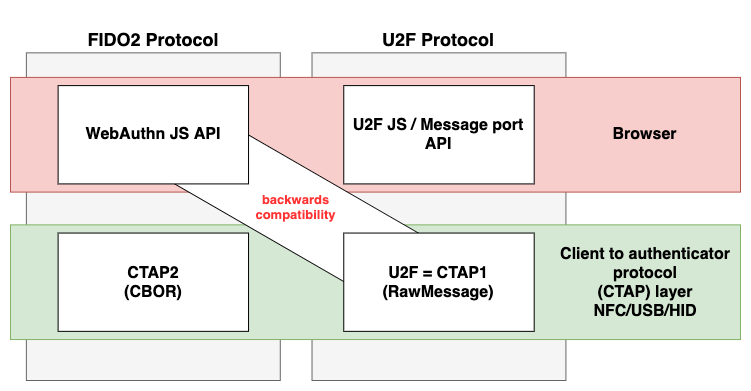
# FIDO2 與 U2F 關係



FIDO2 = WebAuthn JS + CTAP2 (CBOR)

U2F = U2F JS + CTAP1(RawMessage)

* **FIDO：**

即Fast IDentity Online（線上快速身份驗證）的縮寫，或稱FIDO 聯盟。該聯盟主要致力於構建安全、開放、防網絡釣魚的無密碼身份驗證標準。

FIDO 系列協議是由FIDO 聯盟制定的一套協議，包括通用認證框架UAF（Universal Authentication Framework）、通用第二因素認證標準U2F（Universal 2nd Factor）以及FIDO2。

當說到使用 “FIDO” 時，通常是指使用這三種協議中的任何一種，因為從概念的角度來看，這三者基本一致，只是結構有所區別（UAF——TLV，U2F——RAW，FIDO2——CBOR）。

* **CTAP：**

即客戶端到認證器協議（Client to Authenticator Protocols），對HID、NFC 以及BLE 等傳輸協議進行一系列定義，描述了啟用CTAP 的設備如何使用這些協議與客戶端通信。U2F 和FIDO2 認證器均具備這些特性，對應的名稱為CTAP1 和CTAP2.

* **U2F：**

即通用認證框架，連同UAF 一起，是互聯網領域第一個預防網絡釣魚攻擊的身份驗證協議。U2F 標準於2014 年首次公佈，該標準以web 為中心，支持USB、NFC 以及BLE 傳輸，並對低級傳輸、信息格式以及JS API 等內容進行了具體說明。

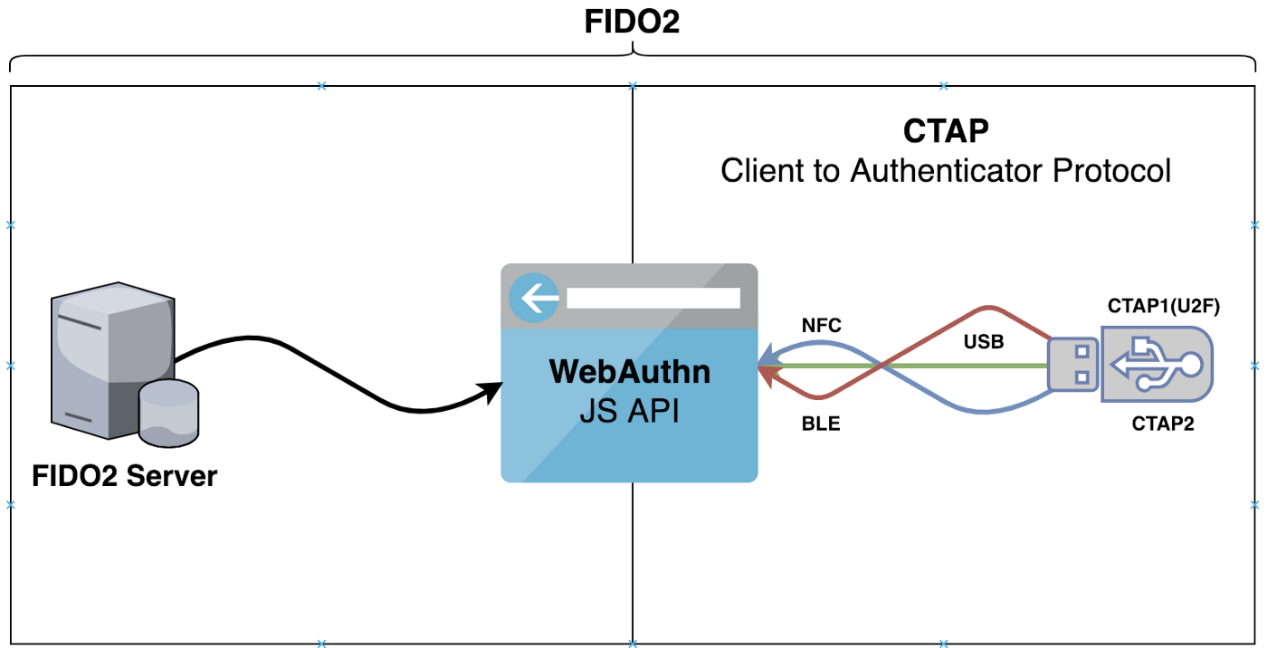
* **CTAP1：**

CTAP1 是U2F 協議的正式名稱，U2F 使用RawMessage 格式。

* U2F JS A

即2014 年在Google Chrome 瀏覽器中推出的一個僅支持U2F 的傳統API。由於該API 只支持U2F 且只有極少數瀏覽器支持，目前已被淘汰。相比之下，現在的WebAuthn 能夠支持U2F 和FIDO2 標準，更具現代意義。

* FIDO2：即滿足現代化、簡便性、安全性、防網絡釣魚、無密碼身份驗證的一個新協議。其核心規範包括WebAuthn（客戶端API）以及CTAP（認證器API）。
* CTAP2：FIDO2 協議底層部分的正式名稱。FIDO2 使用CBOR 編碼響應結構，可以理解為JSON，但與TLV 有些類似。CTAP2 規範定義了FIDO2 請求如何轉換為CTAP1/U2F 請求，以及CTAP1/U2F 響應如何轉換為CBOR/FIDO2 響應。不過，值得注意的是，U2F 並不時FIDO2 協議的一部分。
* WebAuthn：即描述用於創建和管理公鑰憑證接口的瀏覽器JS API。WebAuthn 標準由W3C 組織牽頭制定，符合現代互聯網要求。WebAuthn 能夠與CTAP2/FIDO2 和CTAP1/U2F 認證器對話。此外，還會接受所需標準的編碼請求，並基於協議對響應進行解碼或重新編碼。因此，儘管CTAP2 規範中也定義了CTAP1/U2F 轉換，但都是在WebAuthn 中實現。
* 認證器：FIDO 認證器是指向服務器進行用戶認證的實體，可以是軟件（如移動應用程序），也可以是硬件（如安全密鑰）。
* 安全密鑰：指支持FIDO 的硬件認證器，例如Yubikey、Feitian 以及TrustKey 等硬件產品。



**常見問題解答**

1、U2F 是FIDO2 的一部分嗎？  
-不是。U2F 是用於預防網絡釣魚第二因素認證的一個單獨標準。FIDO2 能夠向後兼容目前的U2F 認證器。

2、FIDO2 就是WebAuthn 嗎？  
-不是。WebAuthn 只是FIDO2 協議的一部分。所以，正確的說法是“我的服務器支持FIDO2 身份驗證”。由於WebAuthn 是FIDO2 項目中最廣為人知的規範，所以人們常常存在“FIDO2 就是WebAuthn” 的錯誤認知。

3、所有的安全密鑰都可以叫作Yubikey 嗎？  
不是。Yubikey 是Yubico 的安全密鑰產品，只是市面上眾多密鑰產品中的一種，其他安全密鑰還包括TrustKey、Feitian Bio Pass、Open Source Solokey 以及Google Titan Key 等等。所以，只有在特指Yubico 的產品時，你可以說Yubikey，否則都應該稱為“安全密鑰”。

(1)

本規範是 FIDO2 項目的一部分，FIDO2 項目包括本規範並與 W3C [[WebAuthn]](https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#biblio-webauthn)規範相關。本規範涉及兩個 CTAP 協議版本：

1. CTAP1/U2F 協議，由 U2F 原始消息規範[[U2FRawMsgs]](https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#biblio-u2frawmsgs)定義。CTAP1/U2F 消息可通過其類似 APDU 的二進制結構來識別。CTAP1/U2F 也可稱為 CTAP 1.2 或 U2F 1.2。後者是用作本規範多個部分基礎的 U2F 規範版本。實現 CTAP1/U2F 的認證器通常稱為 U2F 認證器或 CTAP1 認證器。
2. CTAP2 協議，其消息以[CTAP2 規範的 CBOR 編碼形式](https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#ctap2-canonical-cbor-encoding-form)進行編碼。實現 CTAP2 的身份驗證器稱為 CTAP2 身份驗證器、FIDO2 身份驗證器或 WebAuthn 身份驗證器。

CTAP1 和 CTAP2 共享相同的底層傳輸：

[USB 人機接口設備 (USB HID)](https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#usb)、

[近場通信 (NFC)](https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#nfc)

[藍牙智能/藍牙低功耗技術 (BLE)](https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#ble)。