

TeleTrust-Konferenz

28.06.2022, Berlin

FIDO: Passkey as a Platform-independent Passwordless Sign-in Mechanism

Dirk Balfanz • Google

FIDO Authenticators come in different shapes and sizes

Some are dedicated devices.

Some are built into
general-purpose devices.

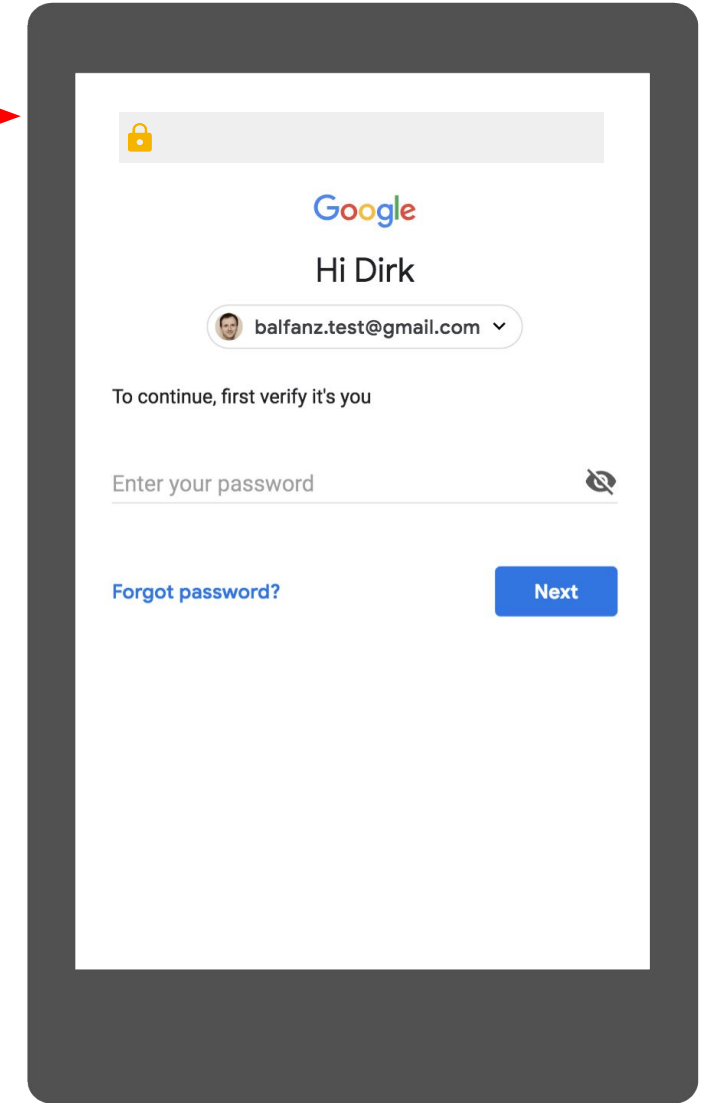
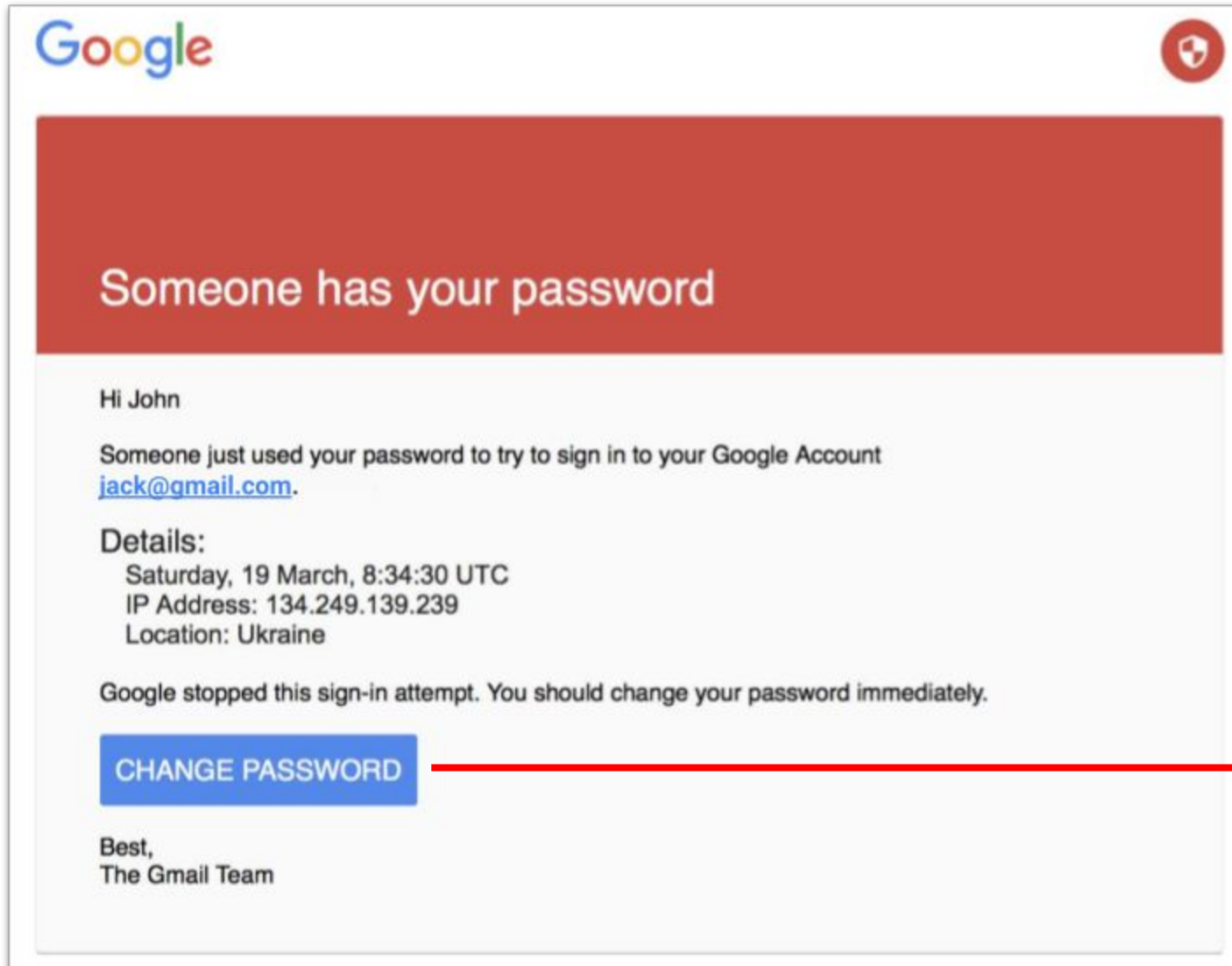


FIDO Authenticators come in different shapes and sizes

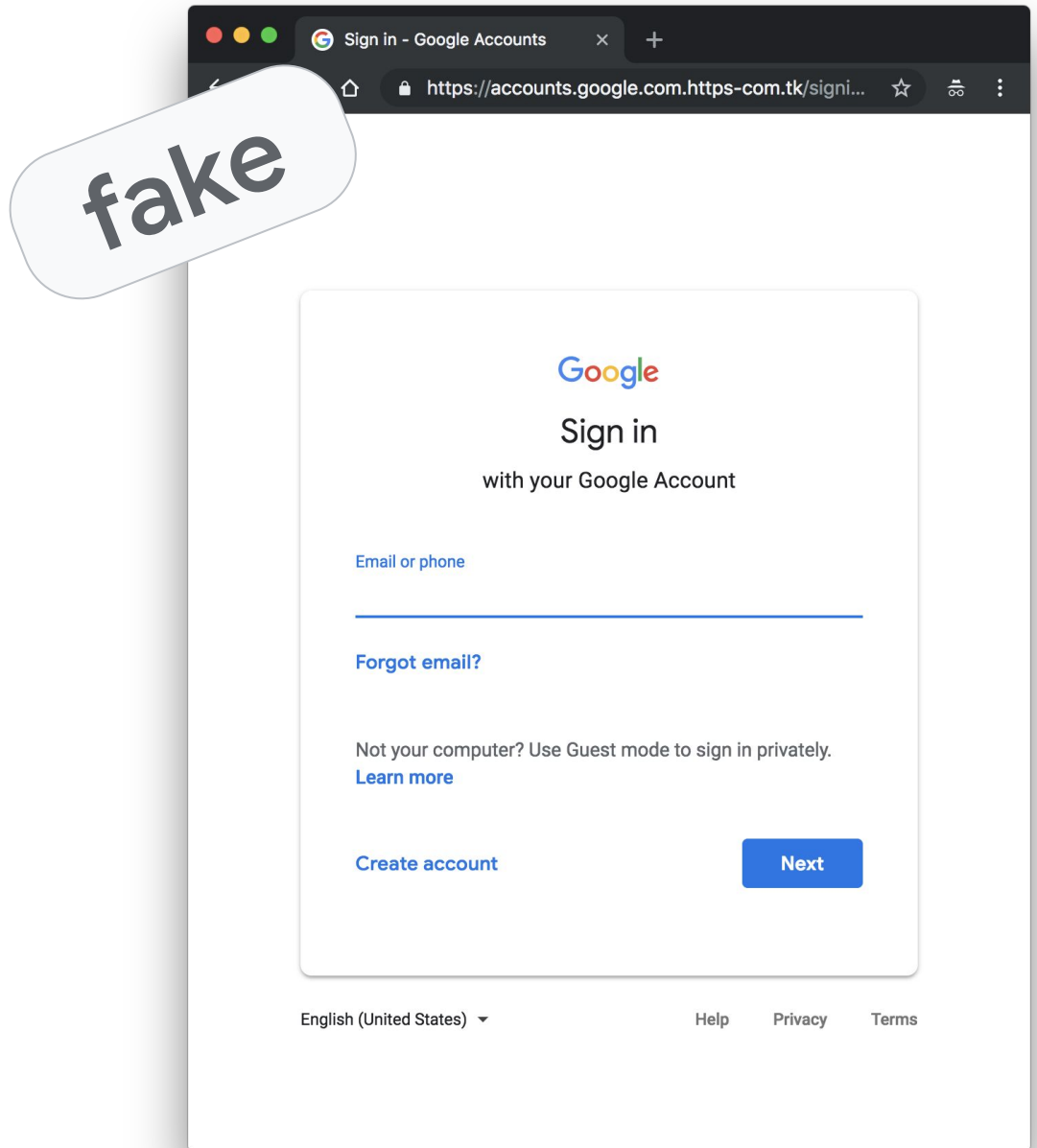
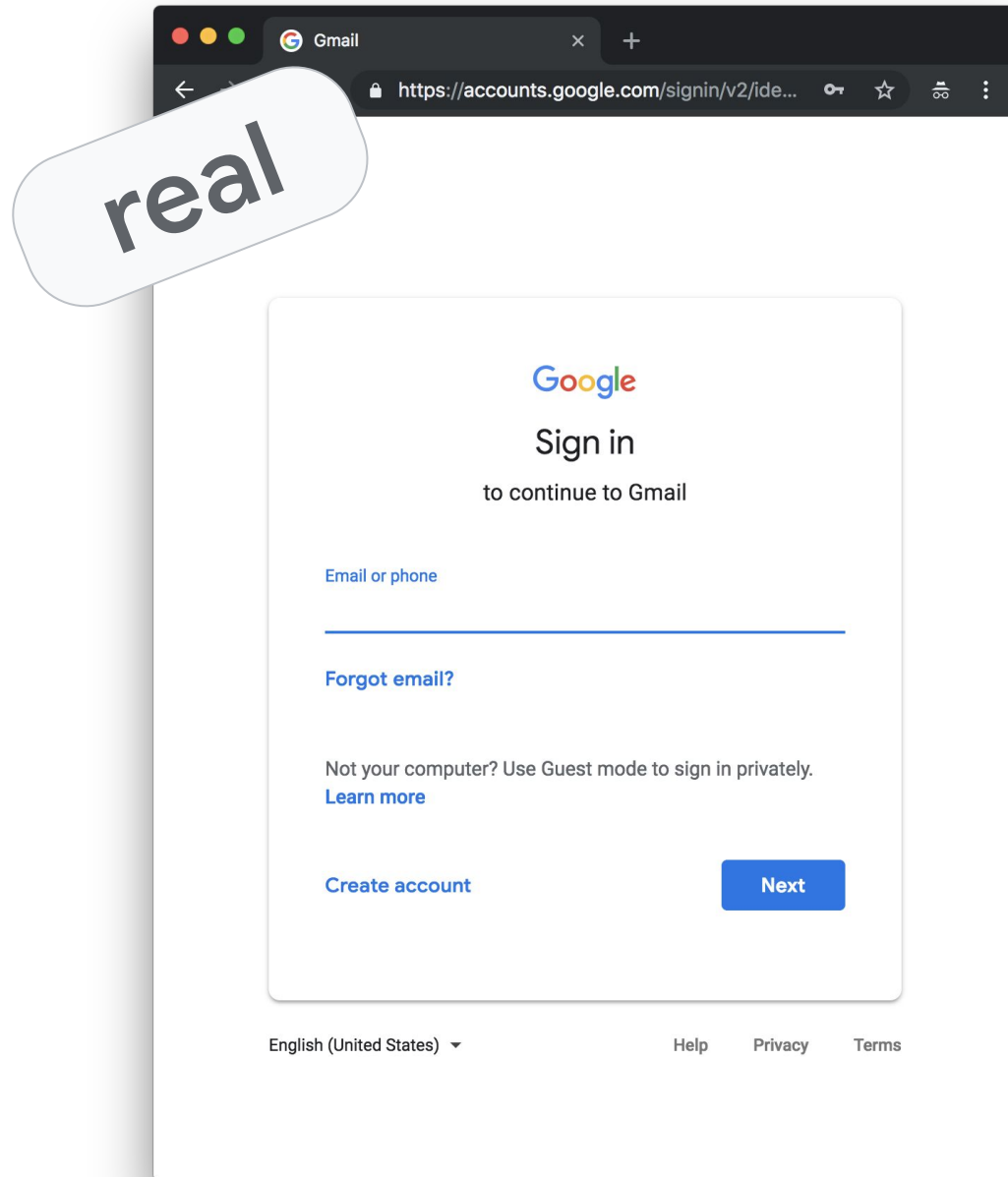
But all implement the
phishing-resistant FIDO standard.



MFA ≠ Phishing-Resistant



MFA ≠ Phishing-Resistant



MFA ≠ Phishing-Resistant

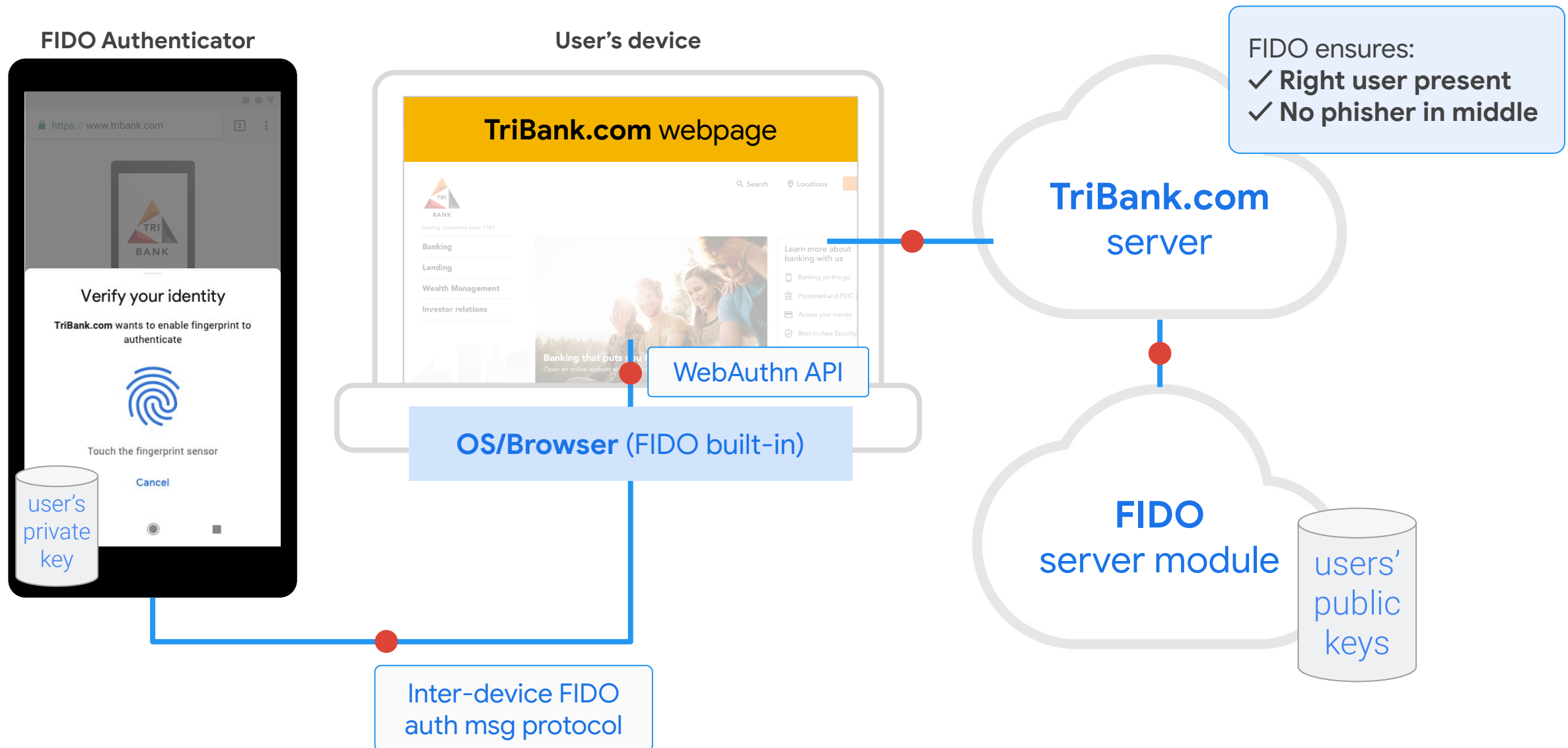
real

This screenshot shows the authentic Google 2-Step Verification interface. The browser's address bar displays the official Google URL: `https://accounts.google.com/signin/v2/cha...`. The page features the Google logo, the title "2-Step Verification", and a message: "This extra step shows it's really you trying to sign in". Below this, a dropdown menu shows the email address "balfanz.test@gmail.com". The verification step is titled "2-Step Verification" and states: "A text message with a 6-digit verification code was just sent to (...)23". A link "Enter the code" is provided. There is a text input field with "G-" and a checkbox labeled "Don't ask again on this computer" which is checked. At the bottom, there are links for "More options" and a blue "Next" button. The footer includes "English (United States)", "Help", "Privacy", and "Terms".

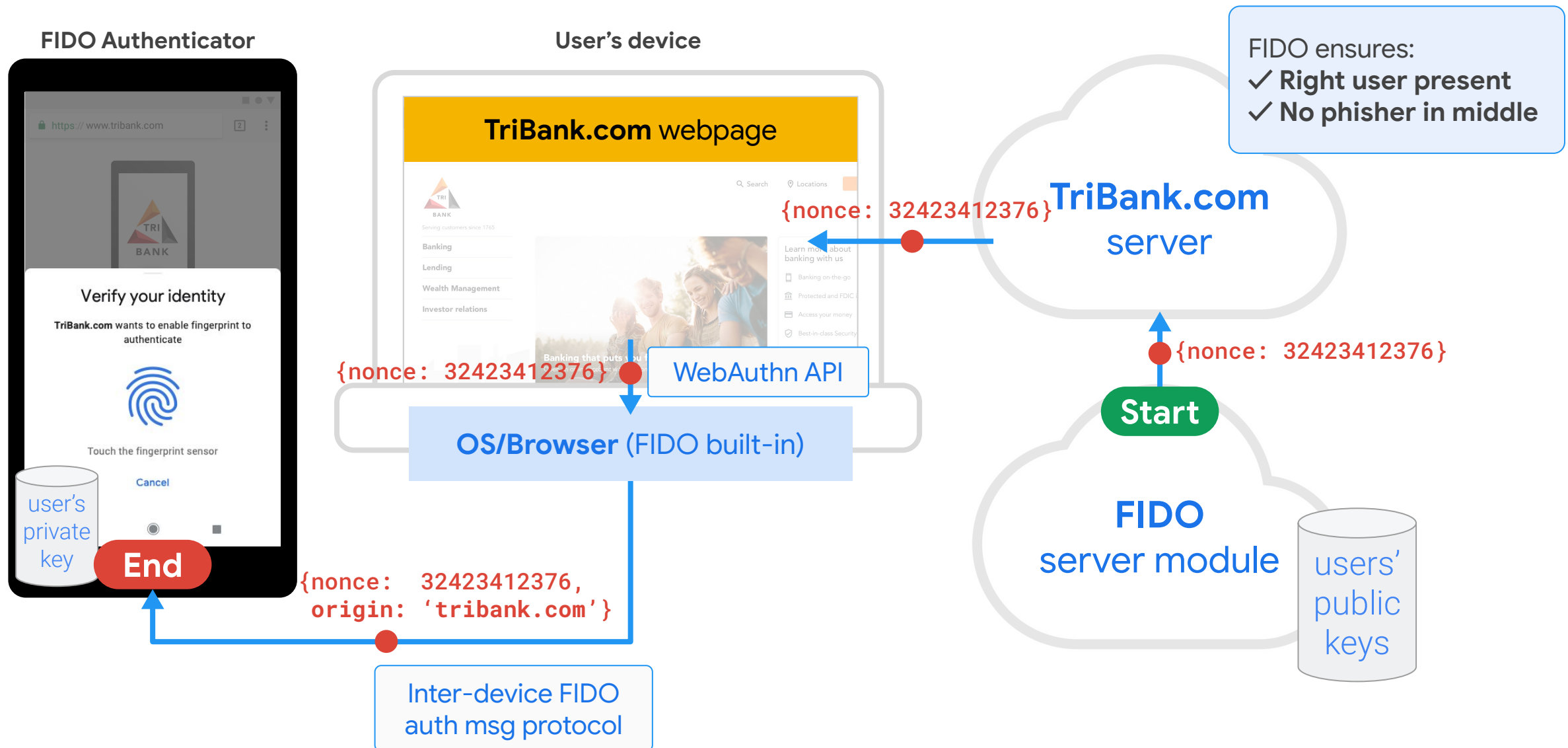
fake

This screenshot shows a phishing page that mimics the Google 2-Step Verification interface. The browser's address bar displays a suspicious URL: `https://accounts.google.com.https-com.tk/signi...`. The page layout is identical to the real one, including the Google logo, "2-Step Verification" title, and the message "This extra step shows it's really you trying to sign in". The email address in the dropdown is "balfanz.test@gmail.com". The verification step is titled "2-Step Verification" and states: "A text message with a 6-digit verification code was just sent to (...)23". A link "Enter the code" is provided. There is a text input field with "G-" and a checked checkbox labeled "Don't ask again on this computer". At the bottom, there are links for "More options" and a blue "Next" button. The footer includes "English (United States)", "Help", "Privacy", and "Terms".

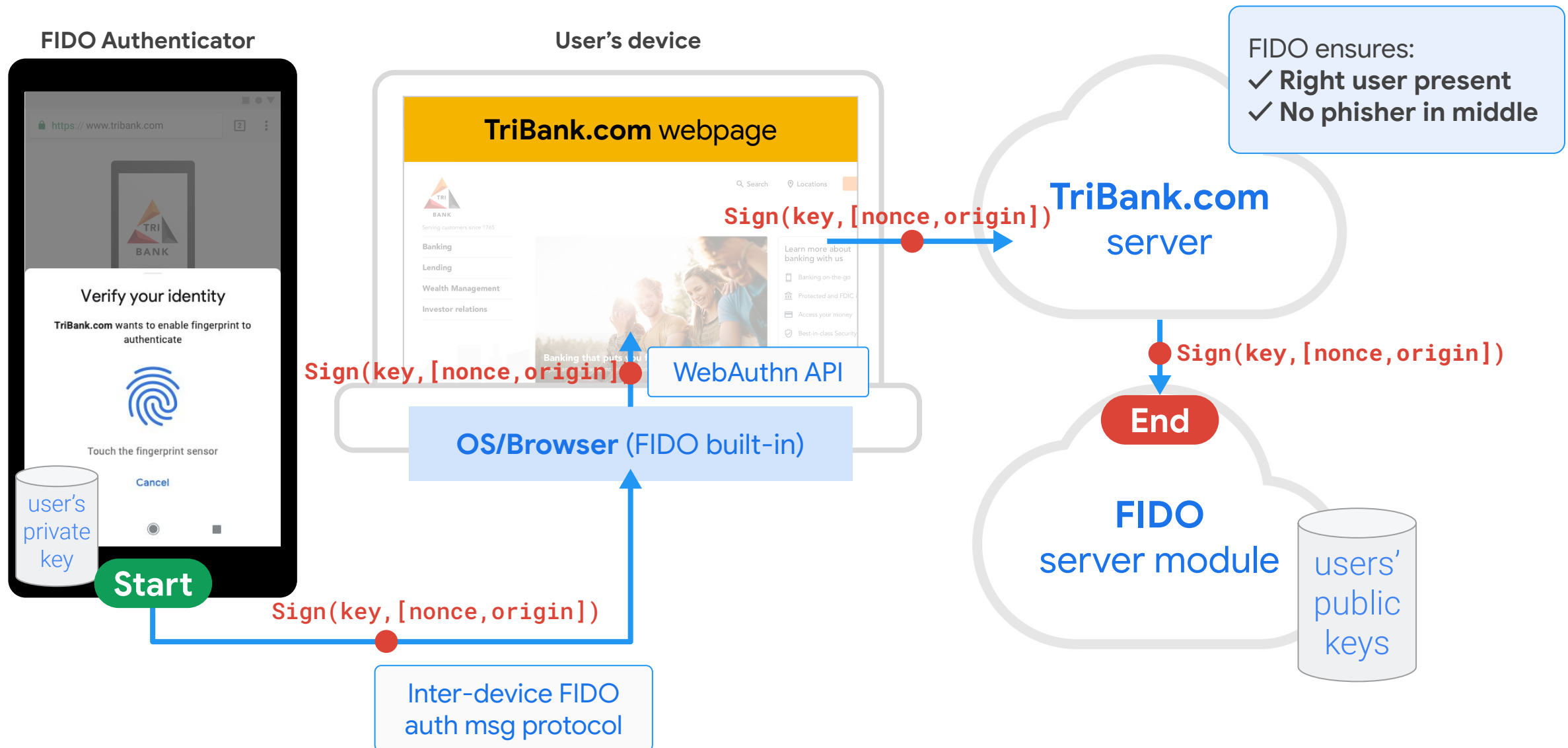
FIDO Authentication: It's the right user + No phisher in the middle



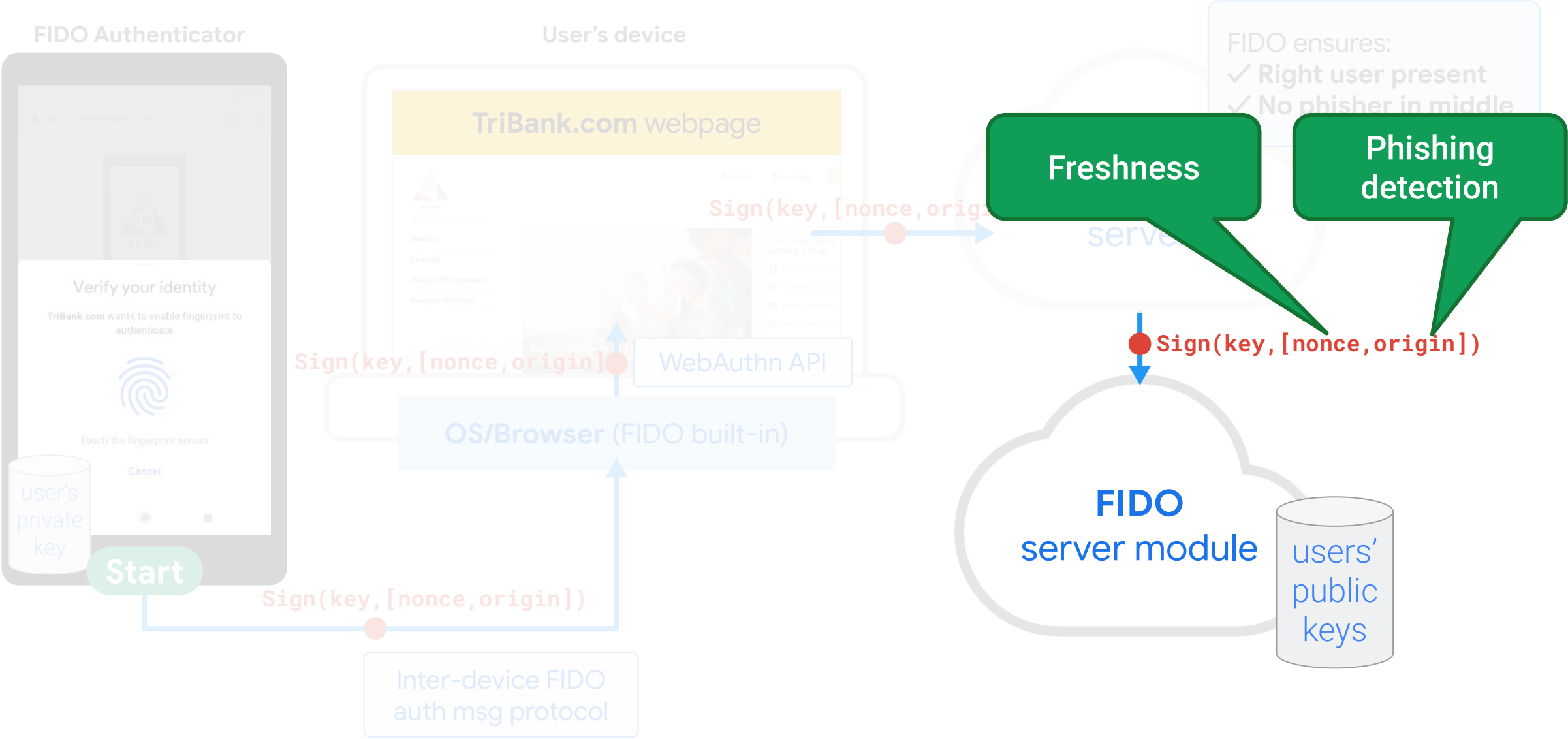
FIDO Authentication: It's the right user + No phisher in the middle



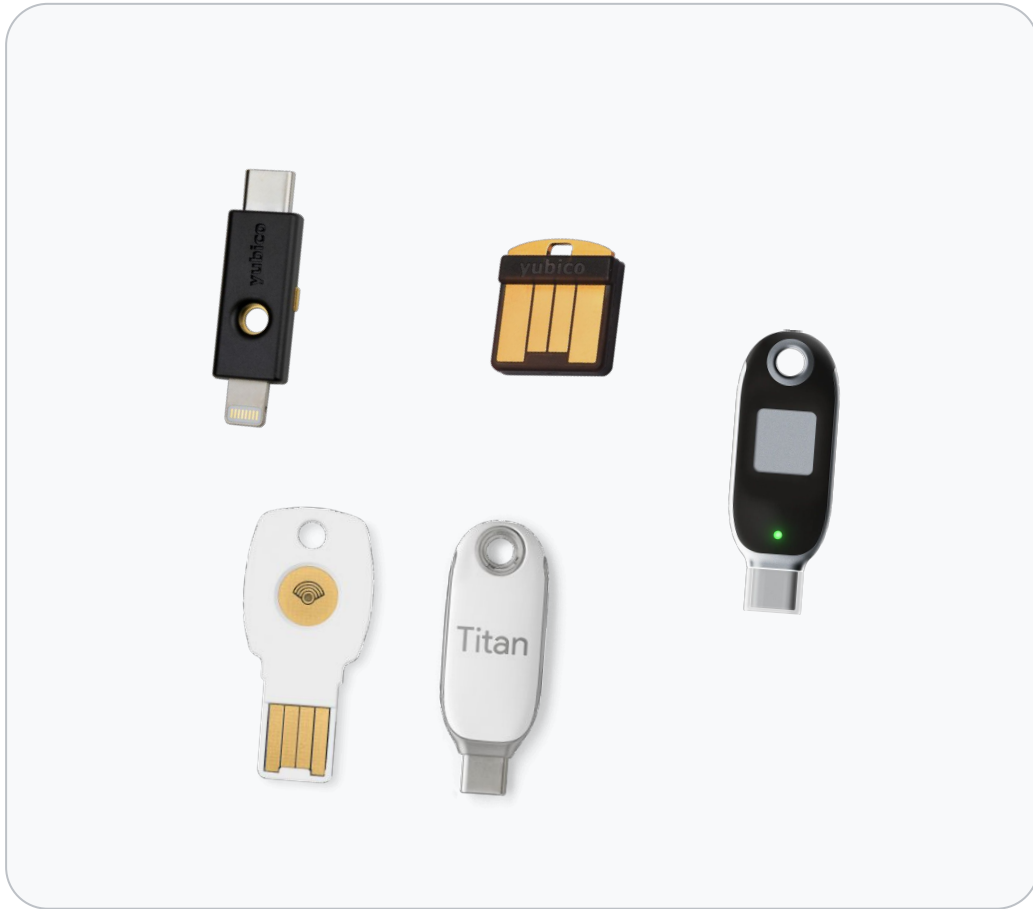
FIDO Authentication: It's the right user + No phisher in the middle



FIDO Authentication: It's the right user + No phisher in the middle



FIDO before passkeys



security keys



platform authenticators

FIDO before passkeys

Great alternative to smart cards

- accessible from web
- no readers needed

Great alternative to other second factors

- phishing resistant

Adopted in high-security scenarios (e.g., Google's Advanced Protection program) as MFA solution.

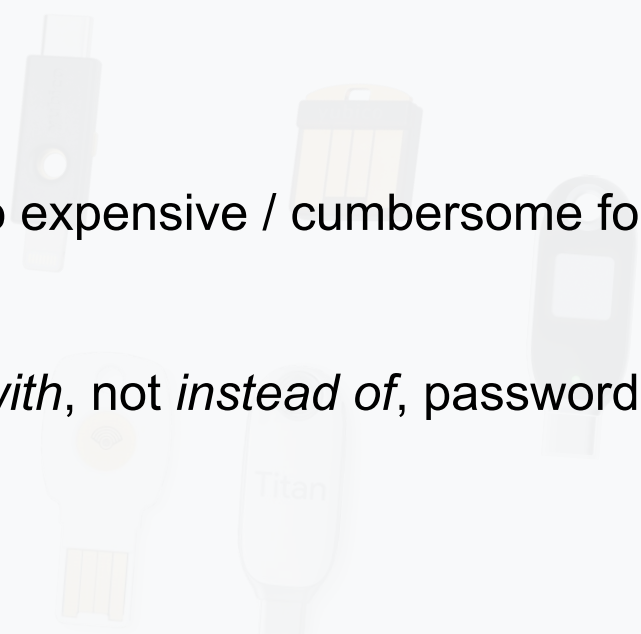
security keys

Simple & secure biometrics-triggered sign-in

Useful as re-authentication on devices where the user has signed in some other way beforehand.

platform authenticators

FIDO before passkeys



Still too expensive / cumbersome for most.

Used *with*, not *instead of*, passwords.

security keys



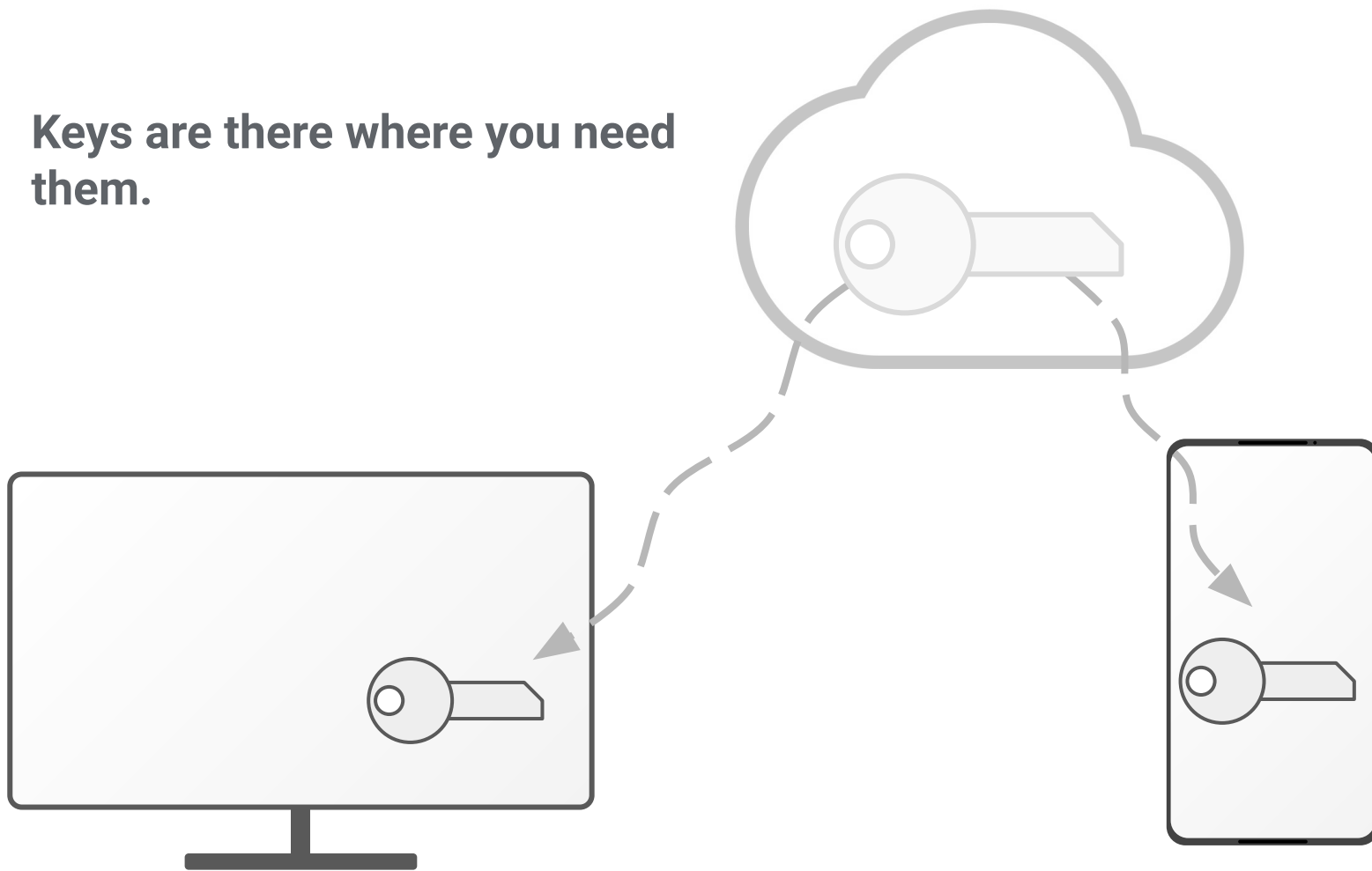
Not available on new devices.

Used *with*, not *instead of*, passwords.

platform authenticators

FIDO with passkeys

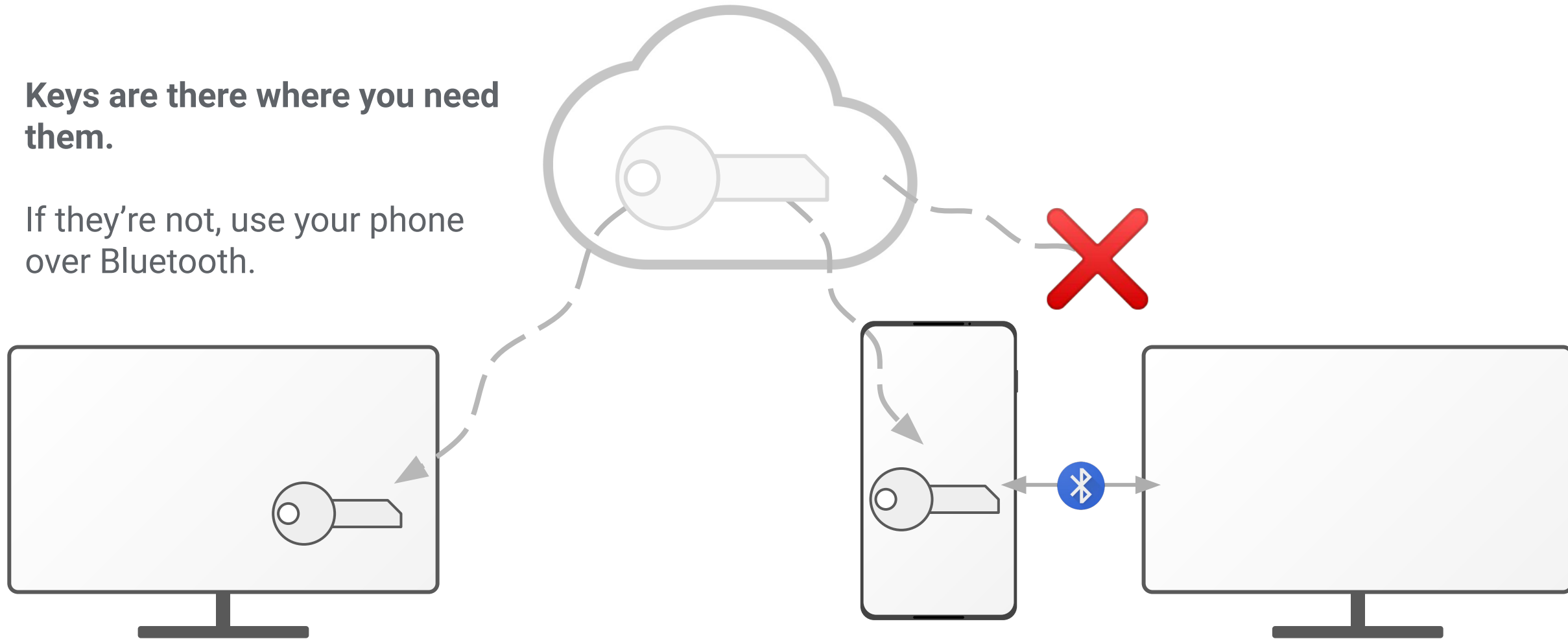
Keys are there where you need them.



FIDO with passkeys

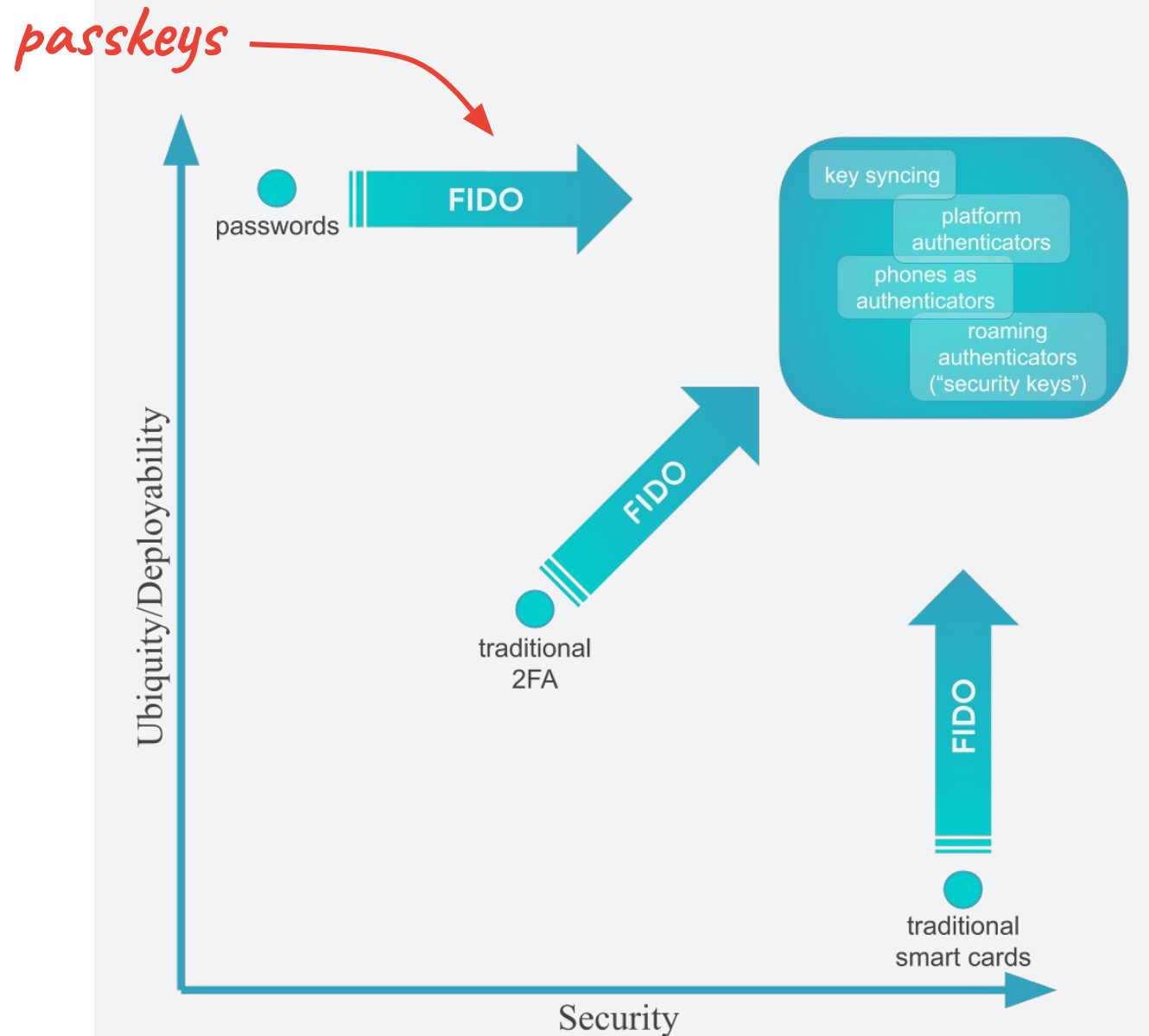
Keys are there where you need them.

If they're not, use your phone over Bluetooth.



Passkeys

FIDO credentials that *replace* the password, rather than *accompany* the password.

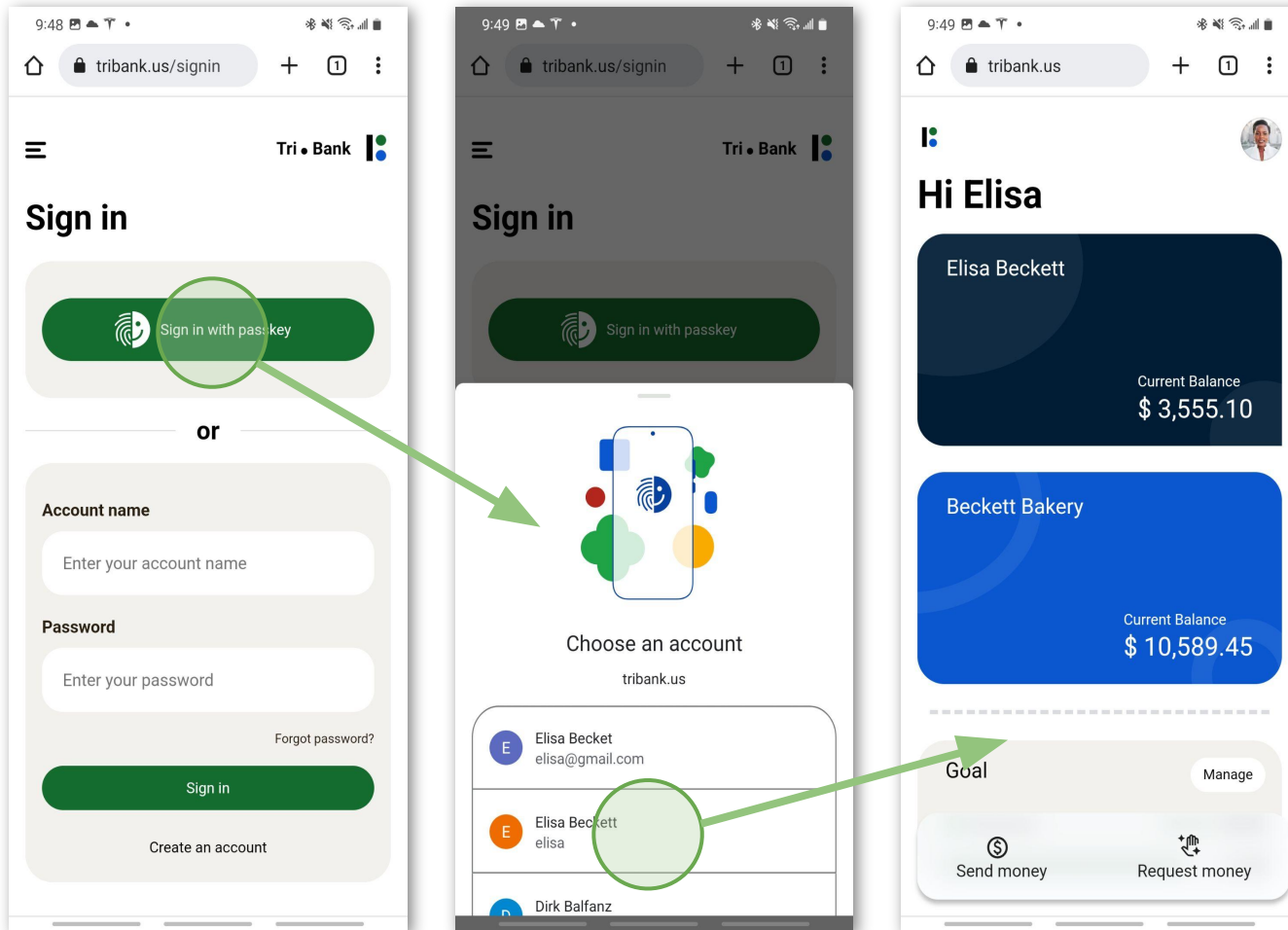


Authentication for app developers

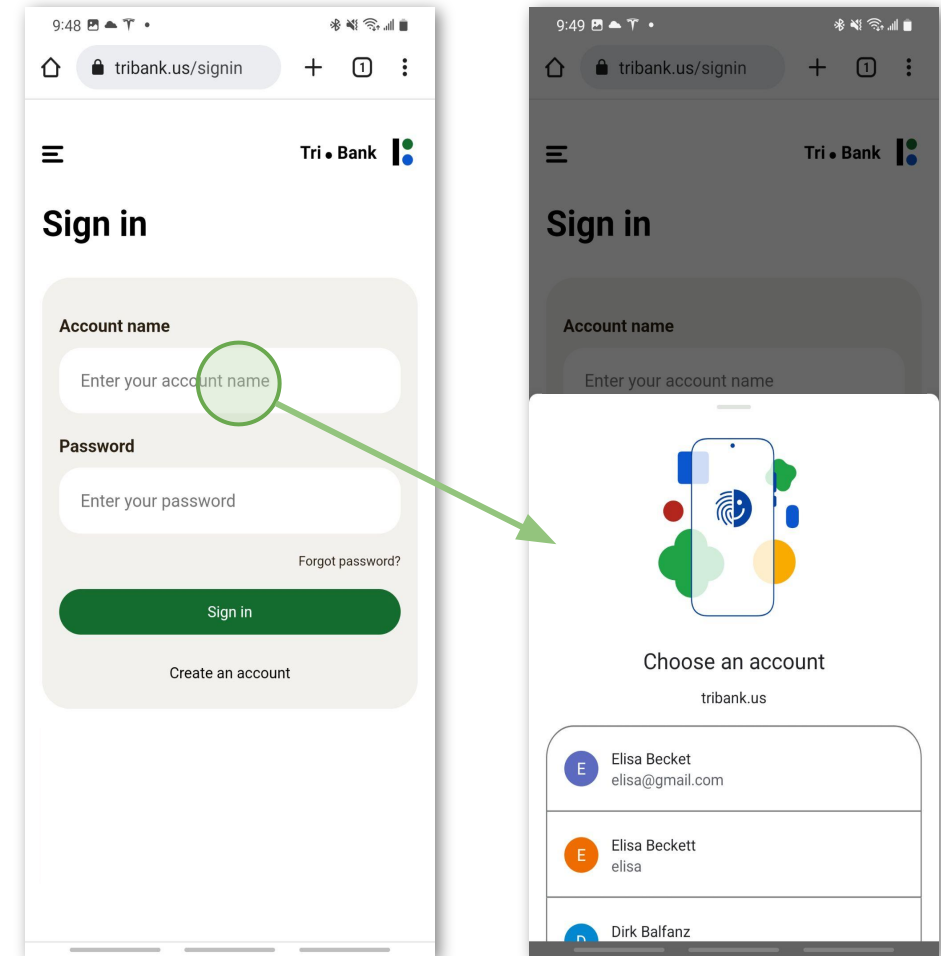


Passkeys can be used *instead* of passwords

not actual UI



UX pattern #1: with a dedicated passkey button



UX pattern #2: integrated into password form

Thanks!