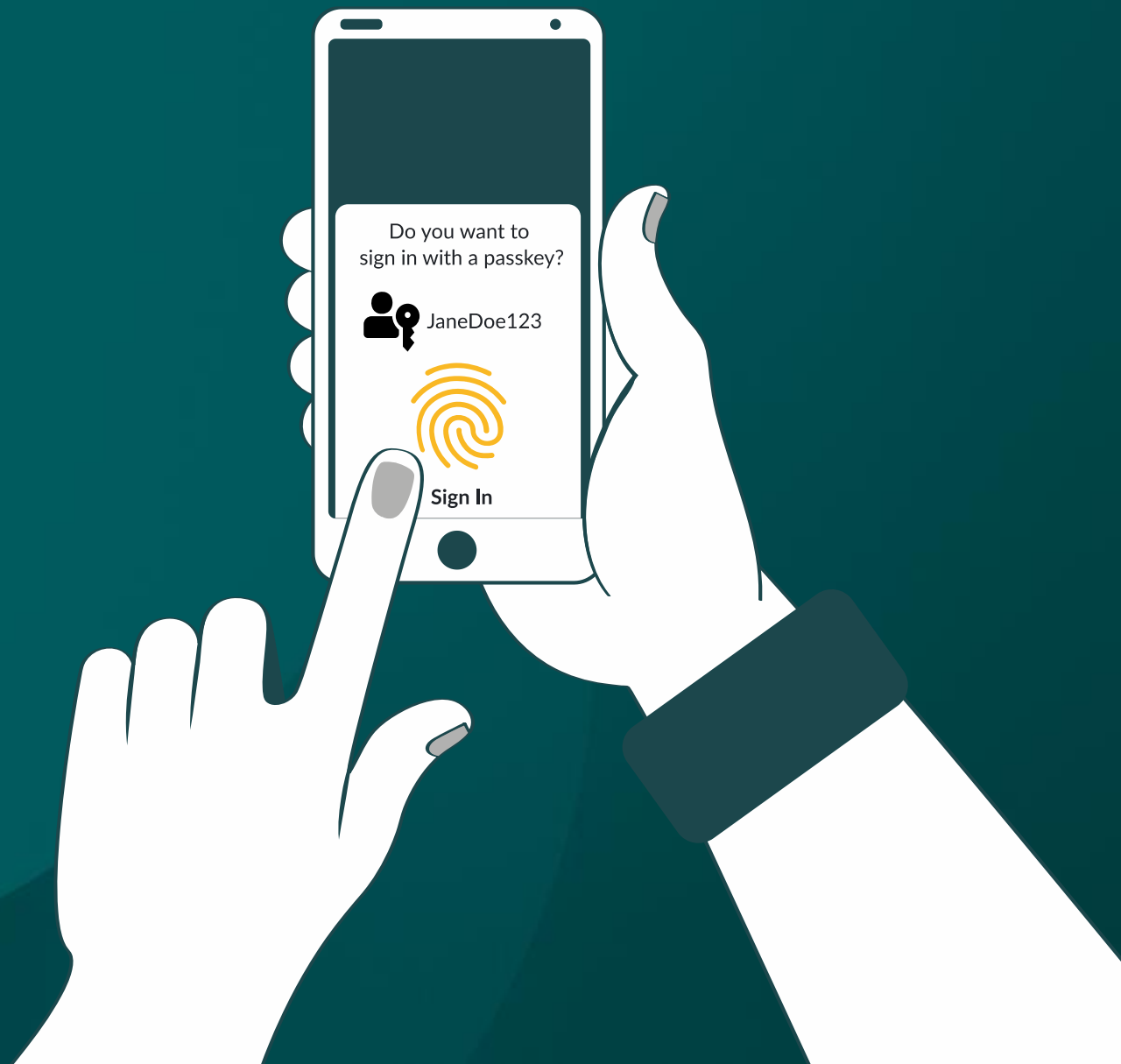


# FIDO Alliance Overview

**Andrew Shikiar**

Executive Director & CEO

March 2025



# What is the FIDO Alliance?



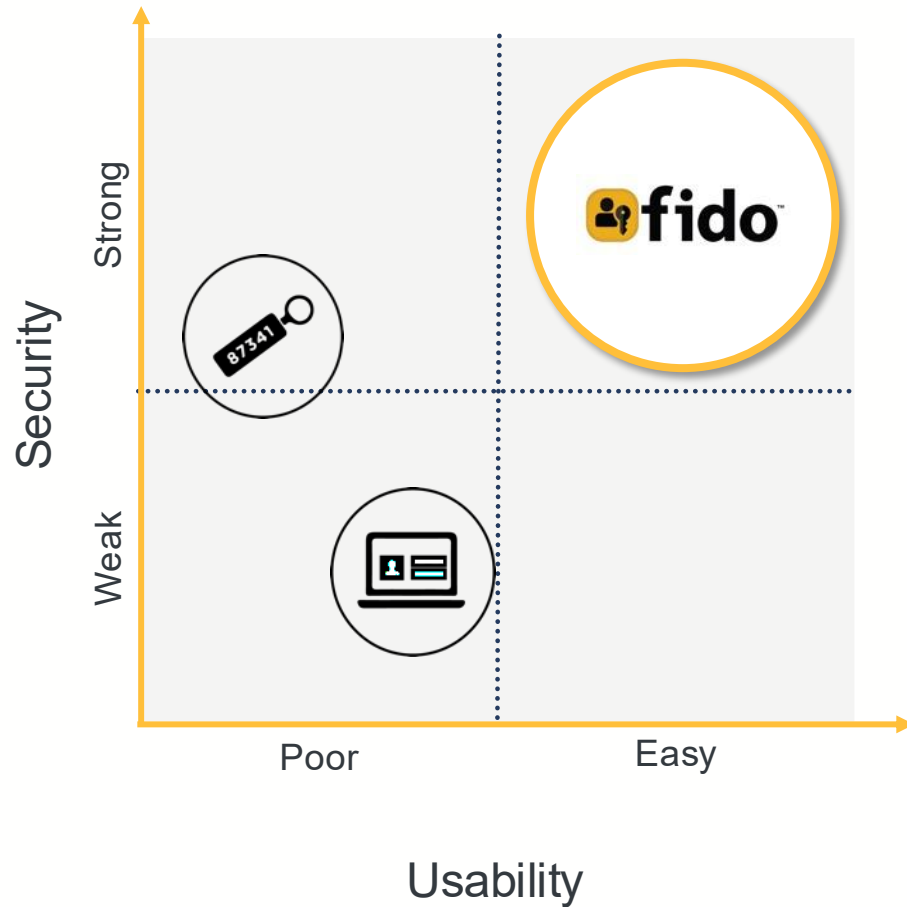
The FIDO Alliance is an open industry association with a focused mission: **reduce the world's reliance on passwords.**

# Backed by 300+ 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 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...

77%

Hacking-related breaches  
involve stolen credentials  
(Verizon)

42%

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)

78%

Use the same password for  
more than one account  
(Forbes)

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

**New Microsoft 2FA Bypass Attack  
Warning – Dangerous and Sneaky, Act  
Now**

**Forbes**

**‘Adversary in the middle attacks’ are  
becoming hackers’ go-to method to  
bypass MFA**

**ITPro.**

**MFA bypass becomes a critical security  
issue as ransomware tactics advance**

 **HELPNETSECURITY**

**Poor MFA, identity attacks dominate  
threat landscape in Q3 2024**

 **MEDIA**

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

# Generative AI adds fuel to the phishing fire

As threat actors target victims faster and more efficiently than ever before

703%

Credential phishing attacks  
rose in H2 of 2024  
(Slashnext)

53%

of consumers reported more  
suspicious messages and  
online scams in 2024  
(FIDO Alliance)

35%

Increase in identity-related  
cloud incidents in 2024 vs 2023  
(Crowdstrike)

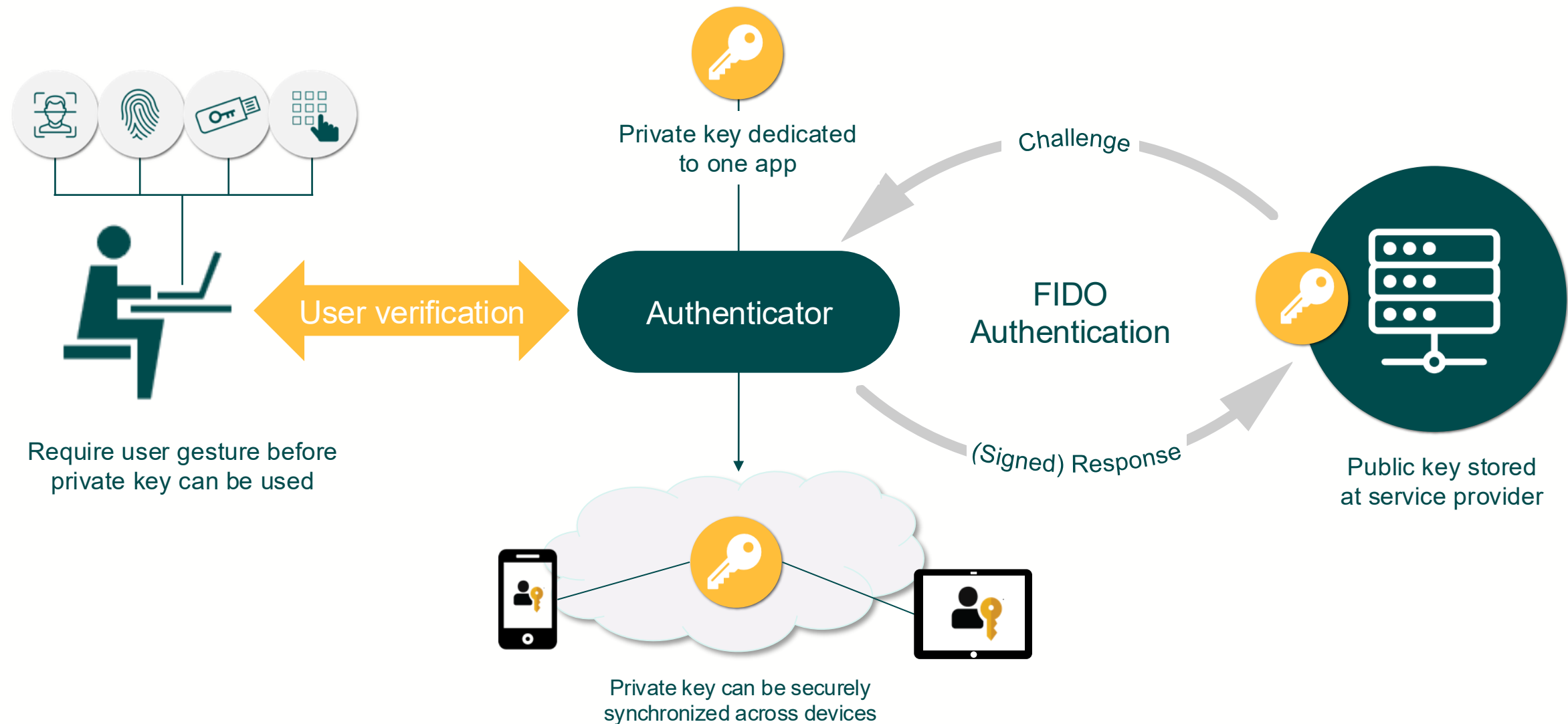
4151%

Rise in malicious phishing  
emails since Q4 2022 &  
ChatGPT  
(SlashNext)

Easily phished or socially engineered, difficult to use and maintain



# Phishing-Resistant Authentication with Passkeys



Chrome on Windows



Firefox on Windows

Chrome on Android

Edge on Android

Apps on iOS



**Available**



Safari on iOS

Chrome on Mac

Edge on Mac

Edge on Ubuntu



Chrome on iOS

Edge on iOS

Apps on Mac

**Today!**

Apps on Android

Chrome on Ubuntu

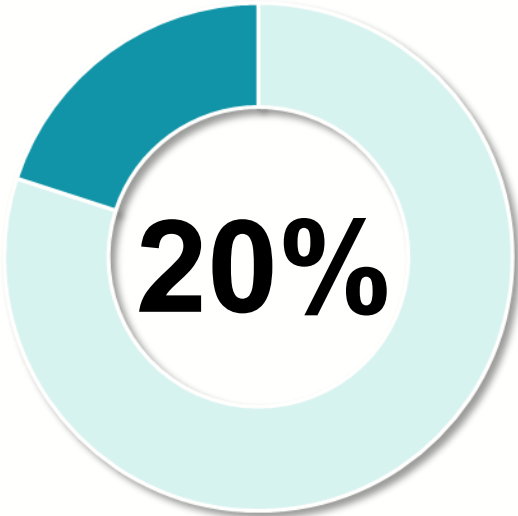
Safari on Mac



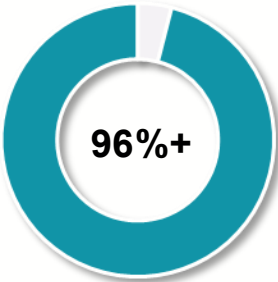
Edge on Windows

# Passkey adoption by the numbers

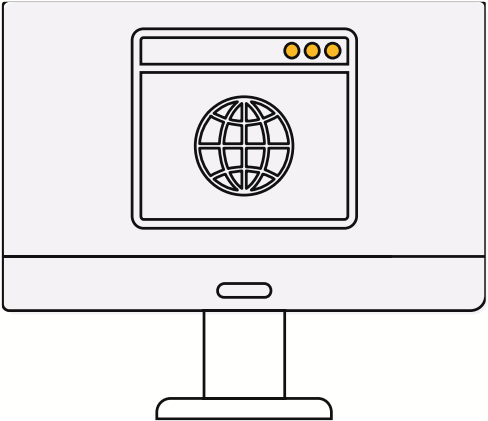
(Since October 2022)



of the world's top  
100 websites and services

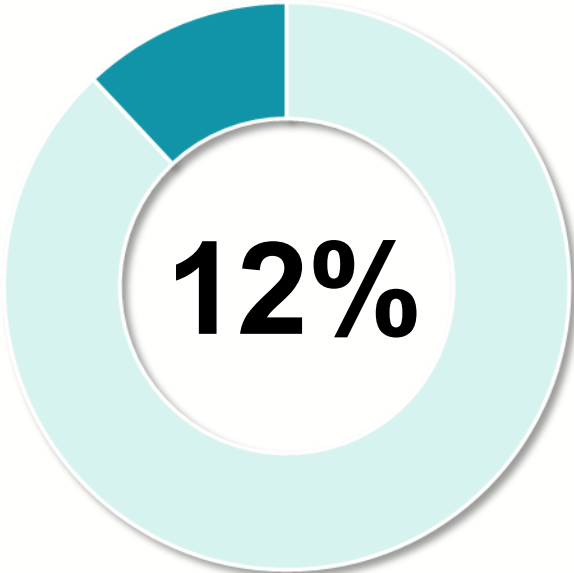


of active  
browsers

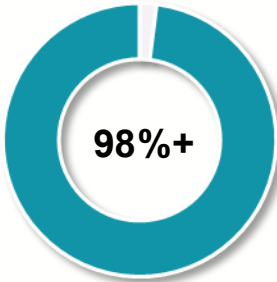


More  
than **15B**

accounts can now leverage  
passkeys for sign in



of the world's top  
250 websites and services



of mobile  
devices

# Adoption Snapshots

## Consumer



PlayStation®



## Enterprise



DocuSign



T Mobile

## Government





## **Certification unlocks the value of open standards**

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

### **Conformance-oriented testing:**

- Ensures products adhere to specifications
- Promotes ecosystem interoperability

### **Performance-oriented testing:**

- Measures strength of biometric capabilities
- Validates performance and compliance with companion security programs
- Complements industry testing schemes



## Certification unlocks the value of open standards

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



**1,200+ FIDO Certified products**

## FIDO Certification Programs

### User Authentication

- Functional Certification
- Authenticator Level Certification

### Biometric Components

- Biometric Component Certification

### Identity Verification

- Face Verification Certification
- Document Authenticity Certification

### Device Onboarding

- FIDO Device Onboard Certification



# Certification Business Benefits



Standardization  
for industry



Market  
differentiation



Regulatory  
compliance



Consumer &  
Enterprise protection

# FIDO's Role in Government Policy



FIDO specifications offer governments newer, better options for strong authentication...

---

...but governments have had to update some policies to support the ways in which FIDO is different.

As technology evolves,  
policy needs to  
evolve with it.

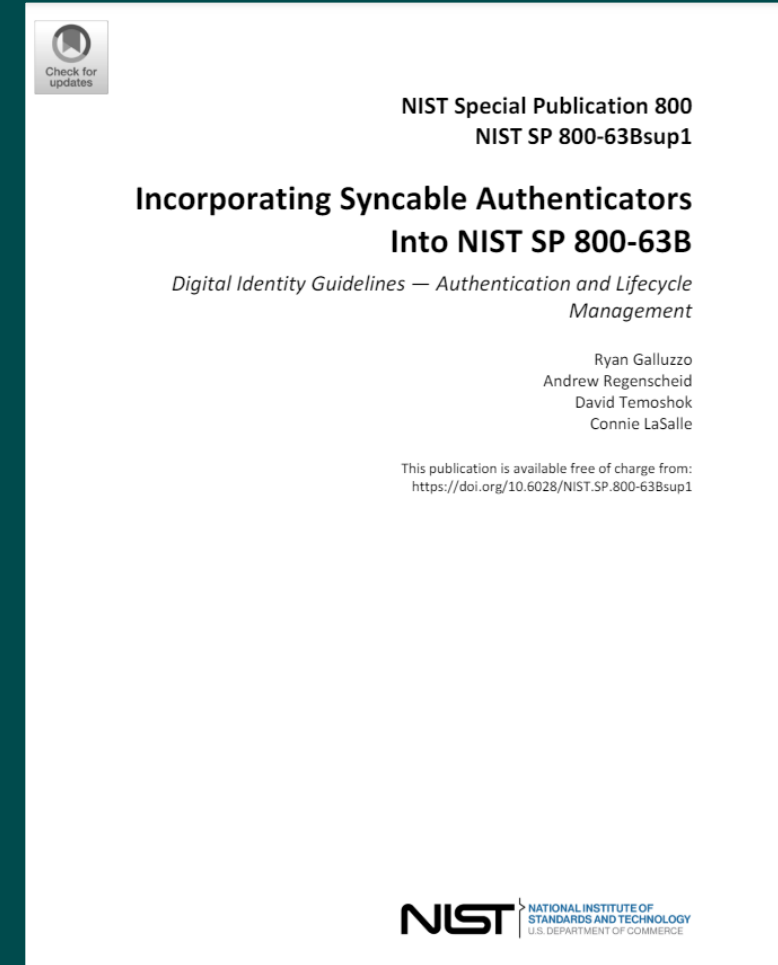




# Regulatory recognition of synced credentials

## 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

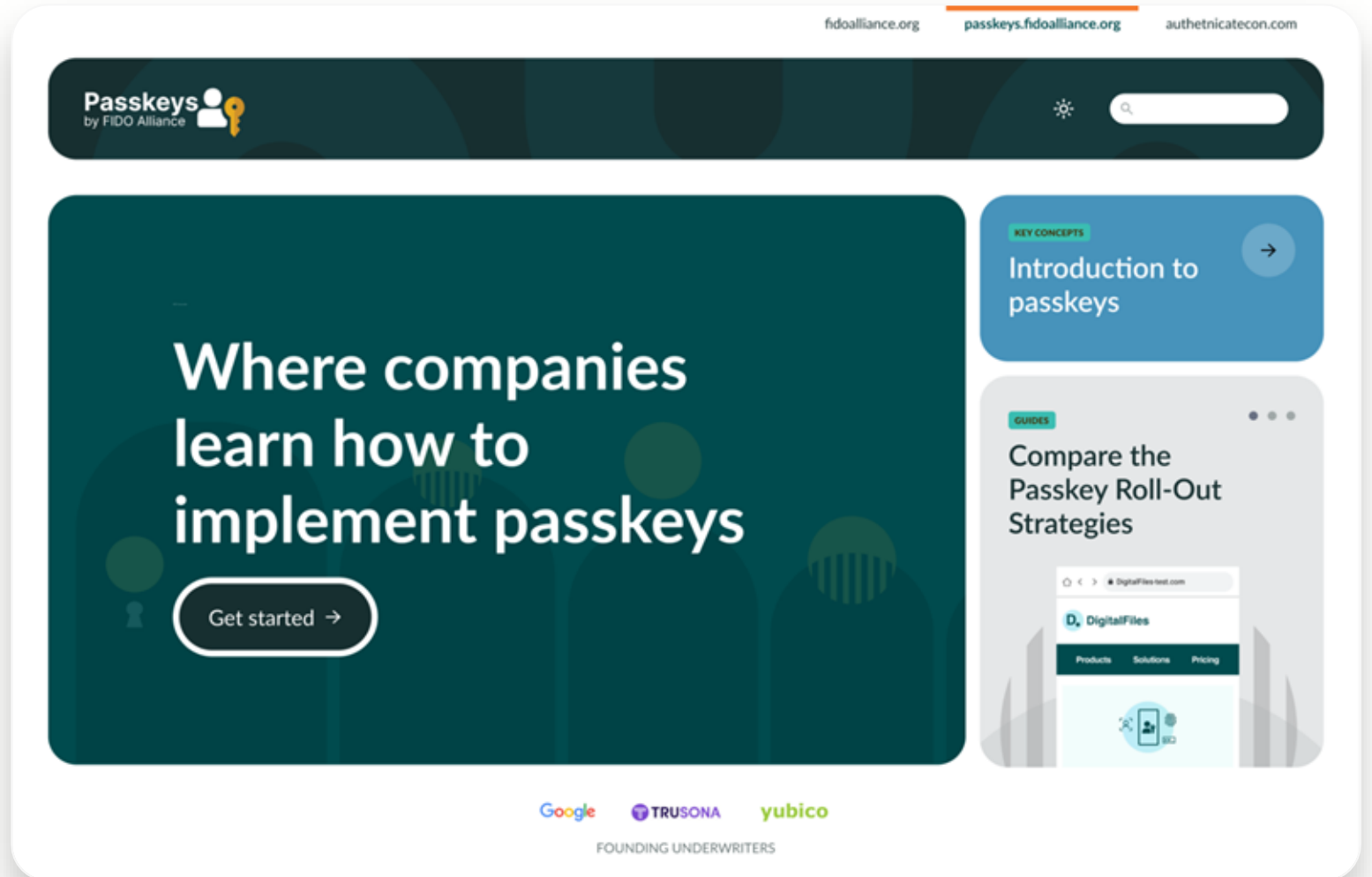
# New Resource: Passkey Central

## The #1 global resource for passkeys:

- Trusted
- High traffic
- Authoritative
- Comprehensive
- Content not found elsewhere

## By the numbers

- Available in four languages
- 60+ pages of cohesive content
- Dozens of new infographics
- Helpful downloads like Cost Worksheets and sample slide decks for RPs
- End-to-end deployment guides



Visit <https://passkeycentral.org>

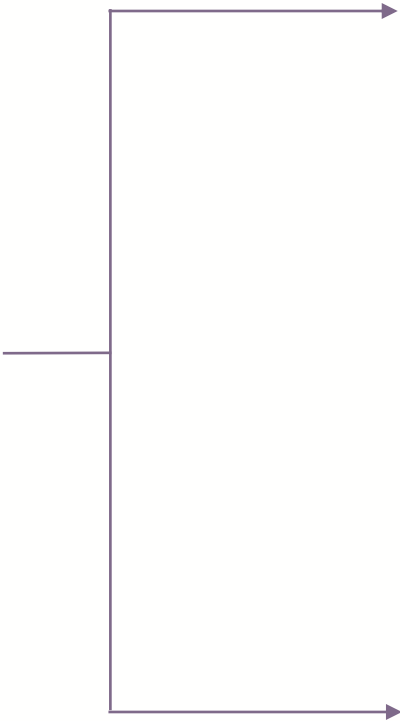
# FIDO Alliance Organizational Overview



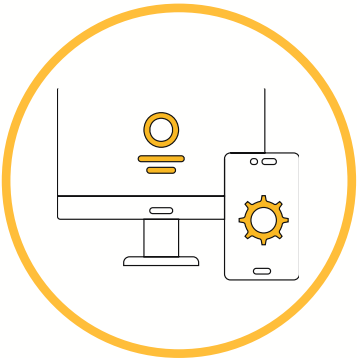
# FIDO Alliance Structure



Membership  
Levels



Technical  
Workstreams



Marketing & Adoption  
Workstreams

# Membership Levels

## Board

Sets strategy and overall direction for Alliance

## Sponsor

Leads development through FIDO working groups and in marketplace

## Associate

Networking opportunities at member events; participate in broader ecosystem

# 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 they 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 Government Deployment Subgroup
- User Experience (UXWG)
- Payments Working Group (PWG) 



# 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

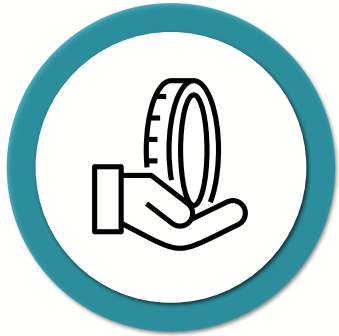
# Special Interest Groups

- 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
  - Large RP SIG
  - Hardware Security Key SIG
  - Automotive SIG

# Study Groups / Committees

- Study Groups and Committees are formed within FIDO Alliance from time to time to tackle key topics and/or to inform long-term strategy
- Current examples include:
  - Trust Signals Study Group
  - RP Deployment Trends Committee
  - Digital Credentials Committee

# 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

# Participation, Marketing and Commercial Benefits

	Board	Sponsor	Government	Associate
Sets the strategic direction of the Alliance	✓			
May contribute to specification requirements & development	✓	✓	✓	
May participate in WGs	✓	✓	✓	
May take advantage of member-only co-marketing opportunities	✓	✓	✓	✓
Eligible for FIDO certification discounts and promotional activities	✓	✓	✓	✓
Eligible for discounts on event sponsorships	✓	✓	✓	✓
May attend and participate in any plenary meeting	✓	✓	✓	✓

# Get Involved with FIDO Alliance to...

-  Develop and share best practices with other experts from peer organizations
-  Bring technical, policy and business requirements to FIDO specifications & initiatives
-  Showcase your company's thought leadership
-  Take part in FIDO Alliance's worldwide market development programs
-  Receive discounts and co-marketing support for FIDO Certification

# Additional resources

## Membership benefits:

[More info](#)

## Email:

[info@fidoalliance.org](mailto:info@fidoalliance.org)

## Twitter:

[@FIDOAlliance](https://twitter.com/FIDOAlliance)

## LinkedIn:

[linkedin.com/company/the-fido-alliance](https://linkedin.com/company/the-fido-alliance)



---

## Andrew Shikiar

Executive Director & CEO

---

[andrew@fidoalliance.org](mailto:andrew@fidoalliance.org)

+1-310-489-3159

# Thank you