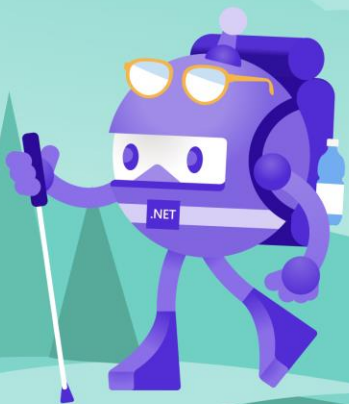


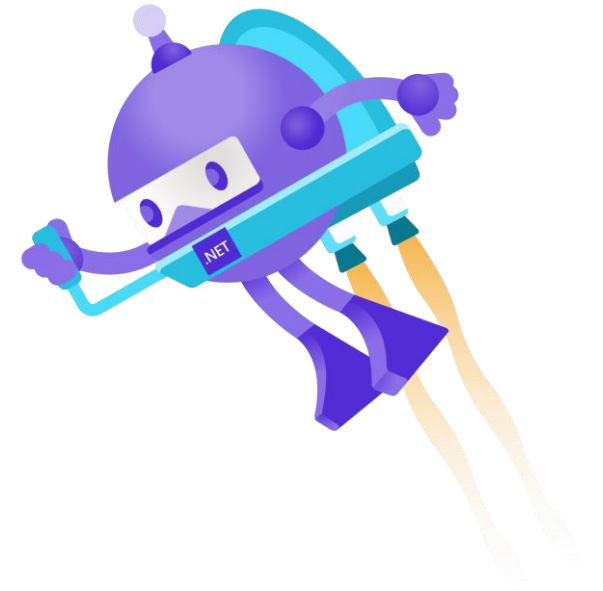
# .NET Conf

探索 .NET 新世界

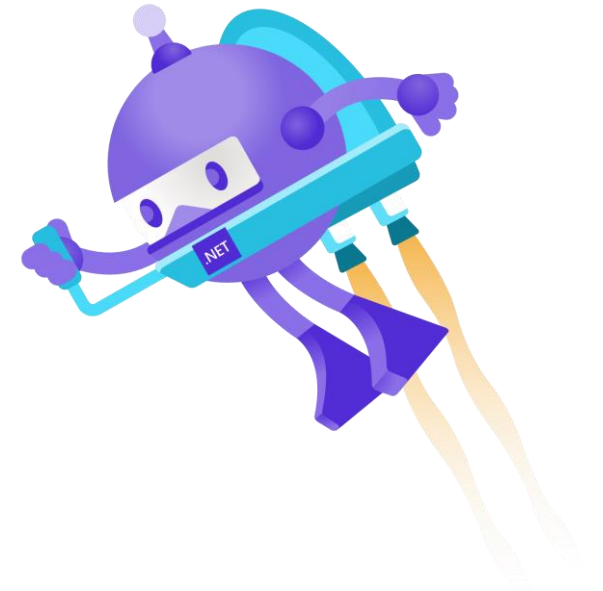


# 無碼時代終於要來了嗎

Kevin Yang



# 現況 & 問題



# 問題

- 密碼複雜度
- 需定期更換密碼
- 密碼太多記不住
- 密碼重複使用
- 網站沒有認真看待你的密碼
- 釣魚網站
- ....更多擾人的問題

# 使用者登入方式

- 帳號密碼登入
- 連結登入
- 多重要素驗證 (Two Factor Authentication)
- 第三方登入 (ex. Google, MS, Facebook, GitHub etc.)
- 無密碼登入

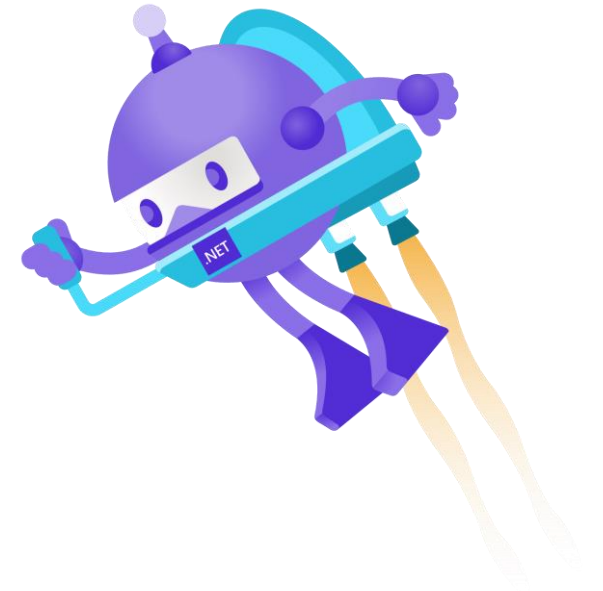
# MFA

- Multi-Factor Authentication 多重要素驗證
- 目的: 透過兩種以上的認證機制，來增加安全性
- 常見的方式
  - 簡訊
  - Email
  - 手機 App (ex. Google 身份驗證器)
  - OTP
- 問題
  - 簡訊會有收不到的問題
  - 被這一類的 Email 給淹沒

# 其他可能代替密碼的選項

- 生物辨識
  - 指紋 辨識
  - FaceID
  - Windows Hello
- 安全模組
  - 電腦主機板內建 (TPM: Trusted Platform Module)
  - 實體金鑰裝置 (ex. Yubikey)

# 歷史簡介





# FIDO

- FIDO: Fast Identity Online ([網站](#))
- 歷史
  - July 2012 – 發起
  - Feb 2013 – 正式亮相
  - Apr 2013 – Google, Yubico, NXP 加入
  - Feb 2014 – Samsung Galaxy S5 可以使用指紋來購物 (PayPal 結帳)
  - Feb 2015 – MS announced Windows 10 會支援 FIDO 認證
  - Feb 2016 – 開始發展 FIDO2
  - **Apr 2018 – FIDO2**
  - Mar 2019 – WebAuthn 成為標準
  - Jan 2020 – Apple 加入

# FIDO 1.0

- 兩種規格:
  - UAF (Universal Authentication Framework)
  - U2F (Universal 2<sup>nd</sup> Factor)

## PASSWORDLESS EXPERIENCE (UAF standards)



## SECOND FACTOR EXPERIENCE (U2F standards)



圖片來源: <https://fidoalliance.org/specifications/>























# W3C

- April 2018 很重要的一年
- FIDO2 and Client-To-Authenticator Protocol(CTAP) 正式啟用
- FIDO2 包含 Web Authentication JavaScript API
- 主流瀏覽器 Chrome, FireFox, Edge 確定會支援
- Android, Windows 10 及未來 MS 技術都會支援 FIDO 驗證
- March 2019 – WebAuthn 正式定案

# 支援程度

# FIDO Platform/Browser Support

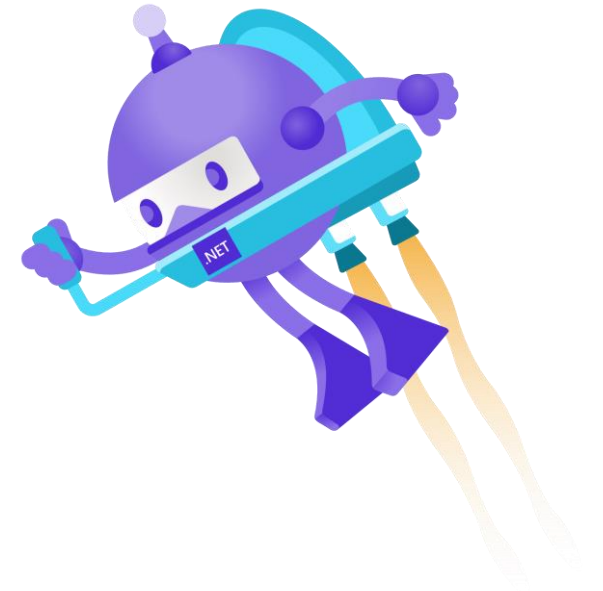
Updated 6/29/2020

U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API	
 Chrome/Windows				 Edge/Windows				 Firefox/Windows				 Safari/iOS			
U2F		CTAP2		U2F		CTAP2		U2F		CTAP2		U2F		CTAP2	
USB	NFC	BLE	Hello	USB	NFC	BLE	Hello	USB	NFC	BLE	Hello	USB	NFC	BLE	Plat
U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API	
 Chrome/Android				 Edge/Android				 Firefox/Android				 Safari/macOS			
U2F		CTAP2		U2F		CTAP2		U2F		CTAP2		U2F		CTAP2	
USB	NFC	BLE	Plat	USB	NFC	BLE	Plat	USB	NFC	BLE	Plat	USB	NFC	BLE	Plat
U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API		U2F API		WebAuthn API	
 Chrome/macOS				 Edge/macOS				 Firefox/macOS							
U2F		CTAP2		U2F		CTAP2		U2F		CTAP2		U2F		CTAP2	
USB	NFC	BLE	Plat	USB	NFC	BLE	Plat	USB	NFC	BLE	Plat	USB	NFC	BLE	Plat
								</							

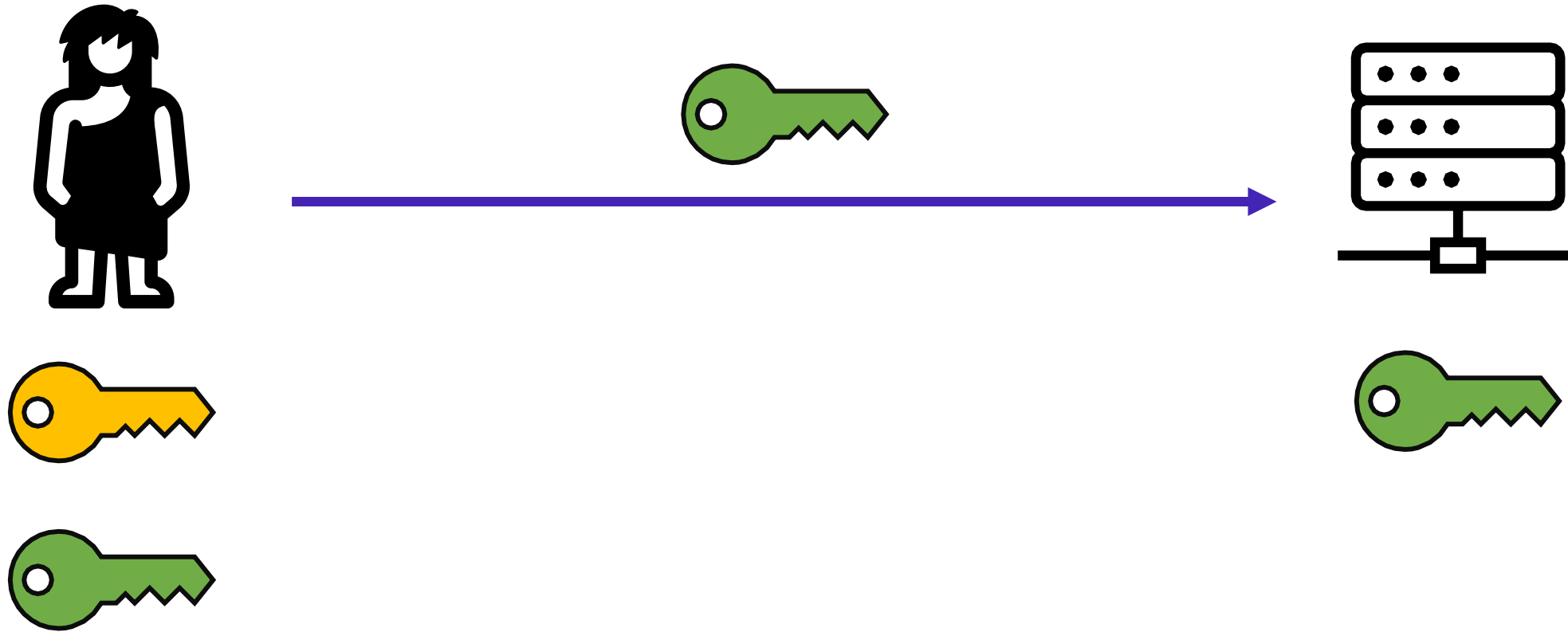
支援程度 – 最後一塊拼圖

Safari on iOS 14, MacOS Big  
Sur and iPadOS 14  
Support FIDO Authentication

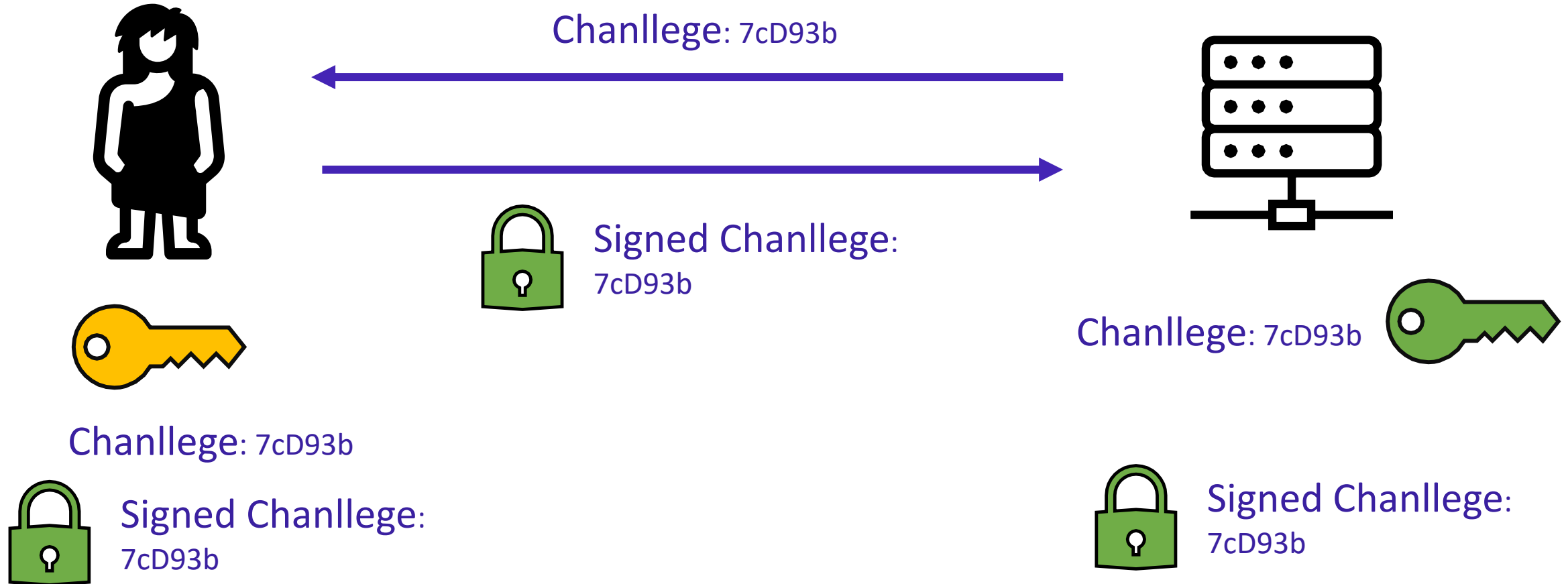
# WebAuthn



# 流程 - 註冊

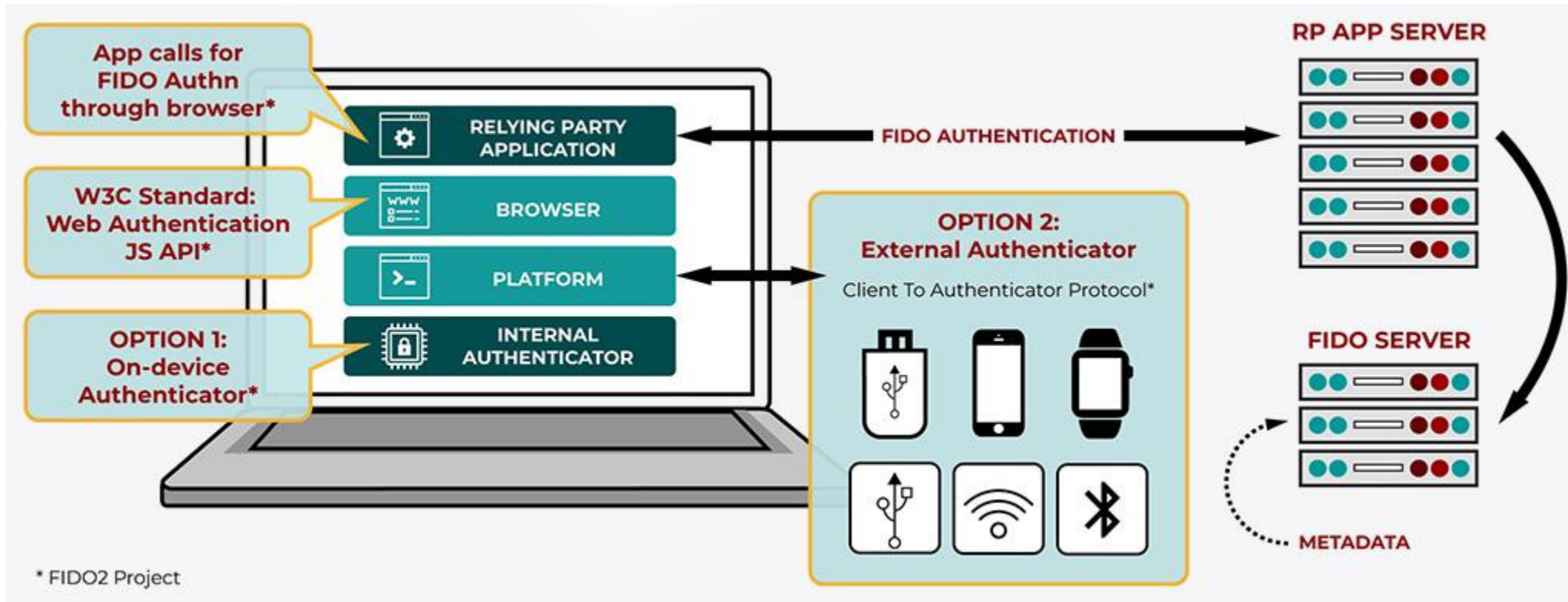


# 流程 - 驗證





# 運作流程



圖片來源: <https://fidoalliance.org/fido2/>

# 硬體 – Cross Platform



照片來源: Yubico

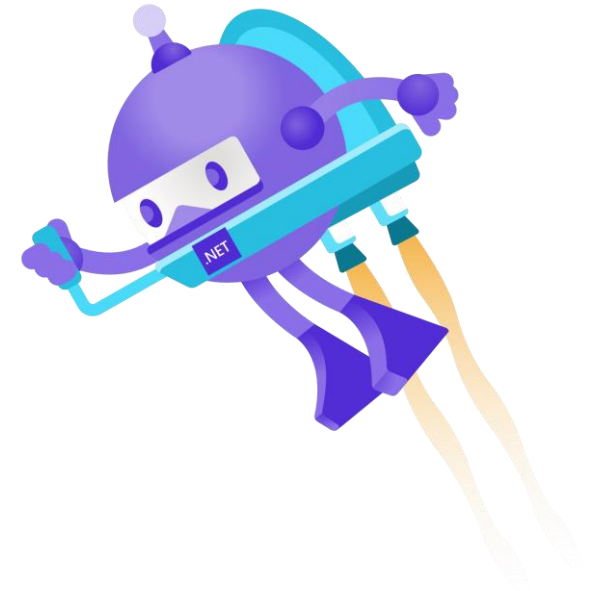
# Platform Authenticators

- 電腦
- 筆電
- 手機

# 有支援的網站/服務

- GitHub
- Google
- Microsoft
- ...etc

# 程式碼實做





# Client Library


## Using WebAuthn

Get started using WebAuthn with one of these libraries:


Go


 duo-labs/webauthn


 Duo Labs

 Server


Go


 duo-labs/webauthn.io


 Duo Labs

 Demo


Go


 koesie10/webauthn


 Koen Vlaswinkel

 Server


Java


 duo-labs/android-webauthn-authenticator


 Duo Labs

 Authenticator


Java


 google/webauthndemo


 Google

 Demo


Java


 webauthn4j/webauthn4j


 Yoshikazu Nojima

 Server


Java


 Yubico/java-webauthn-server


 Yubico

 Server


Javascript


 fido-alliance/webauthn-demo


 Fido Alliance

 Demo


.NET


 abergs/fido2-net-lib


 Anders Åberg

 Server/Demo


Python


 duo-labs/py\_webauthn


 Duo Labs

 Server/Demo


Ruby


 cedarcode/webauthn-ruby


 Cedarcode

 Server

Chrome Extension

 google/virtual-authenticators-tab

 Nina Satragno

 Authenticator

<https://webauthn.io/>

# 參考資料

- [FIDO History](#)
- [Beyond Passwords: Simpler, Stronger Authentication with FIDO2](#)
- <https://webauthn.io/>
- [USB-Dongle Authentication](#)
- [範例程式碼](#)



# 延伸閱讀

- Sign-up form best practices
  - YouTube 影片
- OWASP Cheat Sheet Series
- 一起來了解 Web Authentication



# Kevin Yang (楊捷凱)

- Microsoft Most Valuable Professional
- Angular GDE
- Blog : <https://blog.kevinyang.net/>
- FB Page : <https://www.facebook.com/CKNotepad>
- Organizer:
  - Angular Taiwan
  - Angular Online Study Group
  - GDG Taichung



# Thanks for joining!

Ask questions on Twitter using #dotNETConf



.NET Conf  
2020

# 特別感謝

91APP  
Technical Network



KKKTIX



  
HackMD



 Microsoft

 Build School

STUDY4  
為 學 習 而 生

以及各位參與活動的你們

