Microsoft

eiC 2018
12TH EUROPEAN IDENTITY & CLOUD CONFERENCE

Deprecating the Password: A Progress Report

Dr. Michael B. Jones
Identity Standards Architect, Microsoft
May 17, 2018

The password problem

Alpha-numeric passwords are hard for humans to remember and easy for computers to guess

On mobile devices entering passwords is hideous

Credential reuse across multiple services increases attack surfaces

Even the strongest passwords are easily phishable

Nobody likes passwords

Quantifying the Problem

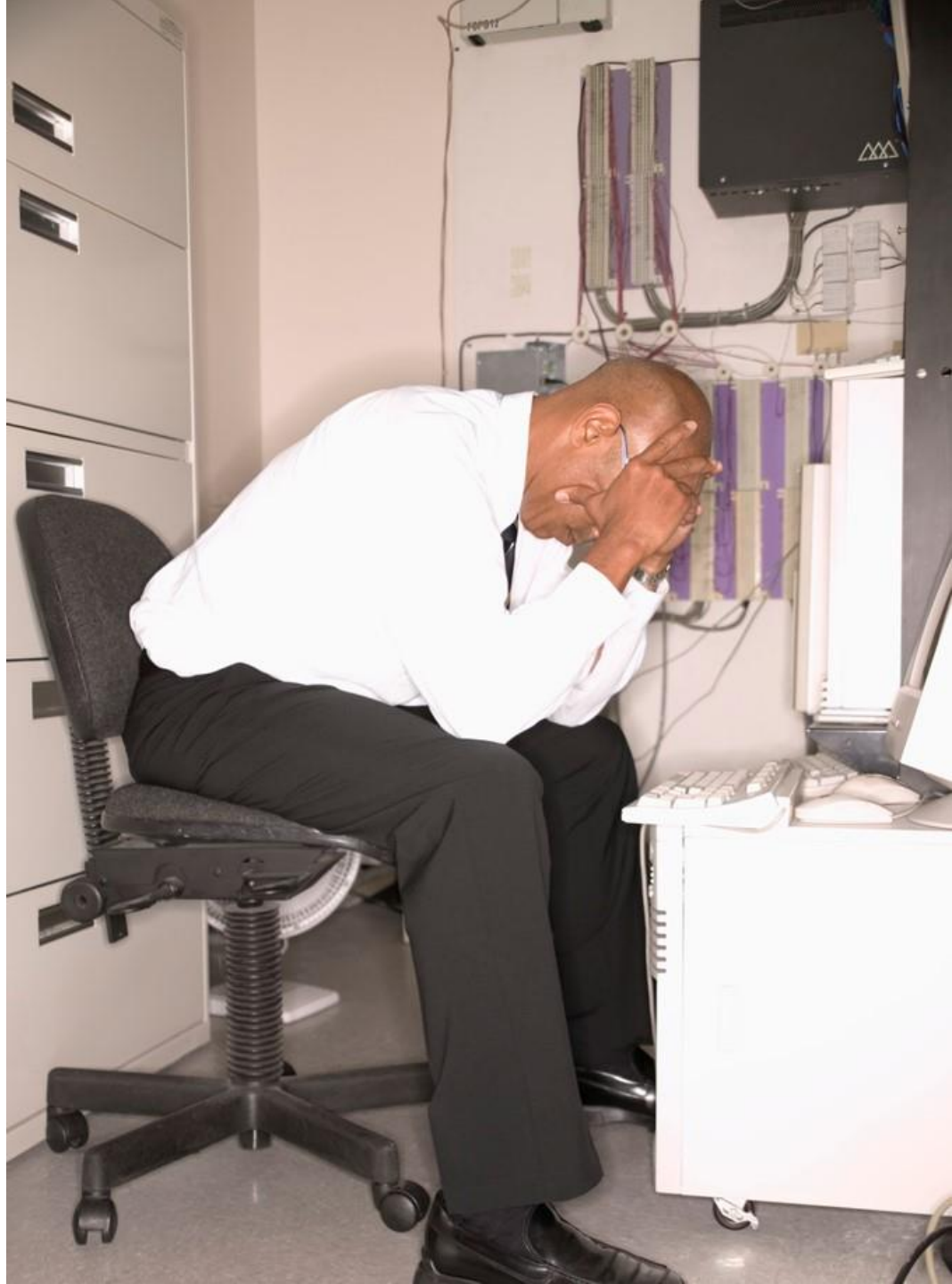
#1 cost for Enterprise IT departments

81% of data breaches in 2016 involved weak, default, or stolen passwords[1]

1 in **14** phishing attacks were successful in 2016[1]

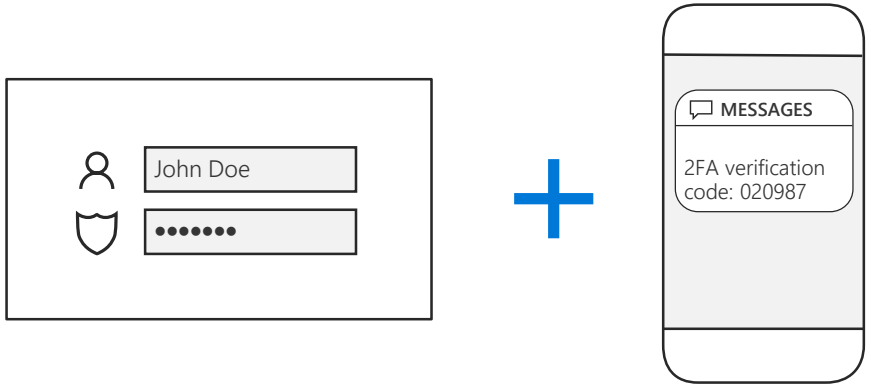
1,579 breaches in 2017, a **45%** increase over 2016[2]

[1] Verizon 2017 Data Breach Report
[2] Theft Resource Center 2017



Nobody likes passwords

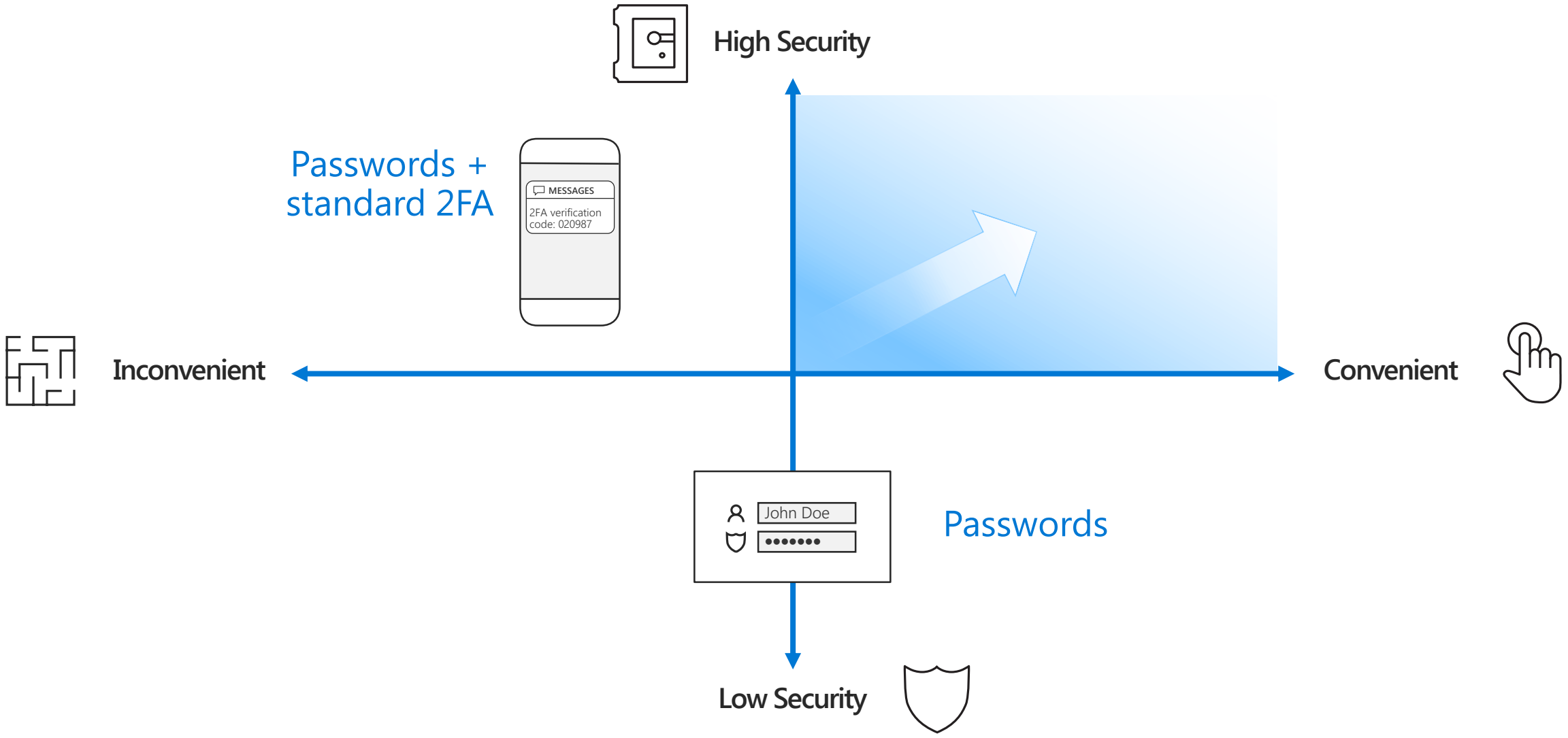
Passwords + 2FA is more secure, but also more complicated and difficult to use



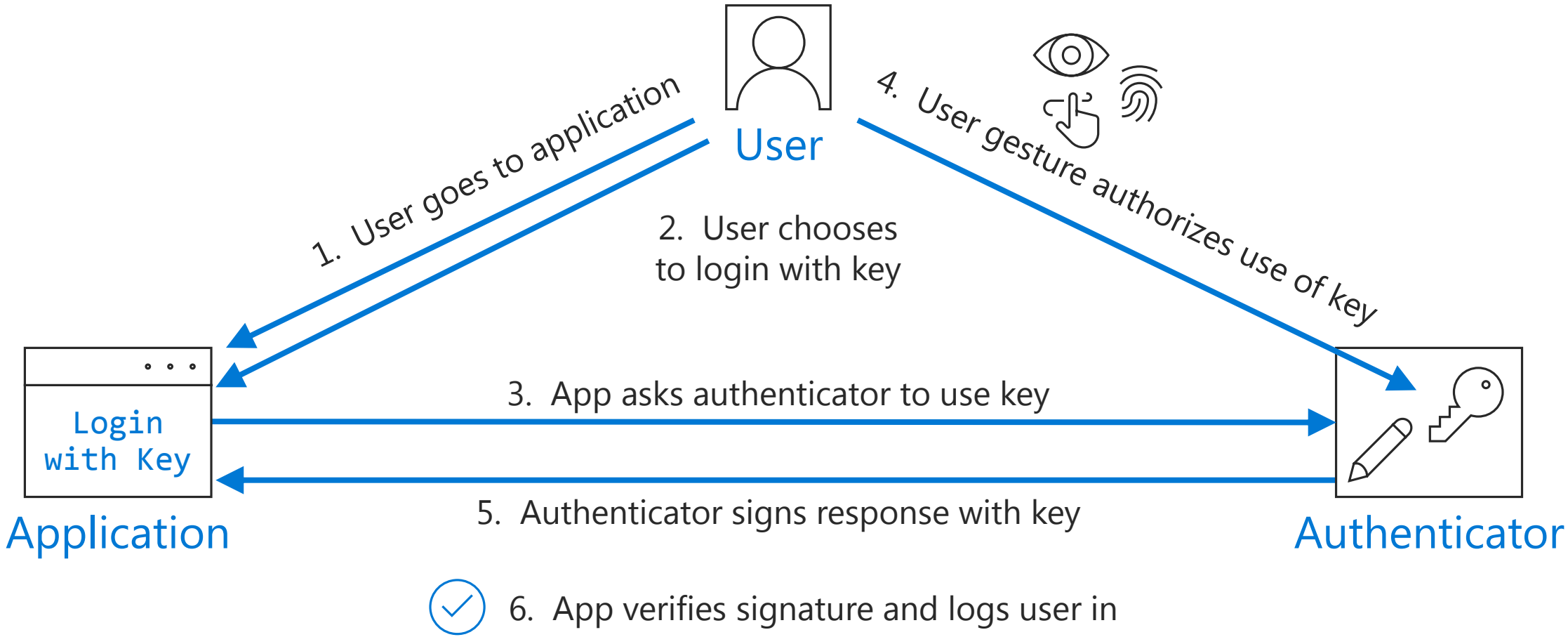
Passwords

2FA

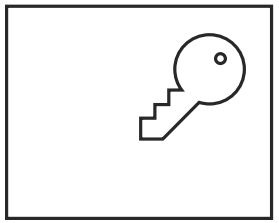
The search for better



The password alternative: Logging in using an asymmetric key

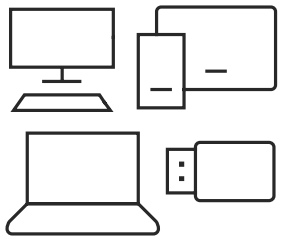


What's an authenticator?



An authenticator is an abstraction that

- Can securely use private keys for authentication
- Will only use those keys when prompted by a user gesture



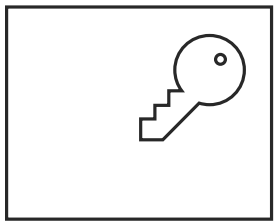
What kinds of places might keys for an authenticator be?

- TPM on laptop
- Secure element on phone
- Storage on connected authenticator device
- Encrypted by the authenticator and held elsewhere for it

What kinds of user gestures might prompt user of keys?

- Biometric
- PIN
- Touch

What's strong about using an authenticator?



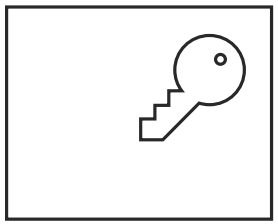
Authenticators

Don't expose any secrets like passwords that can be stolen or guessed

Keep a pairwise private key private and sign with it – providing proof of possession

Only use the key when authorized by a user gesture

What's simple about using an authenticator?



Authenticators

- Remember the key pair for you
  - instead of you remembering a password
- Use a single gesture from you, such as matching your face
  - instead of you having to type a password

The standards making it possible

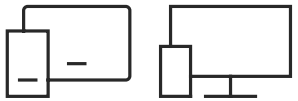
W3C Web Authentication (WebAuthn)

Enables sign-in with methods stronger than passwords
with authenticators using securely held private keys
that use the private key only with user permission
which is given to the authenticator with a user gesture
such as a biometric or PIN.

FIDO 2 Client to Authenticator Protocol (CTAP)

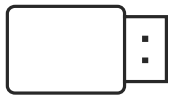
Can be used with WebAuthn
to enable use of remote authenticators
such as those on mobile phones or connected devices
to be used when signing in.

The devices making it possible



Phones and PCs w/ biometric authentication

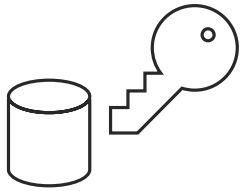
Face, fingerprint, iris, etc.



External authenticator devices

Second factor devices commonly available

Prototype first factor devices being tested



Secure key storage

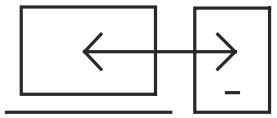
Trusted Platform Modules (TPMs)

Trusted Execution Environments (TEEs)

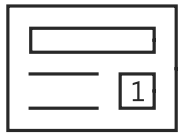
Secure Elements (SEs)

We increasingly have devices well-suited for use as authenticators!

Is WebAuthn for the first or second factor?

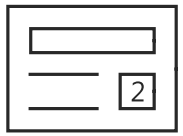


It is for both use cases



When first factor, user is logged in directly using authenticator

Requires that the user gesture be specific to the user



When second factor, authenticator augments first factor

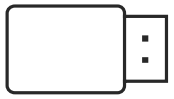
The first factor is often a traditional username/password

The second factor tests user presence, but need not be user-specific

This is the way that existing U2F devices are used

Example first factor user experience

Using a FIDO2 authenticator to sign into an Azure Active Directory account on Windows



The authenticator is the USB device

The user gesture used is providing a fingerprint

- Could also be facial recognition or a PIN

Demo

fido2

Password-less authentication


Welcome! Use your security key to sign in.
12:01
Saturday, April 14

Password-less authentication

What did you just see?

FIDO2 authenticator signing in to Windows April 2018 update

Improves user experience because there's no password

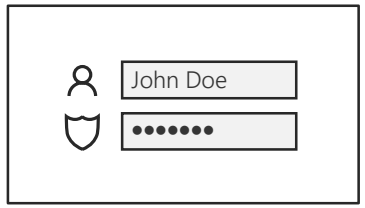
Why is it more secure?

Combines something you have with something you are (or something you know, in the PIN case)

Biometric unlocks the private key on the TPM, then that private key is used to sign for the cloud

Authenticator connects to platform through USB, a physical transport, establishing physical presence

Example second factor user experience

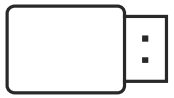


Provide first factor with username and password

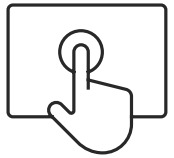
Same as it ever was

Use Yubico YubiKey as second factor for a Google account

This is using the FIDO U2F protocol predating WebAuthn and FIDO 2



The authenticator is attached by a USB port



The user gesture is touching a capacitive touch sensor

Note that this is not user-specific, since anyone could successfully touch it

You've seen this before so I'm not showing it here again today

Standards status

W3C Web Authentication (WebAuthn) achieved Candidate Recommendation (CR) in March 2018

http://www.w3.org/TR/2018/CR-webauthn-20180320/

Support by Chrome, Firefox, and Edge demonstrated at 2018 RSA Conference

Interop tested among multiple browser and authenticator vendors

FIDO 2 Client to Authenticator Protocol (CTAP) achieved Review Draft 4 (RD4) in March 2018

https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html

Progressing in parallel with W3C WebAuthn

FIDO board voted to make RD4 publicly available as an Implementation Draft

Interop tested among multiple browser and authenticator vendors

Demo participants at April 2018 RSA Conference

Web Browsers

Websites/Servers

nok nok

PayPal

Biometrics

Windows Hello

Security Key

yubico

Key takeaways

There are good alternatives to passwords in use today
Passwords are being used for fewer and fewer identity interactions
Devices are increasingly enabling authentication without passwords
New standards are enabling cross-platform password-less authentication

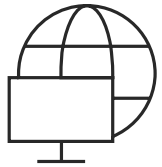
---

The days of having to use passwords for everything you do are numbered!

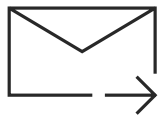
Where can I participate & learn more?

W3C Web Authentication working group
https://www.w3.org/WebAuthn/

FIDO2 Project
https://fidoalliance.org/fido2/



My blog
http://self-issued.info/



E-mail me
mbj@microsoft.com

Microsoft