中華民國內政部
MINISTRY OF THE INTERIOR, R.O.C. (TAIWAN)

TWID
身分識別中心

TAIWAN FidO 行動身分識別系統
推廣說明會

中華民國內政部
MINISTRY OF THE INTERIOR, R.O.C. (TAIWAN)

TWID
身分識別中心

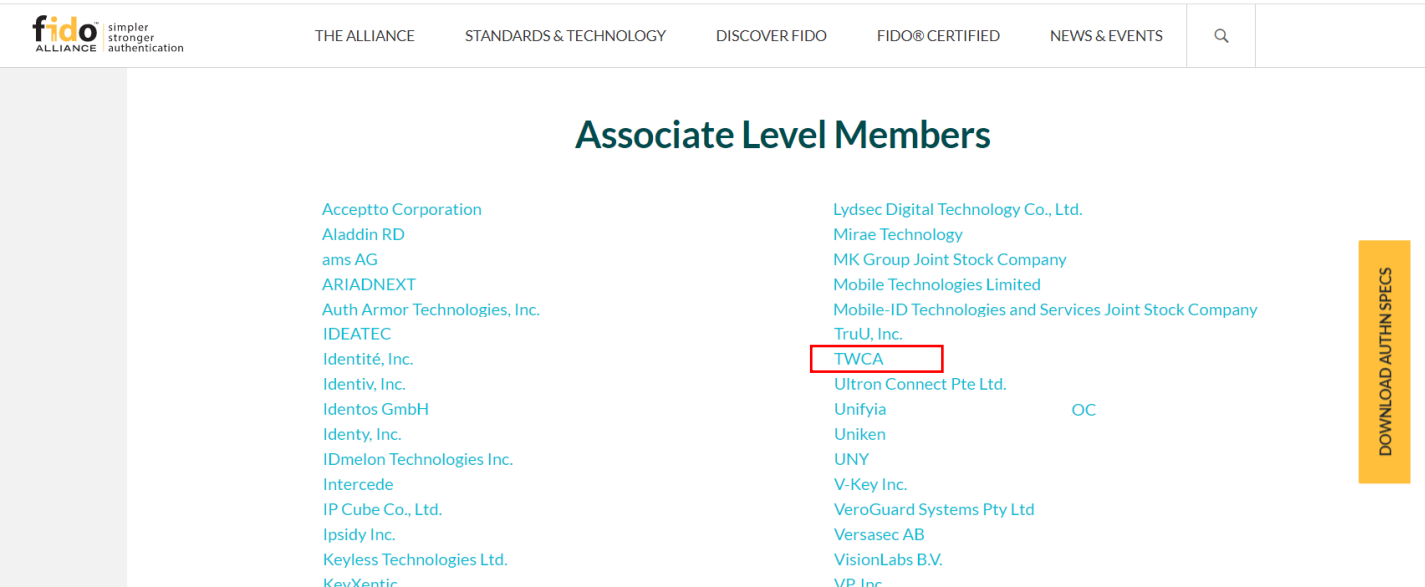
FIDO與身分識別機制的比較

專案經理 臺灣網路認證 彭冠瑋

Fast Identity Online (**FIDO**) 國際聯盟成立於2012年美國麻州，致力於結合**公開金鑰、生物特徵**等技術，提供便利及**安全之網路身分識別機制**，並建立產業標準

本部於 108 年 9 月採用 FIDO 國際標準建置完成「**TAIWAN FidO 試辦案**」，以自然人憑證綁定行動裝置，使用指紋或臉部辨識，以**免插卡、免密碼**方式，即可驗證登入政府網站

本部與臺網以符合 FIDO 國際標準建置完成「TAIWAN FidO」行動身分識別系統，於 109 年正式加入fido聯盟的政府會員。



首先，先來看一下

FIDO的起源與發展

起源--傳統帳號密碼機制的資安問題及挑戰

1 **Forgetful**

為降低帳號密碼被猜測及盜用，多數應用服務導入強制性複雜密碼原則，並要求前數次已使用之密碼不可重複使用，使得使用者在記憶密碼上形成困擾。

2 **Phished**

即便在強制性複雜密碼原則保護下，使用者仍容易遭受釣魚攻擊(PhishingAttack)如詐欺 E-mail、詐騙電話等而使得帳號密碼被竊取。

3 **Key logged**

透過加密或圖形碼確認等機制強化安全認證，但透過設備端監聽、中間人攻擊，自動辨識圖形碼等等駭客手法還是能取得使用者帳號密碼。

4 **Reused**

一般使用為了記憶方便，多數習慣用同一組帳號密碼在多個應用服務平台 使用，因此一旦密碼被盜，往往造成所有應用服務都被竊取。

資料來源:中華民國資訊安全學會

實名制興起，使用者真實身分驗證需求增加

傳統密碼機制為共存於同個伺服器中

以金融服務最多使用的OTP來說，用戶在手機上接收驗證碼後輸入，但自己與伺服器雙方都知道帳號與密碼以驗證，像是個分享祕密的過程。因此近年這種機制也被認為不夠安全，仍面臨網路釣魚與中間人攻擊的風險。

生物辨識(Biometric)機制興起

運用人體身上的特徵來做為識別的密碼，因此在技術的開發上必須選擇準確度高及容易使用的辨識特徵以利使用，其可區分為生理特徵（如臉 形、指紋、虹膜）及行為特徵（如聲音、簽名、密碼），以準確度來說，「生理特徵」在唯一性及安全性上優於「行為特徵」。

辨識速度快、體積小、技術成熟度高、不受環境影響

生理特徵　　行為特徵

	指紋	臉形	手形	虹膜	語音	靜脈	DNA	步姿
獨特性 (Uniqueness)	高	低	中	高	低	高	高	低
永久性 (Permanence)	高	中	中	高	低	高	高	低
便利性 (Collectability)	高	高	高	中	高	中	低	高
接受度 (Acceptability)	高	高	高	中/低	高	高	低	低
辨識效能 (Performance)	中/高	低/中	中	高	低	中	低	中
技術成熟度 (Maturity)	高	中	中	中/高	中	中	低	中/低

1. 獨特性：所提供的特徵是必須可以與他人分別
2. 永久性：特徵不會隨著時間改變
3. 便利性：特徵是否容易採集
4. 接受度：辨識特徵擷取的安全性
5. 辨識效能：該特徵辨識各種效能的評估
6. 技術成熟度：使用生物辨識技術的應用產品功能成熟度

資料來源:中華民國資訊安全學會

FIDO讓身分驗證改至用戶端進行分散風險

FIDO 認證模式，由三個元素構成：

(1) 身分驗證裝置(Authenticator attachment)：

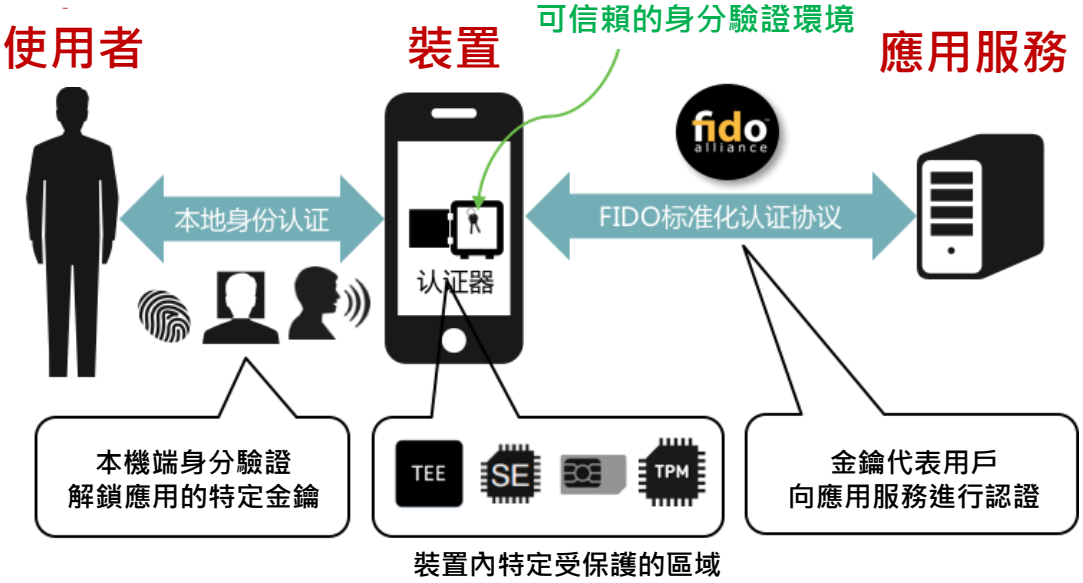
分為平台式(例如生物辨識系統)與可攜式(例如USB)

(2) 認證器(Credential storage)：

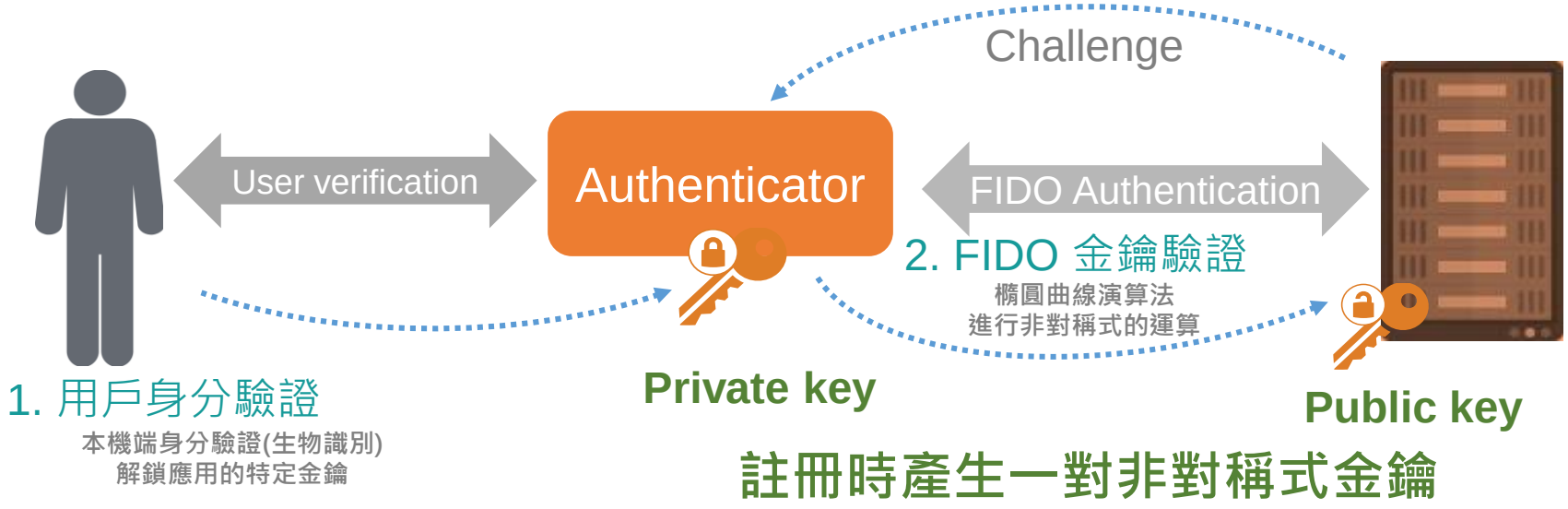
分為用戶端(僅存私鑰)和伺服器端(儲存公鑰)，功能包含儲存生物特徵或密碼，以認證使用者、產生金鑰對，並儲存私鑰及運算身分識別時所需之資訊。

(3) 驗證元素(Authentication factors)：

用戶所擁有的識別要素，例如指紋、人像等生物辨識要素或密碼。



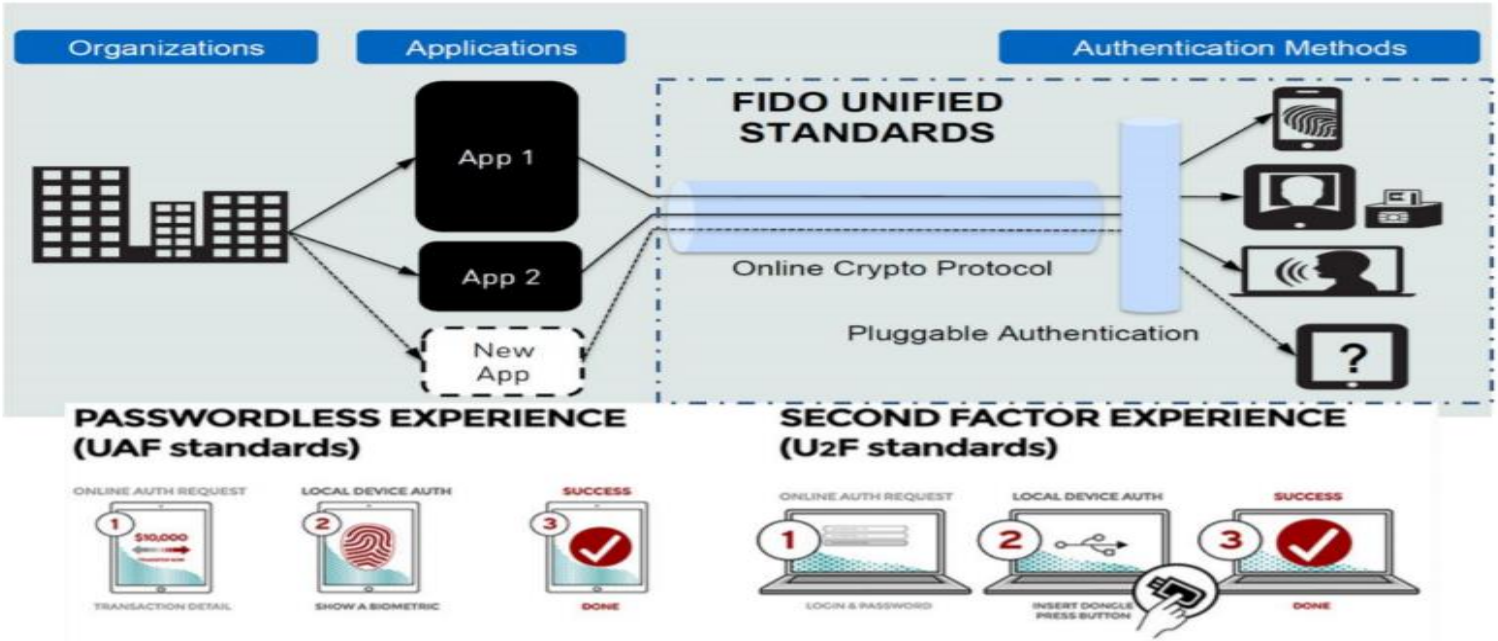
FIDO身分驗證原理與流程



FIDO 將身分認證分成 2 個階段：

1. **[用戶身分驗證]**使用者在裝置端，藉由其生物特徵或動作來解開裝置上的私鑰。
2. **[金鑰識別]**再利用私鑰進行簽章運算，傳到伺服器與對應的公鑰進行比對確認。

FIDO 身分驗證協定



UAF 協定主要針對行動應用發展

- 適用於具備安全元件及生物辨識晶片之智慧型使用者終端設備(如智慧手機)。
- 透過演算法產生相配對的安全公私鑰會取樣使用者生物特徵
- 以此作為驗證使用者依據與 UAF 伺服器溝通，驗證使用者生物 特徵所綁定的身分之合法性

U2F 協定主要針對個人電腦搭配雲端應用發展

- 透過插入一個具備生物辨識功能的硬體 U2F Token(如 USB Dongle、智慧卡等)
- 於瀏覽器上以生物辨識當第二認證因子(2nd Factor)，降低使用者對密碼的依賴並提高認證安全性。
- 當使用者需認證時，使用者於該認證器上感測其生物特徵，並由其中的安全元件透過演算法產生相配對的安全公私鑰(Public-Private Key)，以此作為驗證使用者依據與 U2F 伺服器溝通，驗證使用者生物特徵所綁定的身 分之合法性。

FIDO 身分驗證協定-FIDO 2

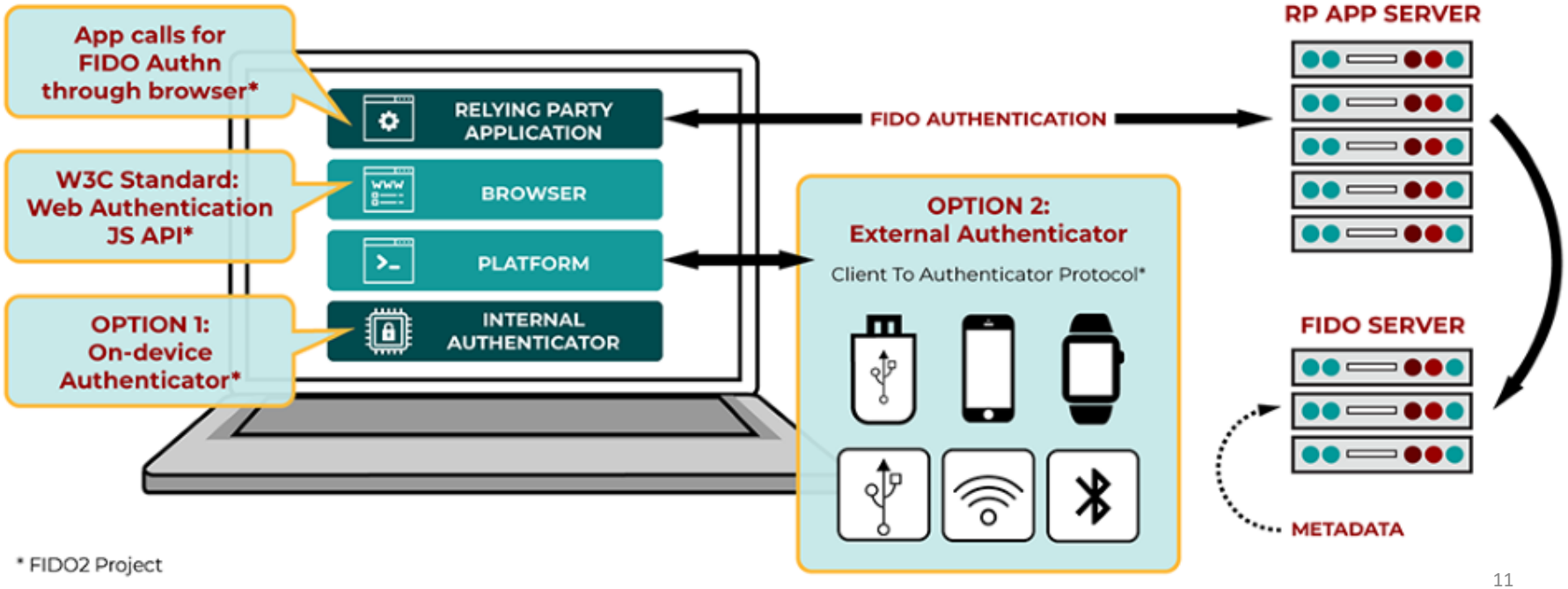
FIDO 聯盟於2018年提出 FIDO2認證模式

(1) WebAuthentication（WebAuthn）

WebAuthn定義了一個標準化的Web API，該API可被植入瀏覽器或相關的網路平台架構中，以讓網路服能使用FIDO驗證

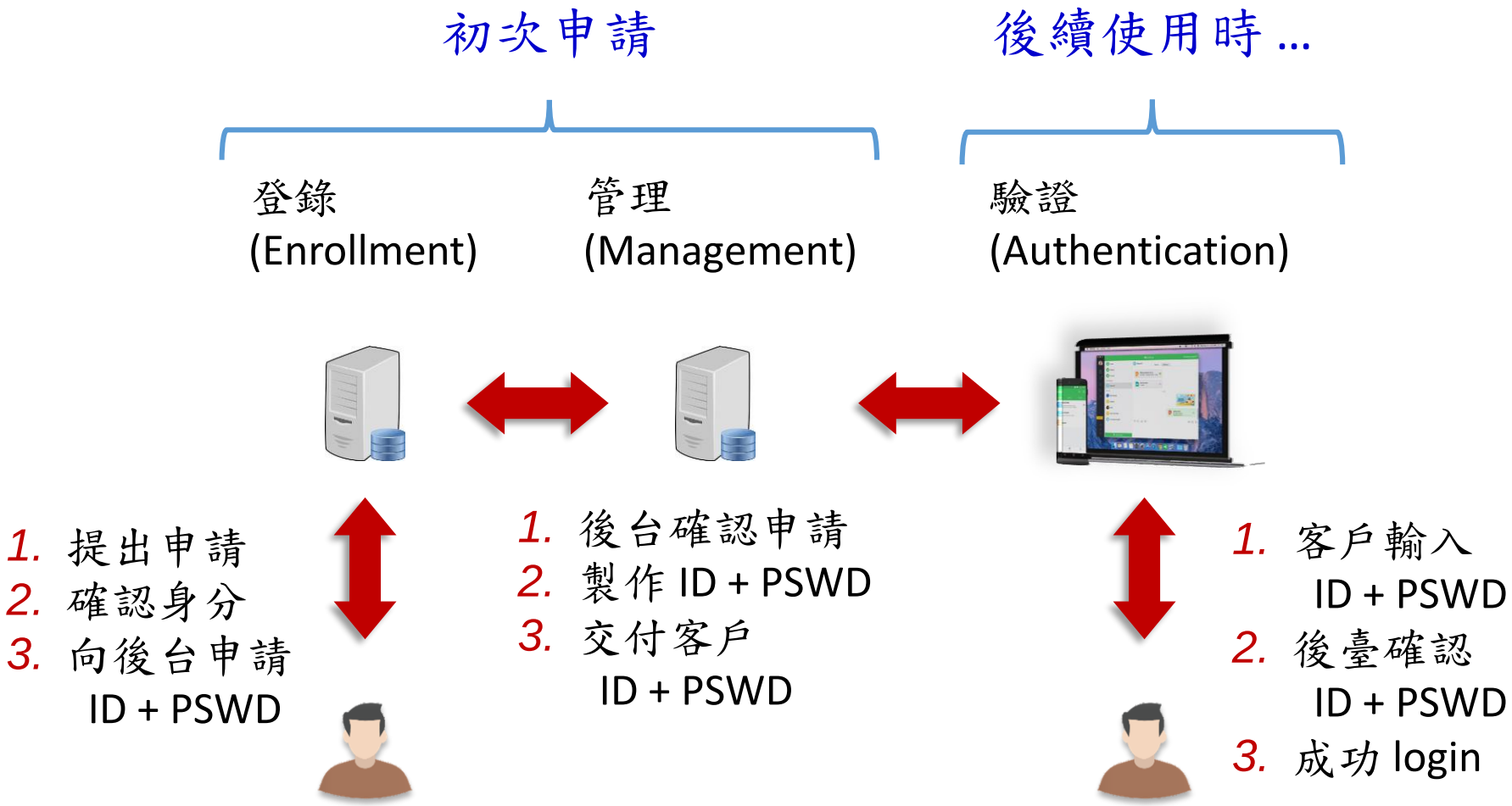
(2) Client-to-Authenticator Protocol，CTAP：

CTAP則允許諸如手機或FIDO安全鑰匙等外部裝置能搭配WebAuthn使用，以作為桌面應用程式或網路服務的身分驗證器。



再來了解在網路上
進行身分識別的機制與其標準

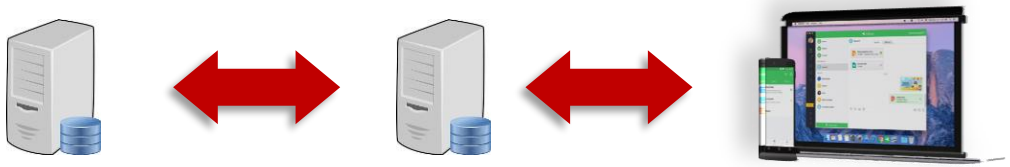
一個完整的身分識別機制, 包括三個主要的功能 … （以 ID + PSWD 為例）



一個完整的身分識別機制, 包括三個主要的功能 ...　　(TW FidO 的作法)

初次申請　　後續使用時 ...

登錄 (Enrollment)　　管理 (Management)　　驗證 (Authentication)



1. 以自然人憑證
   確認客戶身分
2. 客戶下載 TW FidO APP
   產製 (公鑰私鑰)
   公鑰存後台 DB
   私鑰存客戶 APP
   私鑰以手機生物識別
   做為啟動機制

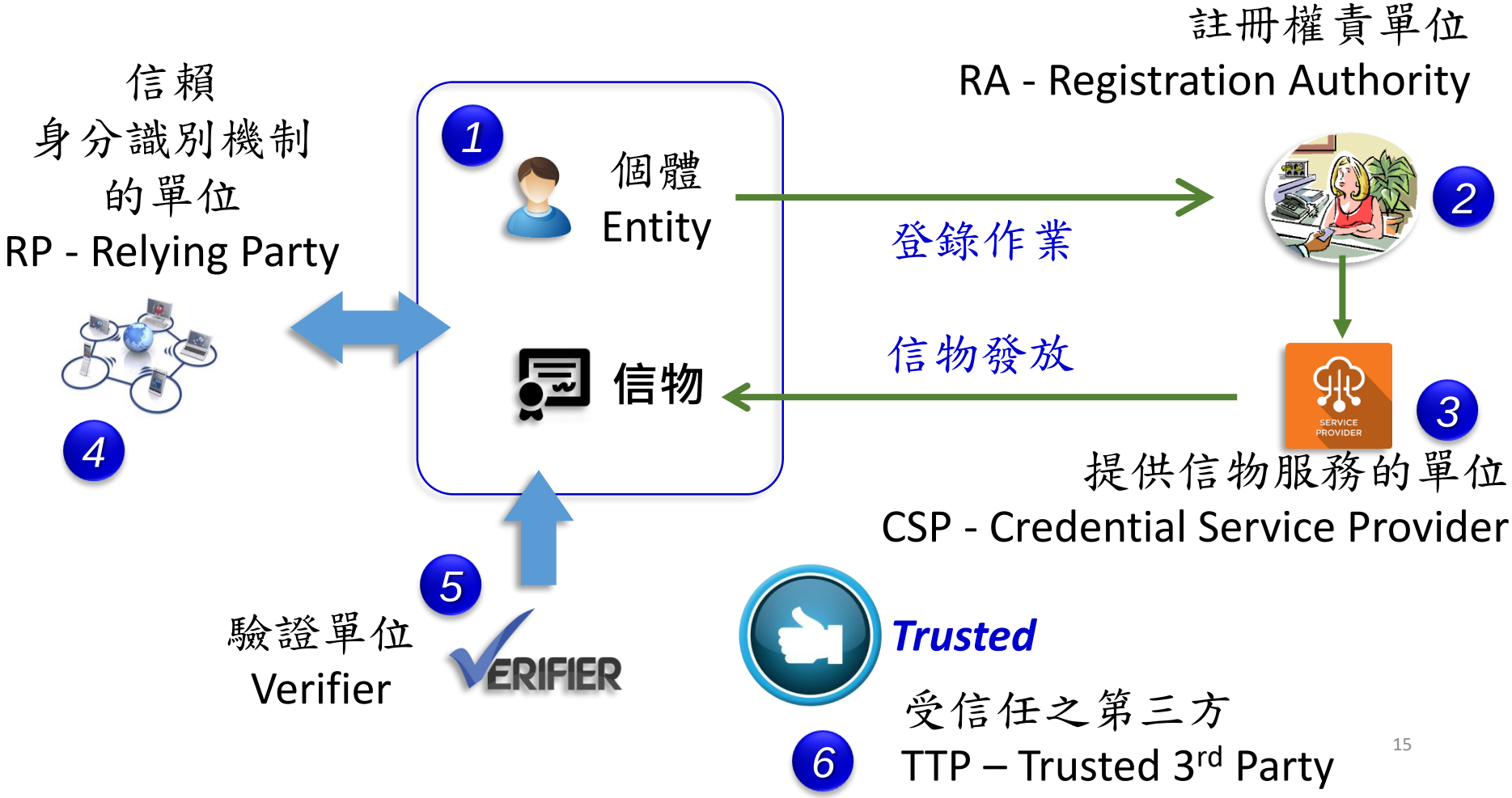
1. 提出申請
   TW FidO
2. 使用
   自然人憑證
   進行身分識別

1. login 時
   以手機生物識別機制
   啟動手機內之私鑰
   加密 Msg 傳送至後台
2. 後台以公鑰
   驗證 加密 Msg
   以確認客戶身分

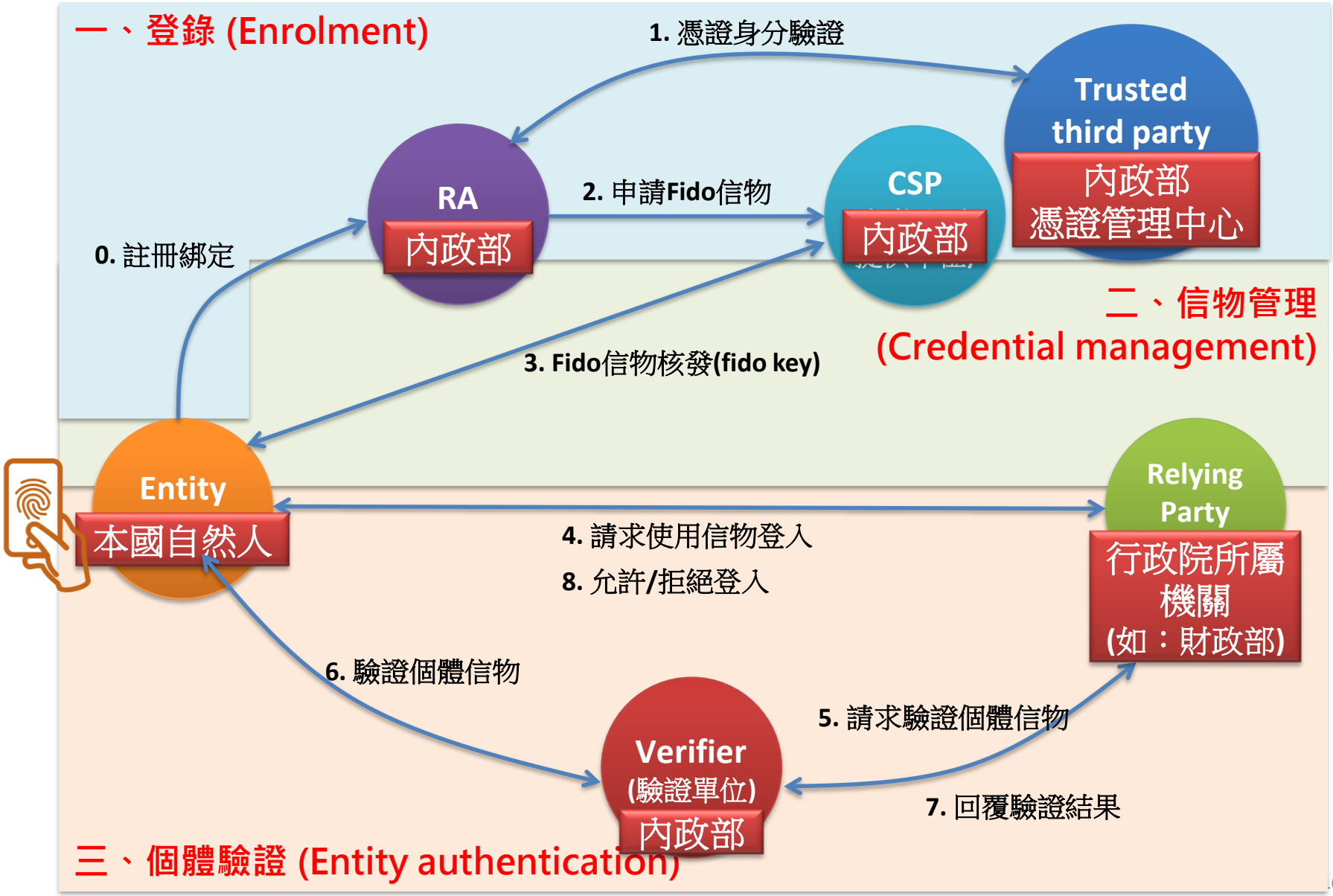
ISO29115--個體身分驗證信賴架構

ISO/IEC 29115 的全名為：

International Standard ISO/IEC 29115:2013 (E),
Entity Authentication Assurance Framework(簡稱 EAAF)



TW FidO--個體身分驗證信賴架構



ISO/IEC 29115 將信賴等級分為四個等級：

依三個執行階段的嚴謹程度分級 Level of Assurance

登錄
(Enrolment)

信物管理
(Credential Management)

個體身分驗證
(Entity Authentication)

信賴等級	對驗證機制的「信賴度」
LoA1 低 Low	具少許或幾乎無可信度可言 Little or no confidence
LoA2 中 Medium	具某種程度的可信度 Some confidence
LoA3 高 High	可信度高 High confidence
LoA4 極高 Very high	可信度極高 Very high confidence

ISO/IEC 29115　將信賴等級分為四個等級：

依三個執行階段的嚴謹程度分級 Level of Assurance

哪些應用適合使用 TW FidO
做為身分識別 機制？
應用單位必須依據
TW FidO 之作業特性
進行評估

TW FidO

自然人憑證

信賴等級	對驗證機制的「信賴度」
LoA1 低 Low	具少許或幾乎無可信度可言 Little or no confidence
LoA2 中 Medium	具某種程度的可信度 Some confidence
LoA3 高 High	可信度高 High confidence
LoA4 極高 Very high	可信度極高 Very high confidence

TW FidO
在市場上的定位與使用流程

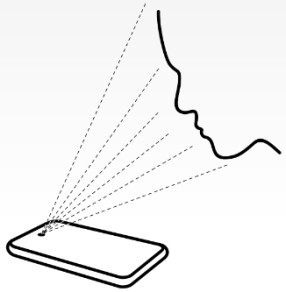
TAIWAN FidO 臺灣行動身分識別機制

- 行動裝置、**生物辨識與安全模組**發展成熟
- 新世代網路身分識別 FIDO 2標準崛起
- 取代內政部自然人憑證登入(FIDO2)
- 行動+無密碼新時代

TW FidO註冊及綁定程序

1. 下載安裝臺灣行動身分識別 TW FidO APP
2. 準備讀卡機及自然人憑證
3. 使用自然人憑證進行身分驗證

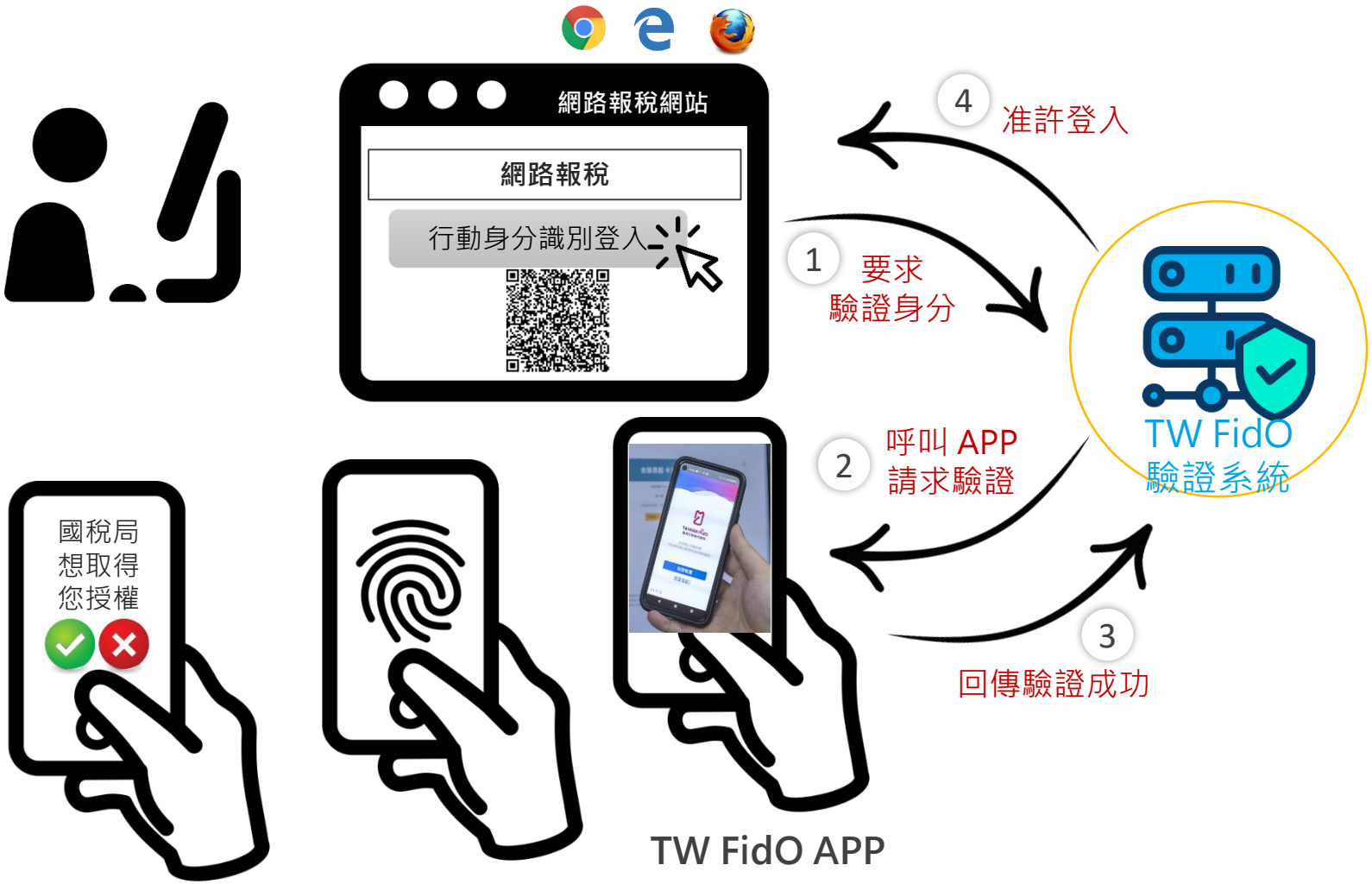
4. APP 接著引導使用者以指紋辨識或臉部辨識進行認證



Done!

手機綁定後，可以生物辨識，透過免密碼方式，快速驗證登入政府網站

TW FidO驗證程序


網路報稅網站
網路報稅
行動身分識別登入
4
准許登入
1
要求
驗證身分
TW FidO
驗證系統
2
呼叫 APP
請求驗證
3
回傳驗證成功
國稅局
想取得
您授權
TW FidO APP

TW FidO的定位

1. 一個安裝在個人手機 APP 中的

   行動身分識別機制

2. 目前申辦的方式僅限於

   使用**自然人憑證**線上申請

3. 可以在登入網站或應用系統時

   做為**實名制身分識別**使用

4. 在 ISO 29115 的規範中屬於**第三級安全強度**

   與自然人憑證同，僅次於最高等級第四級

TW FidO
與其他身分識別機制的比較

身分識別信物


自然人憑證

TAIWAN FIDO 臺灣行動身分識別
TW FidO

晶片金融卡


金融下單憑證


金融硬體憑證


行動電話認證

驗證持有手機SIM卡+
電信公司留存個人資料

Question1 : 各信物應用的差異在哪?

Question2 : 我的系統可以使用那些信物?

Question3 : 這些信物驗證強度是否足夠?

1.信物認證強度差異

依據ISO 29115的精神，依照註冊、驗證、管理的嚴謹程度給予其信賴等級的高低差異。

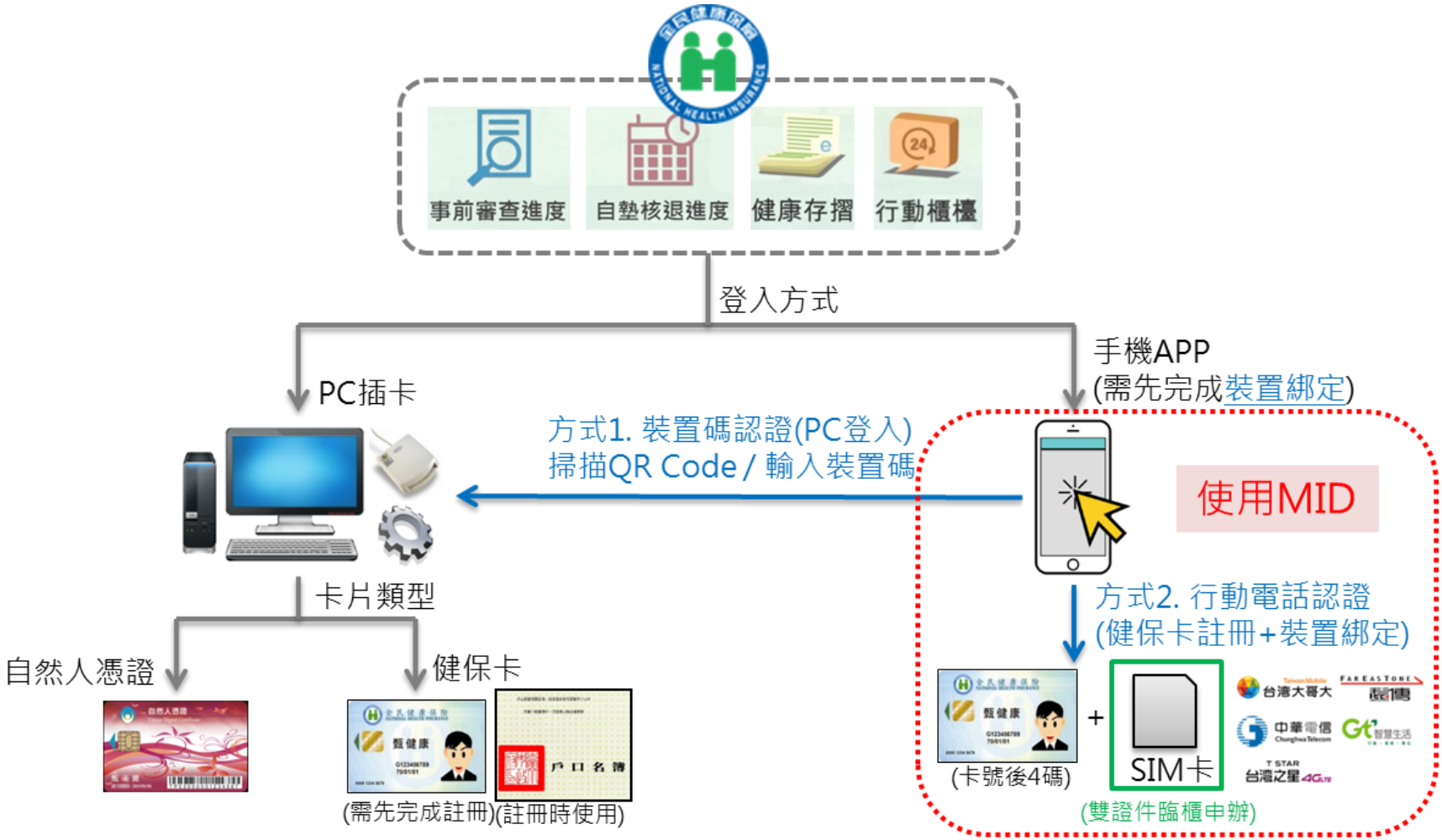
2.依據安全等級選擇適用驗證信物

依應用提供服務內容之安全等級，亦可參考現行業界的使用場景作為參考指標。

3.標準的參照

國發會訂定之身分識別機制強度方向一致。

健保快易通 採用行動電話認證



※註：「健康存摺」另支援以電腦或裝置瀏覽器使用一般登入(無需插卡)，但限曾以PC插卡或APP登入者。

報稅認證方式 5 + 1

之前的報稅有五種工具.
今年新增”行動電話認證”

使用方式：進行Mobile ID
身分識別+輸入健保卡號

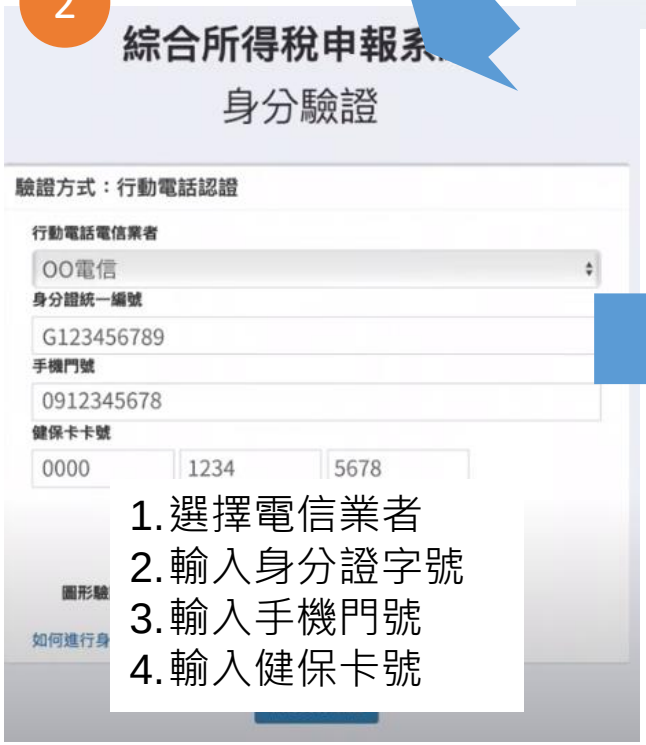
綜合所得稅可使用行動電話認證、行動身分識別(TW FidO)

在六種工具中"行動電話認證"、"行動身分識別"。

TAIWAN FIDO 臺灣行動身分識別

1

2



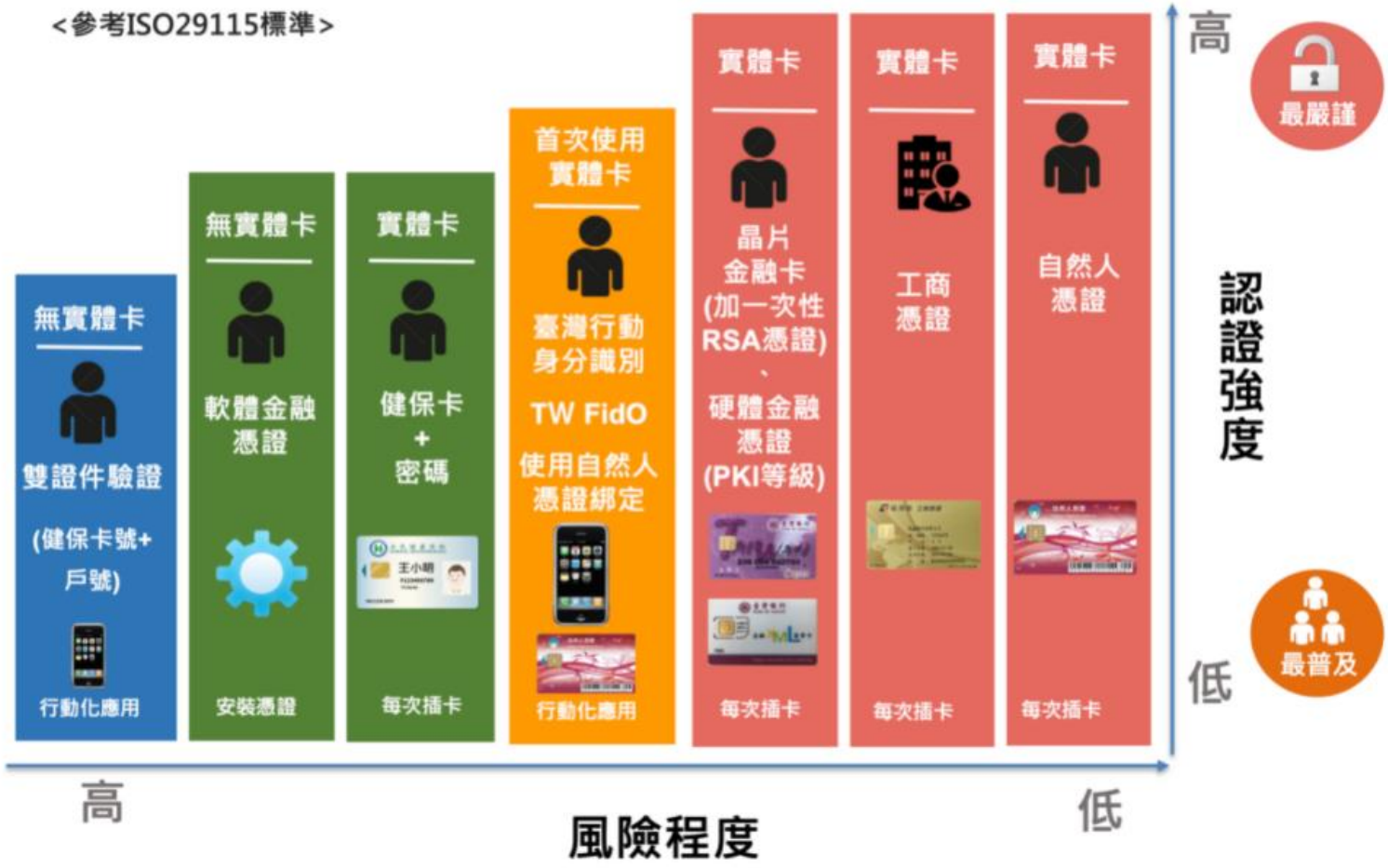
1. 選擇電信業者
2. 輸入身分證字號
3. 輸入手機門號
4. 輸入健保卡號

3

拿出本人手機掃描
PC螢幕上的QR碼

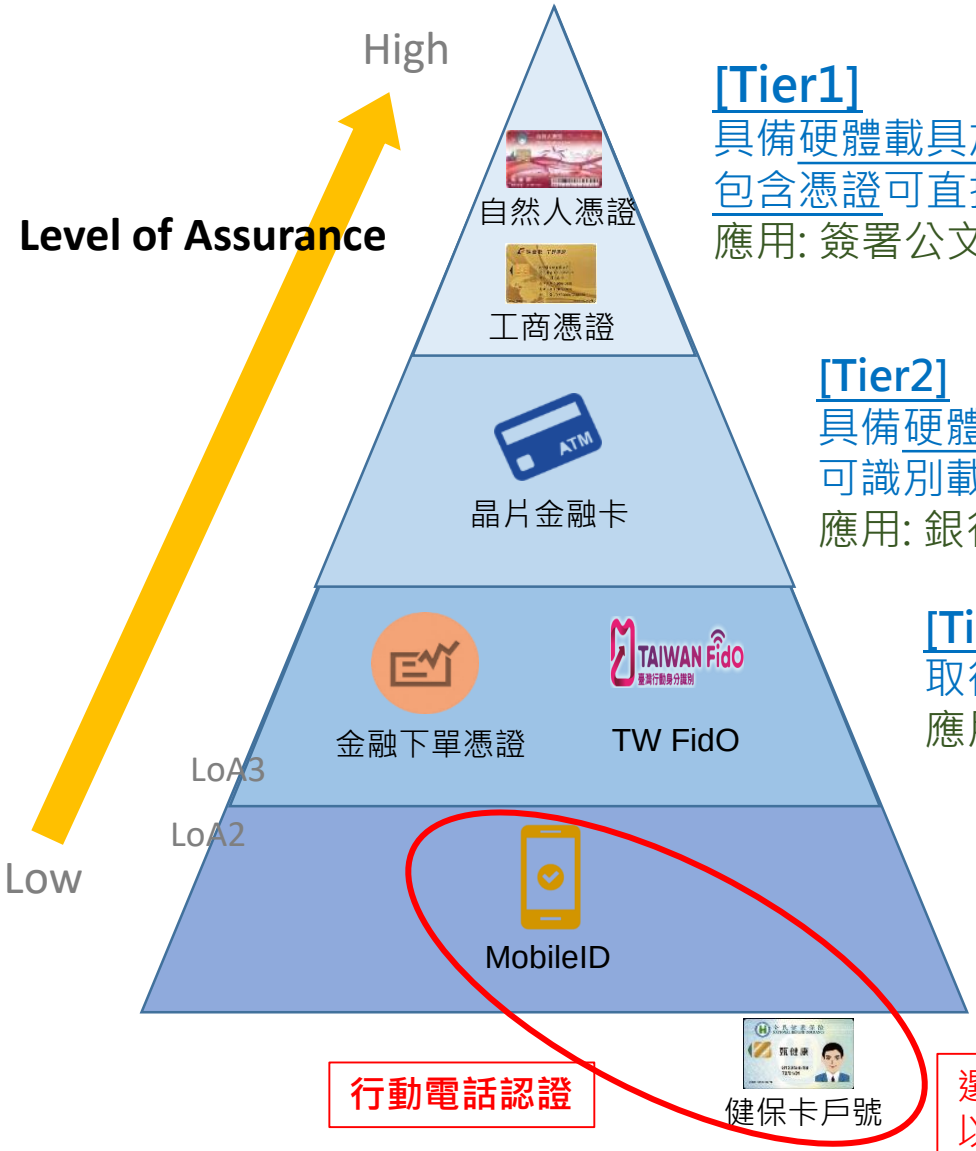
按下確認後回到 PC
線上版繼續操作

身分識別信物比較



資料來源:國發會網站

身分識別信物比較



[Tier1]
具備硬體載具加密保護，
包含憑證可直接做為身分識別與數位簽章
應用: 簽署公文、申辦勞保業務

[Tier2]
具備硬體載具加密保護，
可識別載具持有人與相關資訊
應用: 銀行、投信、券商線上開戶

[Tier3]
取得、驗證相對嚴謹之加密保護軟體信物
應用: 網路報稅、股東投票

[Tier4]
使用單因子做為驗證信物
應用: 台北通、關貿、健保署

行動電話認證

選取多項信物提升為信賴互補多因子
以提升其驗證安全等級要求，

中華民國內政部
MINISTRY OF THE INTERIOR, R.O.C. (TAIWAN)

TWID
身分識別中心

TAIWAN FidO 行動身分識別系統
申請說明

維運經理 臺灣網路認證 藍天浩

綱要

- 介接情境
- 申請流程
- 問題與討論

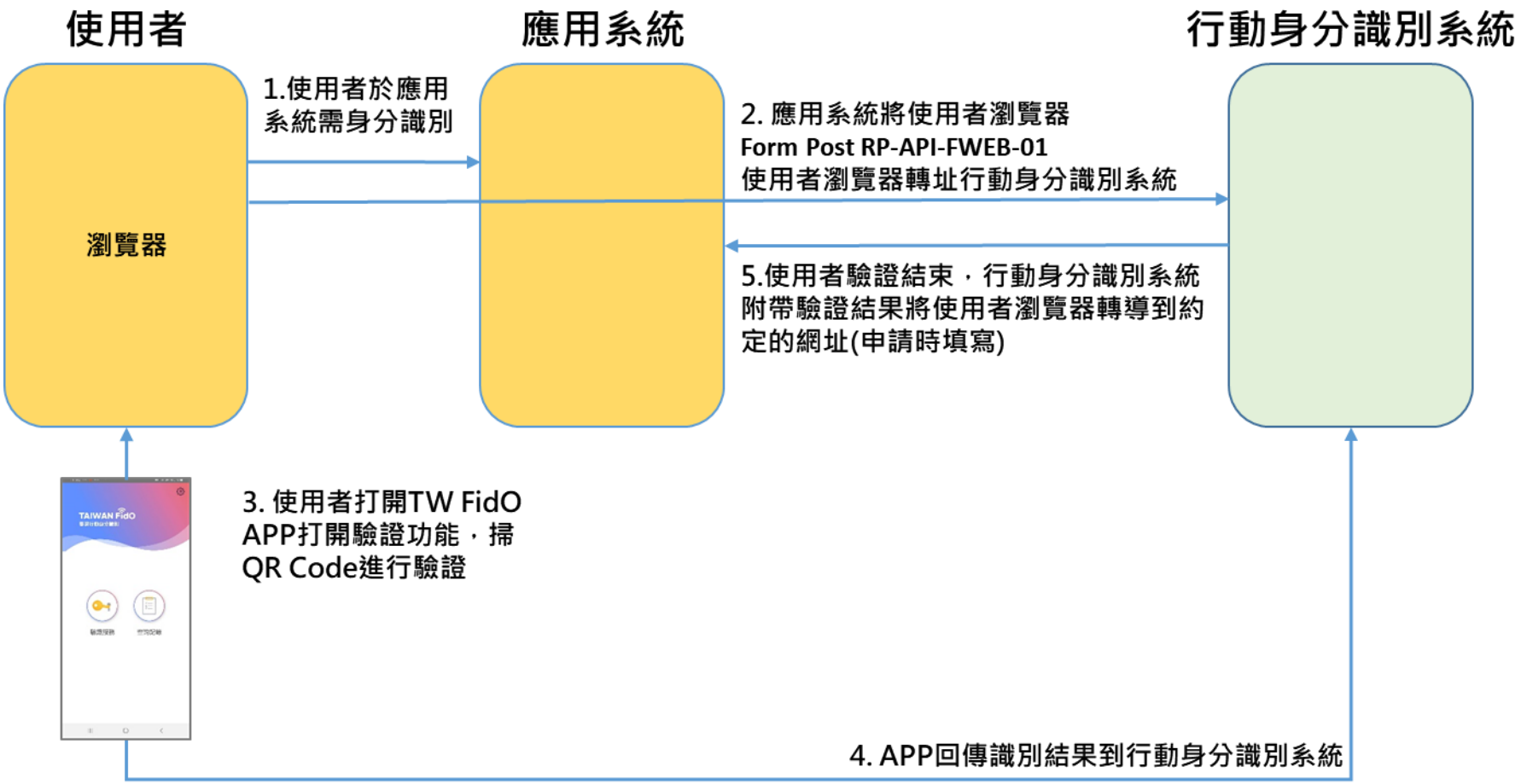
https://fido.moi.gov.tw/

介接情境

1. 應用系統網頁導頁至行動身分識別系統(APP)
2. 應用系統網頁導頁至行動身分識別系統(USB)
3. 應用系統產生QR Code
4. 行動身分識別系統推播至APP

介接情境

1. 應用系統網頁導頁至行動身分識別系統(APP)

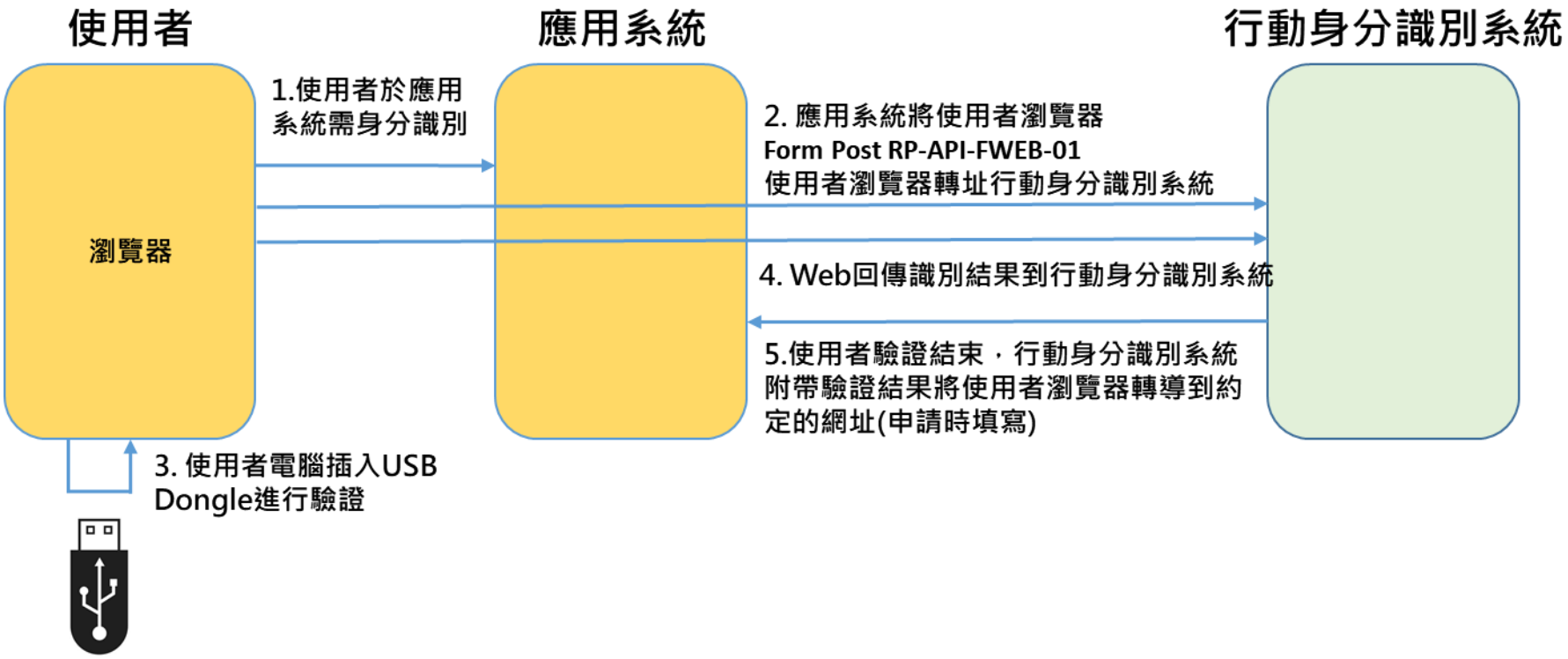


介接情境

1. 應用系統網頁導頁至行動身分識別系統(APP)

介接情境

2. 應用系統網頁導頁至行動身分識別系統(USB)

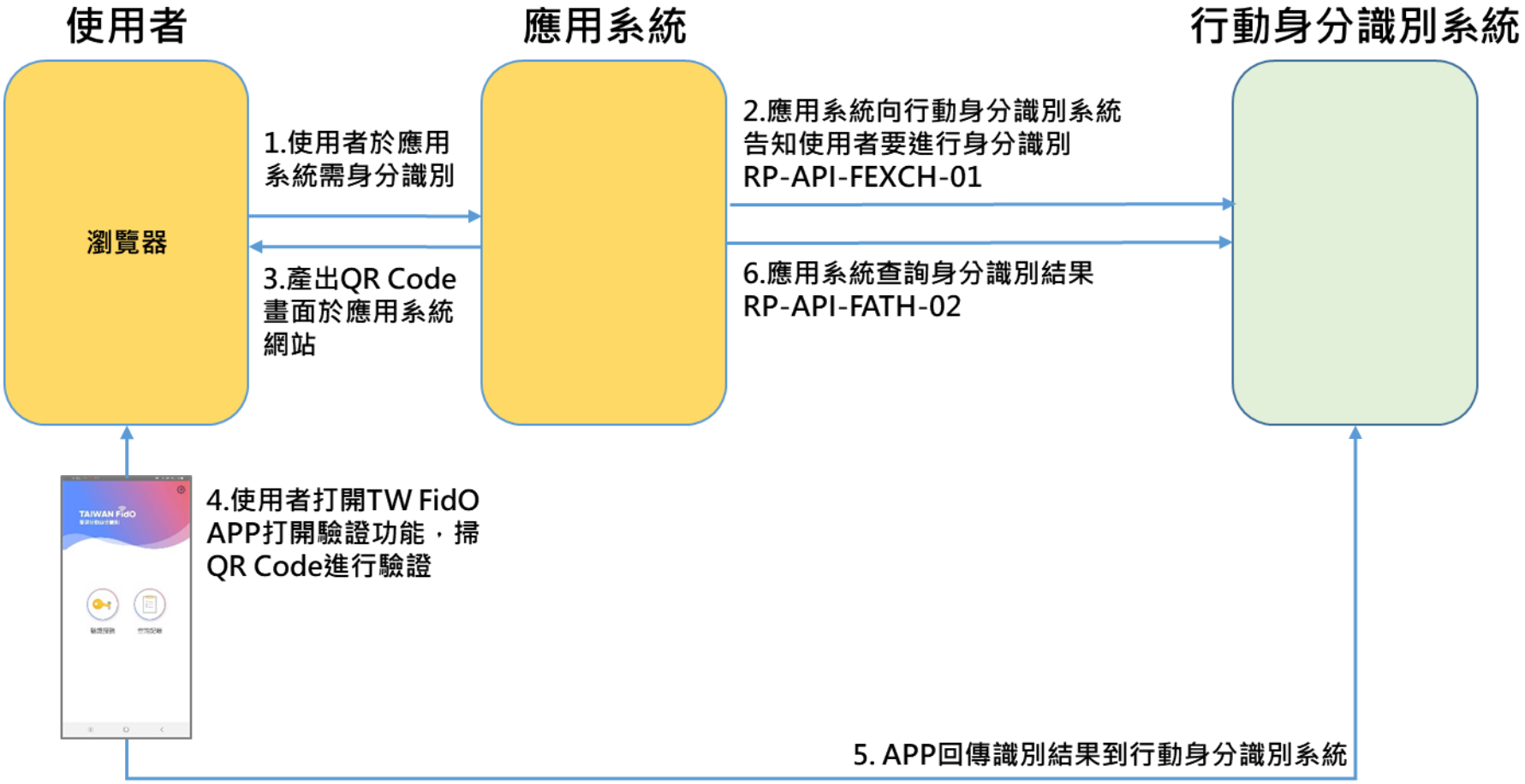


介接情境

2. 應用系統網頁導頁至行動身分識別系統(USB)

介接情境

3. 應用系統產生QR Code

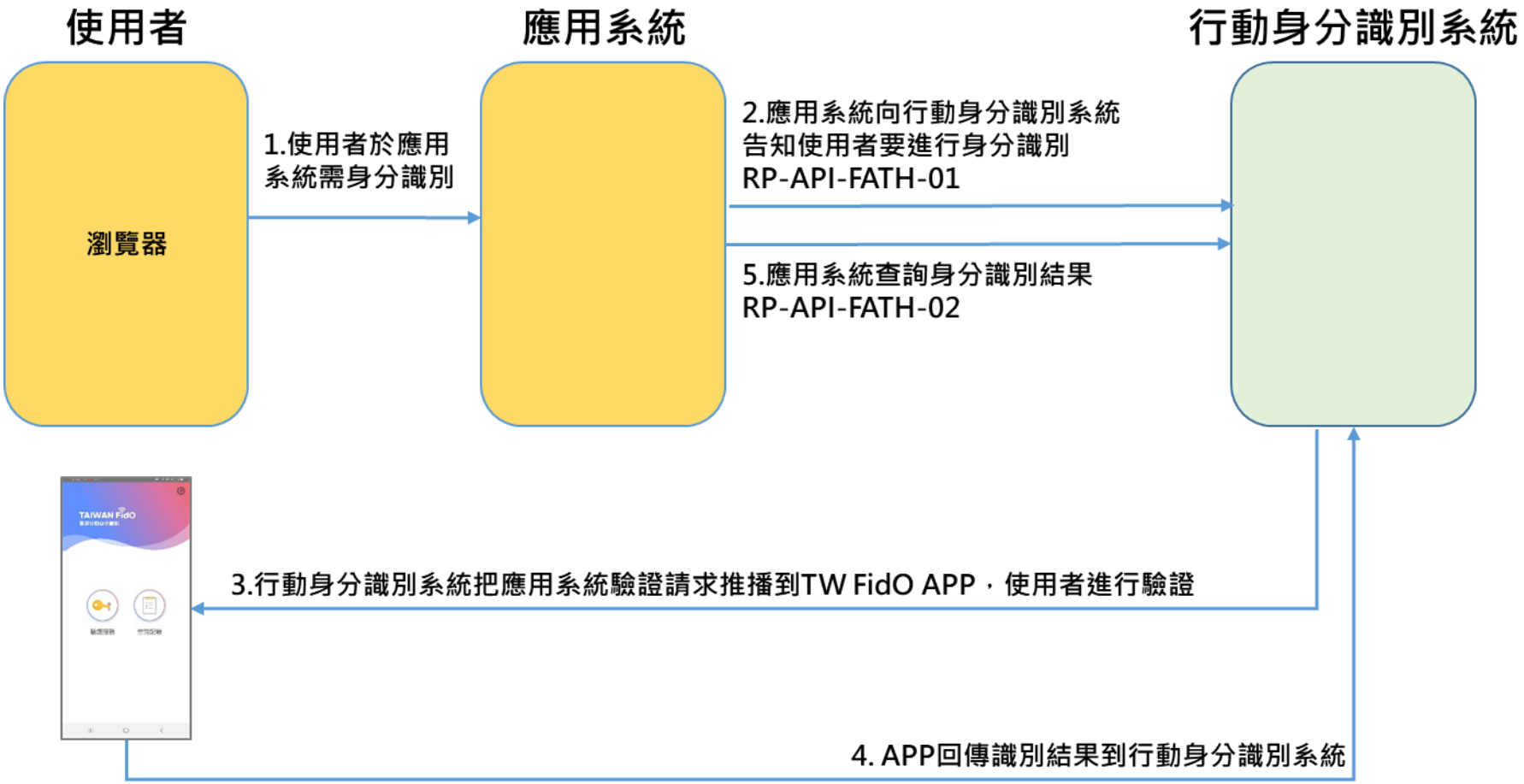


介接情境

3. 應用系統產生QR Code

介接情境

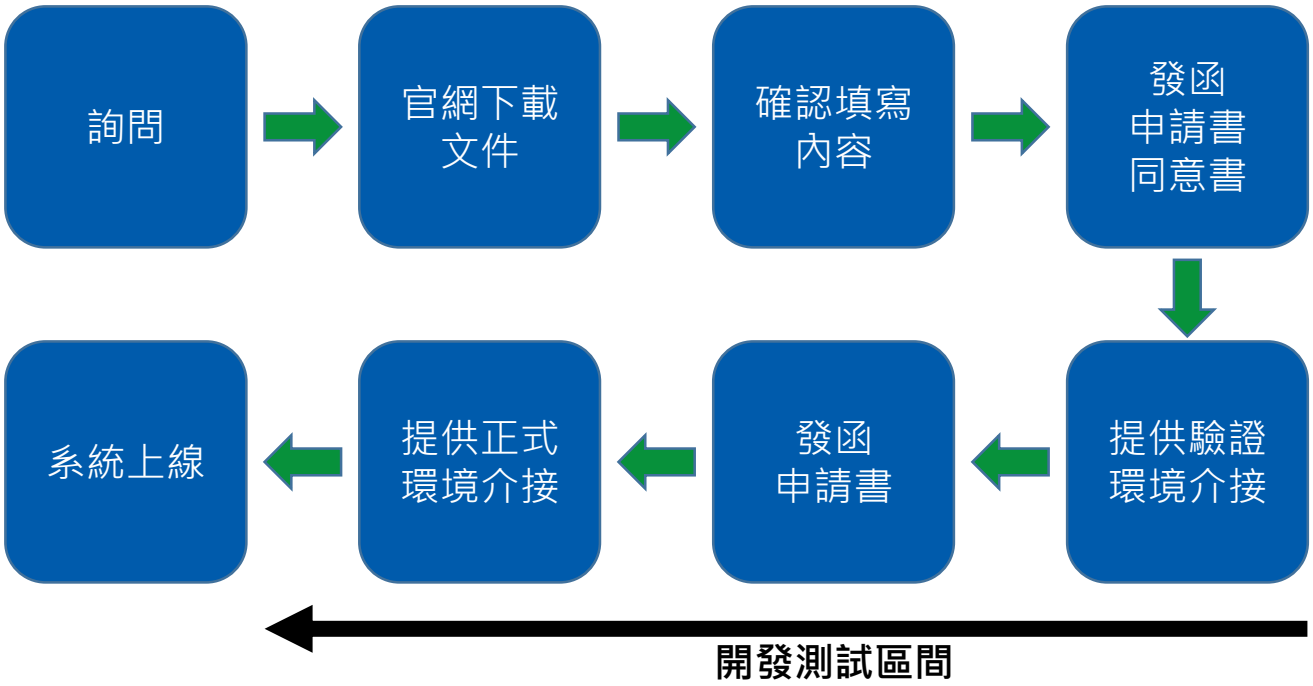
4. 行動身分識別系統推播至APP



介接情境

4. 行動身分識別系統推播至APP

申請流程


詢問
官網下載文件
確認填寫內容
發函申請書同意書
提供驗證環境介接
發函申請書
提供正式環境介接
系統上線
開發測試區間

申請書

TAIWAN FidO 臺灣行動身分識別服務申請書

申請日期：　　□新增　□異動　□刪除

1. 申請環境(擇一)	□正式環境 □驗證環境
2. 機關名稱(部會/縣市政府)	
3. 單位名稱(局/處/署/中心…)	
4. 申請介接應用系統中文名稱	
5. 申請介接應用系統說明	
6. 申請介接應用系統服務對象(可複選)	□政府機關 □公營事業 □學術機關 □公司行號 □一般民眾 □公務人員 □其他
7. 申請介接應用系統現有身分識別方式(可複選)	□組織憑證 □工商憑證□自然人憑證 □醫事憑證 □電子憑證 □健保卡 □戶口名簿戶號 □會員管理 □其他
8. 申請介接應用系統高峰時機(可複選)	□1月 □2月 □3月 □4月 □5月 □6月 □7月 □8月 □9月 □10月 □11月 □12月
9. 申請介接應用系統每月預估服務量	每月平均服務量(擇一)： □未滿1萬 □1~10萬 □11~20萬 □21~50萬 □51萬以上 高峰月分服務量(擇一)： □未滿1萬 □1~10萬 □11~20萬 □21~50萬 □51萬以上

申請書

10.申請介接應用系統資訊安全分級(擇一)	(依據行政院資通安全會報頒布之「資訊系統分級與資安防護基準作業規定」分級) □低 □中 □高	
11.RP-API-FWEB-01 成功導頁 URL	(參見服務介面說明網頁轉導模式，若不使用可不填)	
12.申請介接應用系統主機 IP	請填寫發動 API 的服務主機對外 IP	
13.介接服務時程	預計驗證環境開發與測試期間： (申請驗證環境後，3 個月內未再申請正式環境，原申請之驗證環境資料將刪除) 預計正式環境對外開放使用日期：	
14.委外服務廠商	名稱： 聯絡人： 電話： Email：	
15.介接單位人員	聯絡人(簽章)： 電話： Email：	代理人： 電話： Email：
	單位主管(簽章)： 電話： Email： (請加蓋申請單位印章戳記)	

注意事項

1. 同一個單位可以申請多個系統
2. 一個系統提供一組系統碼，用來當作呼叫 API 的鑰匙
3. 代理人必須填寫，若無請填寫主管
4. 若需要進行壓力測試，請先告知
5. 本服務僅供政府單位介接

問題與討論