German/US Expert Meeting

IT Security Association Germany (TeleTrusT) in cooperation with FIDO Alliance

San Francisco, 08.05.2024

FIDO Alliance Update

Andrew Shikiar, Executive Director & CEO, FIDO Alliance

David Turner, Sr. Director of Technical Standards, FIDO Alliance

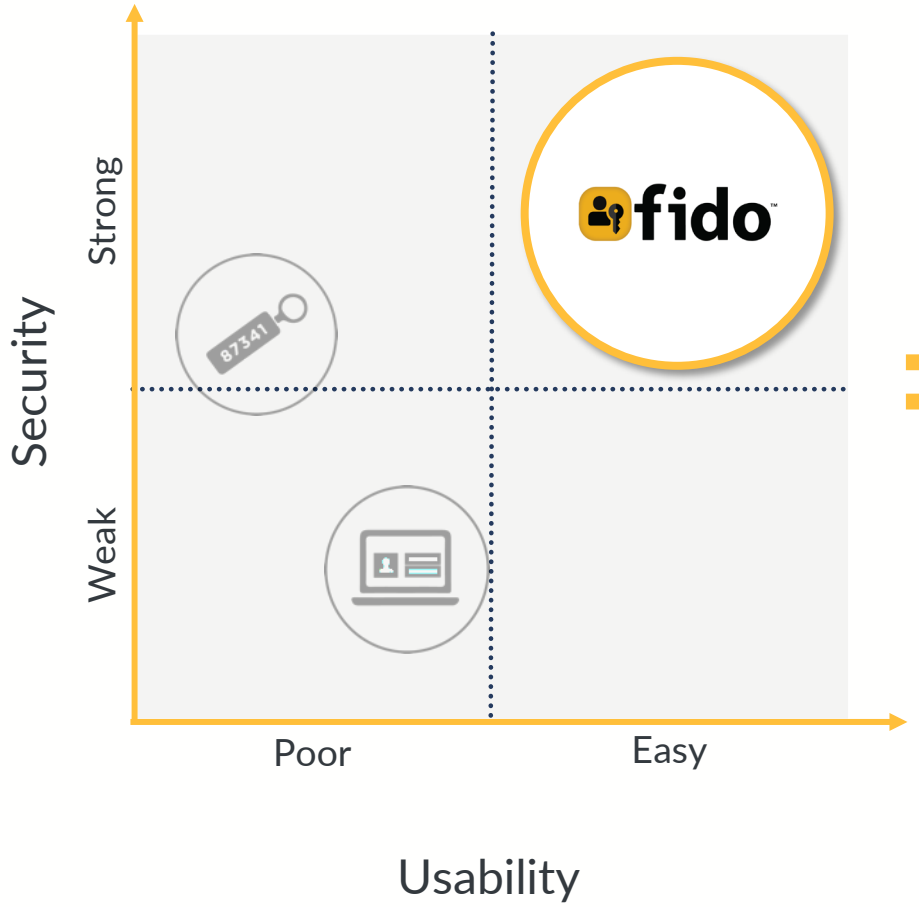
What *is* the FIDO Alliance?

We are a global tech consortium standardizing password-free sign-ins

Backed by global tech leaders

+ Sponsor members | + Associate members | + Liaison members | + Government members

FIDO since 2013: Simpler and stronger



=

Open standards for simpler, stronger authentication using public key cryptography

Single Gesture
Possession-based
Phishing-resistant
Authentication

The very positives …

1. Increase the security of consumer two-factor authentication
2. Offer phishing-resistant multi-factor authentication in a single authenticator
3. Provide great alternative to traditional smart card deployments in high-risk environments

But challenges for scale

1. Inconvenience of physical security keys
2. Challenges with embedded authenticators as a second factor
3. Higher barrier to adoption for users who don’t (want to) use two-factor authentication at all, and are stuck with passwords

The foundation of authentication is fundamentally flawed

When our primary factor is **passwords**...

81% of hacking-related breaches are caused by weak or stolen passwords (Ping Identity)

43% Gave up on a purchase because they forgot their password (FIDO Alliance)

76% Rise in direct financial loss from successful phishing attacks from 2022-2023 (Proofpoint)

64% either use weak passwords or repeat variations of passwords (Keeper)

Easily phished or socially engineered, difficult to use and maintain

Layering on does not work

…then our additional layers – while well-intended and necessary – are there to cover up password problems

Brace for more phishing, scams, data breaches, APT attacks in APAC 2024

ET CIO SOUTHEAST ASIA

The art of MFA Bypass: How attackers regularly beat two-factor authentication

Security Boulevard

Data breach cost Latitude $76 million: Cyber attack on Australian company Latitude Financial saw the personal data of up to 14 million customers stolen.

acs INFORMATIONAGE

Phishing Attacks Rise Sharply in Southeast Asia: Kaspersky Detects Over 43M Email-Based Phishing Attacks Across Region in 2022

BANK INFO SECURITY®

Often still phishable, socially engineered, difficult to use and maintain

Generative AI adds fuel to the phishing fire

1265% Rise in malicious phishing emails since Q4 2022 (Slashnext)

967% Rise in credential phishing in particular since Q4 2022 (Slashnext)

54% Of consumers have noticed phishing messages become more sophisticated in last 60 days (FIDO Alliance)

A fundamental pivot is needed..:

What if we could replace the outdated legacy model of “password + something else” and could replace it with a single factor that was much more secure – and easier to use?

A fundamental pivot is needed..:

What if we could replace the outdated legacy model of “password + something else” and could replace it with a single factor that was much more secure – and easier to use?

If phishing is now the primary threat - a single phishing-resistant authenticator is more valuable (in most cases) than two factors which are both easily phished.

Enter: Synced passkeys

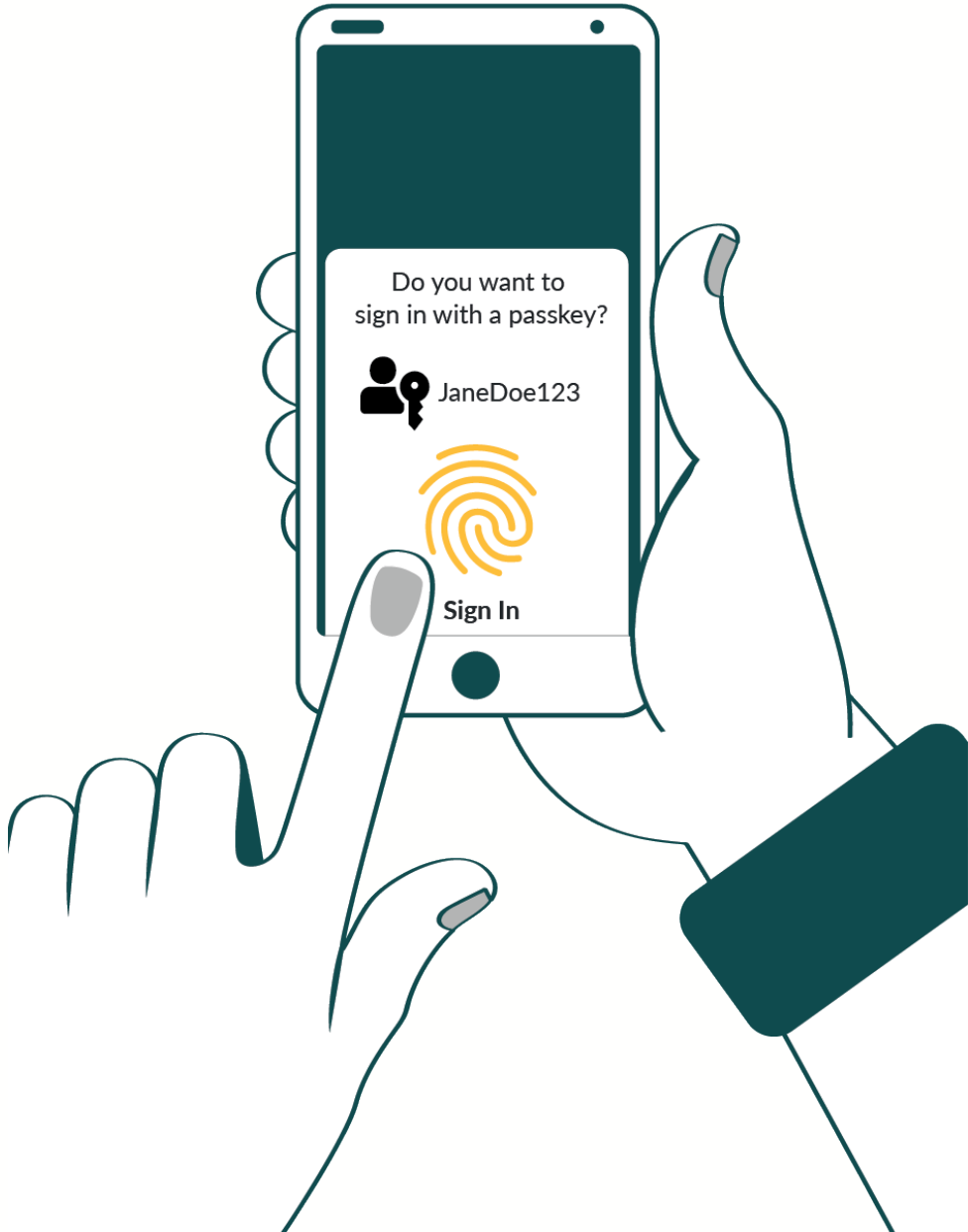
Passkey

/ˈpas, kē/

noun

A FIDO Authentication credential that provides passwordless sign-ins to online services.

A passkey may be synced across a secure cloud so that it's readily available on all of a user's devices, or it can be bound to a dedicated device such as a FIDO security key.



A bit deeper on new(er) terminology

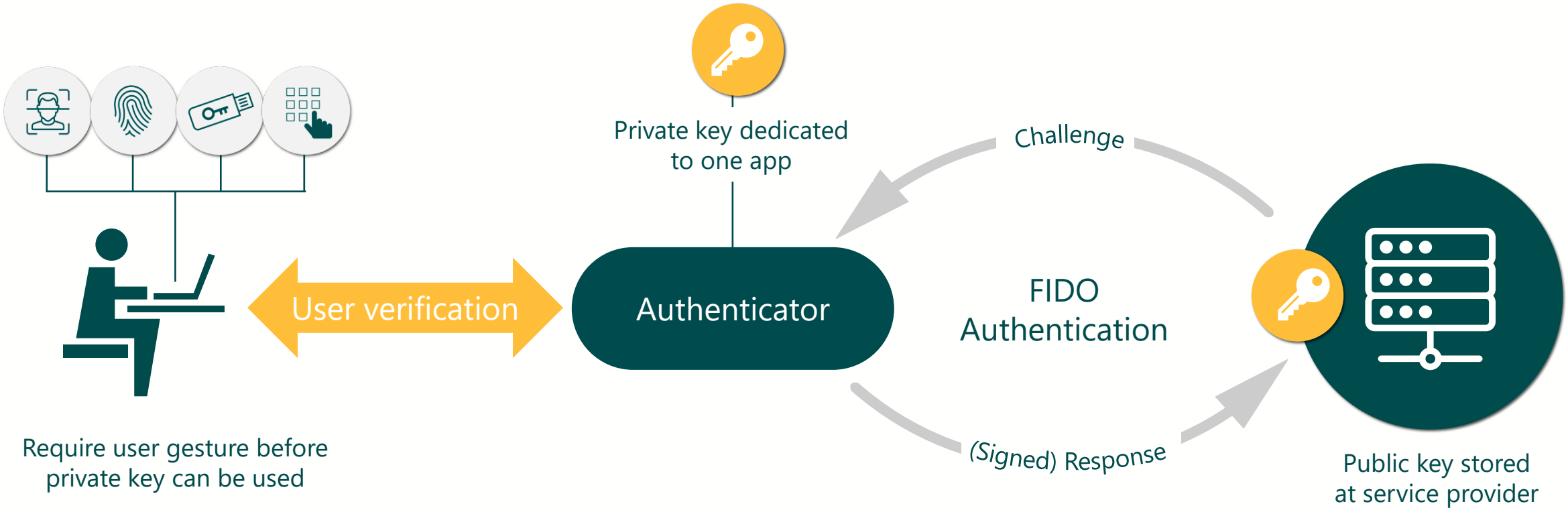
A **passkey** is any passwordless FIDO credential

- Raises the bar for both security and UX
- Is most *commonly* synchronized across a user's devices – but doesn't have to be

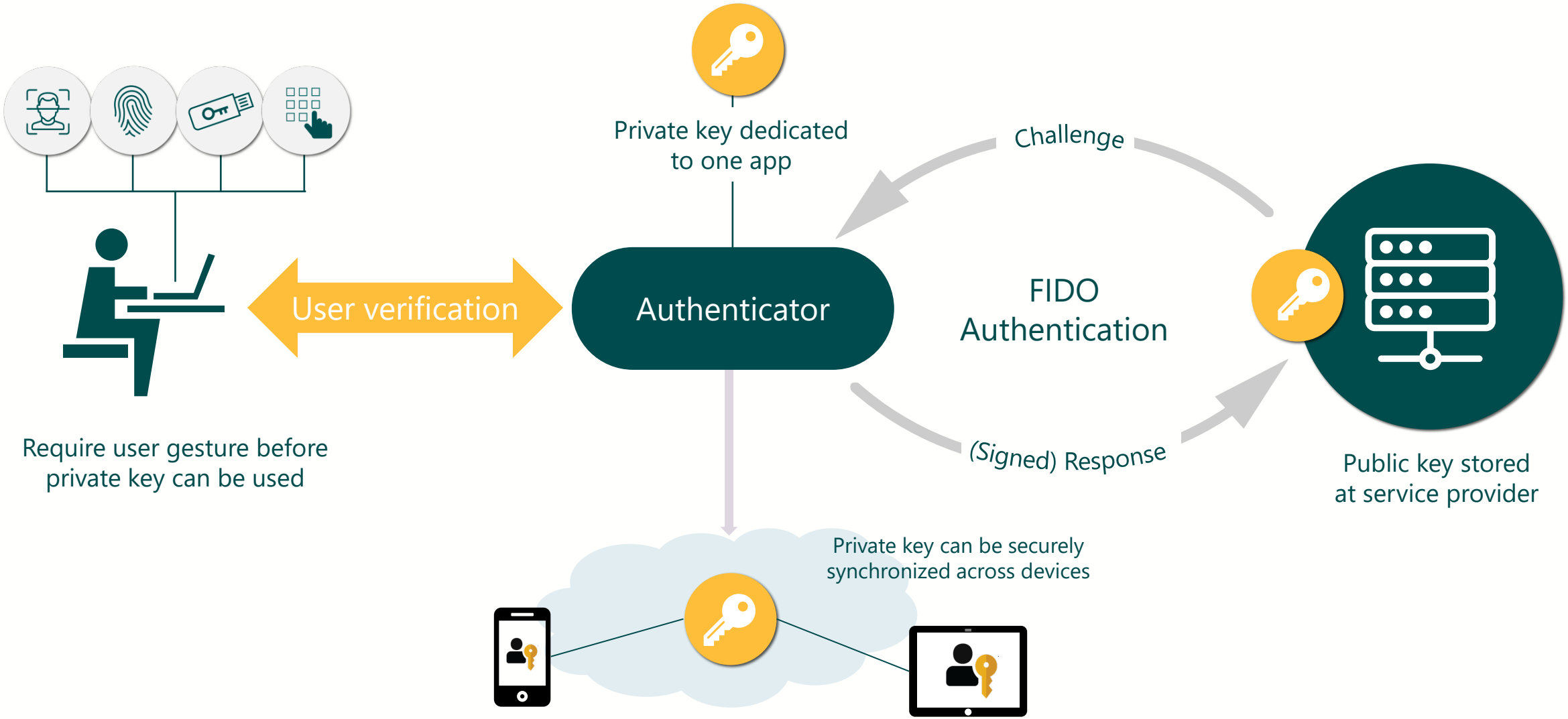
A **passkey provider** might be a platform/OS vendor, or 3rd-party software such as a password manager.

- Facilitates new device bootstrapping and simplifies account recovery
- Security of synced passkeys is the responsibility of the passkey provider
- Live passkey providers include Apple, Google, Dashlane, 1Password

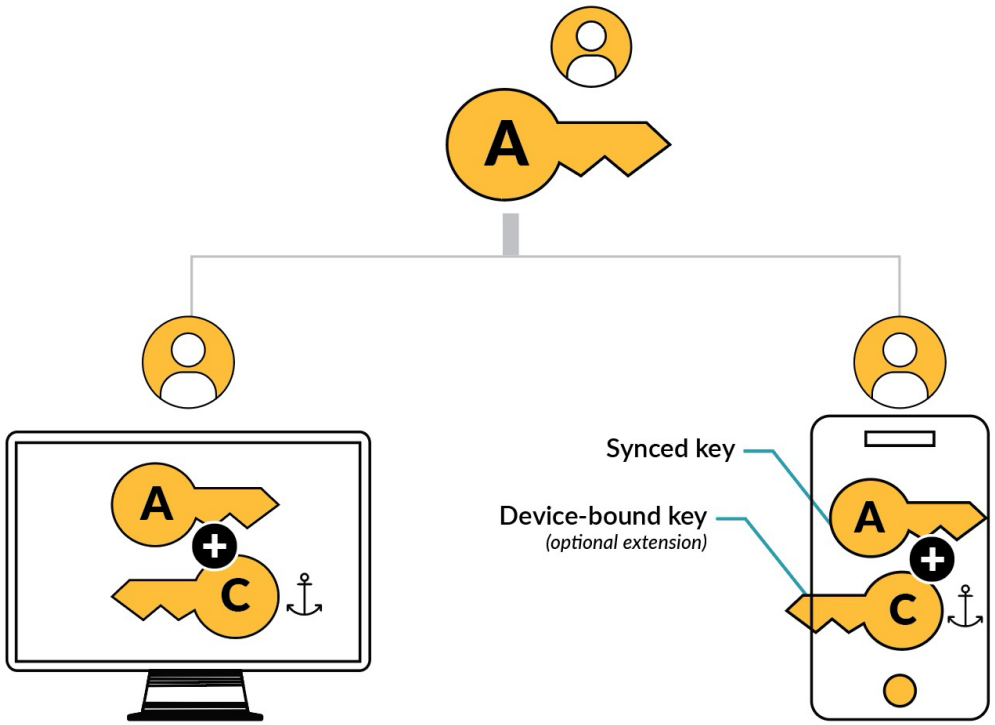
Same approach – with new syncing capabilities



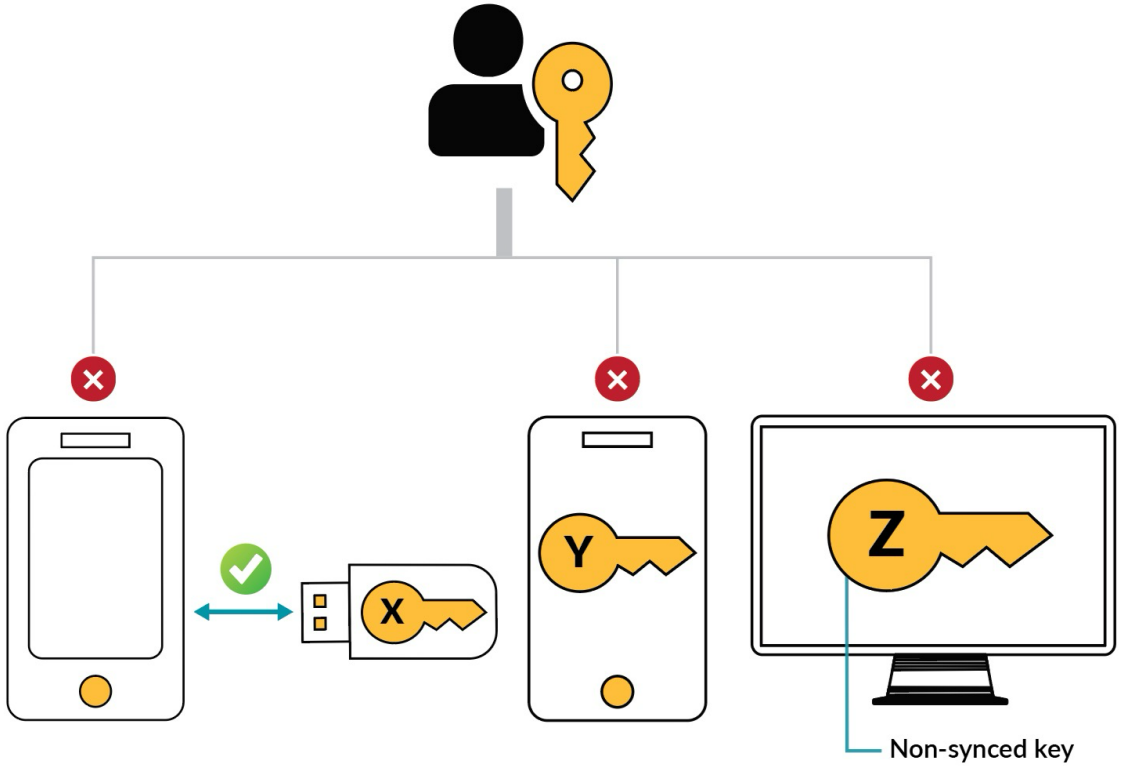
Same approach – with new syncing capabilities



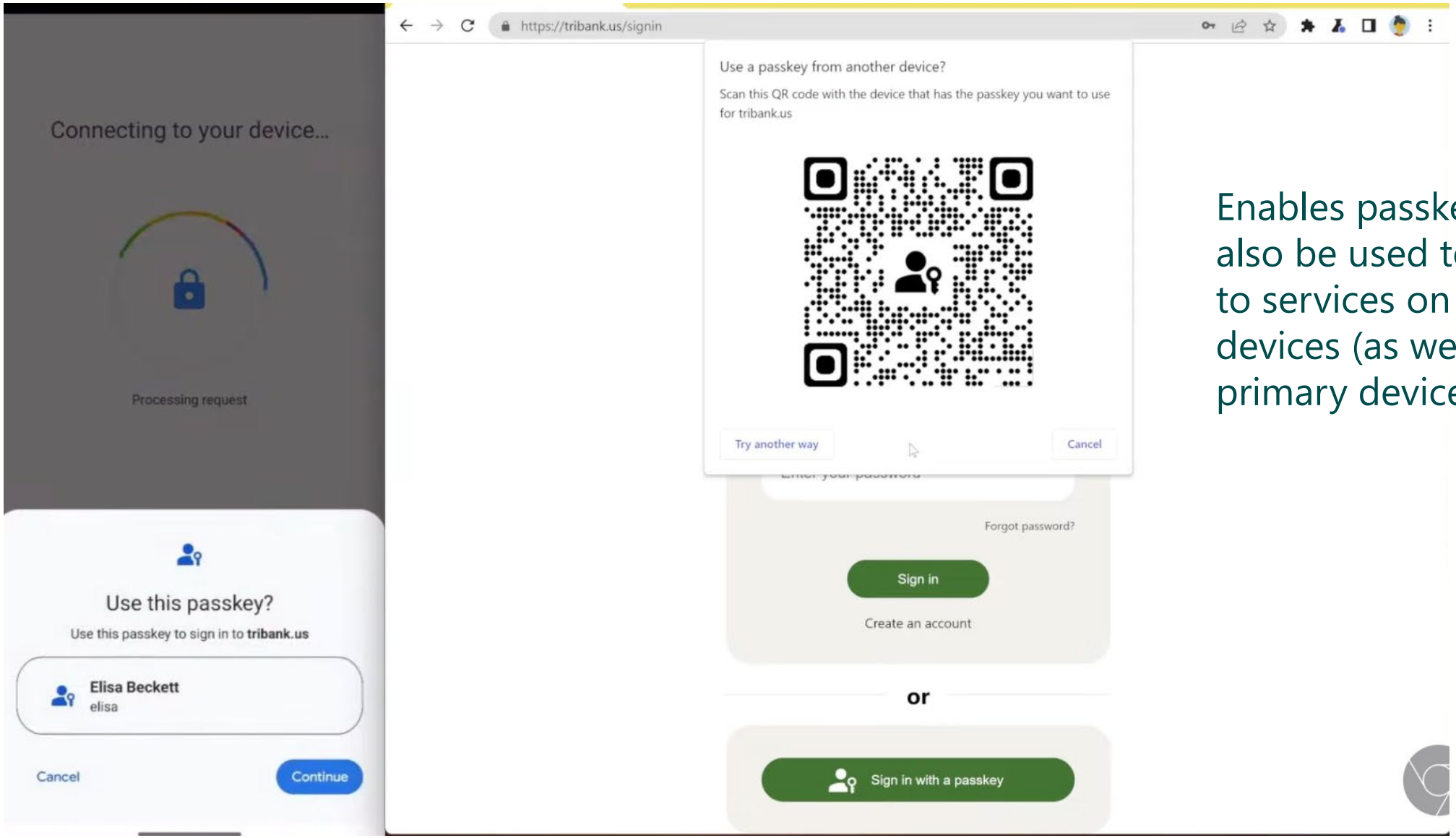
Synced passkeys



Device-bound passkeys



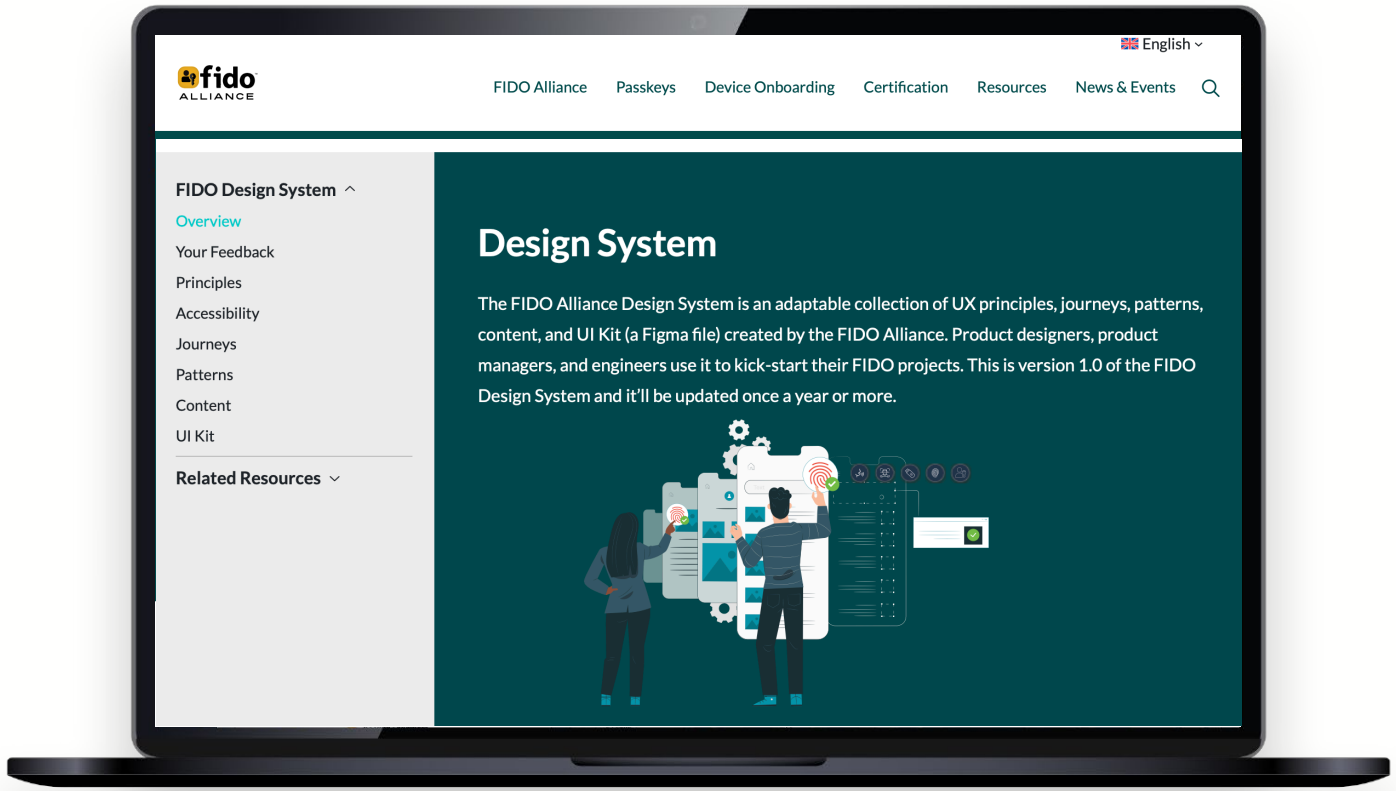
Cross-device authentication



Enables passkeys to be also be used to sign-in to services on nearby devices (as well as on primary device)

Image Credit: Google

FIDO's Focus on Usability



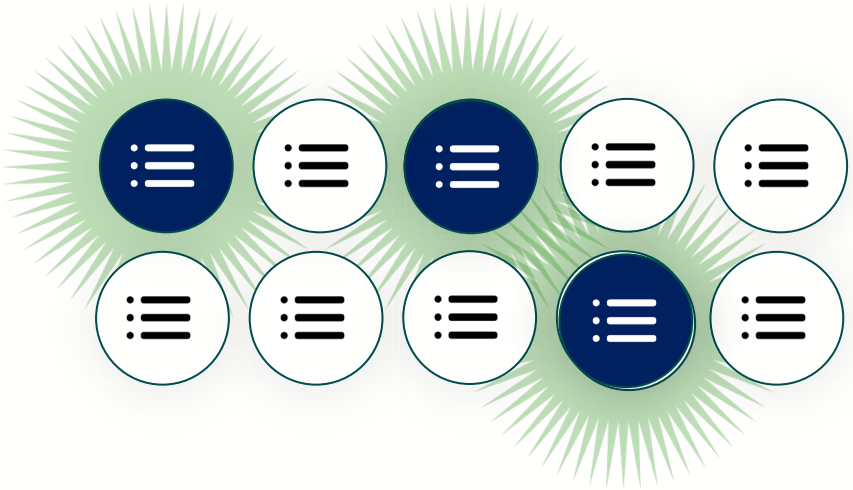
Available Now

- FIDO Design System
  - UX guidelines for passkeys, security keys, and device authenticators
  - UI Kit

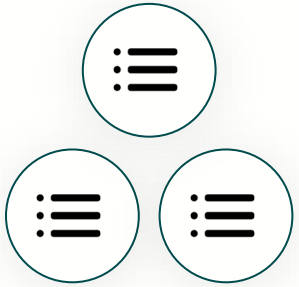
Coming soon: Passkey Resource Center

UX Guidelines

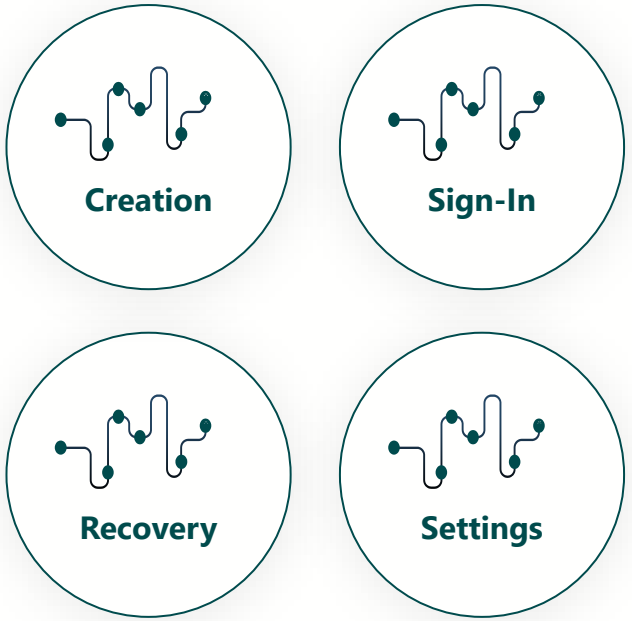
10 UX principles



3 content principles



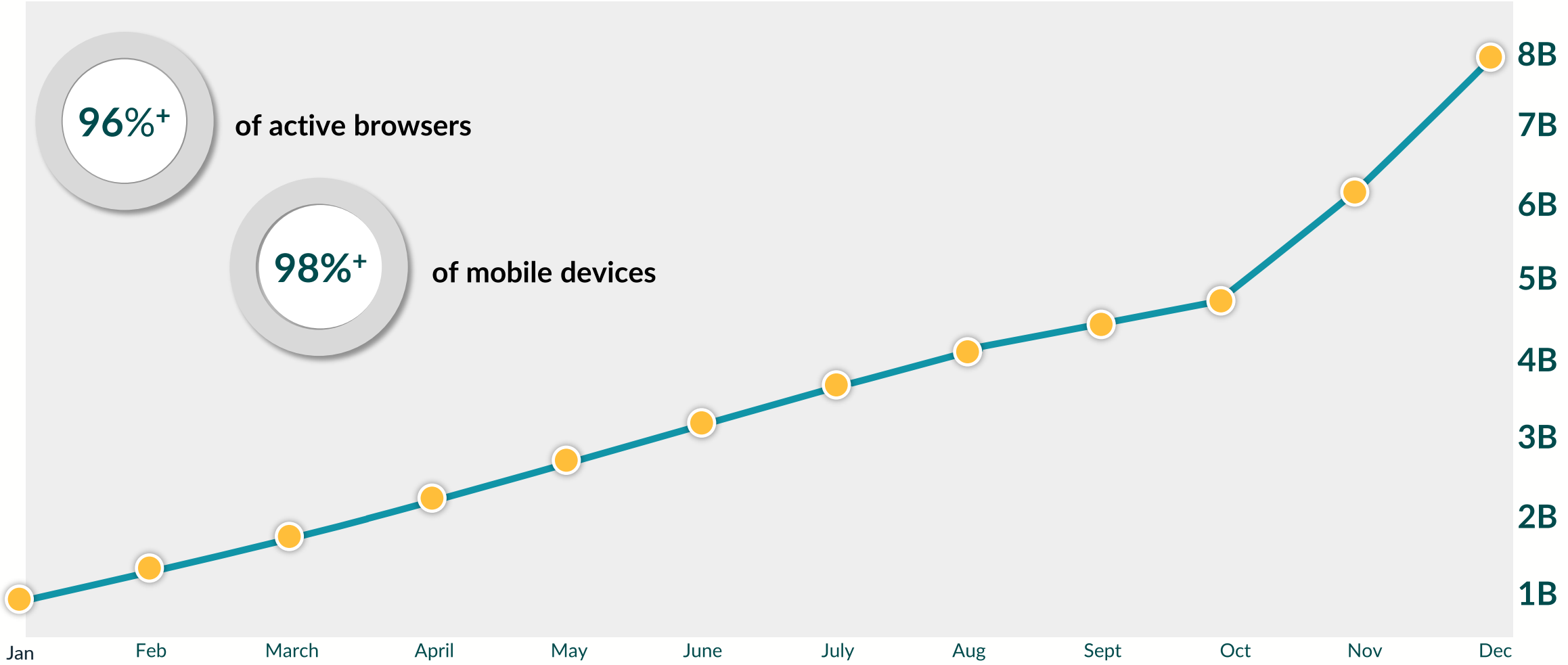
4 user journeys



← View the UX Guidelines

Rapid adoption

of accounts with passkey support



Proven success

TikTok

Within the first few months…
- 97% login success rate
- 14% eligible user adoption rate
- 2% reduction in SMS OTP login

mercari

- Sign-in success rate grew from 67.7% (SMS 2FA) to 82.5% -- over a **21% improvement**
- Authentication time decreased from 17s (SMS 2FA) to 4.4s – nearly **4x faster**

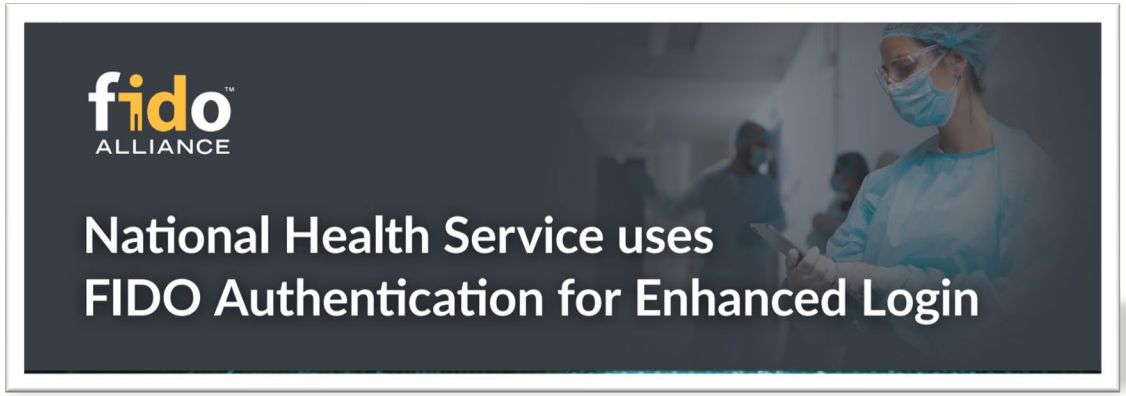
AIR NEW ZEALAND

- 30% opt-in in first 24 hours
- 4.7x improvement time to complete & improvement in success rate
- 50% reduction in abandonment rates
- Reduced account recovery calls and call center attacks

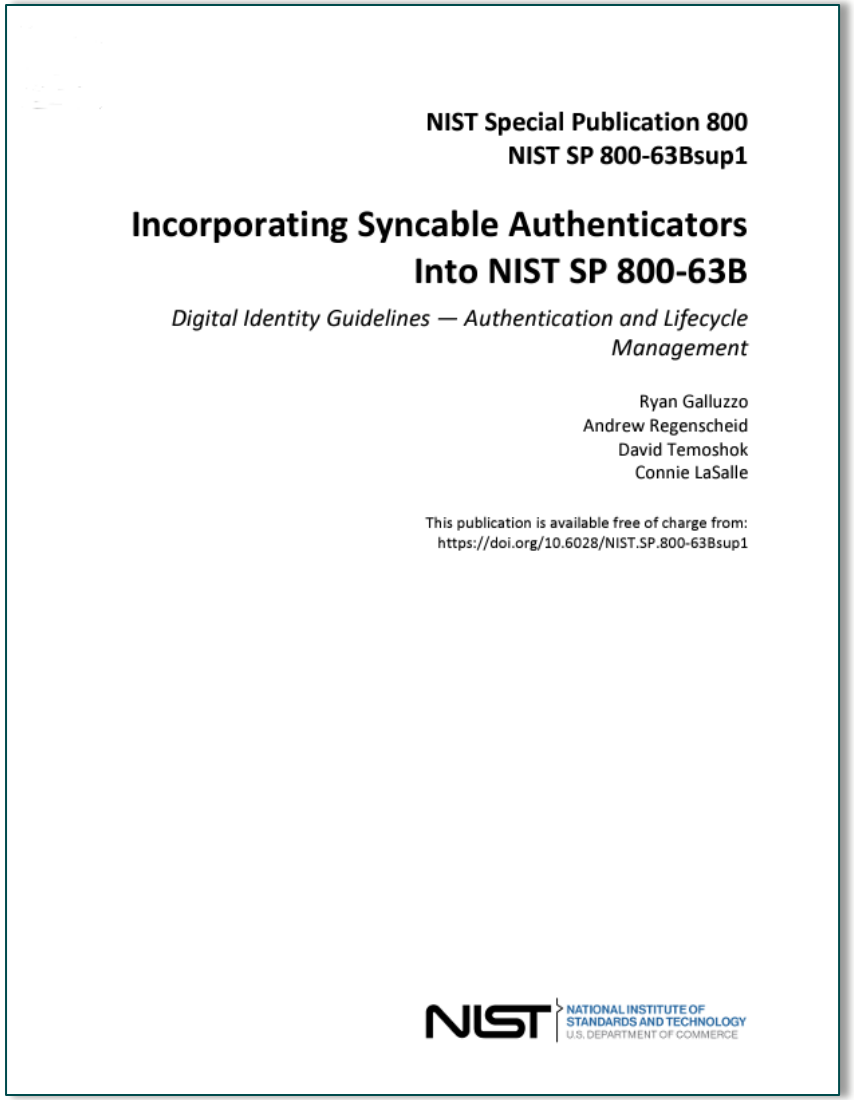
Google

- 4x improvement in sign-in success rate (vs passwords)
- ½ the sign-in time

Government utilization of FIDO Authentication



Reframing the regulatory narrative



NIST Special Publication 800
NIST SP 800-63Bsup1

Incorporating Syncable Authenticators Into NIST SP 800-63B

Digital Identity Guidelines — Authentication and Lifecycle Management

Ryan Galluzzo
Andrew Regenscheid
David Temoshok
Connie LaSalle

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63Bsup1

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Stop checking a box for “MFA”…

… and start thinking about ***phishing resistance*** rather than “factors”

Stop checking a box for “MFA”…

… and start thinking about ***phishing resistance*** rather than “factors”

A synced passkey is always better than a password alone

Stop checking a box for “MFA”…

… and start thinking about ***phishing resistance*** rather than “factors”

A synced passkey is always better than a password alone

If you’re using password + SMS OTP, passkeys are better

Stop checking a box for “MFA”…

… and start thinking about your business requirements

One size doesn’t fit all – consider business , regulatory, and security requirements

- Pair with another factor
- Leverage risk signals
- Require device-bound passkey

Looking forward…

The Old Way: Every Part of the Online Account Lifecycle Susceptible to Attacks

Account Enrollment

KBA

Weak remote IDV systems tricked by synthetic documents and fabricated biometrics

=

Accounts created with stolen or synthetic identities

Authentication

Passwords

Phishable MFA

=

Account takeovers via phishing, man in the middle, credential stuffing and other attacks

Account Recovery/Reverification

Only as sound as 1 and 2!

=

Major vector for account takeover

The New Way: advanced technologies for remote identity verification snuff out attacks

- Reliable and accurate document verification
- Biometric verification checks for liveness to identify spoofs
  - Photos of screens, 2D & 3D masks, image upload manipulation, etc.
- Biometric systems have advanced reliability presentation attack detection

Backed by FIDO Certification programs

Tested by accredited third party labs

Removes need for vendor “bake offs”

- Biometric Component Certification
- IDV Document Authenticity
- IDV Selfie & Face (coming soon)

The New Way: Securing Every Part of the Account Lifecycle

Account Enrollment

Strong remote IDV systems can detect synthetic documents and fabricated biometrics

=

Accounts created only for individuals with proven identity

Authentication

FIDO phishing-resistant authentication with passkeys

=

Strong security at every sign in

Account Recovery/Reverification

As sound as 1 and 2!

=

Accounts are NOT taken over through account recovery and re-verification methods

Questions?