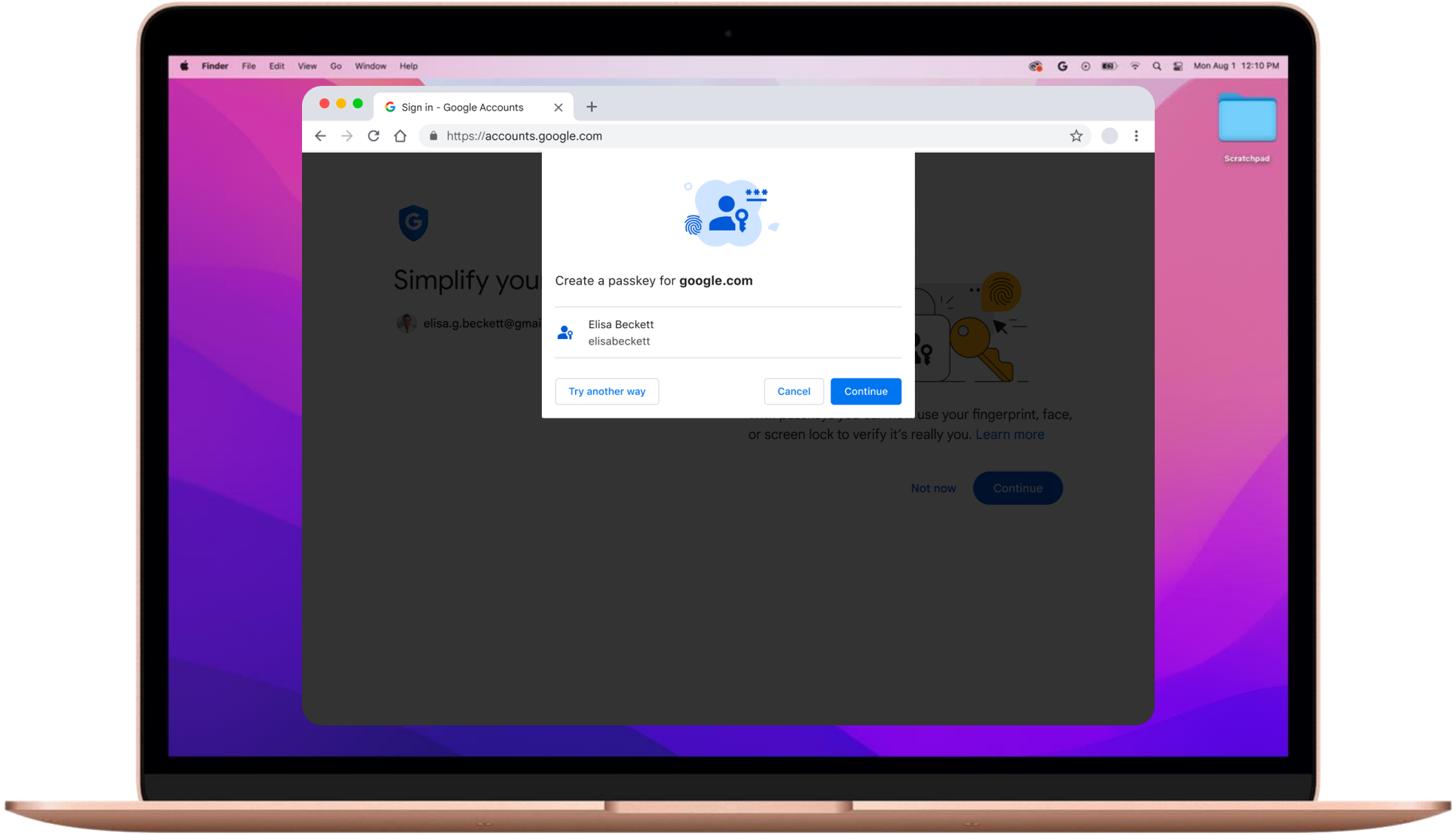
After Elisa enters her username



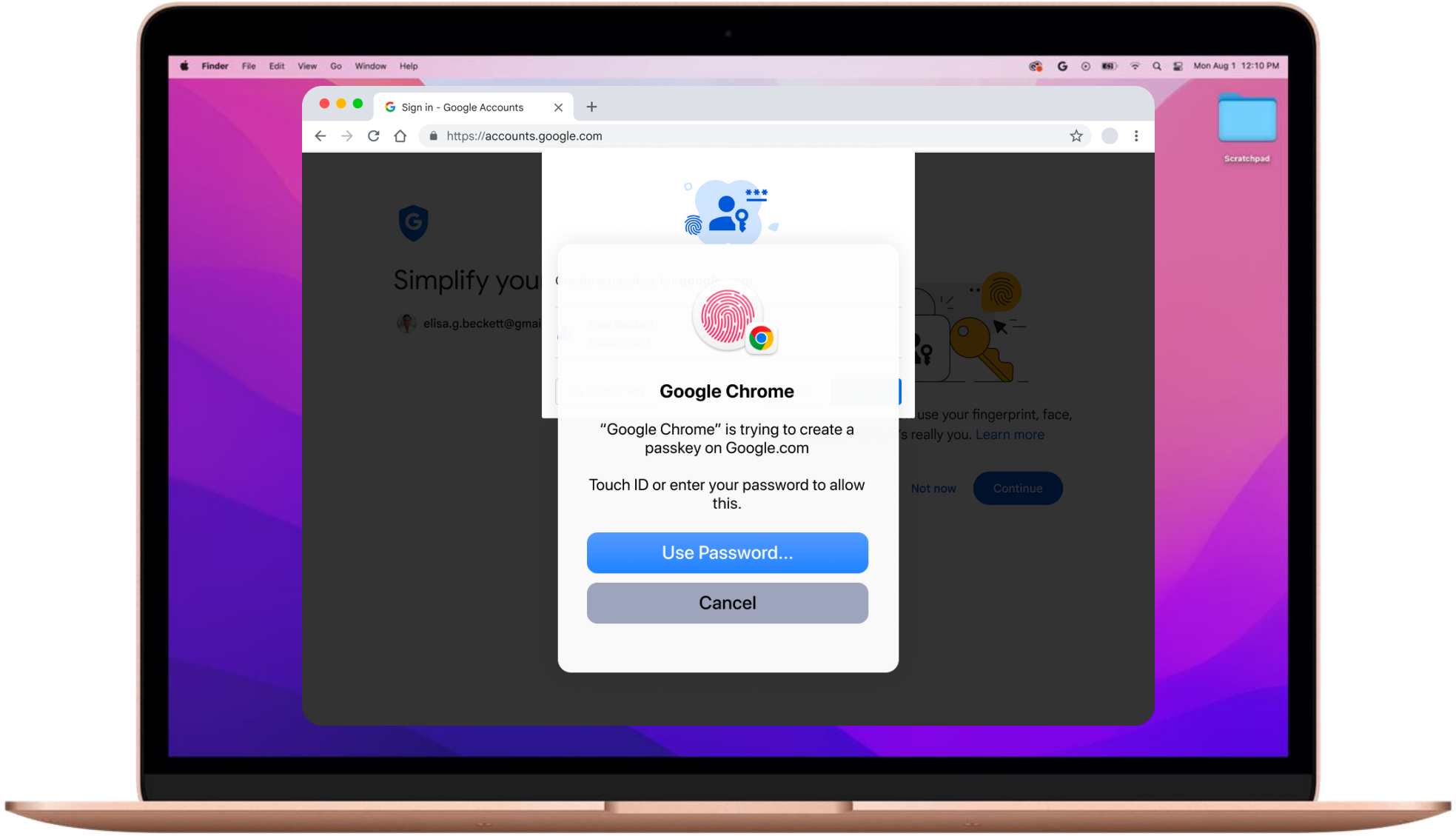
And enters her password



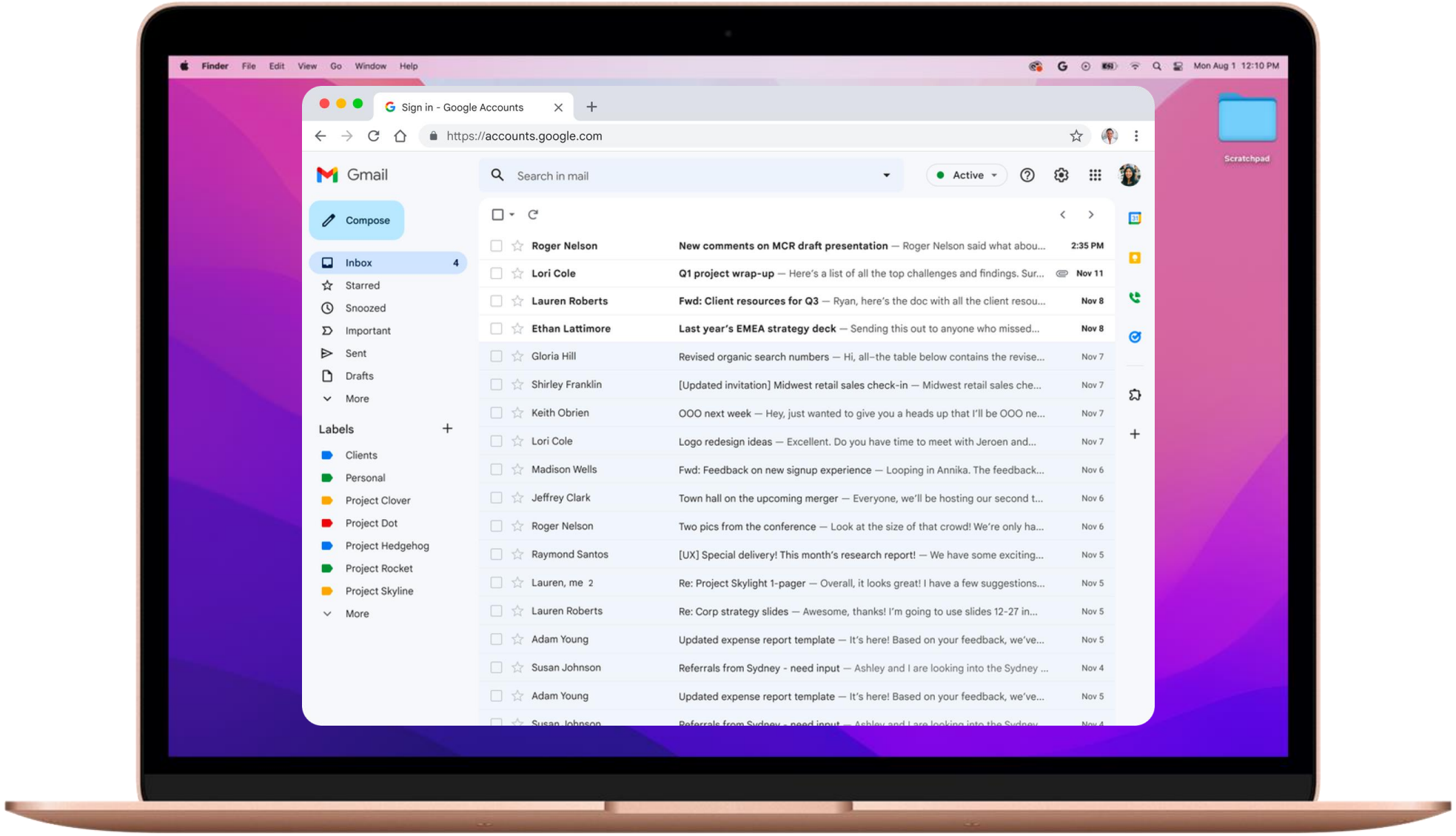
Google.com will detect that Elisa is eligible for passkeys and promote them



Chrome will show Elisa the passkey she's going to create



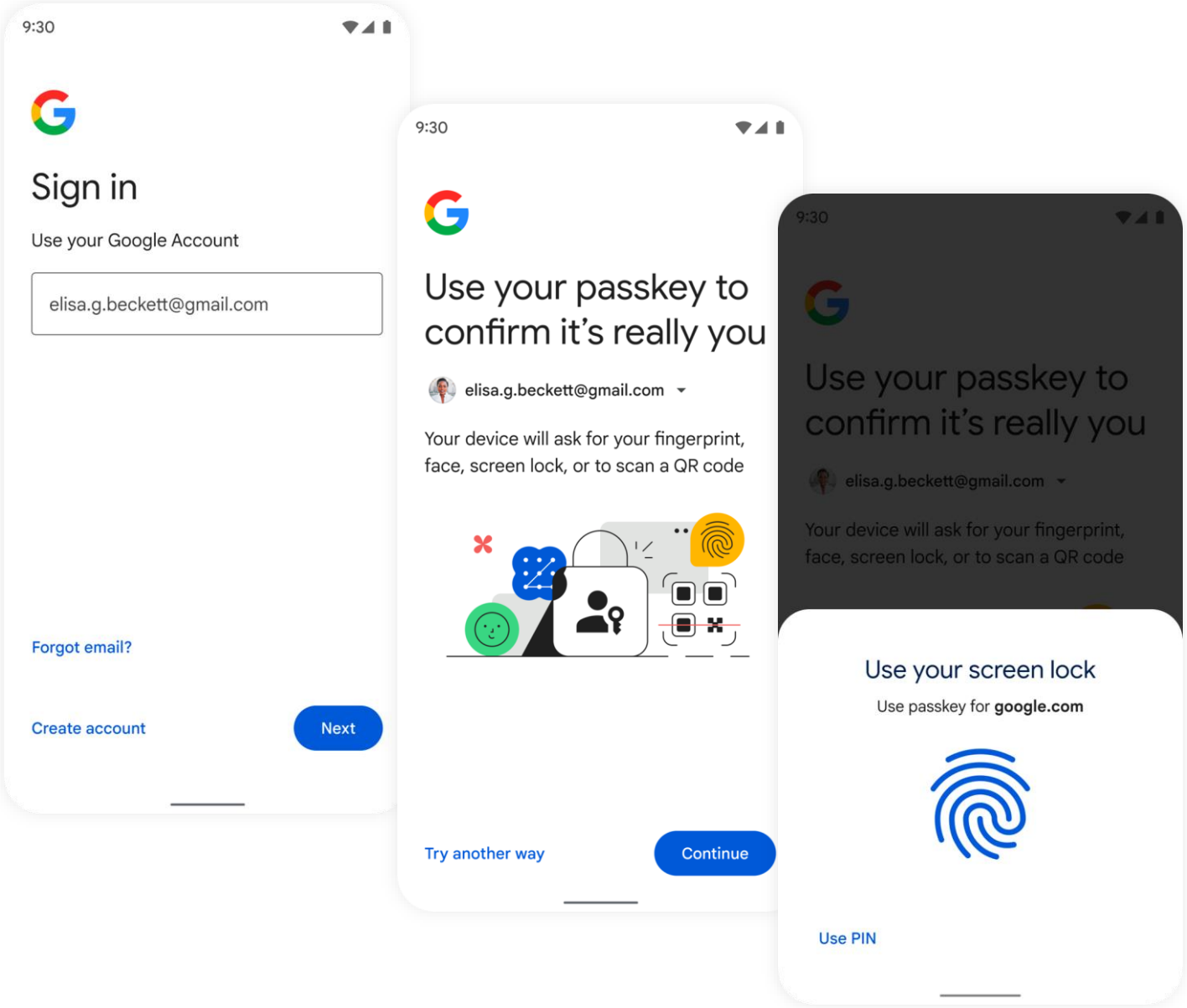
To confirm Elisa's new passkey, the macOS device will prompt Elisa for a biometric verification



Google will create the passkey for Elisa, and she'll be signed in to her Google Account

Signing in with a passkey

We want the passkey authentication experience to be *almost* effortless while ensuring maximum security

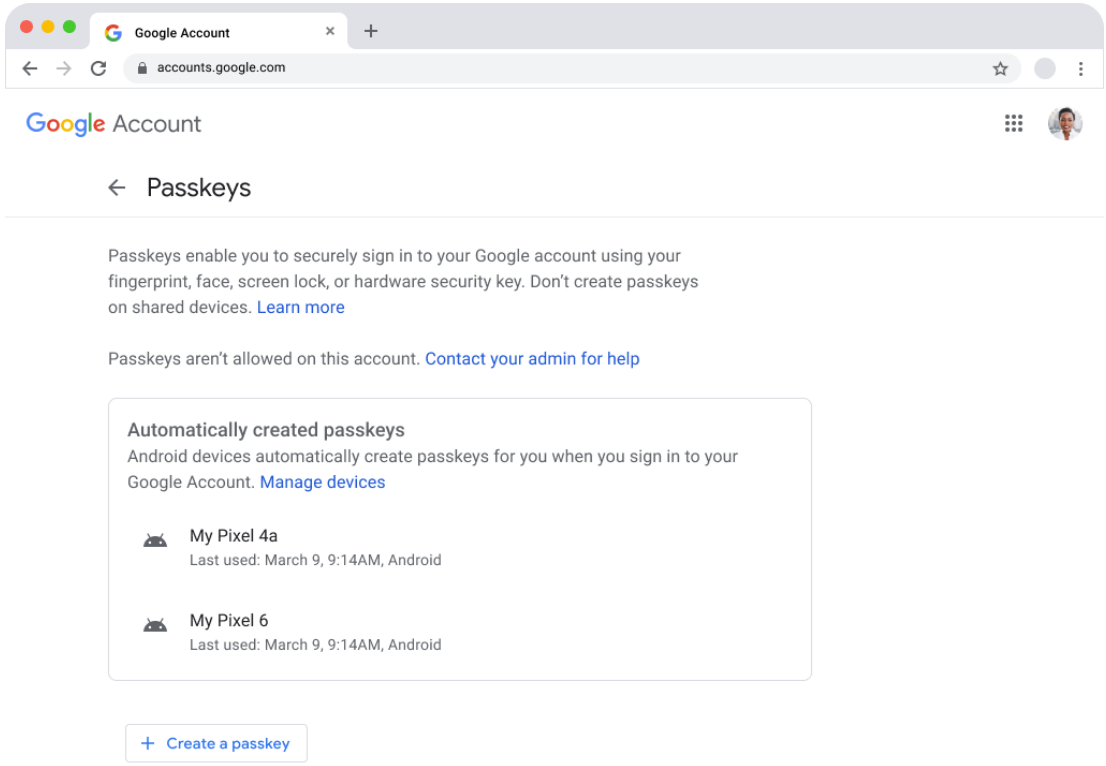


identiverse

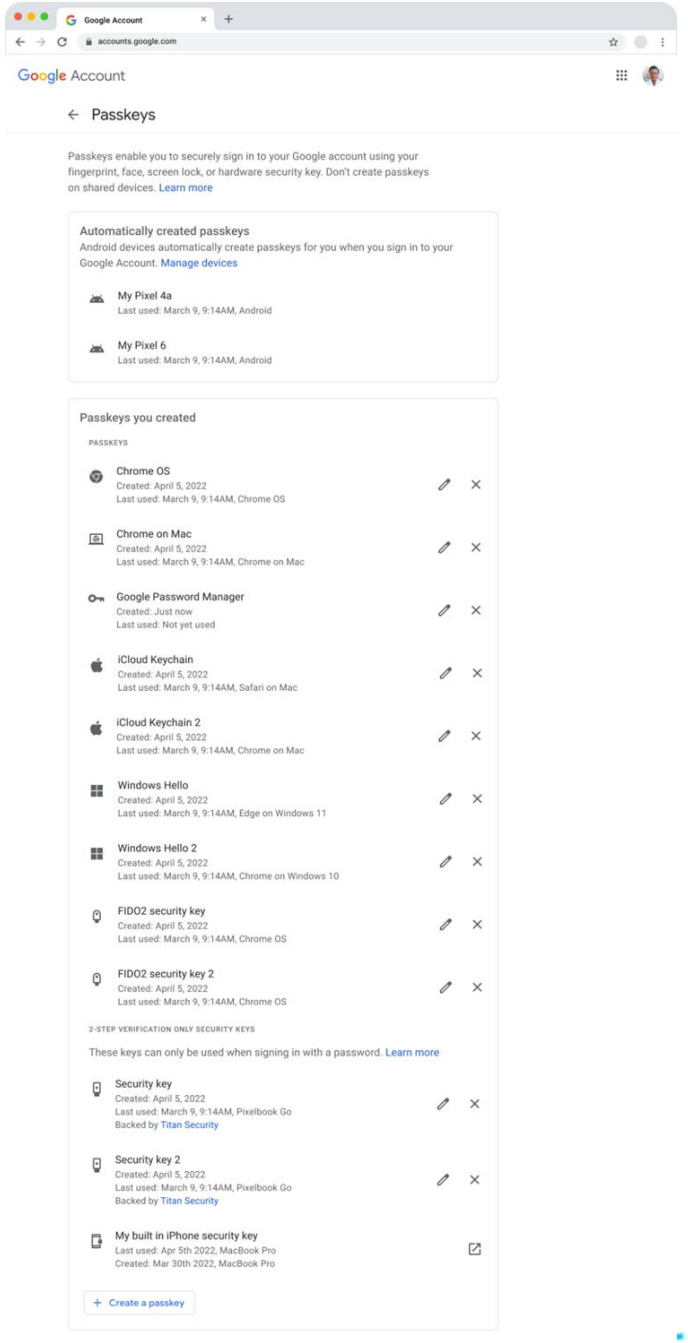
#identiverse

Managing your passkeys

When users go to g.co/passkeys



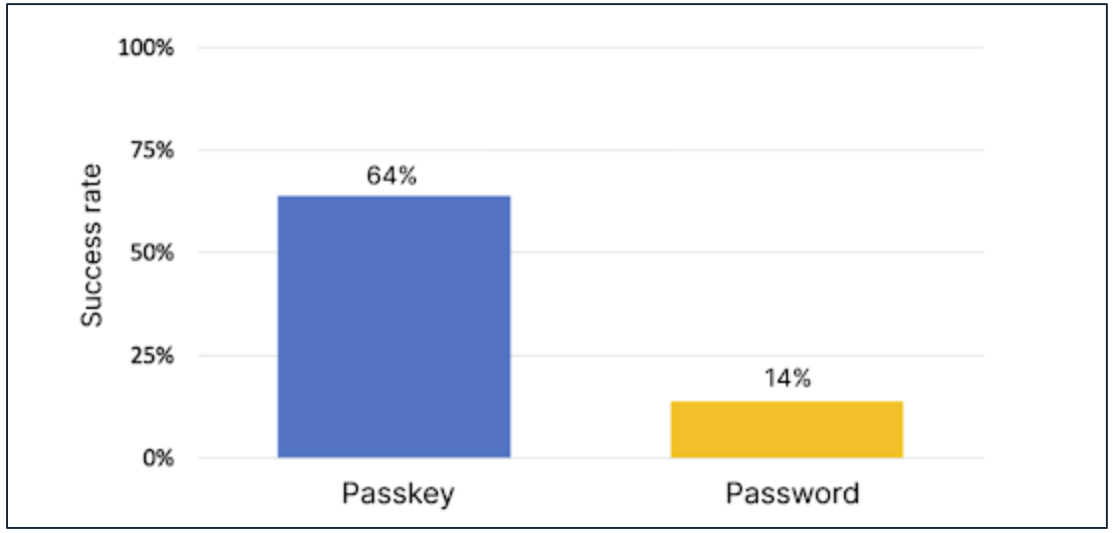
But it could also look like this 😀

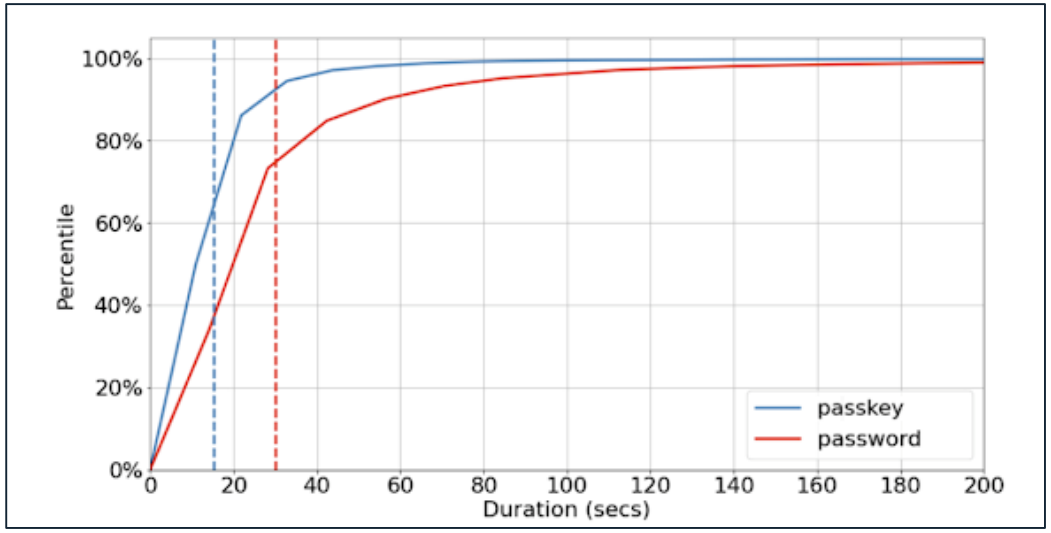


identiverse

#identiverse

So, does this stuff work?





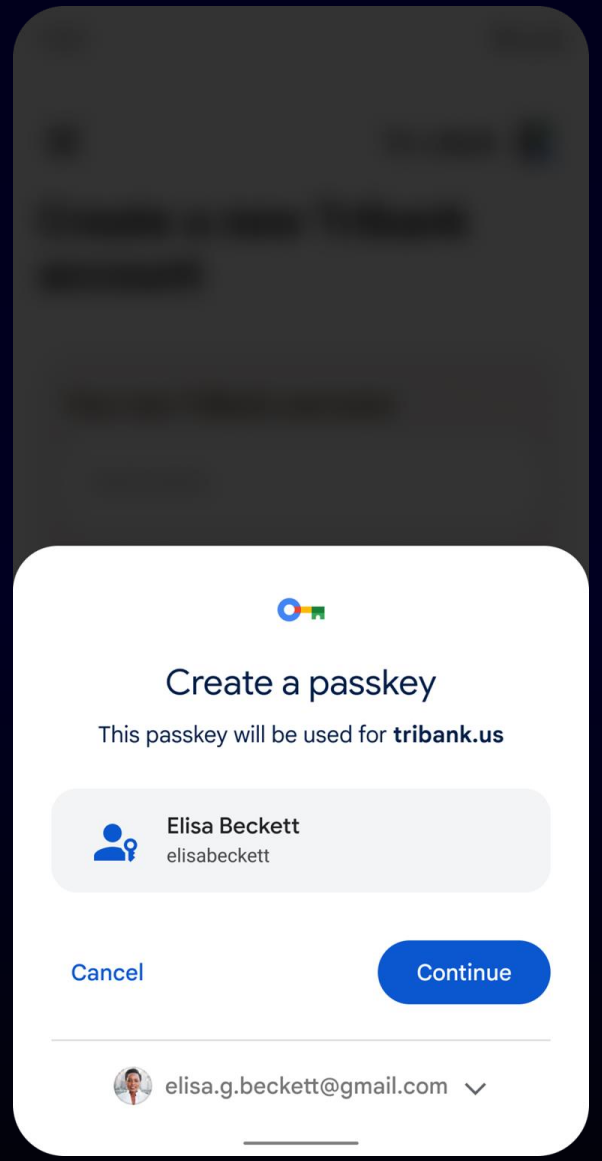
Source: https://security.googleblog.com/2023/05/making-authentication-faster-than-ever.html

I’m convinced. How do I get started?

Create a passkey

```
const publicKeyCredentialCreationOptions = {
  challenge: *****,
  rp: {
    name: "Tribank",
    id: "tribank.us",
  },
  user: {
    id: *****,
    name: "elisabeckett",
    displayName: "Elisa Beckett",
  },
  pubKeyCredParams: [{alg: -7, type: "public-key"},{alg: -257, type: "public-key"}],
  authenticatorSelection: {
    authenticatorAttachment: "platform",
    requireResidentKey: true,
  },
  timeout: 30000
};

const credential = await navigator.credentials.create({
  publicKey: publicKeyCredentialCreationOptions
});
```

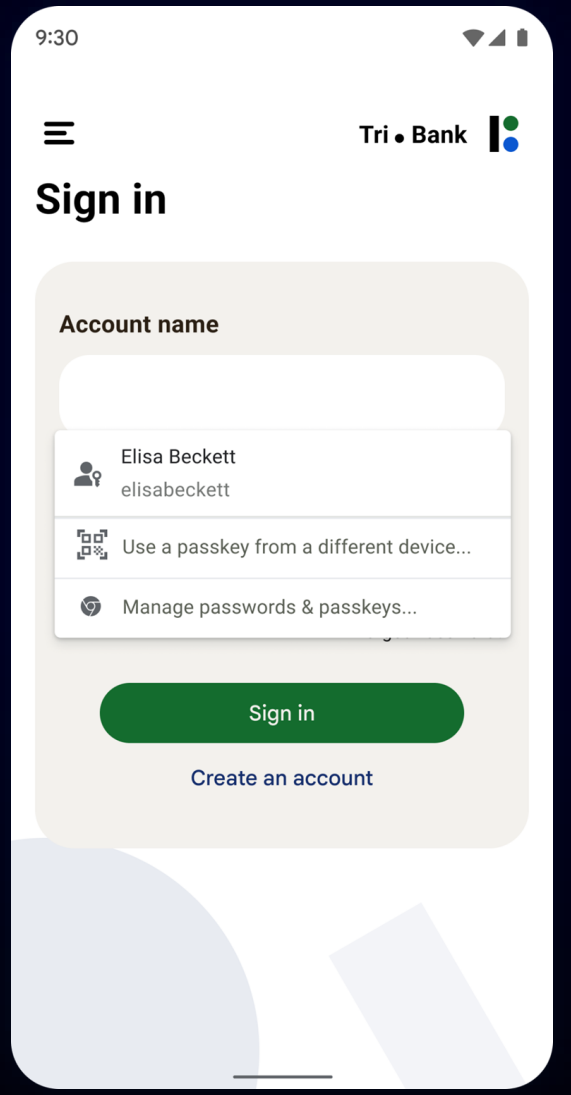


Use a passkey

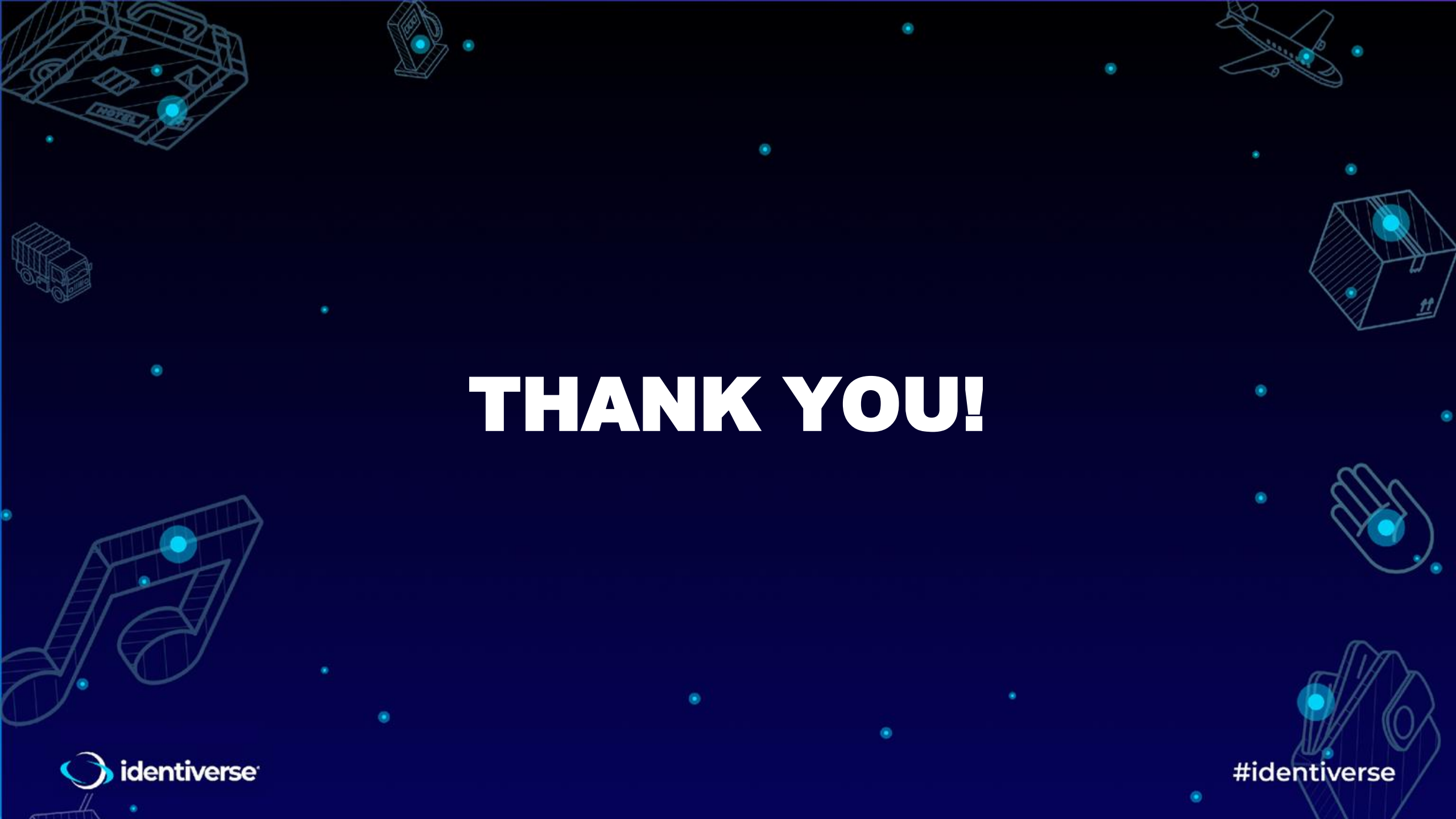
```
// Availability of `window.PublicKeyCredential` means WebAuthn is usable.
if (window.PublicKeyCredential &&
    PublicKeyCredential.isConditionalMediationAvailable) {
  // Check if conditional mediation is available.
  const isCMA = await
PublicKeyCredential.isConditionalMediationAvailable();
  if (isCMA) {
    // Call WebAuthn authentication
  }
}

const publicKeyCredentialRequestOptions = {
  // Server generated challenge
  challenge: ****,
  // The same RP ID as used during registration
  rpId: tribank.us',
};

const credential = await navigator.credentials.get({
  publicKey: publicKeyCredentialCreationOptions,
  signal: abortController.signal,
  // Specify 'conditional' to activate conditional UI
  mediation: 'conditional'
});
```



Please visit g.co/passkey to try this out


THANK YOU!