Utilising FIDO technologies effectively

David Tharm

Wed 2 June, 2021

Giesecke+Devrient
Creating Confidence

Utilising FIDO technologies effectively

FIDO Authentication is the Answer

To the World's Password Problem

- FIDO Alliance

1. *Why is FIDO the Answer to the Password Problem?*
2. *How is FIDO different to other "shared secret" based multi-factor authentication (MFA) solutions?*
3. *What can FIDO technologies be used for ?*

Key Benefits of FIDO

Security
- Based on public key cryptography, not shared secret
- Credentials and biometric data never leave the device, never stored online
- Eliminates risks of phishing, password management & vulnerabilities and replay attacks

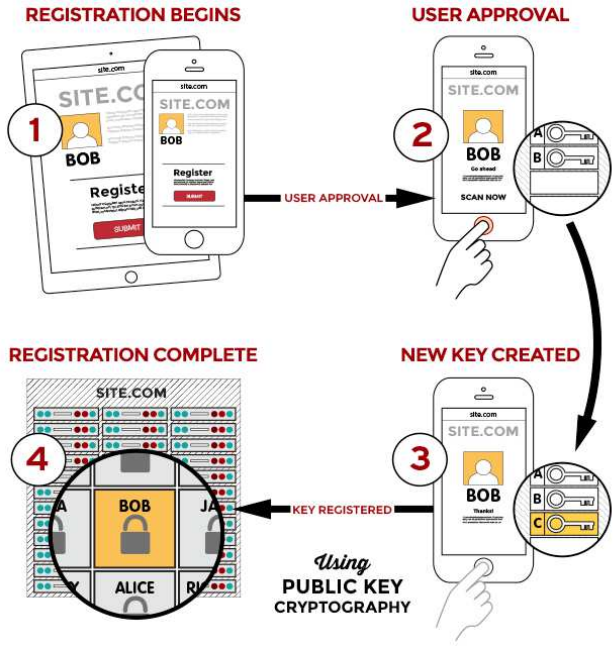
Privacy
- Keys are unique for each online site access
- Keys cannot be used to track users across different sites (cannot be reused, replayed, or shared across services)
- User privacy is strictly protected

Convenience
- Simple to use, easy to deploy and manage
- Works across mobile platforms and leading browsers

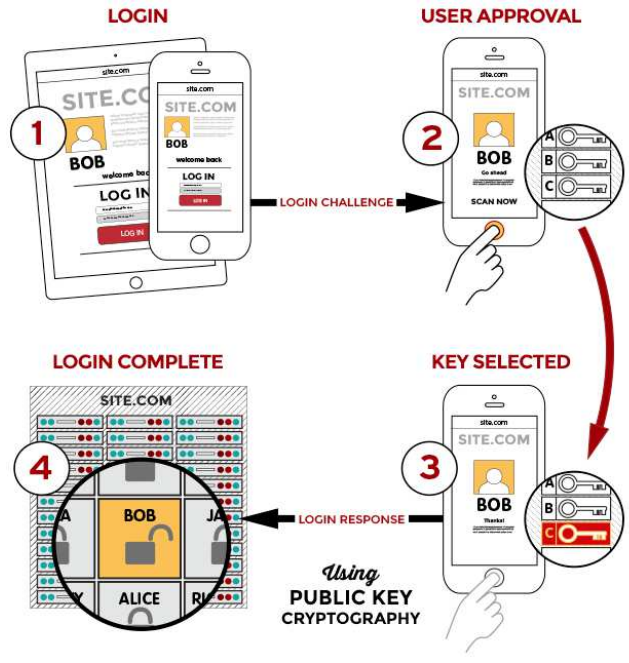
Scalability & Interoperability
- Supported across leading browsers, consumer mobile devices and desktops
- Future proof / No vendor lock-in
- **Standardised framework for building additional functionality**

Source: https://fidoalliance.org

FIDO Explained



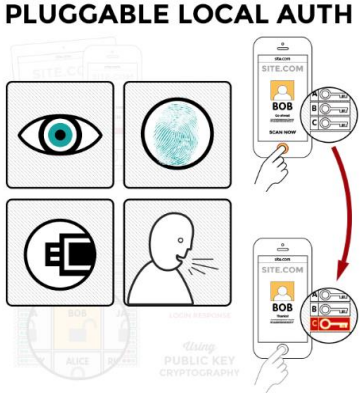
FIDO Registration

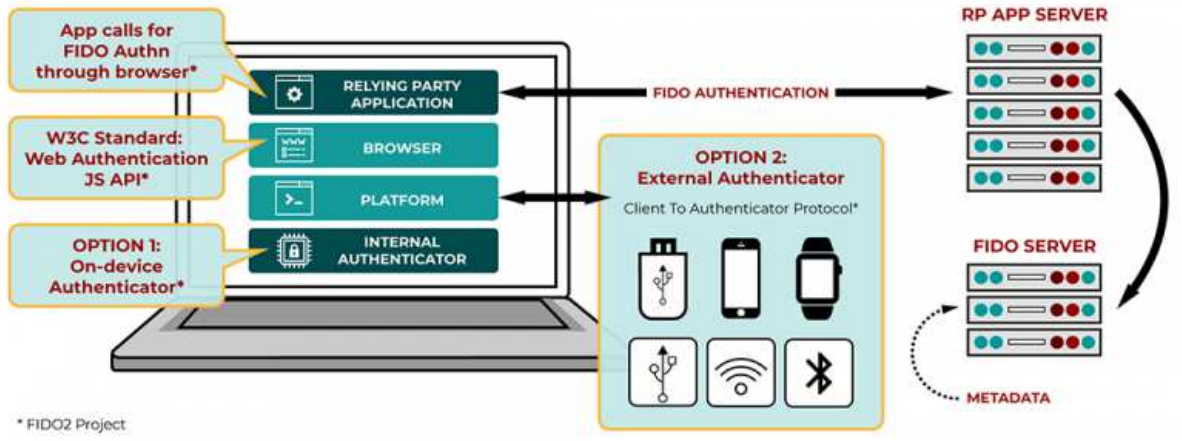


FIDO Authentication

Source: https://fidoalliance.org

FIDO Overview





User Gesture

- User Presence (touch, swipe, etc)
- User Verification (PIN, biometrics, etc)

Authenticator concept

- Multiple keys, multiple usernames per authenticator
- Unique triplet / tuple: (username, RP origin, authenticator) must be unique

Authenticator Types (wrt keys)

- Internal / Bound / Platform Authenticators
  - Software based - eg. WBC + device biometrics
  - Hardware based - TEE, TPM, Secure Enclave, eSE, etc
- External / Roaming / Cross-platform Authenticators
  - Hardware based security key - smartcard, usb token, key fob
  - User Devices – mobile phone, smartwatch, etc

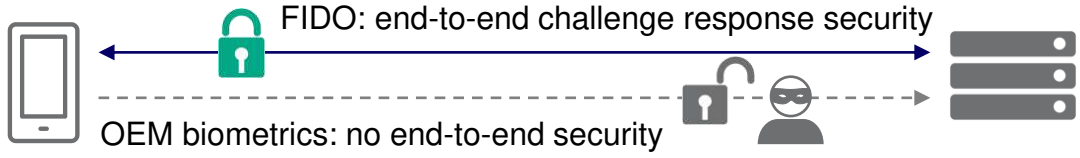
Source: https://fidoalliance.org

Current Pain Points: Usability vs. Security vs. Costs

Solution	Security	Compliance	Usability	Costs
Passwords	↓	↓	↓	↑
OTP lists	↓	↓	→	↑
SMS OTP	↓	→	→	→
OTP token	↑	↓	→	↓
OTP generator	↑	↑	→	↓
Mobile biometrics	↑	↑	↑	↑

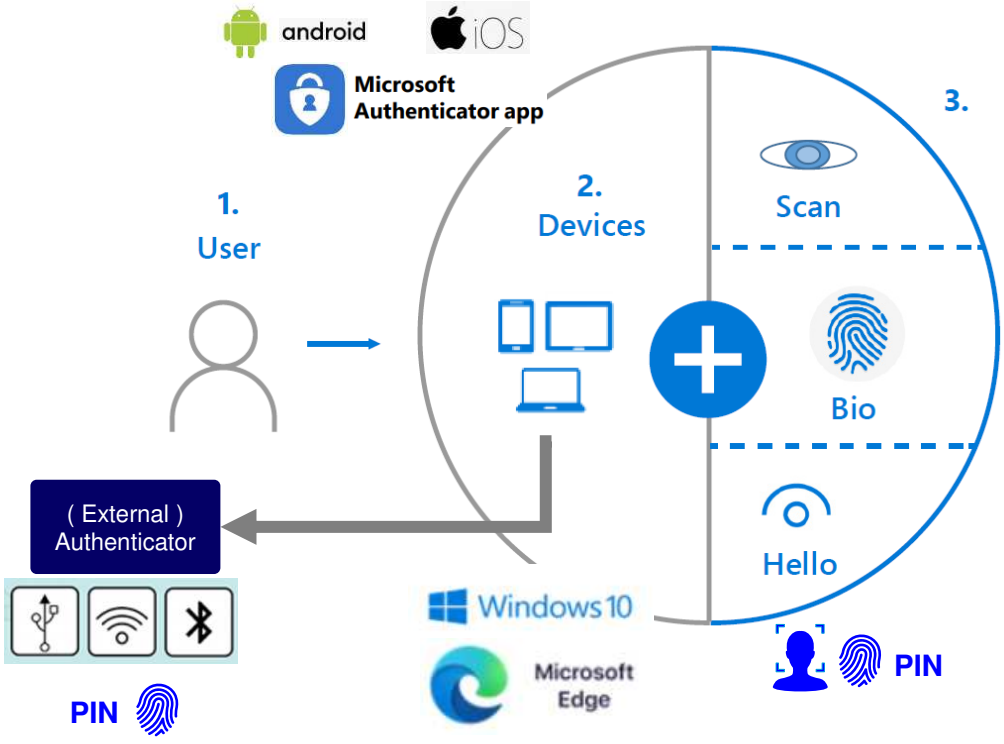
FIDO based mobile biometrics solution offers the best balance of security, compliance, usability and costs

…but we are doing (OEM) biometrics already. So what's the point?



	OEM biometrics	Basic C/R- protocol	FIDO biometrics
Local user verification	✓	✓	✓
Two-factor authentication		✓	✓
End-to-end protocol security		?	✓
Authenticator attestation			✓
Authenticator policy enforcement			✓
Modularity/flexibility of authenticators			✓
Cross-component/cross-industry interoperability			✓
External certification of security and interoperability			✓
3DS2.0 compliance/integration			✓

Enterprise use case - Microsoft moves to passwordless



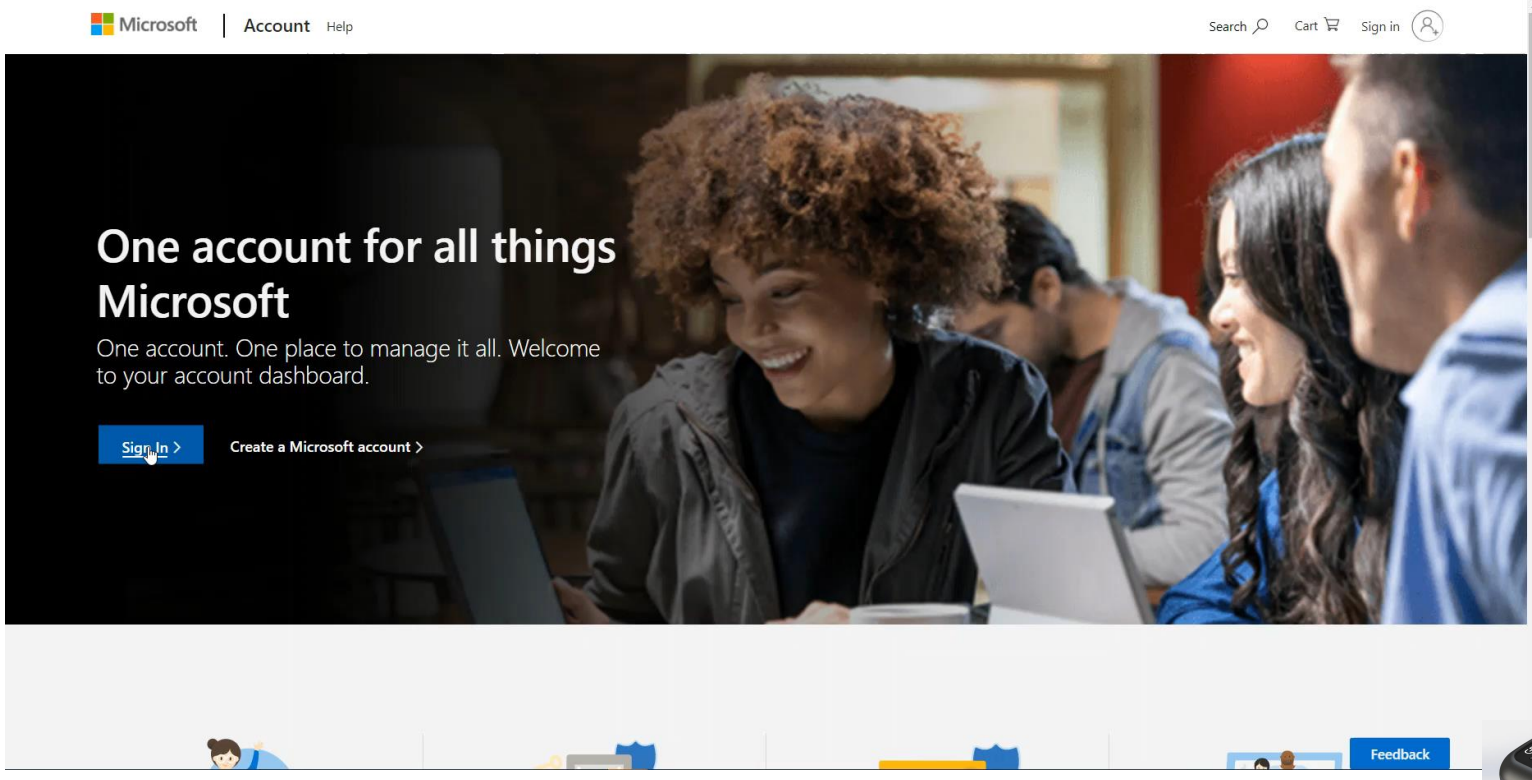
"Azure AD manages more than **1.2 billion identities** and processes over **8 billion authentications** every day." – MS Azure website

"Don't let perfection stand in the way of progress. Every step toward passwordless is a step toward improving your security posture."

- Bret Arsenault, CISO for Microsoft

Based on diagram from: Whitepaper "Password-less protection", Microsoft

Microsoft FIDO2 account sign in via Bluetooth – passwordless & nameless!

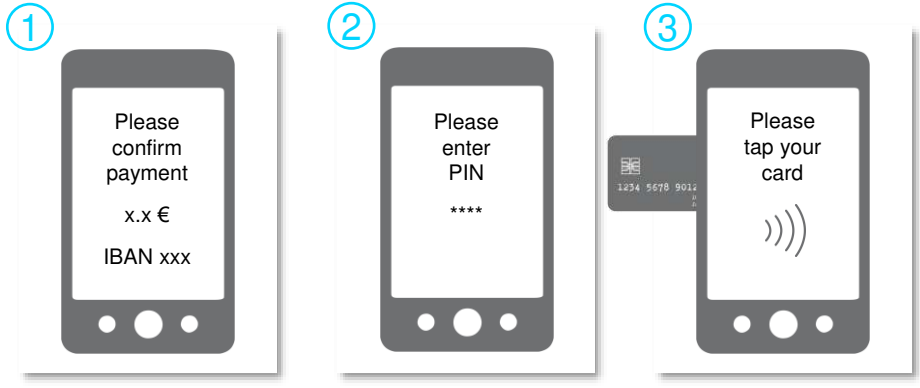


More about this device later …

FIDO in Payment Use Case

Using EMV Card as secure FIDO Authenticator

Convego®tap



Registration

1. User defines own PIN/PW (knowledge factor)
2. User taps EMV card against NFC phone (Android)

Authentication/Transactions

1. Transaction data is displayed (or Login request)
2. User enters own PIN/PW (knowledge factor)
3. User taps EMV card against NFC phone (Android)

Typical use cases

- 2FA for high-value transactions
- App-onboarding of known customer
- Card activation (proof of possession)

Combining FIDO with other authentication standards

G+D Biometric Key Fob

Security at your fingertips:

Efficient, flexible and high security solution to protect your enterprise assets

Physical Access Control

Mobile Payment

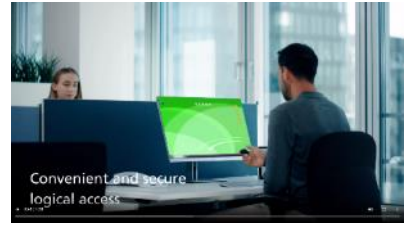
NFC

G+D Mobile Security

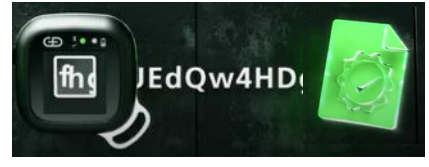
StarSign® Key Fob

Secure Authentication Mobile

Secure Authentication PC



Encryption/Signing



Key Takeaways

1. *The Password "shared secret" Problem is fundamentally solved by the FIDO "public key cryptography" framework*
2. *FIDO authentication provides the optimal approach to enable strong passwordless MFA*
3. *FIDO can be integrated or combined with other technologies to simplify user experience and to provide a strong frictionless user journey*

www.gi-de.com
www.twitter.com/GI_DE_com
www.gi-de.com/youtube
www.linkedin.com/company/giesecke-&-devrient

Password has long passed its "use-by date",
let's get rid of it wherever we can
Use a strong authentication like FIDO
to make our world a simpler and safer place
- DavidT

Wed 2 June, 2021

Thank you

Giesecke+Devrient
Creating Confidence