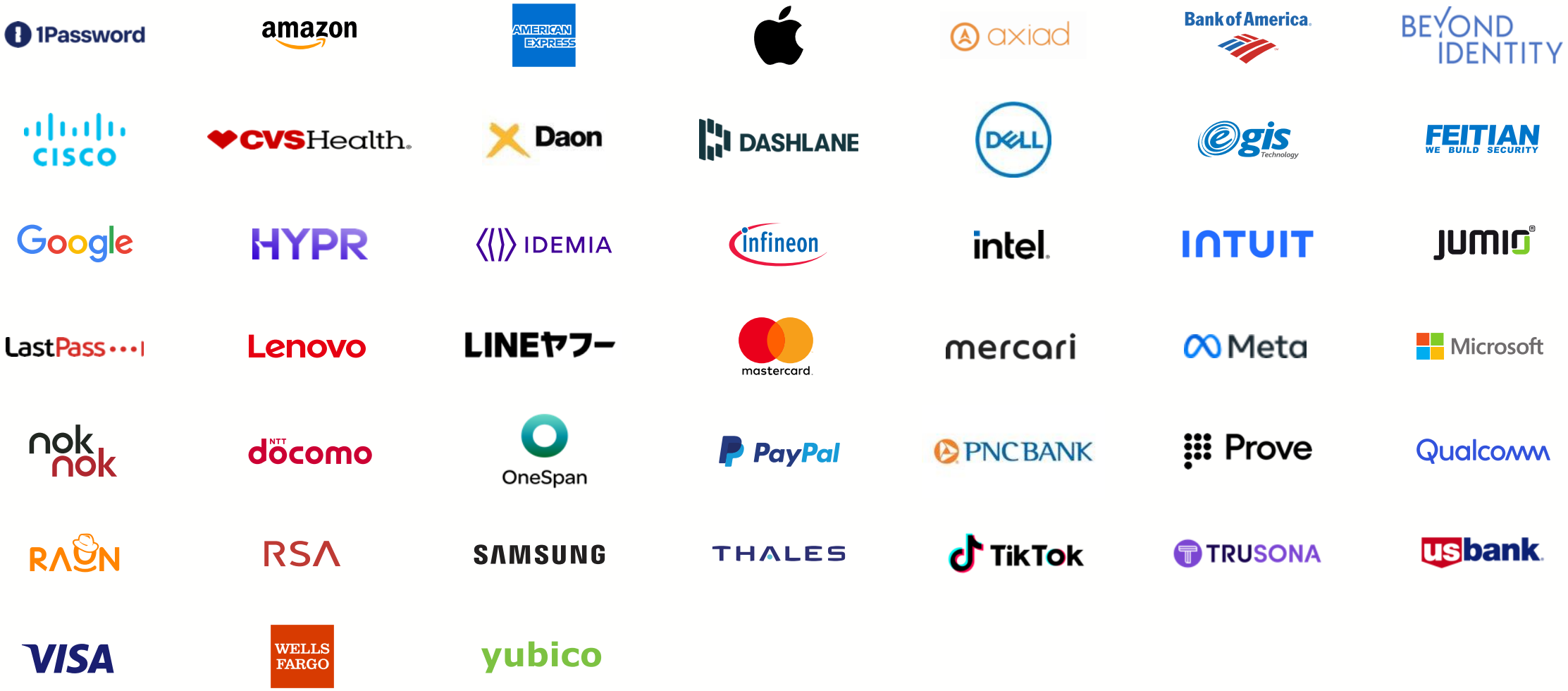
FIDO Alliance Overview

Andrew Shikiar
Executive Director & CEO
October 2024

What is the FIDO Alliance?

The FIDO Alliance is an open industry association with a focused mission: reduce the world's reliance on passwords.

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 –

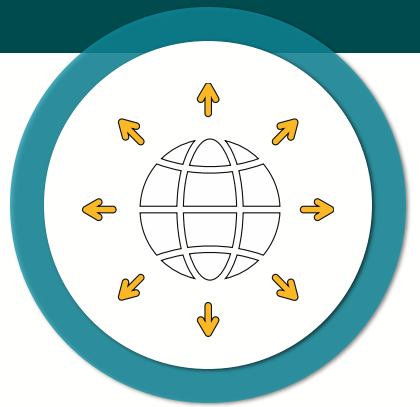
The FIDO Alliance works to fulfill its mission through…

Technical Specifications

Define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords

Industry Certification Programs

Ensure interoperability, security and usability of products, services and components



Market Adoption & Regulatory Engagement Programs

Promote the use of FIDO globally to drive adoption and education

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)

56%

Gave up on accessing an online service because they forgot their password

(FIDO Alliance)

$4.45 million

average cost of a successful phishing attack for an organization

(IBM)

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

4 Ways Hackers use Social Engineering to Bypass MFA

The Hacker News

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

Security Boulevard

Multifactor Authentication Bypass: Attackers Refine Tactics: During the first quarter of 2024, nearly half of all security incidents involved MFA.

BANK INFO SECURITY®

New MFA-bypassing phishing kit targets Microsoft 365, Gmail accounts

BLEEPINGCOMPUTER

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

Generative AI adds fuel to the phishing fire

967%

Rise in credential phishing in particular since Q4 2022

(Slashnext)

1265%

Rise in malicious phishing emails 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?

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.

What is a passkey?

Passkey

/’pas, kē/ noun

Passkeys are a password replacement based on FIDO protocols that provide faster, easier, more secure sign-ins to online services.

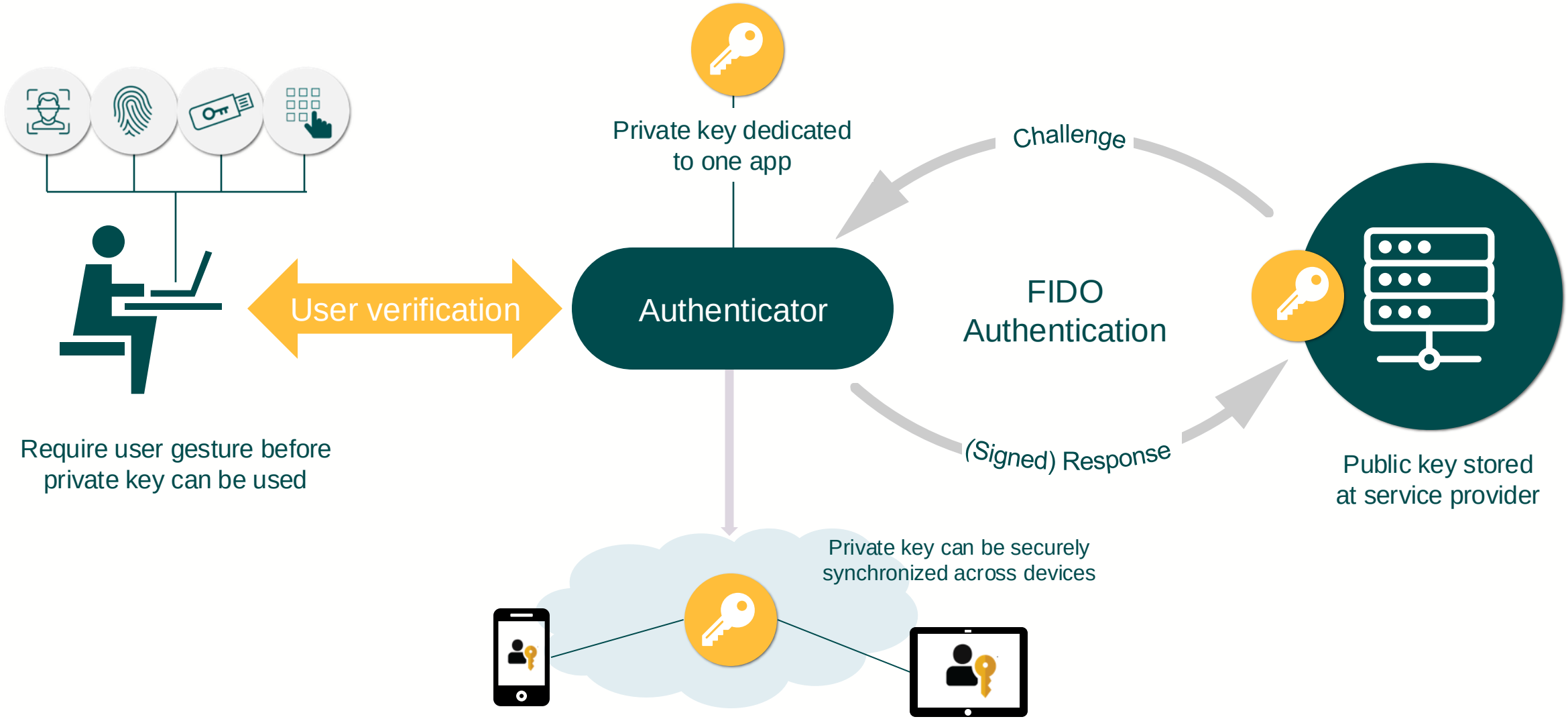
A passkey may be synced across a secure cloud so that it’s readily available on all of a user’s devices, or it can be bound to a dedicated device such as a FIDO security key.

4x simpler

Passkeys are 4x simpler to use since they don’t need to be remembered or typed. You just use your fingerprint, face scan, or screen lock to sign in across all your devices and platforms.

Source: Google

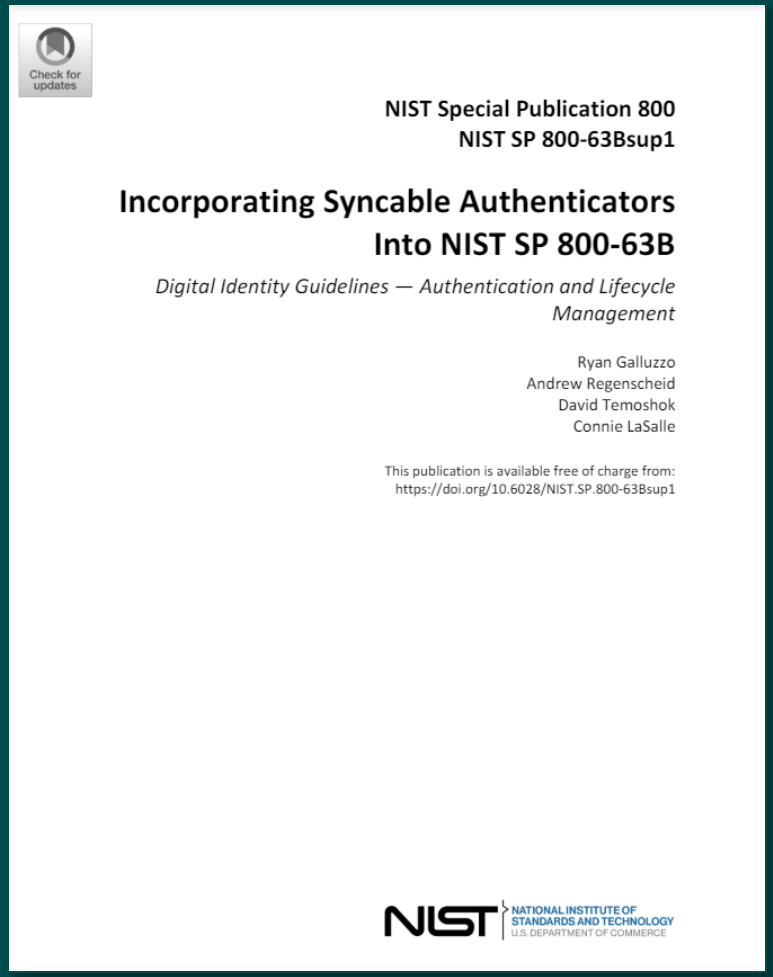
Same approach – with new syncing capabilities



Regulatory recognition of synced credentials

Per CISA:

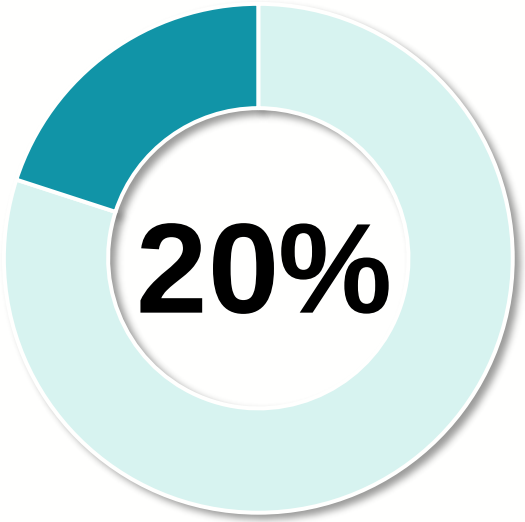
- Manufacturers should seek to increase MFA enrollment among their customers across the board, with an emphasis where possible of **adopting phishing-resistant MFA** and increasing enrollment by administrators.
- Other phishing-resistant forms of authentication, such as passkeys, meet this definition even if they are the sole form of authentication.



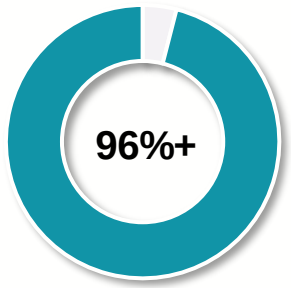
Amends NIST SP 800-63-3 effective **immediately** to recognize synced authenticators at AAL2

Passkey adoption by the numbers

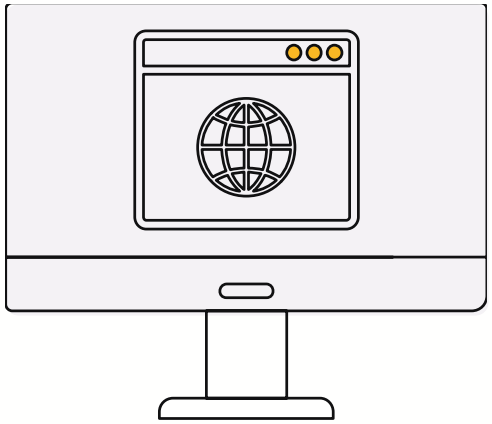
(Since October 2022)



of the world's top 100 websites and services

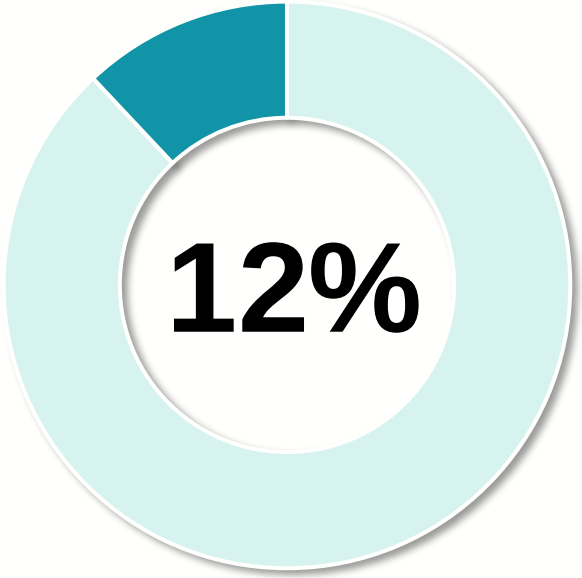


of active browsers

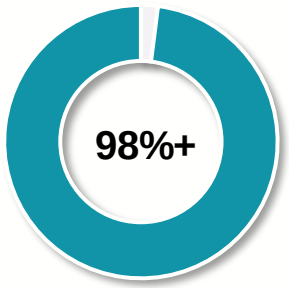


More than 13B

accounts can now leverage passkeys for sign in



of the world's top 250 websites and services



of mobile devices

Some recent deployments

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
- 400M+ accounts have used passkeys
- 1B+ sign-ins with passkeys

Proven success

amazon

Since October 2023

- 175 million passkeys created
- Passkeys available to 100% of customers

PlayStation®

- 24% reduction in sign-in time on web
- 29% of password resets resulted in passkey conversion, removing passwords completely
- 88% of users engaging with passkey content completed the transition and eliminated their passwords

Google

- 30% higher sign-in success rate
- 20% faster sign ins on avg (40-50% on mobile)
- 63% of customers feel passkeys are safer, easier
- 2.5B+ sign-ins & 800M+ accounts using passkeys

Michigan.gov

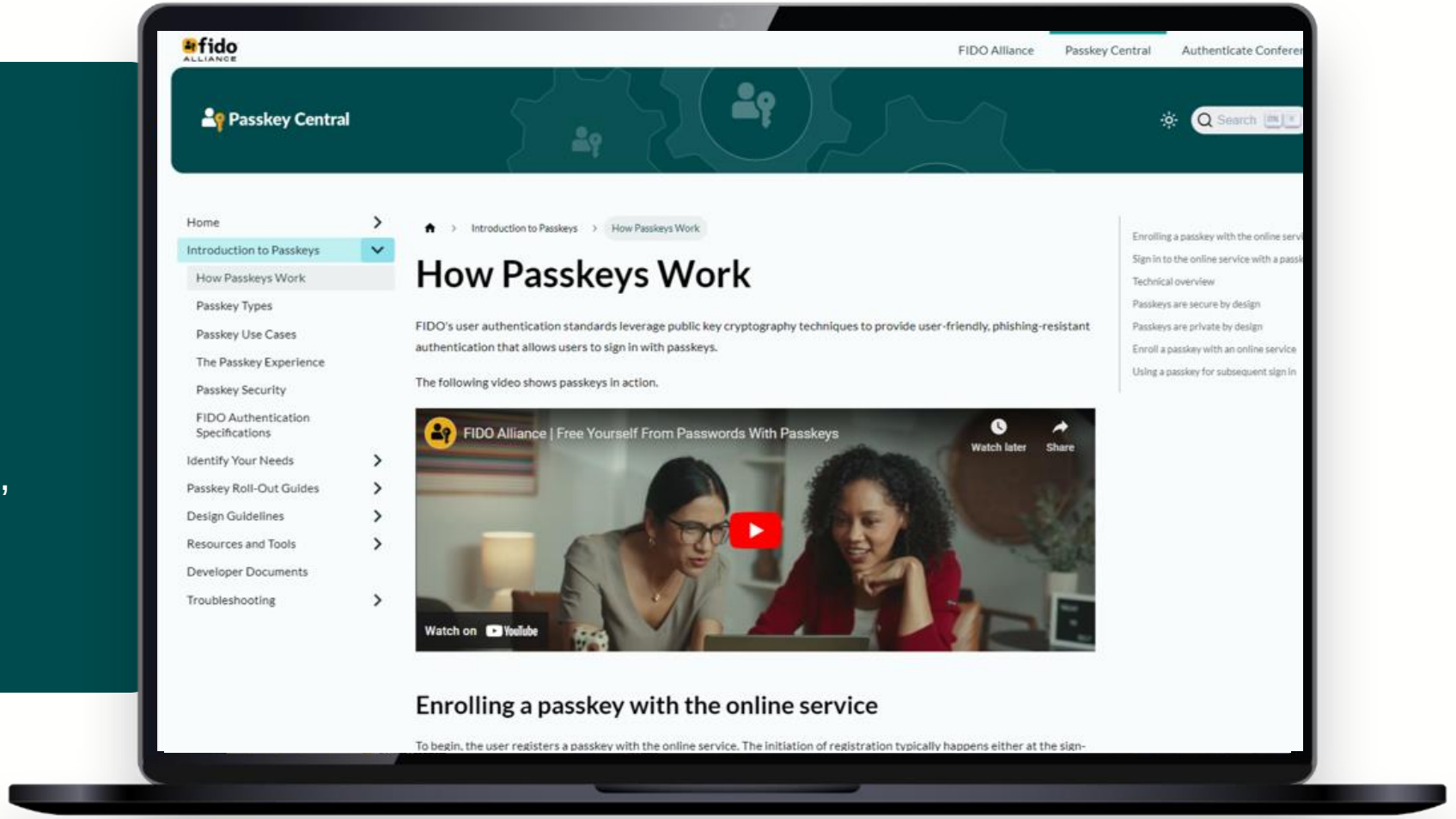
MiLogin service with millions of public users, employees, contractors and partners:

- Abandonment rates dropped from 85% to 13%
- 34.7% Reduction in registration time
- 30% Reduction in IT help desk calls

FIDO’s Focus on Enablement

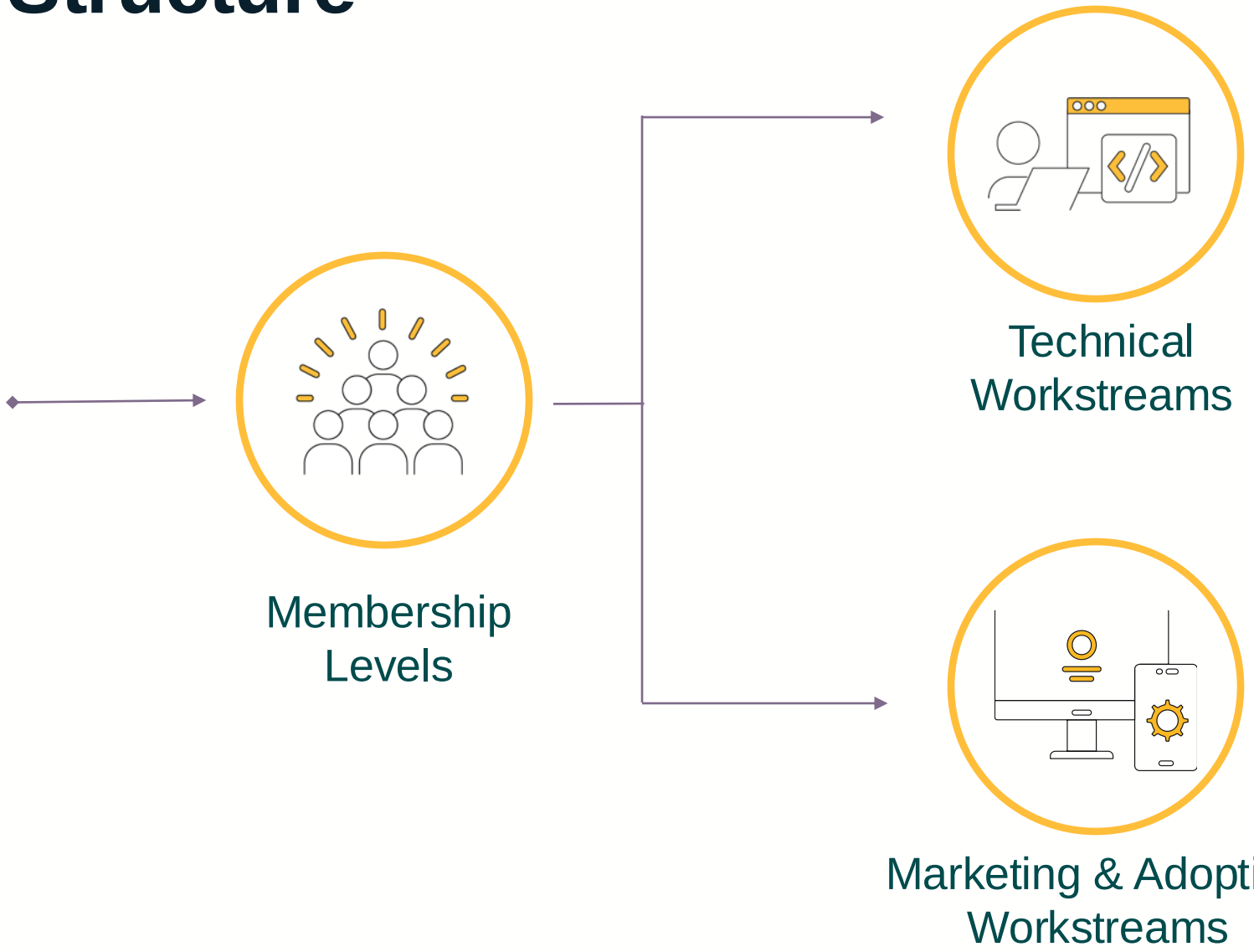
Available Now

- Passkey Central
  - Comprehensive suite of enablement resources
- FIDO Design System
  - UX guidelines for passkeys, security keys, and device authenticators

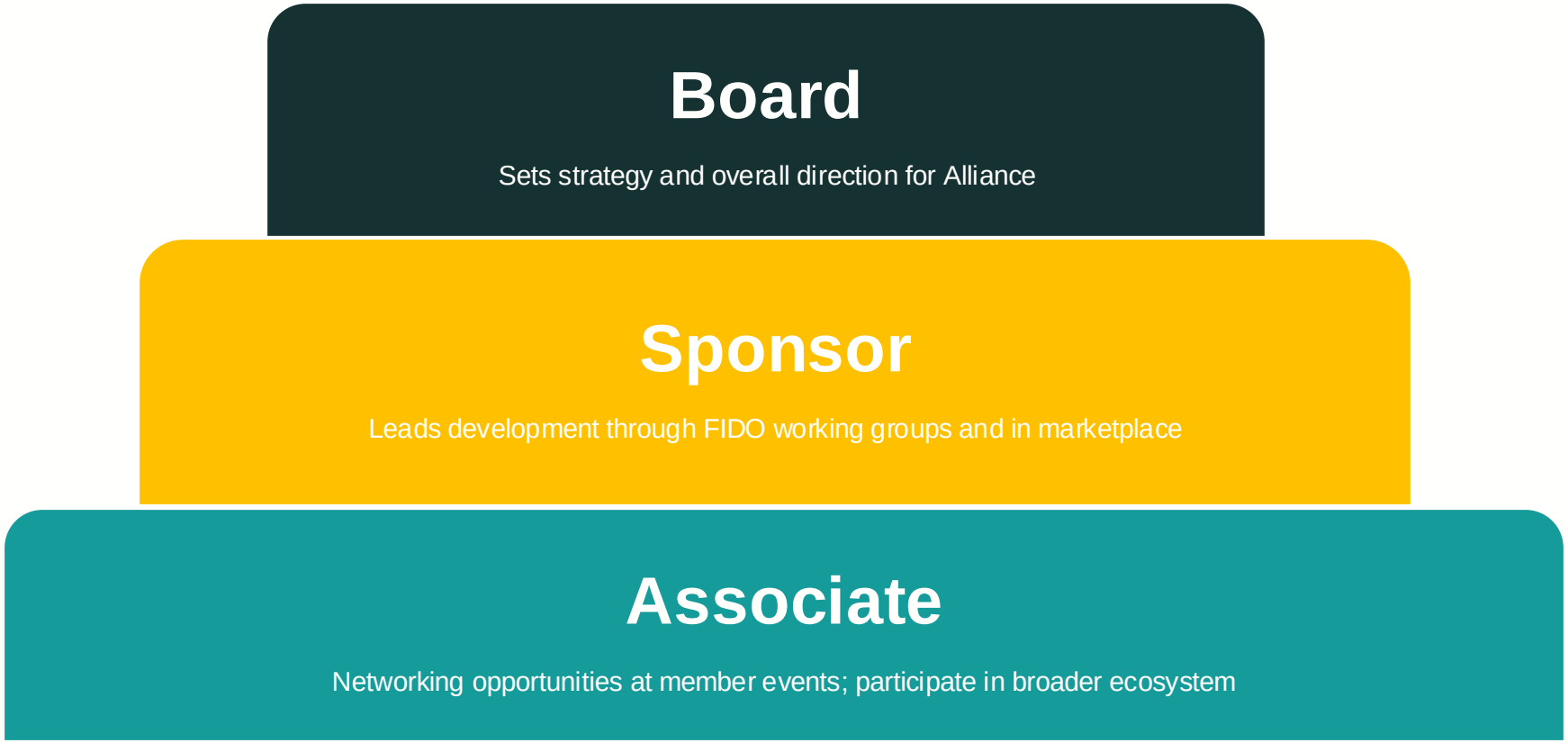


FIDO Alliance Organizational Overview

FIDO Alliance Structure



Membership Levels



Technical Working Groups

- Universal Authentication Framework (UAF)
- FIDO2
- Metadata Service (MDS)
- Device Onboarding

Individuals participating in these groups must acknowledge the IPR Promise their company agreed to when the joined FIDO

Certification-Focused Working Groups

- Security & Privacy Requirements (SPWG)
- Certification (CWG)
- Biometrics (BWG)
- Identity Verification & Binding (IDWG)

Deployment Working Groups

- Consumer Deployment (CDWG)
- Enterprise Deployment (EDWG)
- Government Deployment (GDWG)
  - US Governement Deployment Subgroup
- User Experience (UXWG)

Regional Working Groups & Forums

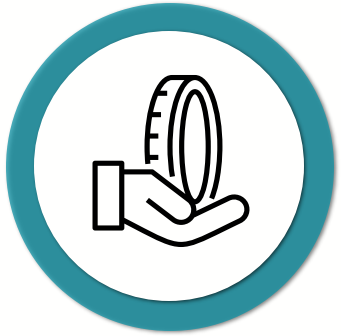
Regional Working Groups are established in strategic parts of the world to educate key stakeholders and policymakers locally

- FIDO China Working Group
- FIDO Europe Working Group
- EU ID Wallets Subgroup
- FIDO India Working Group
- FIDO Japan Working Group
- FIDO Korea Working Group
- FIDO Taiwan Engagement Forum
- APAC Marketing Forum

Special Interest Groups

- Informal member-driven group to enable companies with common interests to discuss FIDO-related matters
- Any Board/Sponsor level member can propose a SIG
- Charter must explicitly state who can/can’t participate
- Current SIGs are:
  - Financial Services SIG
  - Credential Provider SIG

Web Payments Security Interest Group (WP-SIG)



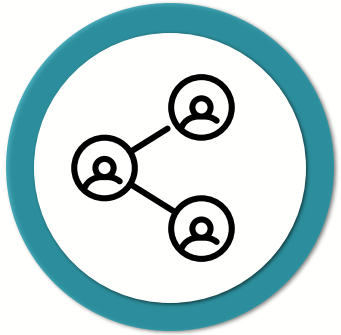
- Co-led by W3C, FIDO and EMVCo
- Administered by W3C - option to request to join as FIDO member on Causeway

Established to enable all three groups to talk under the same confidentiality arrangement about matters related to secure web payments

Membership benefits

Influence

Early Visibility



Peer-based Networking

Gain Insights

Drive Regional Adoption

Establish Best Practices

Engage on Policy Issues

Reduce Certification Fees

Working Closer with FIDO Alliance

- Develop and share best practices with other experts from peer organizations
- Bring technical, policy and business requirements to FIDO stakeholders
- Showcase your company’s thought leadership
- Take part in FIDO market development programs

Additional resources

Membership benefits:
More info

Email:
info@fidoalliance.org

Twitter:
@FIDOAlliance

LinkedIn:
linkedin.com/company/the-fido-alliance

Andrew Shikiar
Executive Director & CEO

andrew@fidoalliance.org
+1-310-489-3159

Thank you