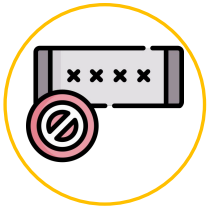

WebAuthn：
打造無密碼登入體驗！

忘記密碼ㄋㄇㄋ

什麼是 WebAuthn？

全名為「Web Authentication」，是一種網頁身份驗證標準，旨在提供更安全且便利的驗證方式，減少對傳統密碼的需求。適用於網路瀏覽器和網站應用程式，支援多種方法，包括生物特徵、硬體驗證器。



無密碼驗證

減少傳統密碼驗證可能容易受到記憶負擔、密碼洩漏等問題。

多種驗證方式

支援多種驗證方式，包括生物特徵識別（指紋、面部辨識）、硬體安全密鑰（USB 驗證器）。

高度安全保障

採用了公開/私有金鑰加密、不可複製的註冊證明等機制，確保身份驗證的安全性。

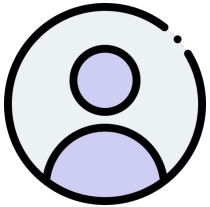
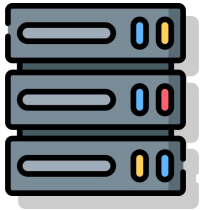
傳統密碼驗證 vs. 無密碼驗證

	傳統密碼驗證	無密碼驗證
身份驗證方式	依賴於用戶選擇和管理的密碼	使用生物特徵、硬體驗證器等
安全性	依賴於用戶生成和記憶的密碼，受到密碼泄露的風險	需要具體的生物特徵或設備，降低密碼泄露和猜測的風險
用戶體驗	需要輸入長、複雜的密碼	快速、便捷的登入體驗
忘記密碼	需要重置流程，在多個設備間同步密碼	用戶不會忘記身份識別方式
未來趨勢	正在逐漸被更現代、更安全的身份驗證方式取代	被視為未來的趨勢，越來越多的平台採用無密碼驗證技術

WebAuthn 核心原理

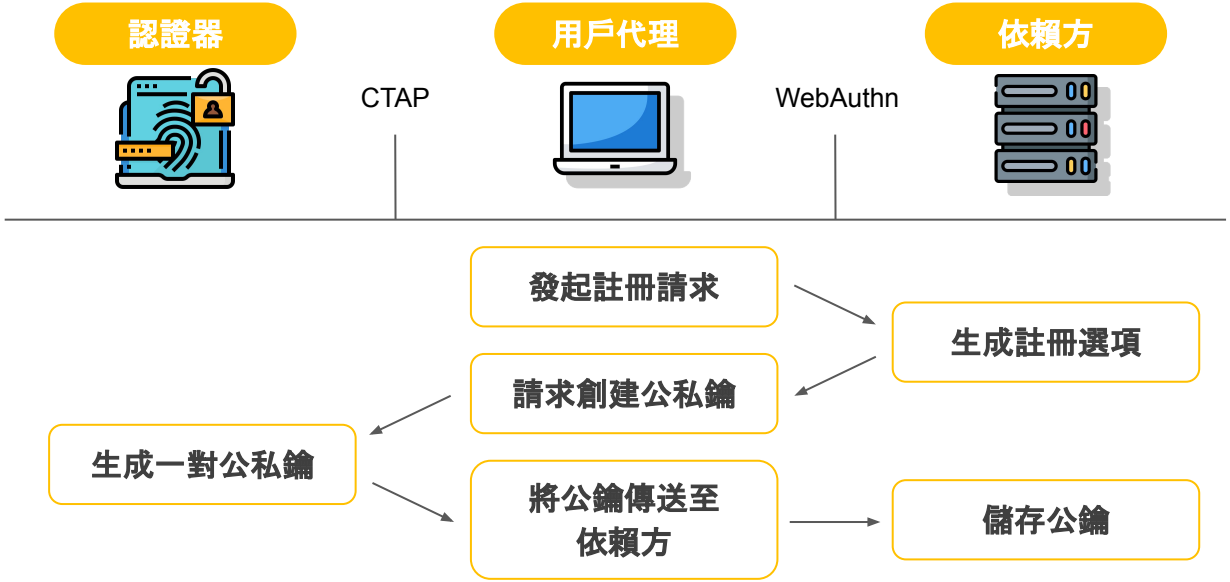
WebAuthn 包含註冊（Registration）和驗證（Authentication）兩個關鍵步驟，確保用 戶和設備進行安全身份驗證。

角色介紹

認證器(Authenticator)	用戶代理(User Agent)	用戶(User)	依賴方(Relying Party)
			
識別設備	瀏覽器	正準備登錄的你	服務提供方

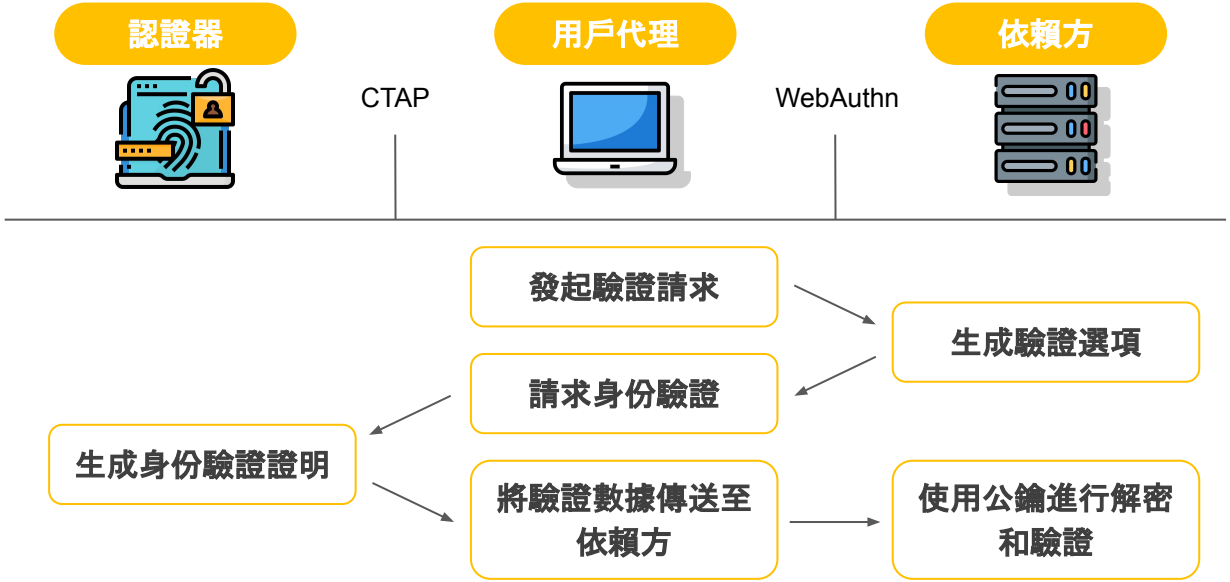
步驟一 - WebAuthn 註冊

註冊流程的目的在於建立依賴方和用 戶之間的認證器資訊和用 戶關聯。在註冊流程中，認證器將生成一對公私鑰，並將公鑰交給依賴方。



步驟二 - WebAuthn 驗證

驗證流程的目的在於確保登入的是使用者本人，依賴方會進行相關的驗證。在驗證流程中，依賴方會將一段文字傳送給認證器，並要求認證器使用其私鑰將該文字進行加密後返回，以進行驗證。

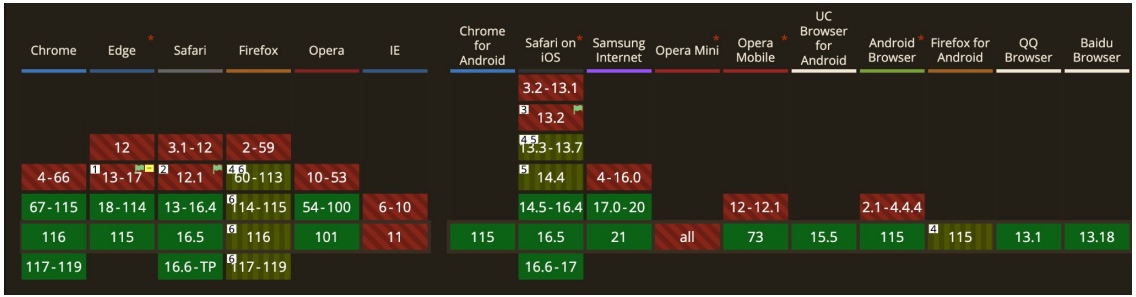


Demo 時間！！！

WebAuthn 導入專案應用

支援度

WebAuthn API 的支援度已經相當廣泛，特別是在現代的瀏覽器和操作系統中。



套件

WebAuthn PHP 庫，它提供了一個方便的方式來處理 WebAuthn 註冊和驗證過程。

FIDO2/Webauthn Support for PHP

Webauthn Framework

WebAuthn 導入專案應用

流程　引入 WebAuthn 後的系統流程將包含以下步驟:

第一次登入	設定 WebAuthn	日後登入
		
1. 使用者首次登入系統時，需要輸入傳統密碼，以便驗證身份。 2. 一旦身份驗證成功，系統可以要求使用者設定 WebAuthn 身份驗證。	1. 系統提示用戶設定WebAuthn身份驗證方式。 2. 用戶的設備將與他們的帳戶相關聯，並生成相應的公私鑰對。	1. 當用戶下一次登入時，可以選擇使用 WebAuthn 進行無密碼登入。 2. 使用者的設備將生成驗證證明。

WebAuthn 的開發限制

硬體支援限制

WebAuthn API 提供控制選項，包括認證器附著方式、使用者驗證要求、要求驗證器儲存私鑰，但**實際的生物識別技術由驗證器和設備來決定**。

實作複雜性

實作 WebAuthn 使用了複雜的加密技術，開發者需要了解之中的實作原理和流程，以及如何正確配置及使用 WebAuthn API。

平台相容性

需要確保 WebAuthn 實作在不同的平台（桌面、移動、不同瀏覽器）皆能正常運作，並提供使用者體驗良好的界面。