

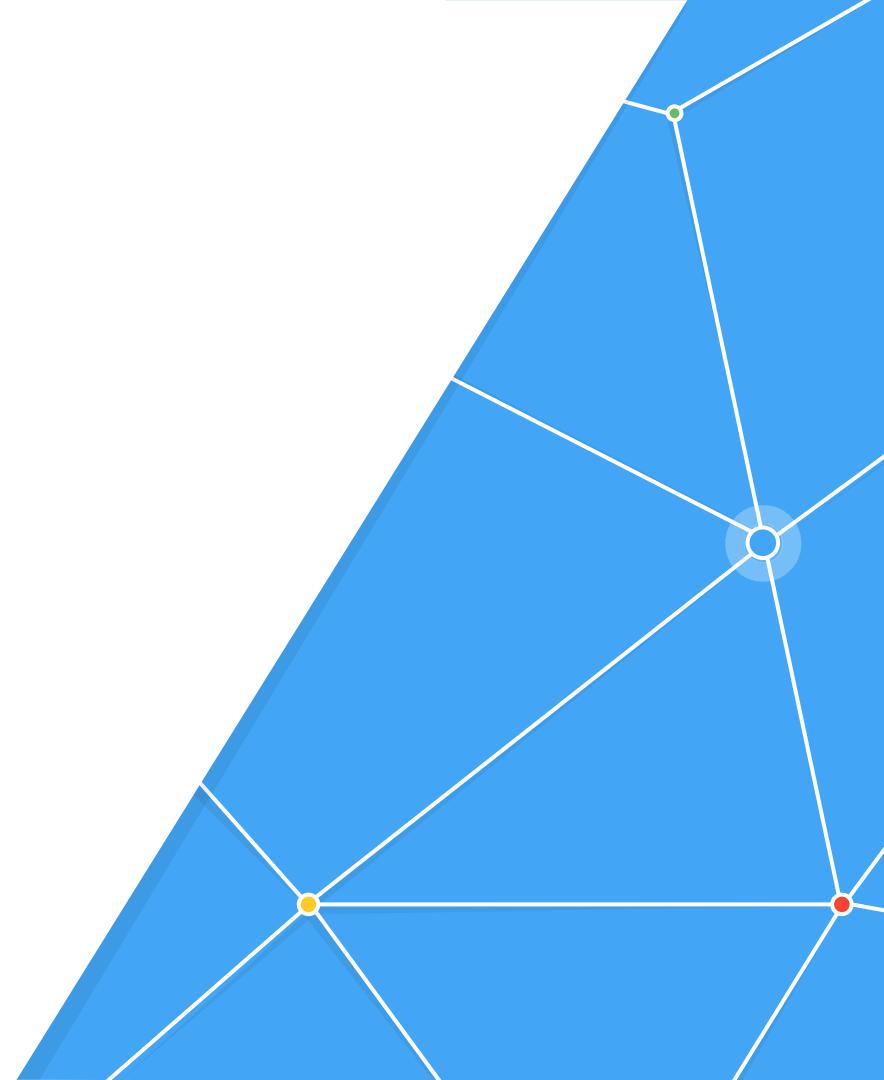


WebAuthn 101

Demystifying WebAuthn

Christiaan Brand

Blackhat 2019



Agenda

01

Passwords aren't
enough

02

MFA - a spectrum of
assurance

03

Enter WebAuthn

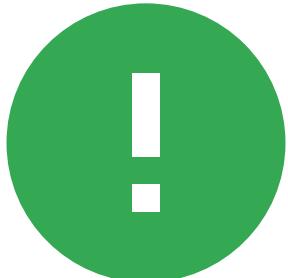
**Passwords
aren't enough**





4.3B+

Credentials leaked
in dumps



17%

Minimum password
reuse rate



110M

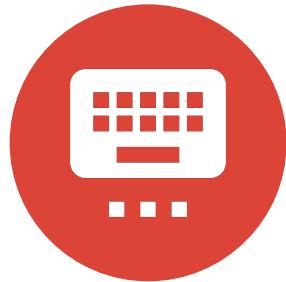
Accounts proactively
re-secured

99.9%

Sources of stolen passwords



Phishing



Keyloggers



Data breach



Stolen credential origin



Password reuse is the largest source

Password breach is the main purveyor of stolen credential with hundred of millions new credential every year



Phishing is the most dangerous source

Phished victims are at the highest risk to get their account compromised



The black market fuel account compromise

There is a whole shadow ecosystem that makes compromised accounts a commodity

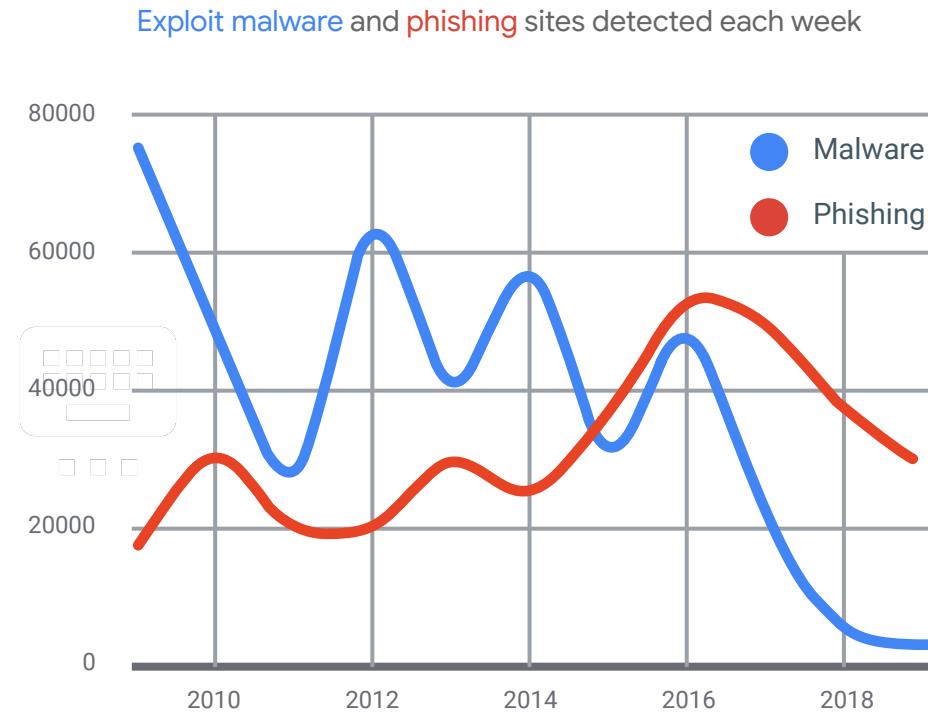
91 % of information security attacks start with phishing

80 % of attacks on businesses include phishing

Source: PhishMe study, cofense.com/enterprise-phishing-susceptibility-report/

Source: UK govt, The Cyber Security Breaches Survey 2019

Phishing overtook
exploit-based
malware in 2016



Source: Safe Browsing (Google Transparency Report)

43%

success rate for
a well designed
phishing page*

76%

of account vulnerabilities
were due to weak or stolen
passwords**

*Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials, 2017

**Verizon 2015 Data Breach Investigations Report

**MFA - a
spectrum of
assurance**



MFA It's a spectrum of assurance

Many different types of MFA exist, all providing different levels of assurance and convenience



SMS / Voice



Backup codes



Authenticator
(TOTP)



Mobile Push



FIDO security keys

Assurance



Titan Security Key



Enhanced account protection

Phishing-resistant 2nd factor of authentication that verifies user's identity and sign-in URL



Trusted hardware

Includes a secure element with firmware written by Google to verify the key's integrity



Open ecosystem

Works with popular browsers and a growing ecosystem of services that support FIDO



Now, your Android phone is also a security key



Enhanced account protection

Strongest 2FA protection against phishing



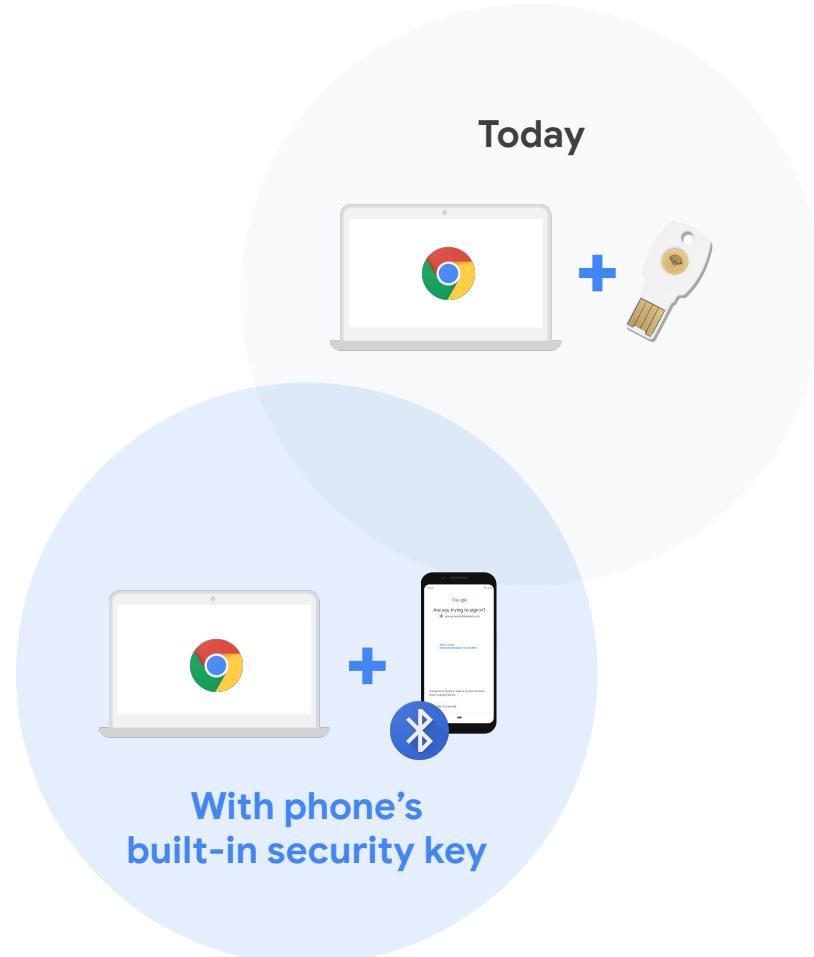
Easy to use

Simple, one-time enrollment process, no app required

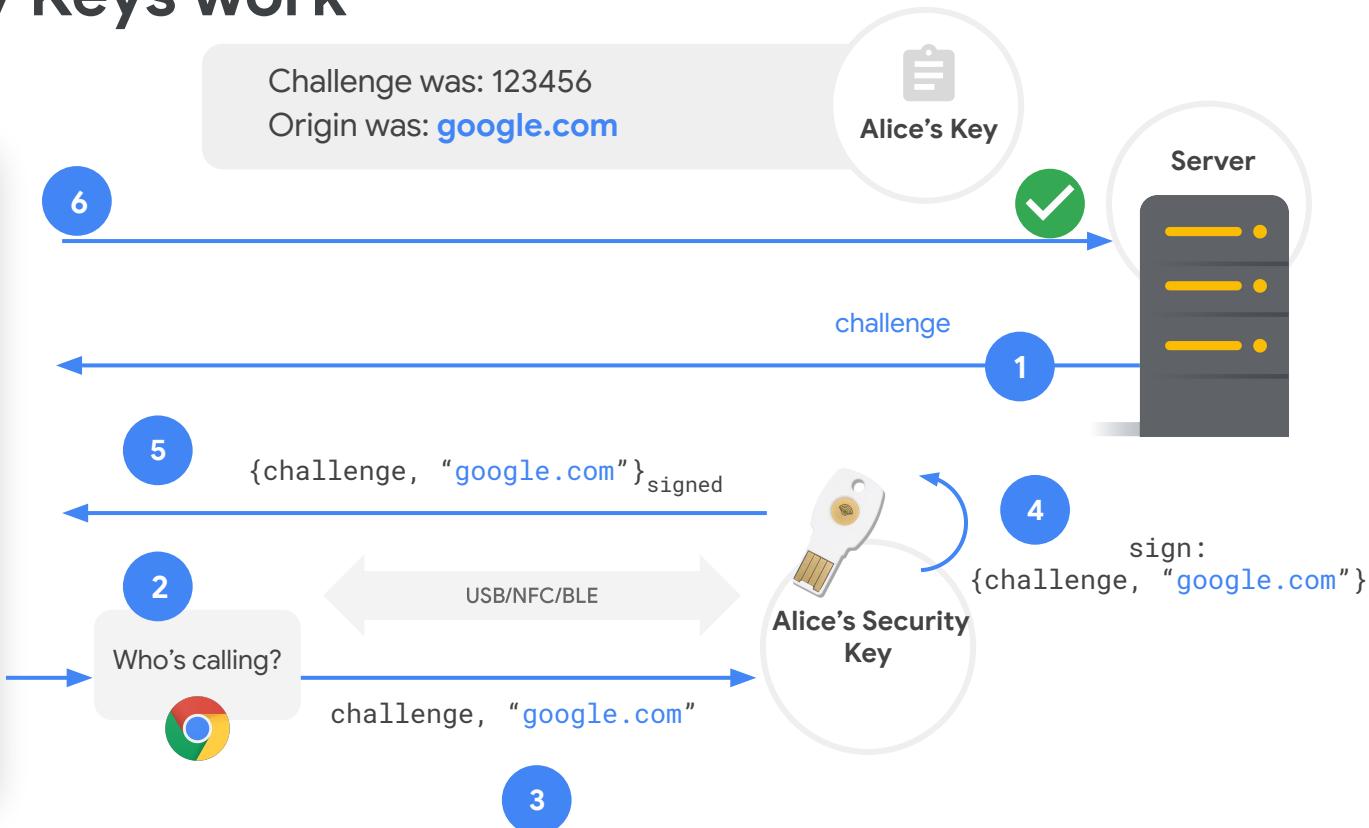
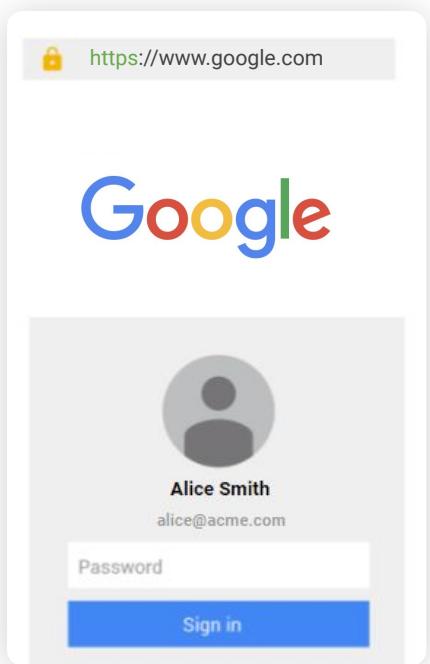


Convenient for users

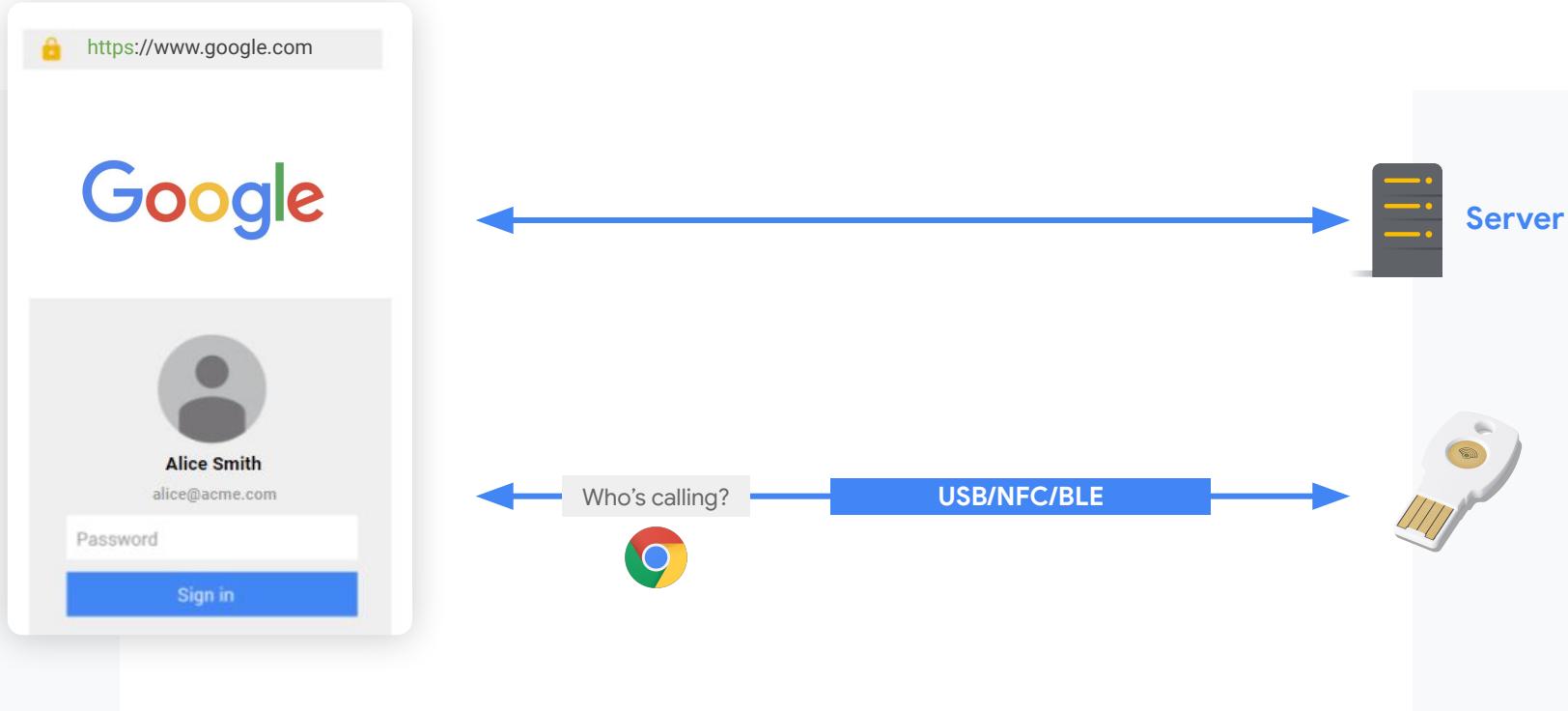
Use the phone which is already in your pocket



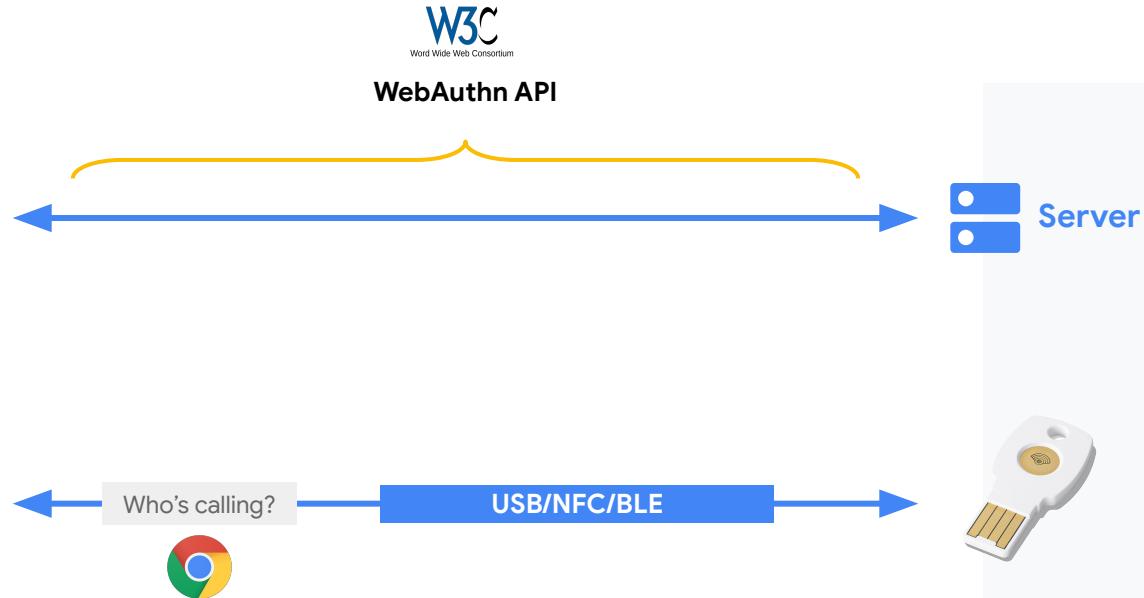
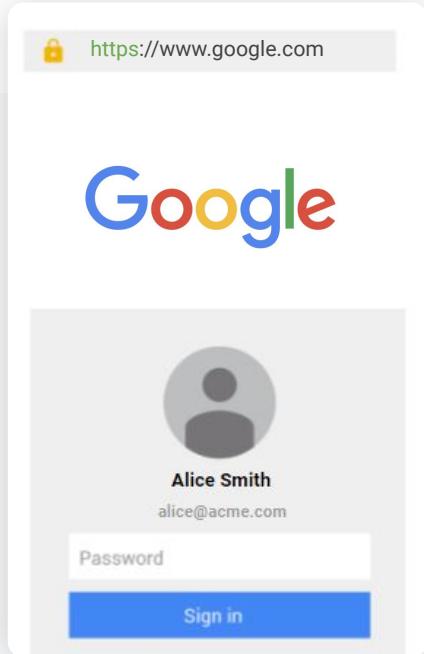
How Security Keys work



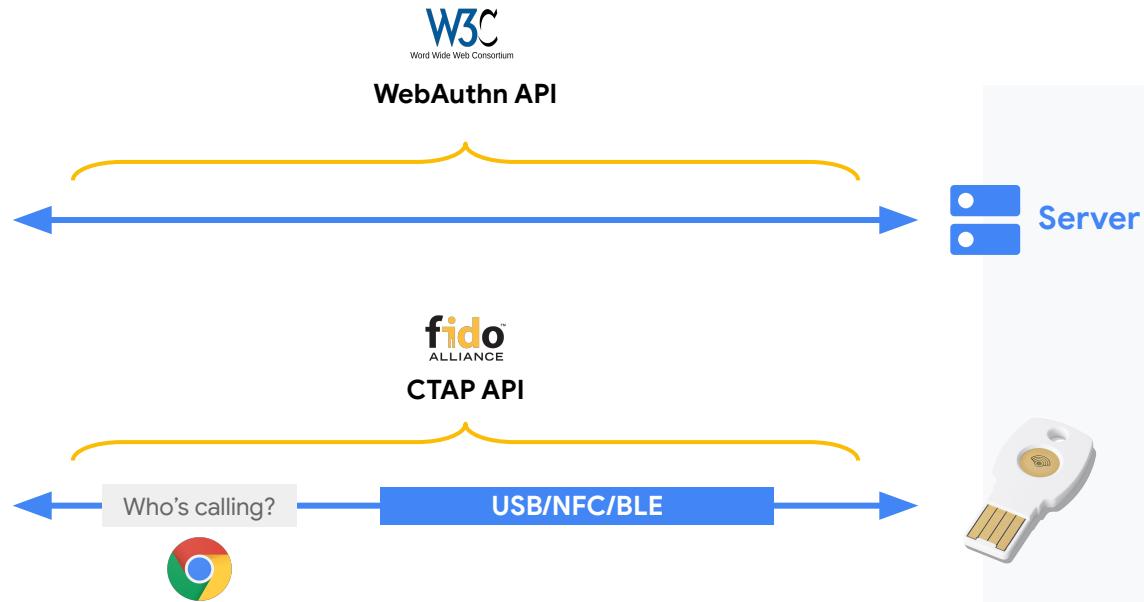
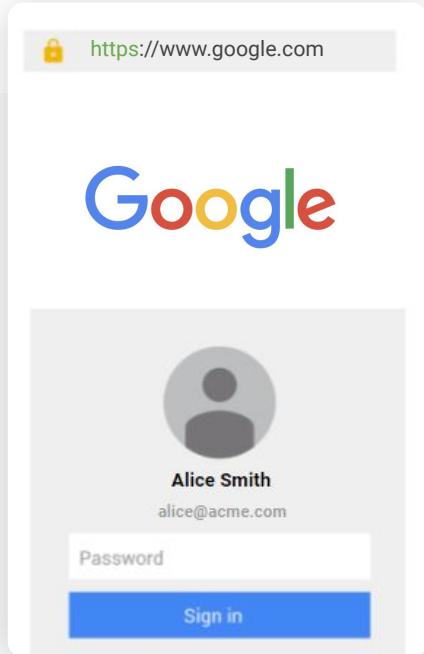
Created with open standards



Created with open standards



Created with open standards



Enter WebAuthn



Introducing WebAuthn

A W3C specification* (Web API)
that allows websites to interact
with authenticators

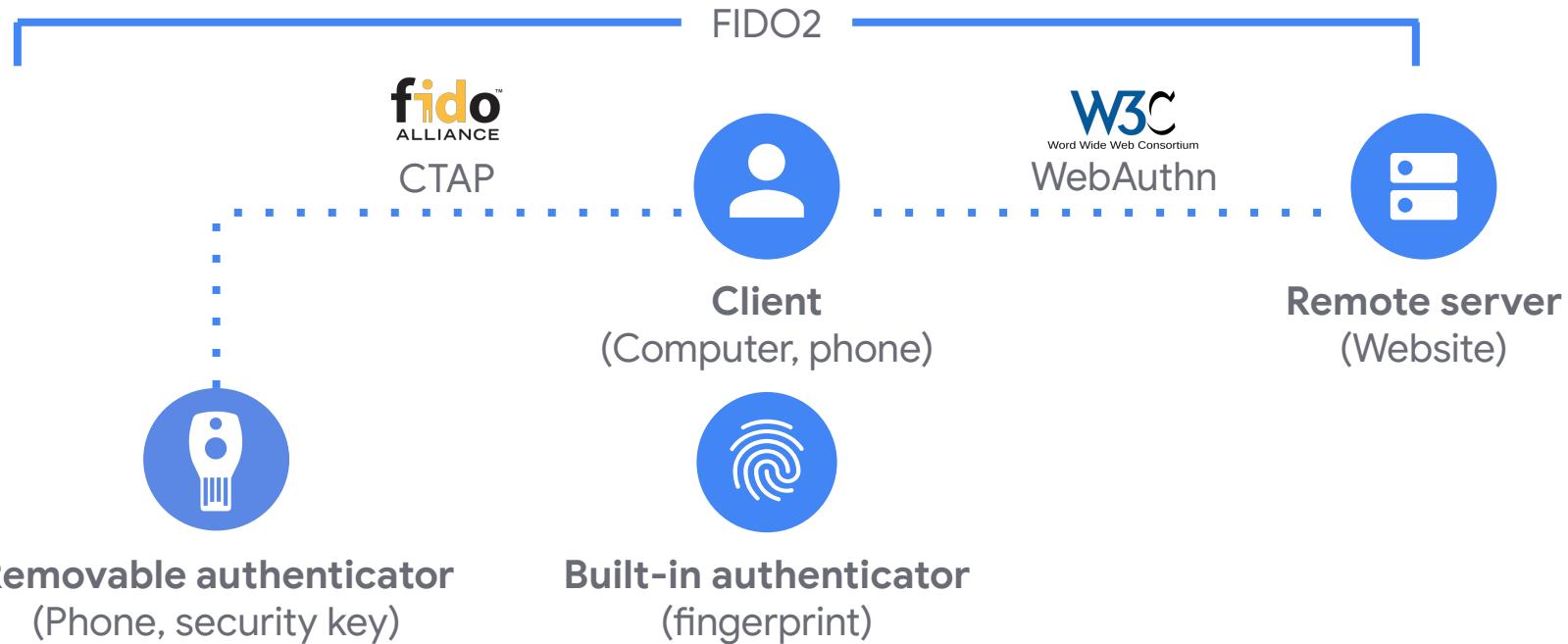


+

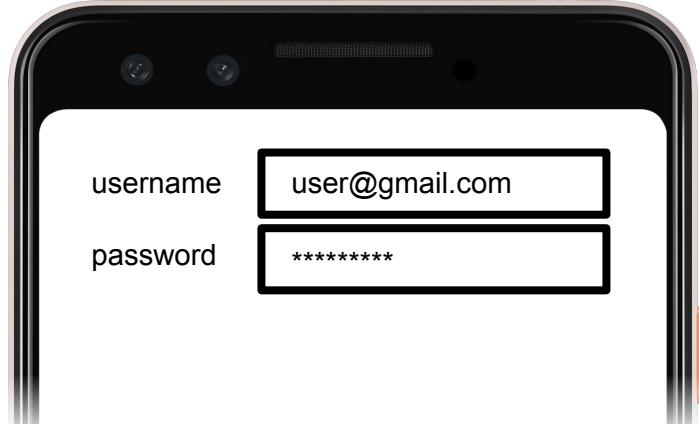


* <https://github.com/w3c/webauthn>

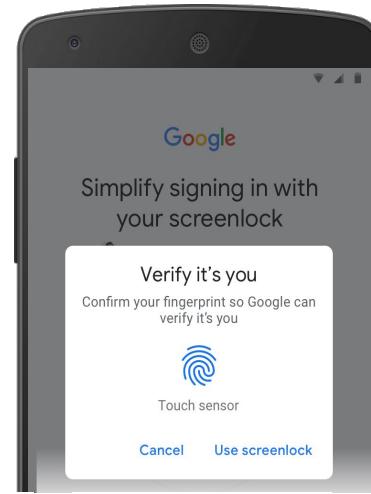
What is WebAuthn? How does it relate to FIDO2?



WebAuthn: two use cases



1. “Bootstrapping” - security key as a 2nd factor



2. “Re-authentication” - biometrics as a way to simplify verifying a returning user

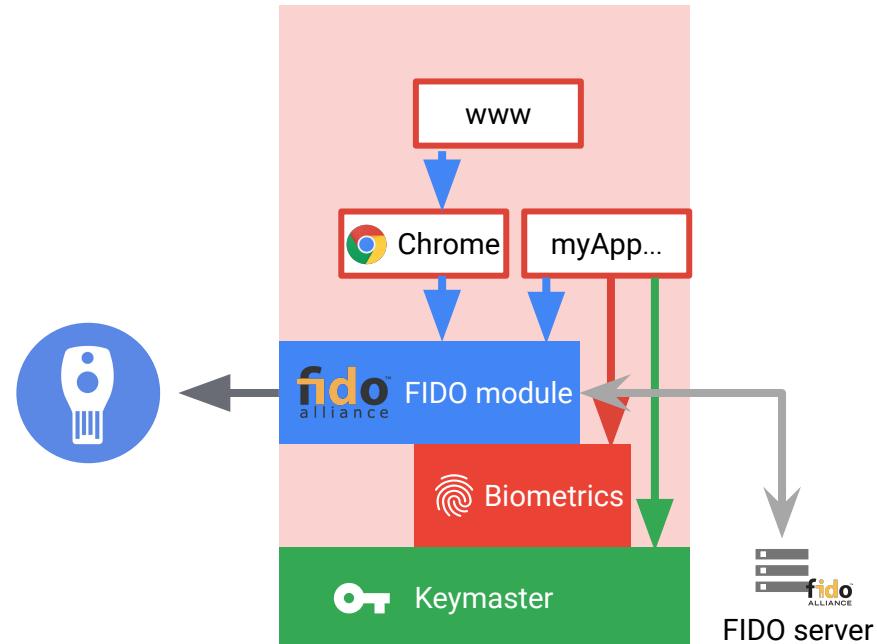
Implemented on Android

Green: Your app can directly talk to the key store to store and use cryptographic keys

Red: Your app can directly talk to the biometric APIs

OR

Blue: Your app and website can talk to the FIDO/WebAuthn APIs that abstracts the keystore and biometric APIs





Meet Elisa

Elisa wants to sign in to her bank

She starts on her mobile browser
and enrolls in fingerprint after
sign-in



Elisa opens launches her mobile browser, Chrome, and goes to Tri-Bank

1. Registering built-in authenticator for re-auth (mobile web)

The screenshot shows a mobile browser displaying the Tri-Bank website at https://www.tribank.com. The page features the bank's logo (a triangle divided into three sections with 'TRI' on top and 'BANK' below) and the text 'Serving customers since 1765'. A prominent orange button invites users to 'Open a new account'. Below this, a menu bar includes 'Banking', 'Lending', 'Wealth Management', and 'Investor relations'. At the bottom, there are navigation icons for back, forward, and search.



She signs in with her
username and password

1. Registering built-in authenticator for re-auth (mobile web)

The image displays two side-by-side screenshots of a mobile web browser on a device. Both screenshots show the same login interface for 'www.tribank.com'.

Screenshot 1 (Left): Welcome screen

- The top bar shows the URL <https://www.tribank.com>.
- The page features the Tri-Bank logo (a stylized triangle composed of orange and grey segments) and the text "Welcome back!".
- A large orange input field is labeled "Username or email".
- An orange "Next" button is located below the input field.
- A "Forgot ID?" link is visible near the bottom of the input field.
- The background shows a blurred city skyline silhouette.

Screenshot 2 (Right): Password entry screen

- The top bar shows the URL <https://www.tribank.com>.
- The page features the Tri-Bank logo and the text "Enter password".
- A large orange input field is labeled "Enter your password" with placeholder text ".....".
- An orange "Sign In" button is located below the input field.
- A "Forgot your password?" link is visible near the bottom of the input field.
- The bottom half of the screen shows a virtual keyboard with letters, numbers, and symbols.



Tri-Bank shows a promo asking Elisa if she wants to opt in to fingerprint to sign in

She opts in and continues to her account

1. Registering built-in authenticator for re-auth (mobile web)

The image displays two side-by-side screenshots of a mobile web browser window, both showing the URL <https://www.tribank.com>.

Screenshot 1 (Left): This screenshot shows a promotional message from Tri-Bank. It features the bank's logo (a triangle divided into three sections with the words "TRI" and "BANK") inside a smartphone icon. Below the phone is a circular button containing a blue fingerprint icon. The text "Mobile Banking is now only one touch away" is displayed in bold black font, followed by the subtext "Fingerprint allows you to sign in quickly and securely." At the bottom of the screen are navigation icons for back, forward, and home.

Screenshot 2 (Right): This screenshot shows the user's account dashboard after opting in. The top bar says "Hi Elisa!" with a small profile picture. The main area shows account details: "E. Beckett" and "NL39 BANK 0300 0652 64". Below this, it shows a "Current Balance" of "\$ 3,589.94". Further down, there is a section for "Beckett Fabrics" with an IBAN number: "IBAN TR93 0006 4000 0011 2341 2345 67". At the bottom are buttons for "Sent money" and "Request money".

What happened behind the scenes?

Silently determined whether a platform authenticator was available:

```
PublicKeyCredential.isUserVerifyingPlatformAuthenticatorAvailable().then(response => {
  if (response === true) {
    //User verifying platform authenticator is available!
  } else {
    //User verifying platform authenticator is NOT available.
}
```

What happened behind the scenes?

Created the credential on the platform authenticator

```
navigator.credentials.create({  
  "publicKey": PublicKeyCredentialCreationOptions  
});
```

What happened behind the scenes?

With values for PublicKeyCredentialCreationOptions

- excludeCredentials = [// add any already registered ids]
- authenticatorSelection.authenticatorAttachment = 'platform'
// other options: 'cross-platform'
- authenticatorSelection.userVerification = 'required'
// other options: 'discouraged' or 'preferred'

Elisa comes back to Tri-Bank
in another session



The next time Elisa opens Tri-Bank on mobile browser, she gets a fingerprint dialog

The image consists of two side-by-side screenshots of a mobile web browser displaying the Tri-Bank website (<https://www.tribank.com>).
The left screenshot shows the main landing page. At the top is the Tri-Bank logo (a triangle divided into three sections with 'TRI' in red and 'BANK' in black) and a 'Sign In' button. Below the logo is the text 'Serving customers since 1765'. A large orange button in the center says 'Open a new account'. To the left of the button is a section titled 'Banking that puts you first' with the subtext 'Open an online account with no monthly fees'. On the far left is a 'Menu' icon.
The right screenshot shows a modal dialog box titled 'Verify your identity' with the subtext 'Confirm your fingerprint so TriBank.com can verify it's you'. It features a blue fingerprint icon and two buttons: 'Touch sensor' and 'Use screenlock'. At the bottom of the dialog is a 'Cancel' button.

Since the user already signed in on this device, the credential ID is encoded in the cookie and the RP requests the “internal” transport only (since they don’t want the user to see prompts about external authenticators).



Using only her fingerprint,
she's able to sign in
without using her
username + password
on mobile web

The image displays two side-by-side screenshots of a mobile web browser interface. Both screenshots feature the logo of 'TRI BANK' at the top.

Screenshot 1 (Left): This is the login screen. It shows a large 'Welcome back!' message above a 'Username or email' input field. Below the input field is a 'Forgot ID?' link. A large orange 'Next' button is centered at the bottom. The background of this screen shows a blurred city skyline.

Screenshot 2 (Right): This is the user dashboard. At the top, it greets the user with 'Hi Elisa!' and shows a small profile picture. Below the greeting, the user's name 'E. Beckett' is displayed, along with their account number 'NL39 BANK 0300 0652 64'. To the right of the account number is the current balance '\$ 3,589.94'. Further down, there is a section for 'Beckett Fabrics' with the IBAN 'IBAN TR93 0006 4000 0011 2341 2345 67'. At the bottom of the dashboard are two buttons: 'Sent money' (with a right-pointing arrow icon) and 'Request money' (with a left-pointing arrow icon).

What happened behind the scenes?

Created a signature using the platform authenticator

```
navigator.credentials.get({  
  "publicKey": PublicKeyCredentialRequestOptions  
});
```

With values for PublicKeyCredentialRequestOptions

- allowCredentials = [// credential associated with session]
- userVerification = true

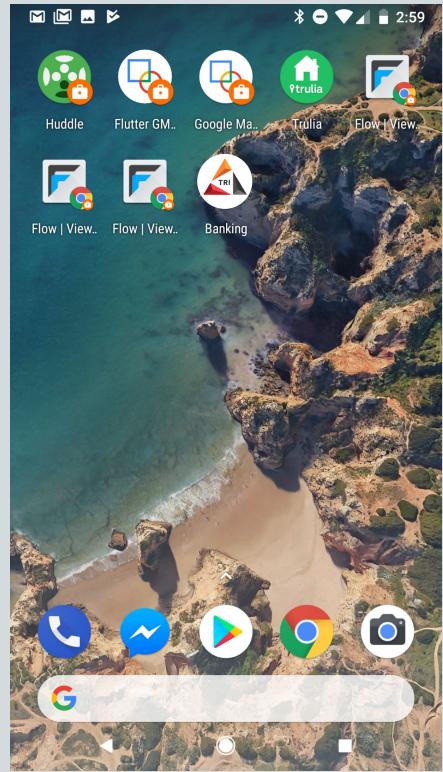
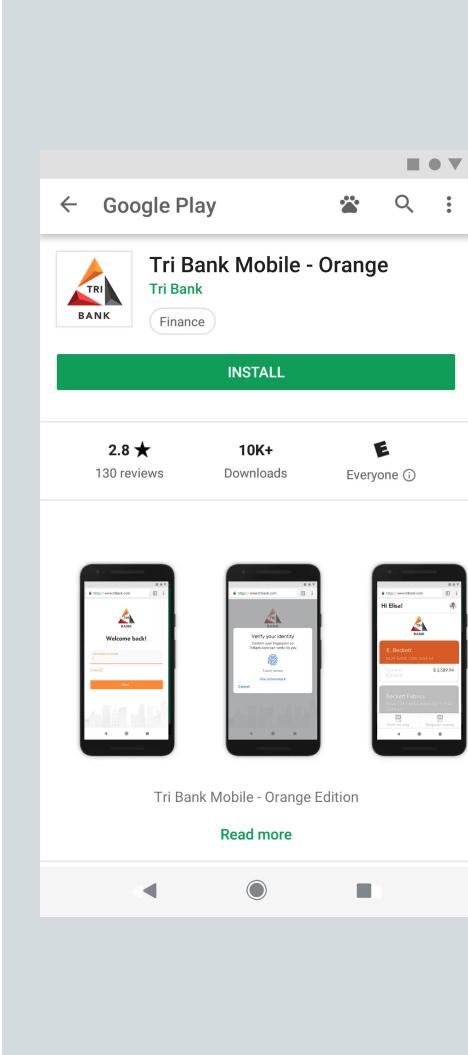


Elisa downloads Tri-Bank
from the Play Store

She launches the app for the first time
to sign in to check her funds



She installs Tri-Bank
from Google Play Store
and opens the app





Elisa chooses
“Sign In” and enters
her username

The image displays two side-by-side screenshots of a mobile application interface. Both screenshots feature a header with three small black dots at the top right corner.

Screenshot 1 (Left): This screenshot shows the main landing page of the app. At the top center is the bank's logo, which consists of a stylized triangle divided into three sections (orange, red, and grey/black) with the word "TRI" above "BANK". Below the logo, the text "Serving customers since 1765" is displayed. A large orange rectangular button with the text "Sign In" is centered below this. Below the button, there are two sections: "Find locations" with a city skyline icon and "Support" with a question mark icon. At the bottom of the screen, there is a navigation bar with three items: "Account" (selected), "Transfers", and "History".

Screenshot 2 (Right): This screenshot shows the sign-in screen. At the top center is the same bank logo. Below it, the text "Welcome back!" is displayed in a bold, black font. Below this, there is a light grey input field with the placeholder "Username or email" and a small orange cursor icon. Underneath the input field is a smaller link "Forgot ID?". At the bottom of the screen is a large orange rectangular button with the text "Next". The bottom navigation bar is identical to the one in the first screenshot, showing "Account" (selected), "Transfers", and "History".



Elisa is now asked to authenticate with the fingerprint dialog

The image consists of two side-by-side screenshots of a mobile banking application. The left screenshot shows a modal dialog box in the foreground, prompting the user to 'Verify your identity' by confirming their fingerprint so that TriBank.com can verify it's them. It offers two options: 'Touch sensor' (represented by a blue fingerprint icon) and 'Use screenlock'. A 'Cancel' button is at the bottom. The background is blurred, showing a city skyline. The right screenshot shows the main banking interface. At the top, it greets 'Hi Elisa!' and displays the user's name 'E. Beckett' and account number 'NL39 BANK 0300 0652 64'. Below this, it shows the current balance '\$ 3,589.94'. Further down, it lists a transaction for 'Beckett Fabrics' with IBAN 'IBAN TR93 0006 4000 0011 2341 2345 67' and a balance of '\$ 45.094.24'. At the bottom, there are buttons for 'Sent money' (with a person icon) and 'Request money' (with a banknote icon).

What happened behind the scenes?

Created a signature using the platform authenticator

```
Fido2ApiClient fido2ApiClient = Fido.getFido2ApiClient(this.getApplicationContext());
```

```
Task<Fido2PendingIntent> result = fido2ApiClient.getSignIntent(requestOptions);
```

With values for requestOptions

- o allowCredentials = [// credential associated with session]
- o userVerification = true



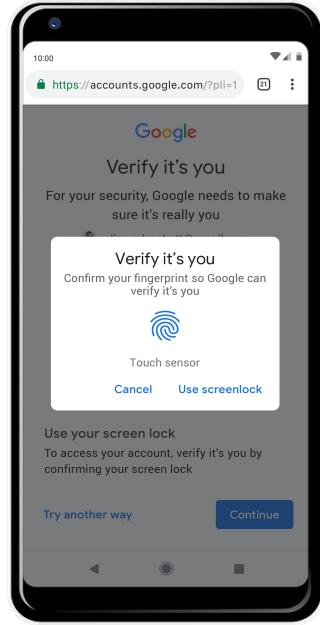


Case study: Yahoo! JAPAN

Reauth using fingerprint reduced
time to sign-in by ...

37.5%

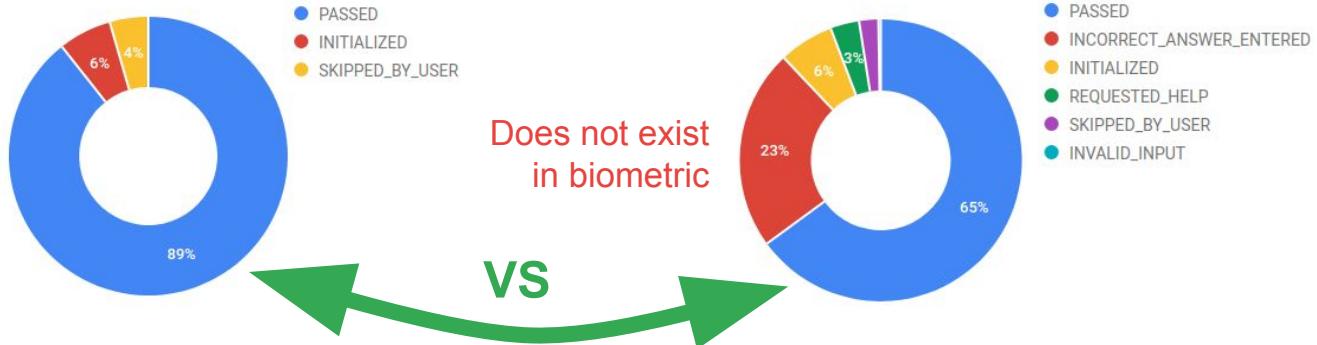
comparing to that of using a password.



Case study: Google

98% of biometric reauth users finish in **38s**

98% of all users enter password in **150s**



Google Internal Data: 2018

Implement WebAuthn today!

- Play with our FIDO server
webauthndemo.appspot.com
- Implement WebAuthn Create and Get methods
codelabs.developers.google.com/codelabs/webauthn-reauth/
- Link your Android app for a seamless login experience
codelabs.developers.google.com/codelabs/fido2-for-android/

Q&A