無密碼的領航者
匯智安全從雲到點全面賦能

無密碼趨勢及應用挑戰

鄭嘉信總經理

匯智安全科技

大綱

落實網路「零信任」的基礎：

- 密碼在使用上的痛點
- 無密碼趨勢

技術典範轉移：

- 生物特徵辨識與及 FIDO Alliance 推動 FIDO2 規範
- FIDO 是一種公鑰密碼應用 (Public Key Cryptographic Application)

如何導入 FIDO2 無密碼認證？

- 如何運用進而善用 (技術知識的門檻)
- FIDO2 生態系統的建立 (夥伴與市場競爭)

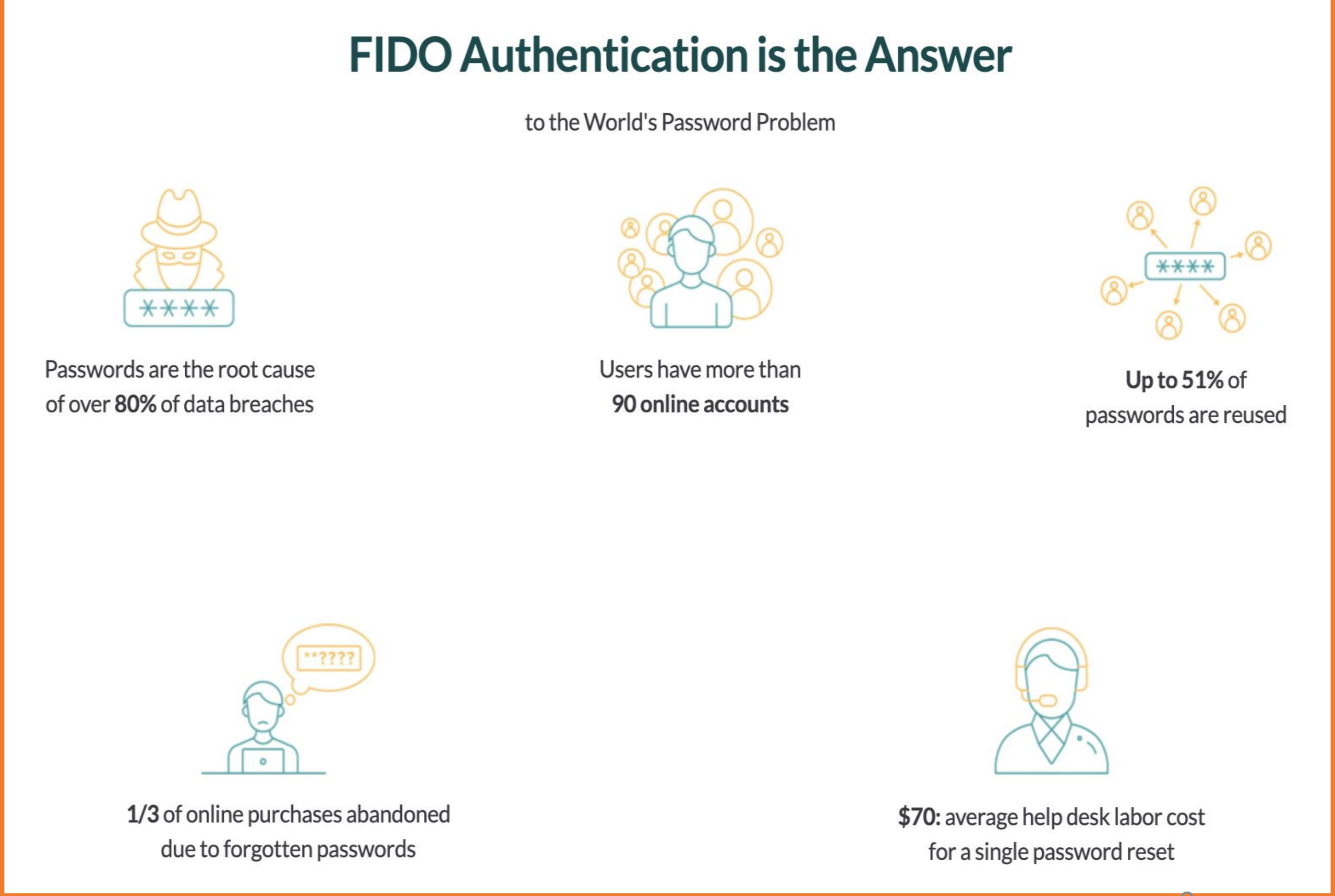
無密碼才能落實網路「零信任」

「零信任」是指 ……
「除非驗證，絕不信任」

但是 ……

身份認證的三個手段：
- What-you-know (密碼)
- What-you-have
- Who-you-are (最強的方式)

密碼是三者最弱的



FIDO Authentication is the Answer

to the World's Password Problem

Passwords are the root cause of over **80%** of data breaches

Users have more than **90 online accounts**

Up to 51% of passwords are reused

1/3 of online purchases abandoned due to forgotten passwords

$70: average help desk labor cost for a single password reset

無密碼真的「大勢所趨」？是否過於樂觀？

- 推動「無密碼」甚至於「不需使用者帳號」認證，以解決網路安全最大潛在破口
  (From Password-less to Username-less)

- 無密碼應用其實分成 to-C 與 to-B
  Public Cloud Services v.s. Enterprise Authentication

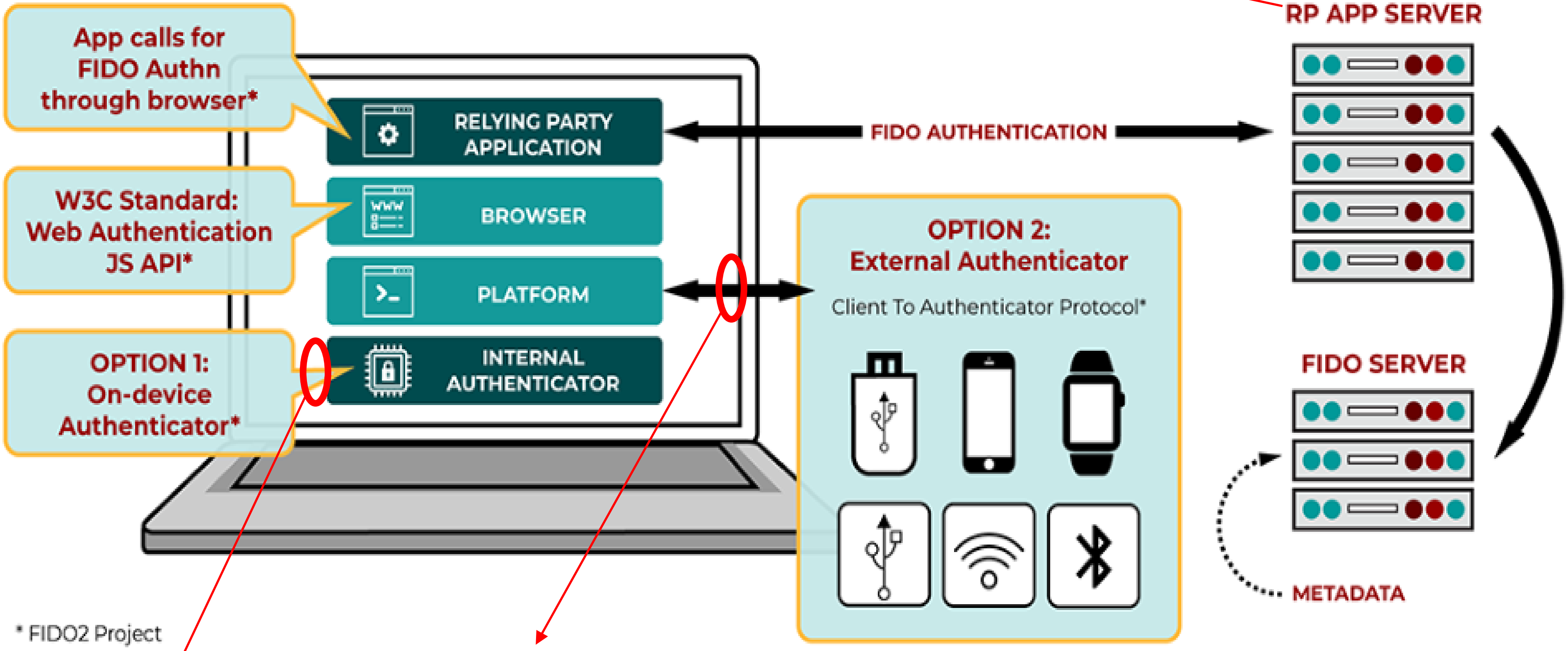
- 企業應用 (to-B) 才是對無密碼認證最強勁的需要
  (Enterprise Attestation/EA)

生物特徵識別與 FIDO 認證

FIDO = Fast IDentity Online 源頭就是想以生物辨識取代密碼

Timeline	Milestones
2009 (BIO)	PayPal、Validity Sensors (被指紋模組大廠 Synaptics 收購) 發想以指紋取代密碼
2013 (MFA)	FIDO Alliance 公開成立，Google、NXP 加入，推廣雙因素認證 (second factor authenticator)
2014	FIDO UAF (Universal Authentication Framework) 標準公布，使用設備生物辨識來啟動 FIDO 密鑰進行無密碼強認證 FIDO U2F (Universal 2nd Factor) 標準公布，使用外部硬體保護 FIDO 強認證密鑰進行認證
2014-2017	Microsoft, Facebook 與 Apple 加入對 UAF/U2F 的支援
2018 (FIDO2)	FIDO2 標準公布，強調一次性無密碼認證協議。 W3C 研議採納 FIDO2 標準制定 WebAuthn (包括外部硬體設備 CTAP 協議)
2019 (WebAuthn)	W3C 正式推薦 WebAuthn ，並獲得所有主流瀏覽器支援。

技術典範轉移


App calls for FIDO Authn through browser*
W3C Standard: Web Authentication JS API*
OPTION 1: On-device Authenticator*
RELYING PARTY APPLICATION
BROWSER
PLATFORM
INTERNAL AUTHENTICATOR
FIDO AUTHENTICATION
OPTION 2: External Authenticator
Client To Authenticator Protocol*
RP APP SERVER
FIDO SERVER
METADATA

RP = Relying Party

* FIDO2 Project

CTAP (Client-To-Authenticator Protocol)

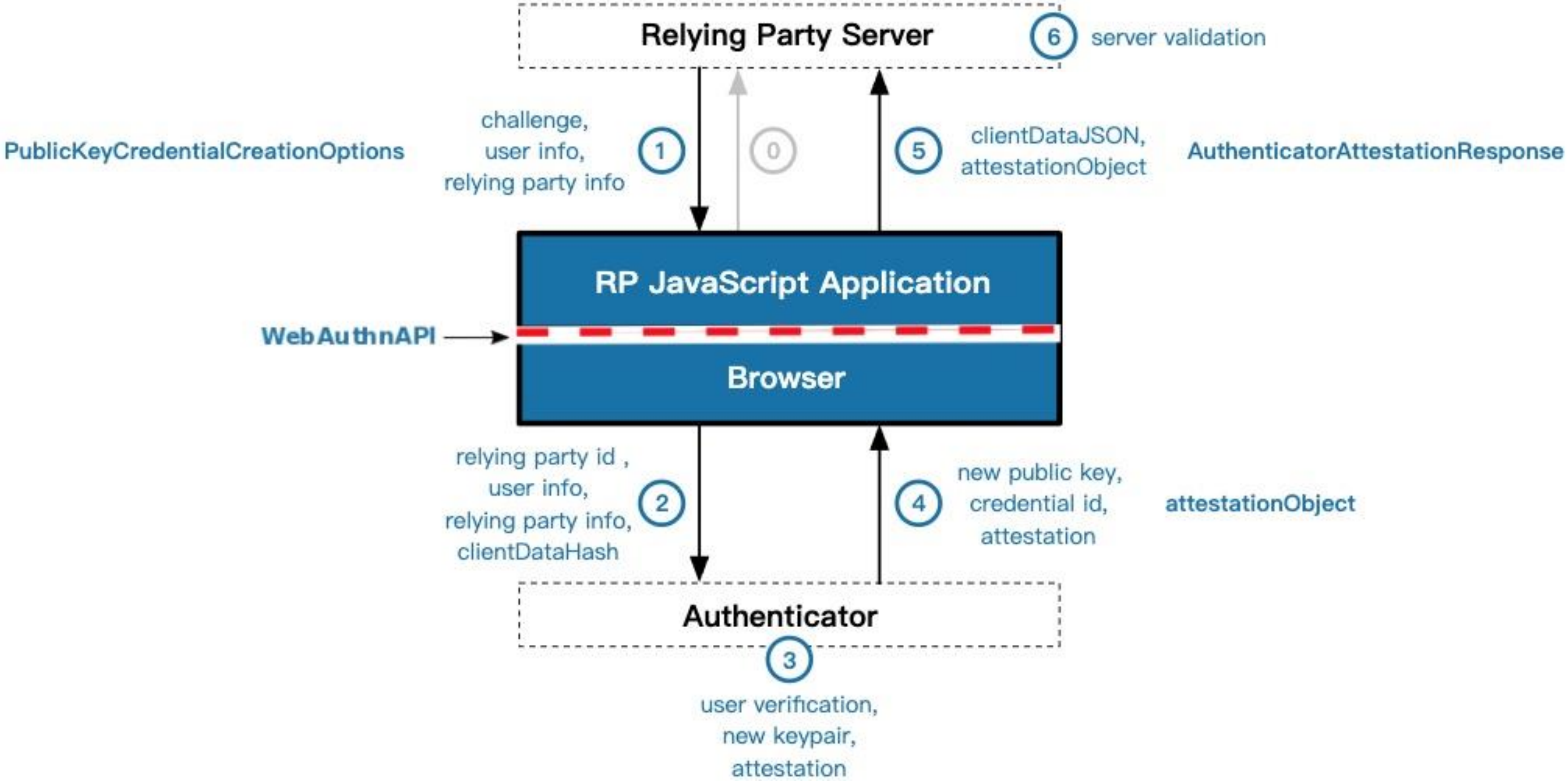
On-device activation by biometric approach

FIDO 是公鑰密碼應用、不是生物特徵驗證

- FIDO 認證是基於：
「使用者對於每一個 FIDO RP 擁有證明自己身份的私鑰」
- FIDO RP 透過 FIDO Server 保存使用者的公鑰
要求被驗證使用者證明自己身份所產生的數位簽章
- 使用者第一次註冊時，要產生專屬金鑰對
並採用 FIDO Server 所信任的公鑰證明自己擁有的公鑰是合法的
然後上傳註冊該公鑰
- FIDO Server 保存使用者的公鑰，
並在每次驗證使用者時，要求使用者產生指定資料的數位簽章，
以證明自己擁有註冊公鑰所對應的私鑰
- 如果沒有獨立管理密鑰的裝置，
FIDO 允許使用者使用生物特徵解鎖保管在電腦裡的私鑰，以產生簽章

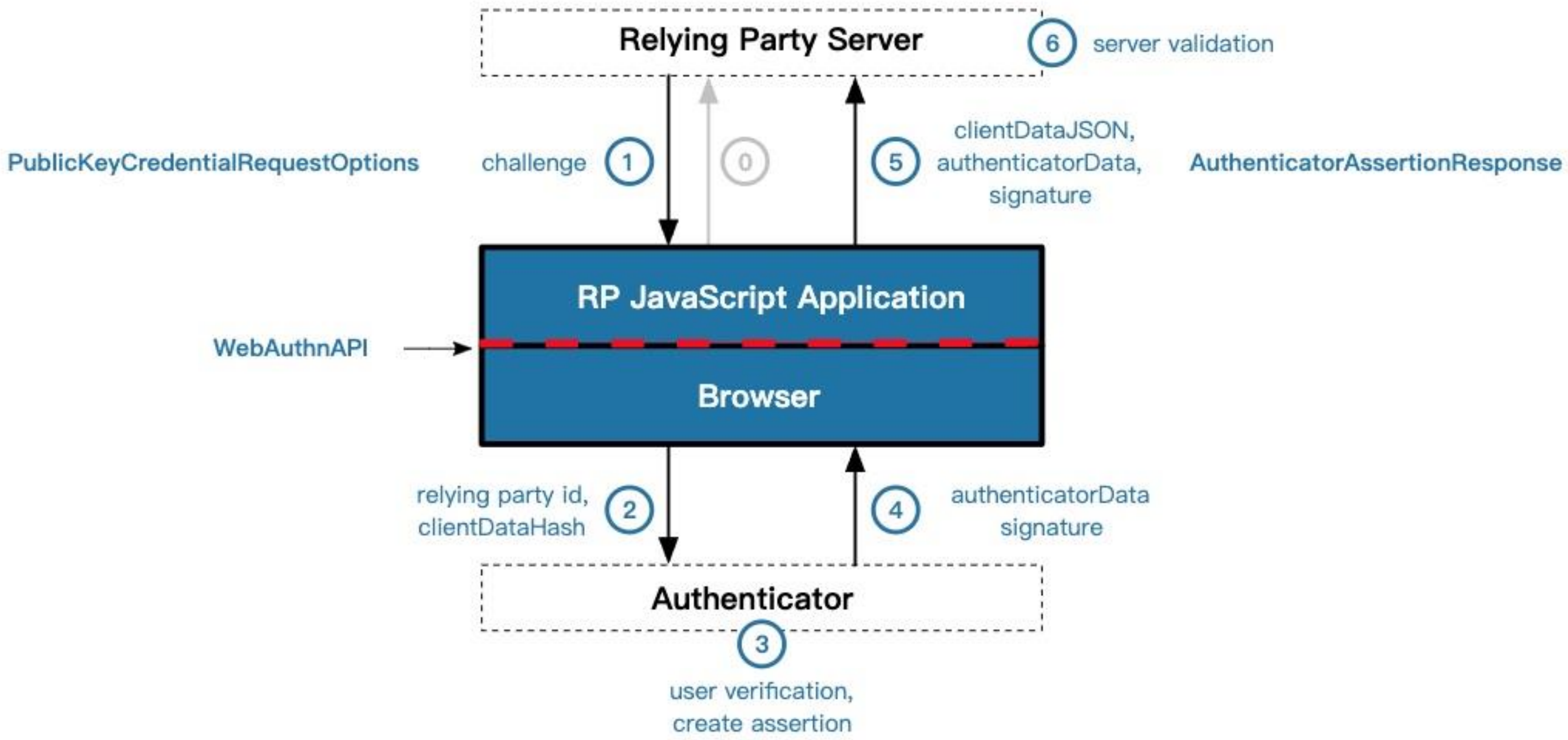
FIDO 使用者註冊公鑰

Registration flow



FIDO RP 驗證使用者

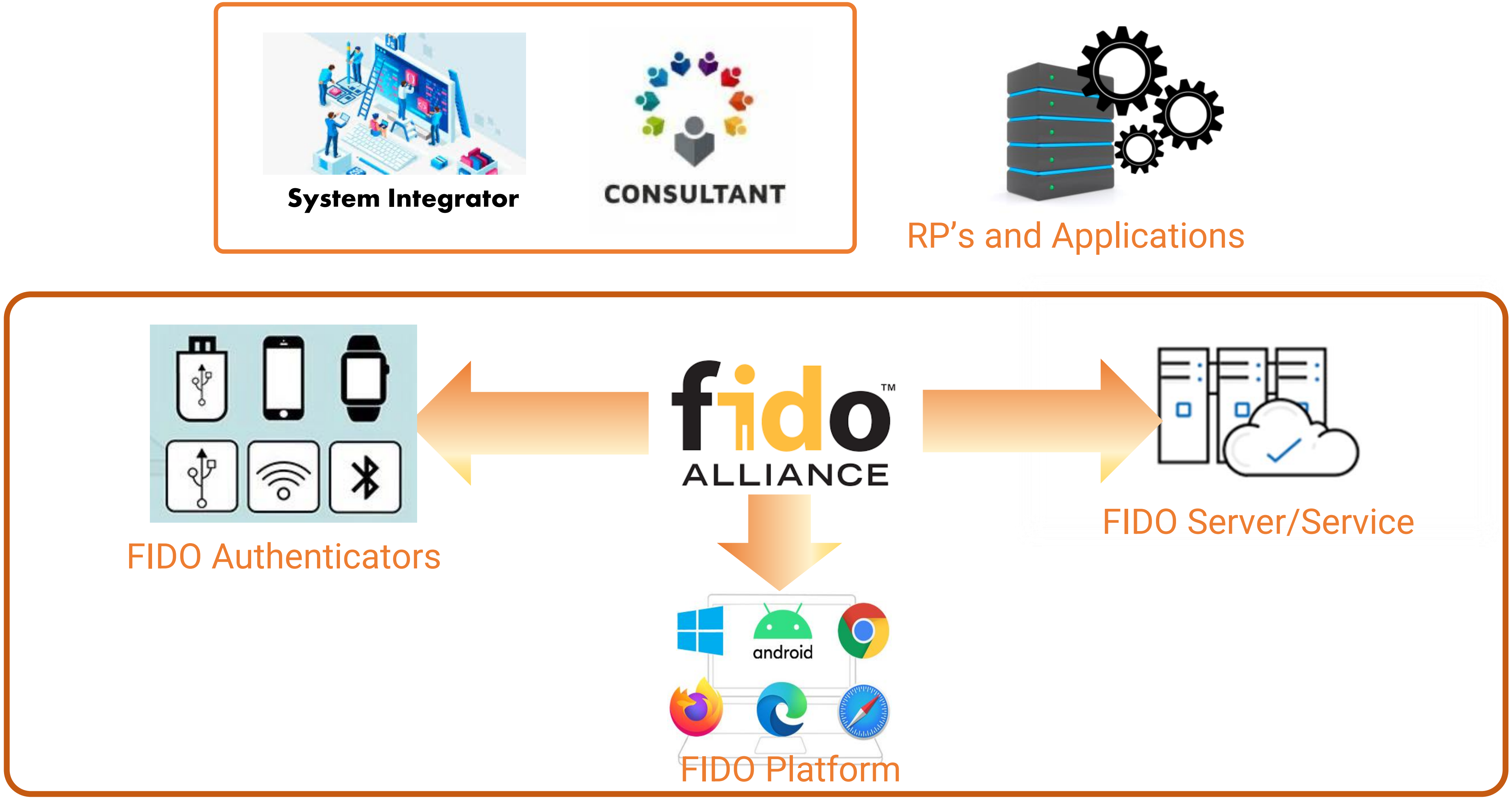
Authentication flow



導入 FIDO 無密碼認證的知識門檻

- FIDO 認證的技術規格：
相對複雜且使用許多密碼演算法
規格框架龐大複雜
- FIDO 認證框架保留許多彈性與實作選項
Authenticator/RP/Server 各有細節，IT 人員難以掌握
- Browser、FIDO UAF 終端、Authenticator 裝置、Server
對支援 FIDO 協議各有立場
- 生物識別雖使 FIDO 認證有親和力
以但根本不是 FIDO 認證的基礎
公鑰密碼系統才是 FIDO 的基礎

FIDO 無密碼認證生態系統



RP’s and Applications

FIDO Authenticators

FIDO Server/Service

FIDO Platform

企業導入 FIDO 無密碼認證需要什麼？

- 了解無密碼認證的真實需求

Authenticators/Platforms/Servers 的選擇

- 實現 FIDO 的企業管理需要

RP’s/企業管控政策

- FIDO Server 的使用與安全性

內部建制或公開服務

- 可靠安全的 Authenticators

安全等級/協議符合認證

定位 FIDO 無密碼技術的賦能者 (Enabler)
才能真正協助企業導入 FIDO 無密碼認證

WiSECURE Technologies (WiSECURE) was founded in 2019, aiming to design standardized hardware security modules in various form factors, including PCIe cards, microSD cards, USB tokens, etc. WiSECURE specializes in cryptographic implementation and key management, which are fundamental in storage encryption, authentication, emerging digital assets, industrial control, IoT, WFH (Working from home), digital rights managements (DRM) and other innovative services and applications.

匯智安全科技

無密碼的領航者
匯智安全從雲到點全面賦能

無密碼實務與落地

梁家榮資訊長

匯智安全科技

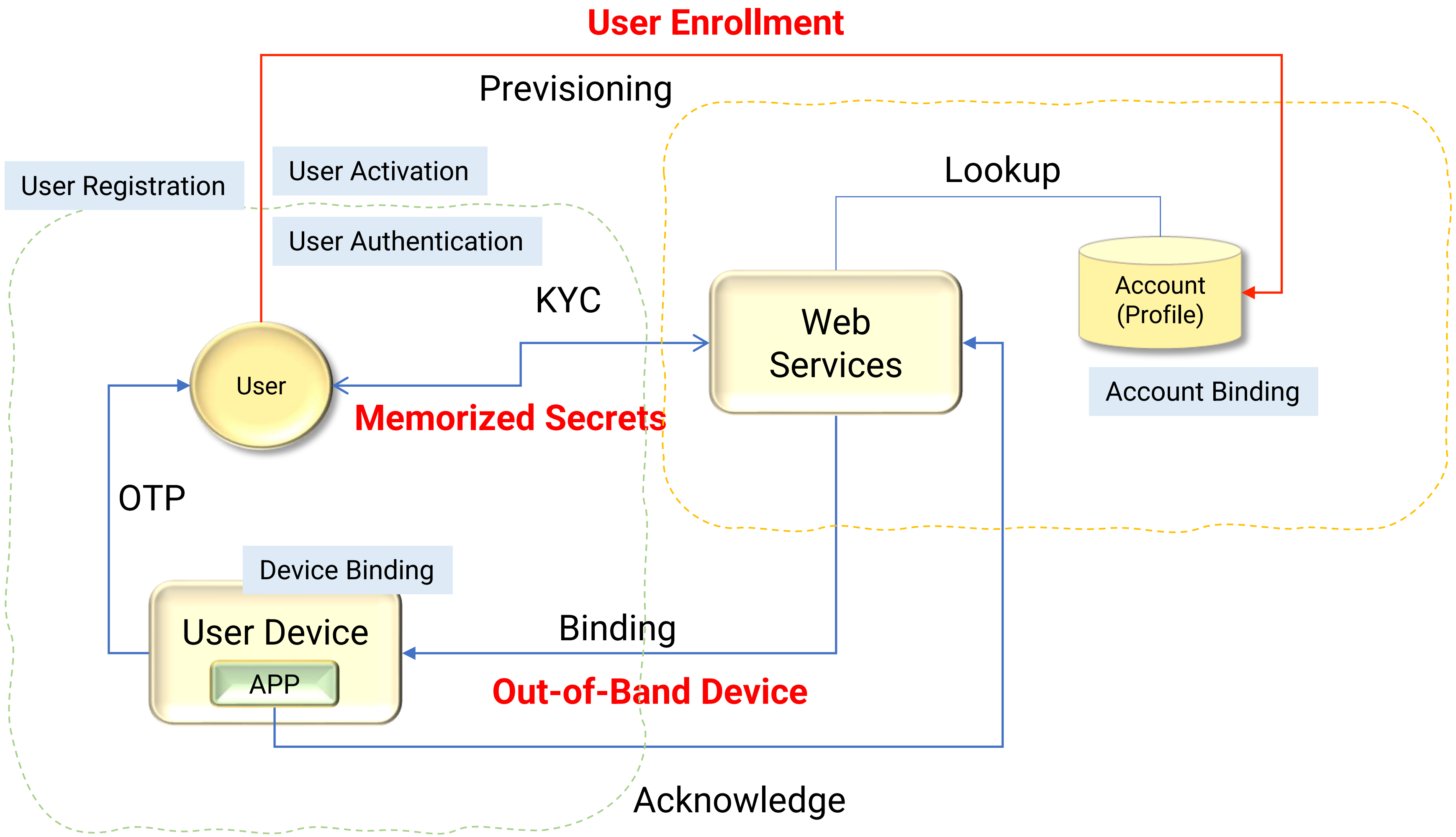
大綱

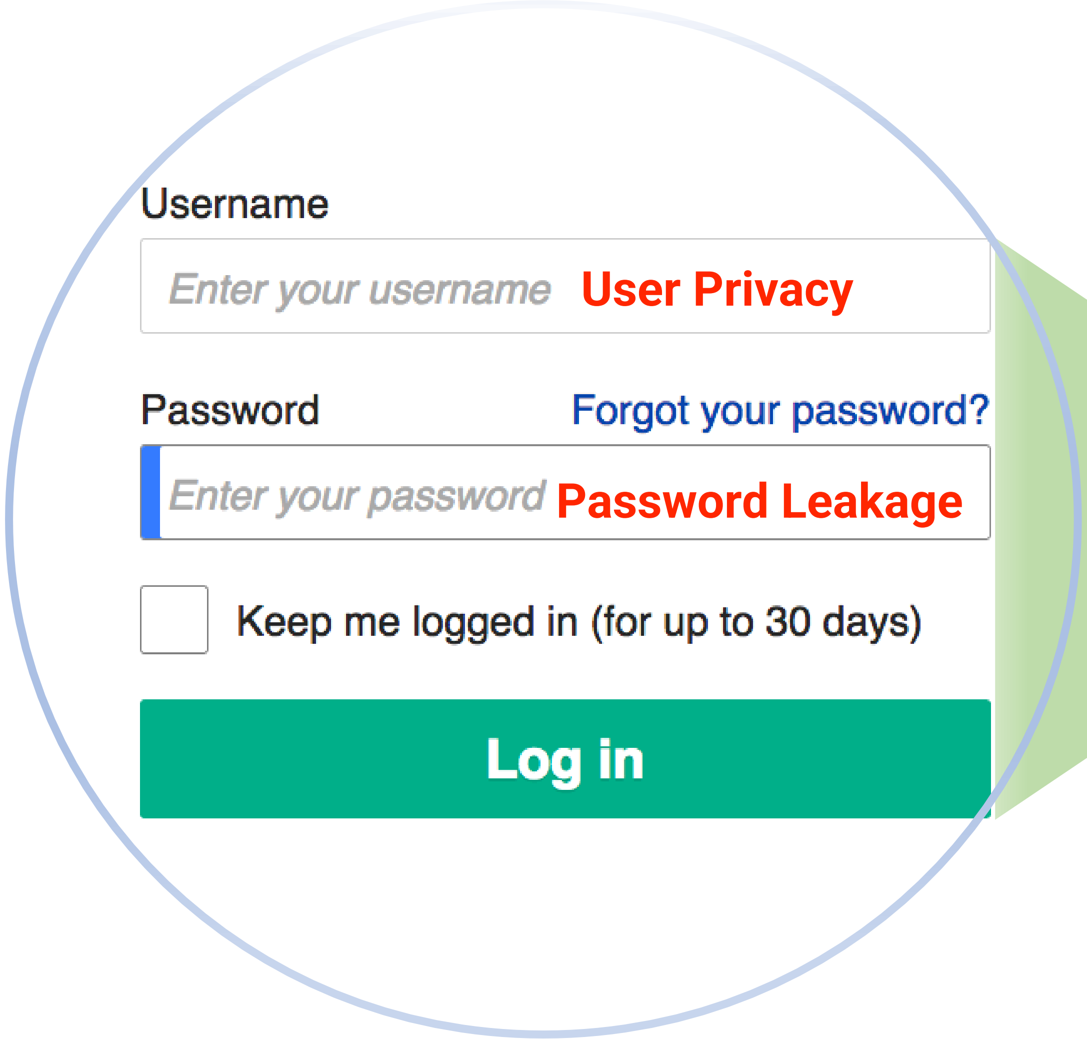
FIDO 無密碼解決方案

- 消費端
  - 方便與安全性
  - 行動裝置認證載具
- 企業端
  - 政策實施與應用環境啟動
  - 多樣化認證載具

匯智安全 FIDO 生態系

- 從晶片、裝置到雲服務
- 企業 FIDO 導入實例及解決方案


User Enrollment
Previsioning
User Registration
User Activation
User Authentication
Lookup
KYC
Account
(Profile)
Web
Services
User
Memorized Secrets
Account Binding
OTP
Device Binding
User Device
APP
Binding
Out-of-Band Device
Acknowledge



Username

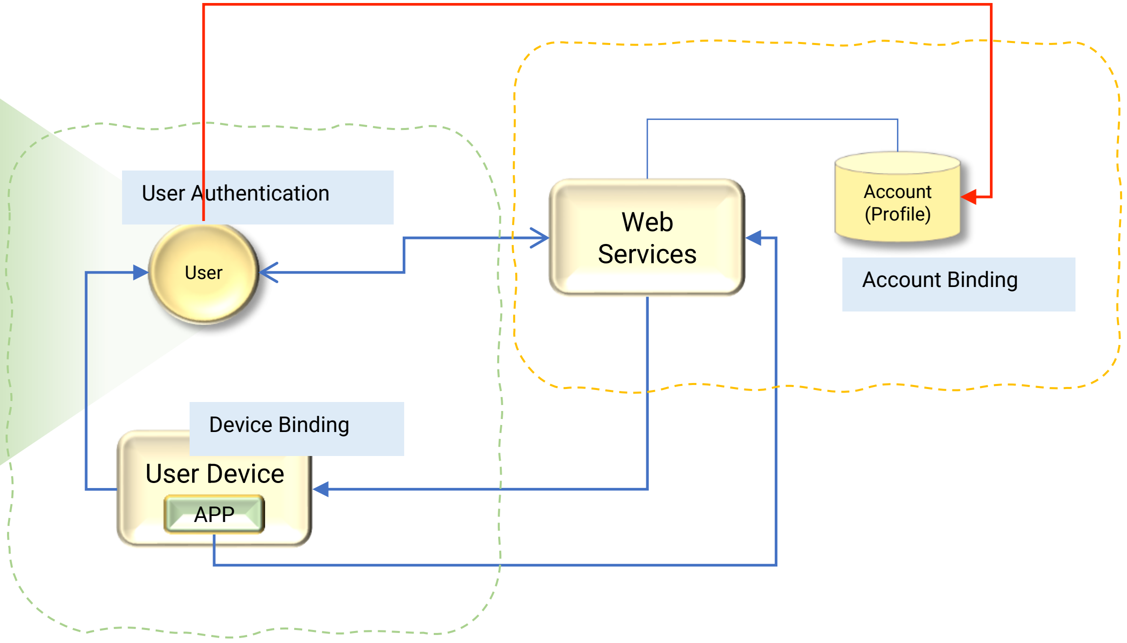
Enter your username **User Privacy**

Password Forgot your password?

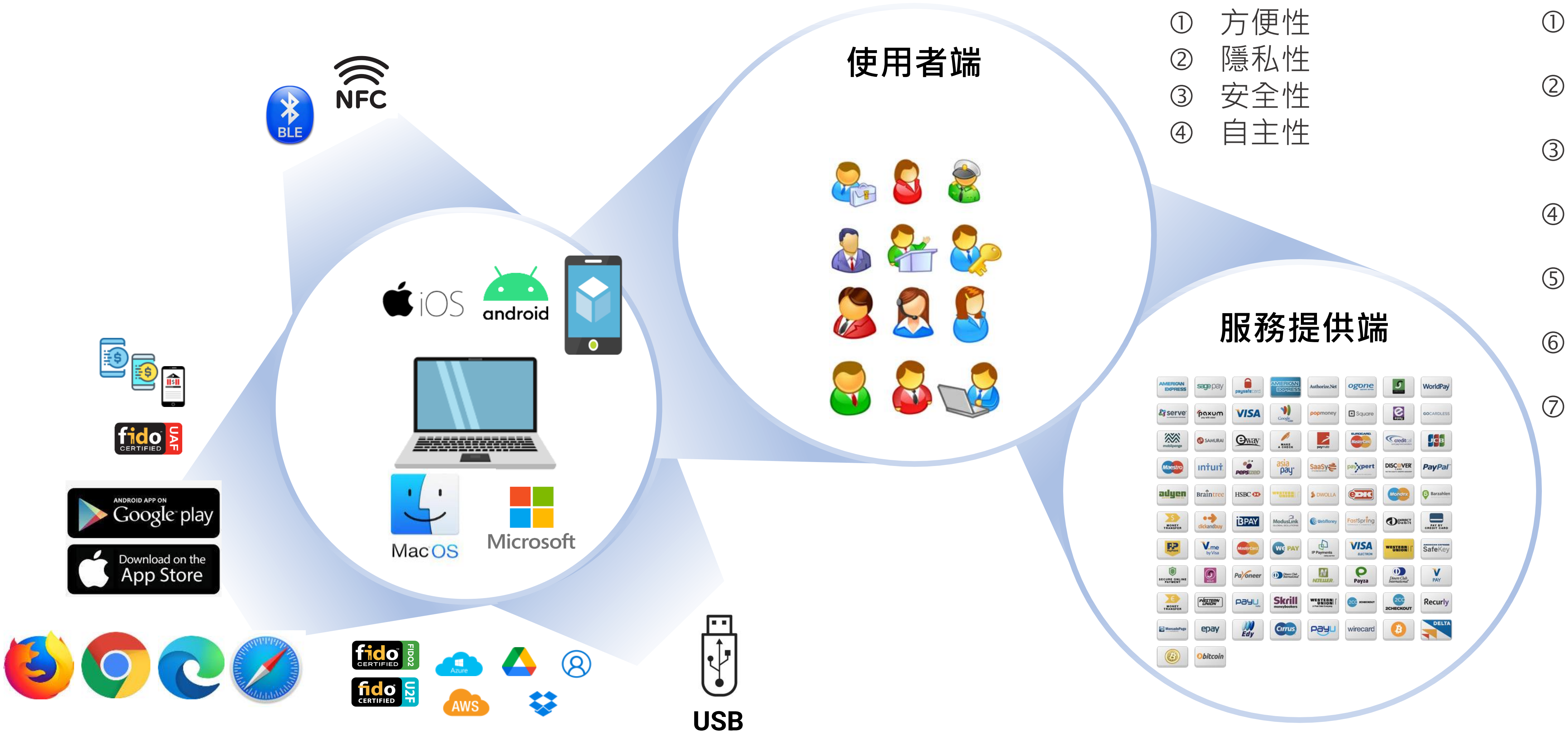
Enter your password **Password Leakage**

□ Keep me logged in (for up to 30 days)

Log in



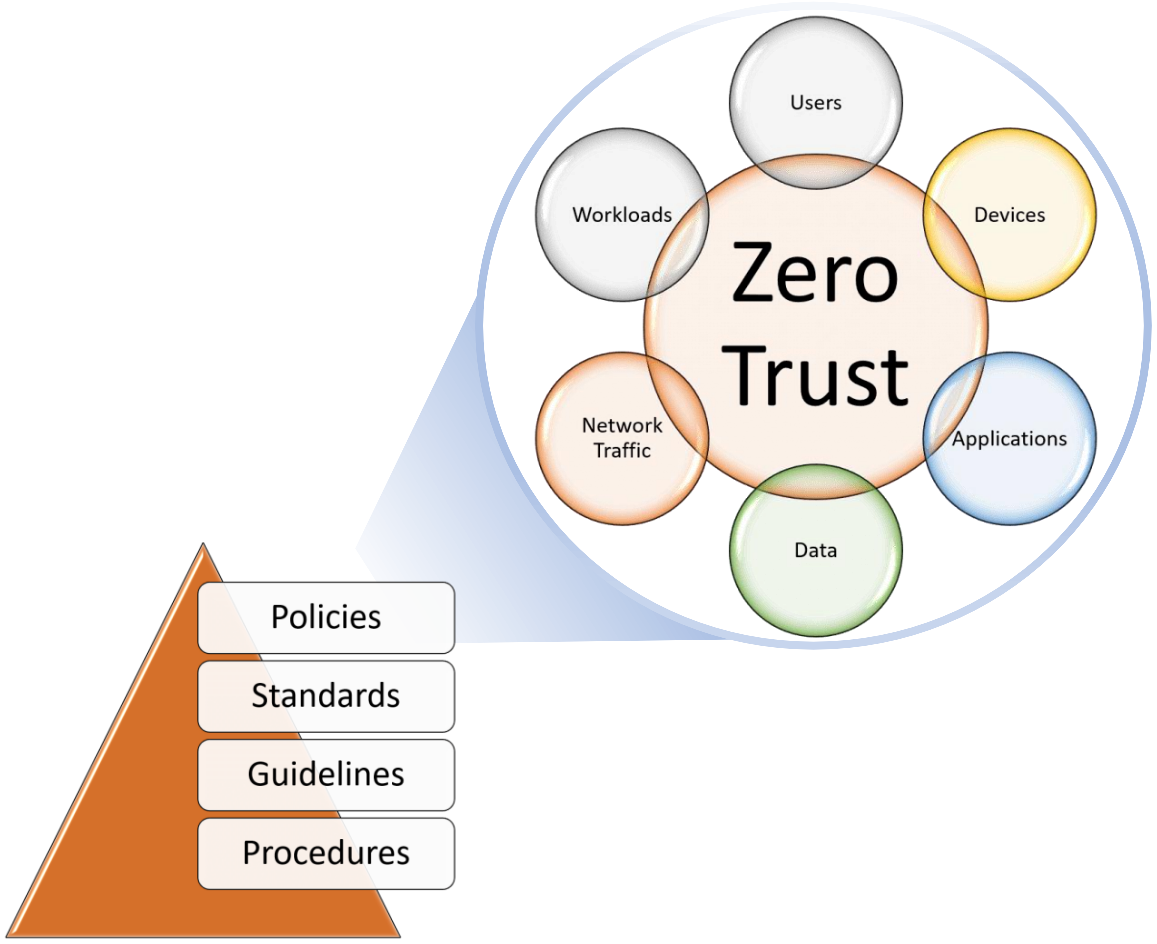
FIDO 無密碼解決方案 消費端



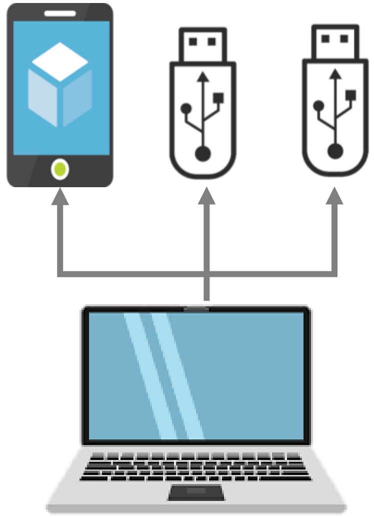
① 方便性
② 隱私性
③ 安全性
④ 自主性

① 標準
互聯驗證
② 共通
平台內建
③ 低廉
建置成本
④ 簡易
操作體驗
⑤ 快速
導入部署
⑥ 可用
維運備援
⑦ 法遵
監理規範

FIDO 無密碼解決方案 企業端 政策實施



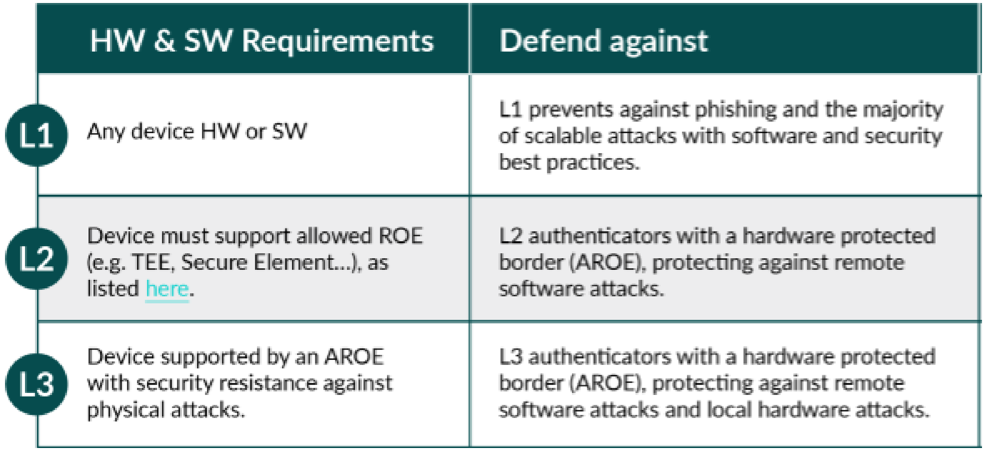
1) **Security Policy**
   1) Zero Trust Architecture
   2) Secure Binding
2) **Governance (In Control, Auditing and Traceability)**
   1) Device Management, Provisioning & Pre-Issuance
   2) Exclusive for Enterprise Applications/Services
   3) Privilege Account of the Legacy Systems
   4) Regulation Compliance eg. GDPR, Digital Identity Guidelines
   5) Auditing
3) **Enterprise Operation**
   1) Backup and Operation Maintenance
   2) Enterprise Assets
   3) Desktop/Endpoint Logon (Azure AD)



Source:
https://www.certmike.com/security-policy-framework/
https://www.atg-it.co.uk/services/cyber-security/mobile-device-management-mdm/
https://www.wirelesssupport.com/Solution/mdm

General Physical Authenticator Requirements

- Rate Limiting (Throttling) 頻次/流量管制
- Use of Biometrics 生物特徵
- Attestation 證書
- Verifier Impersonation Resistance “strongly MitM resistant” 冒充防範
- Verifier-CSP Communications 認證協定
- Verifier-Compromise Resistance 破解防護
- Replay Resistance 複製重傳
- Authentication Intent 識別驗證
- Restricted Authenticators 設備管制



	HW & SW Requirements	Defend against
L1	Any device HW or SW	L1 prevents against phishing and the majority of scalable attacks with software and security best practices.
L2	Device must support allowed ROE (e.g. TEE, Secure Element...), as listed here.	L2 authenticators with a hardware protected border (AROE), protecting against remote software attacks.
L3	Device supported by an AROE with security resistance against physical attacks.	L3 authenticators with a hardware protected border (AROE), protecting against remote software attacks and local hardware attacks.

Source: NIST SP800-63B

Authenticator Assurance Level 2

Memorized Secrets (?) + Out-of-Band Devices

AAL1 ?

Memorized Secrets + Single-Factor Cryptographic Software

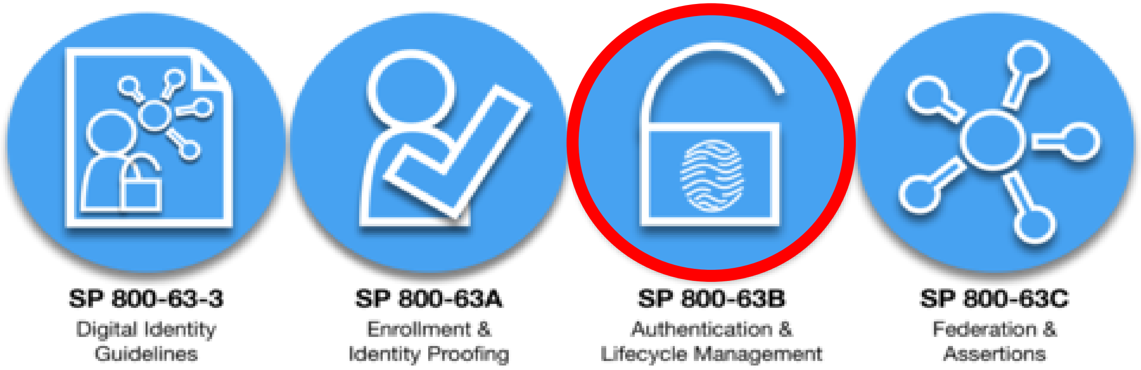
AuthTron M

Multi-Factor Cryptographic Software

AuthTron M

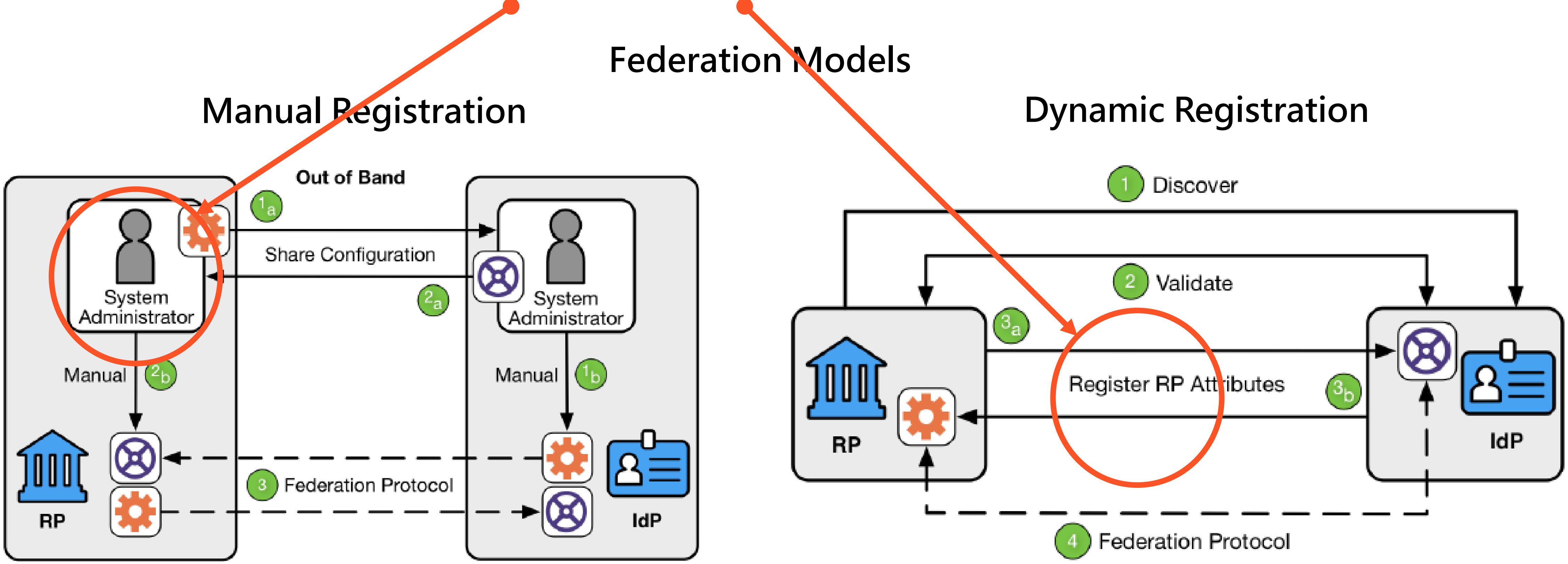
Authenticator Assurance Level 3

Memorized Secrets + Single-Factor Cryptographic Devices

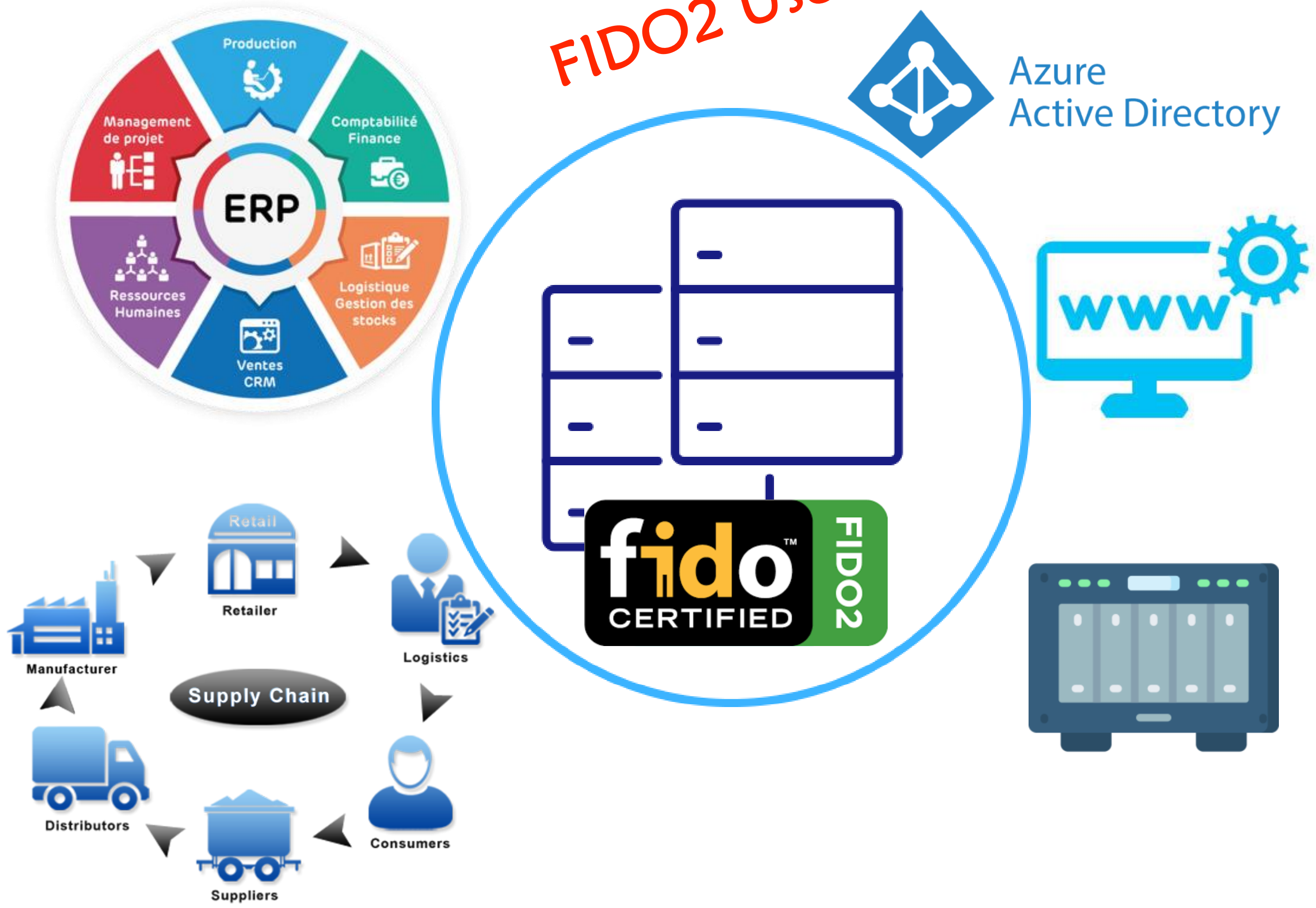

SP 800-63-3
Digital Identity Guidelines
SP 800-63A
Enrollment & Identity Proofing
SP 800-63B
Authentication & Lifecycle Management
SP 800-63C
Federation & Assertions

Issuance, Binding & Device Management !

Federation Models



FIDO2 Use Cases



FIDO2 Server Administrative:

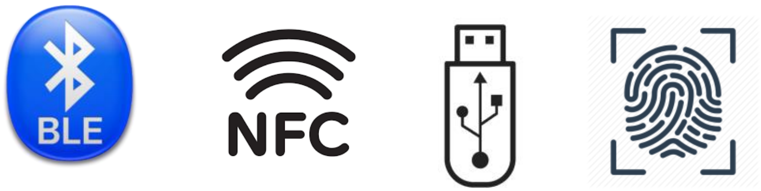
1) Deployment & Runtime Management
2) Device Management
3) RP Domain Management
4) RP Service Link Management
5) Metadata Database Management
6) Account Management (Secure Binding)
7) Audit
8) Logging

Types of FIDO2 Server Deployment:

① FIDO Server Embedded
② FIDO Public Cloud Service
③ On Premise Deployment
④ Private Cloud Deployment

Source:
https://www.flaticon.com/free-icon/nas_4943962
https://icon-library.com/icon/web-applications-icon-12.html
https://www.pinpng.com/download/hJbxbiT_supply-chain-icon-png-187-png-image-supply/
https://dieutek.com/best-erp-software-2019/
https://www.hypr.com/fido-server/

多樣化認證載具及功能模組



FIDO CTAP Features:

① Privacy by Resident Key

② Device Management by Enterprise Attestation

③ Service Credential by Credential Blob

④ Utility Application by Large Blob

Beside Authentication via FIDO.

Thin Client Centric Operation Environment !

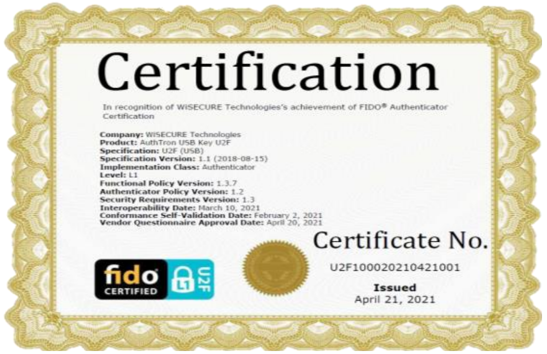
Premium features are required to support full web application.

eID Application, Crypto Service Provider, File Protection Feature, Web Content Protection etc…

Source: https://www.colourbox.com/vector/byod-sign-icon-bring-your-own-device-symbol-vector-11100865

FIDO聯盟認證

April 2021



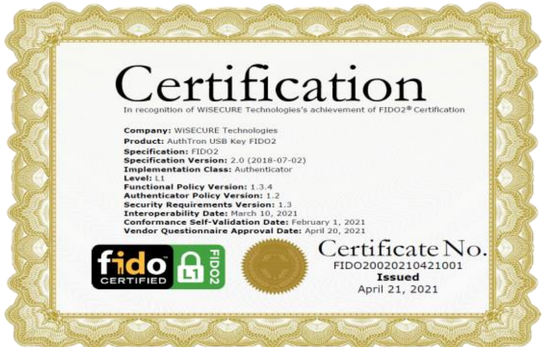
Certification

In recognition of WiSECURE Technologies's achievement of FIDO® Authenticator Certification

Company: WiSECURE Technologies
Product: AuthTron USB Key U2F
Specification: U2F (USB)
Specification Version: 1.1 (2018-08-15)
Implementation Class: Authenticator
Level: L1
Functional Policy Version: 1.3.7
Authenticator Policy Version: 1.2
Security Requirements Version: 1.3
Interoperability Date: March 10, 2021
Conformance Self-Validation Date: February 2, 2021
Vendor Questionnaire Approval Date: April 20, 2021

Certificate No.
U2F100020210421001
Issued
April 21, 2021

U2F Level 1 Authenticator



Certification

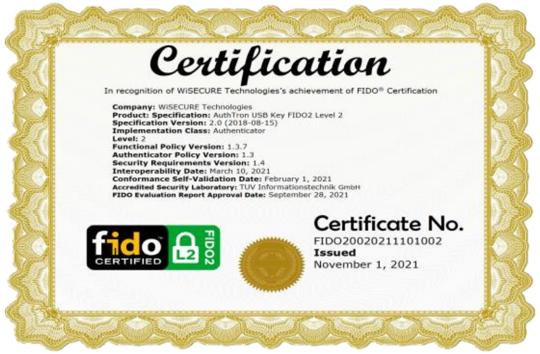
In recognition of WiSECURE Technologies's achievement of FIDO2® Certification

Company: WiSECURE Technologies
Product: AuthTron USB Key FIDO2
Specification: FIDO2
Specification Version: 2.0 (2018-07-02)
Implementation Class: Authenticator
Level: L1
Functional Policy Version: 1.3.4
Authenticator Policy Version: 1.2
Security Requirements Version: 1.3
Interoperability Date: March 10, 2021
Conformance Self-Validation Date: February 1, 2021
Vendor Questionnaire Approval Date: April 20, 2021

Certificate No.
FIDO20020210421001
Issued
April 21, 2021

FIDO2 L1 Authenticator

September 2021



Certification

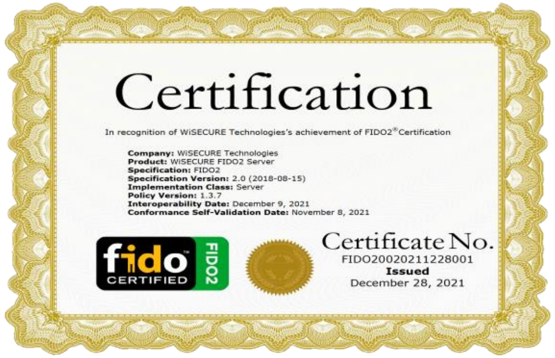
In recognition of WiSECURE Technologies's achievement of FIDO® Certification

Company: WiSECURE Technologies
Product: Specification: AuthTron USB Key FIDO2 Level 2
Specification Version: 2.0 (2018-08-15)
Implementation Class: Authenticator
Level: 2
Functional Policy Version: 1.3.7
Authenticator Policy Version: 1.3
Security Requirements Version: 1.4
Interoperability Date: March 10, 2021
Conformance Self-Validation Date: February 1, 2021
Accredited Security Laboratory: TUV Informationstechnik GmbH
FIDO Evaluation Report Approval Date: September 28, 2021

Certificate No.
FIDO20020211101002
Issued
November 1, 2021

FIDO2 L2 Authenticator (include U2F)

December 2021



Certification

In recognition of WiSECURE Technologies's achievement of FIDO2® Certification

Company: WiSECURE Technologies
Product: WISECURE FIDO2 Server
Specification: FIDO2
Specification Version: 2.0 (2018-08-15)
Implementation Class: Server
Policy Version: 1.3.7
Interoperability Date: December 9, 2021
Conformance Self-Validation Date: November 8, 2021

Certificate No.
FIDO20020211228001
Issued
December 28, 2021

FIDO2 Server

匯智安全 FIDO 生態系　從晶片、裝置到雲服務

FIDO on Chip

UAF SDK

ID Card Authenticator

FIDO2 Cloud Service

PAM Service

MicroSD FIDO Module

USB Authenticator

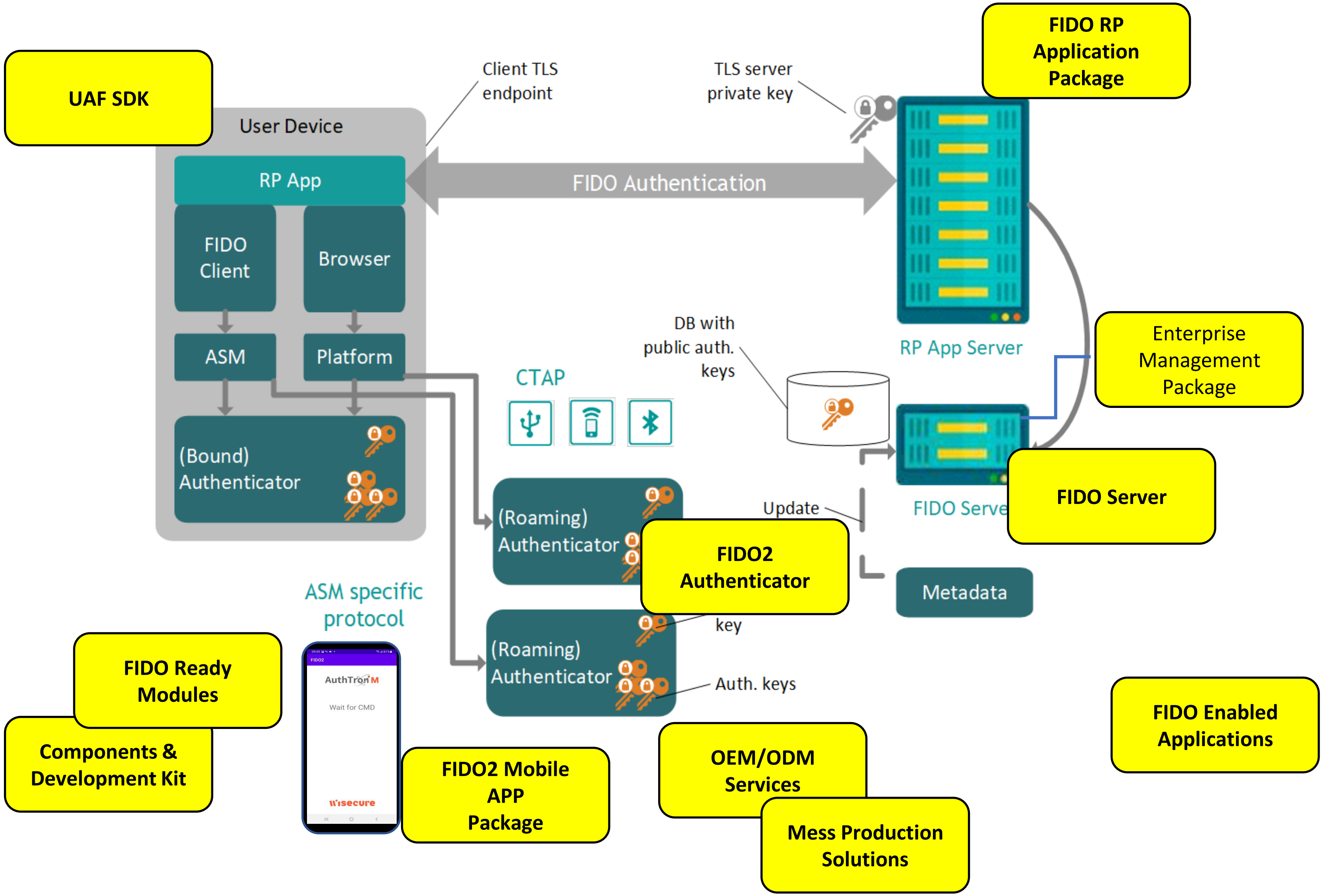
HID Dongle Authenticator

Mobile Authenticator

FIDO2 Server

Source:
https://www.flaticon.com/free-icon/cloud-service_3983126
https://indeed-id.com/indeed-privileged-access-manager
https://pnghunter.com/png/sdk-icon/

匯智安全科技 | 匯智安全 FIDO 生態系 FIDO解決方案 提供全面性完整配套



UAF SDK

User Device

RP App

FIDO Client

Browser

ASM

Platform

(Bound) Authenticator

Client TLS endpoint

TLS server private key

FIDO Authentication

FIDO RP Application Package

RP App Server

DB with public auth. keys

CTAP

Enterprise Management Package

FIDO Server

FIDO Serve

Update

(Roaming) Authenticator

FIDO2 Authenticator

Metadata

ASM specific protocol

(Roaming) Authenticator

key

Auth. keys

FIDO Ready Modules

Components & Development Kit

AuthTron M

Wait for CMD

wisecure

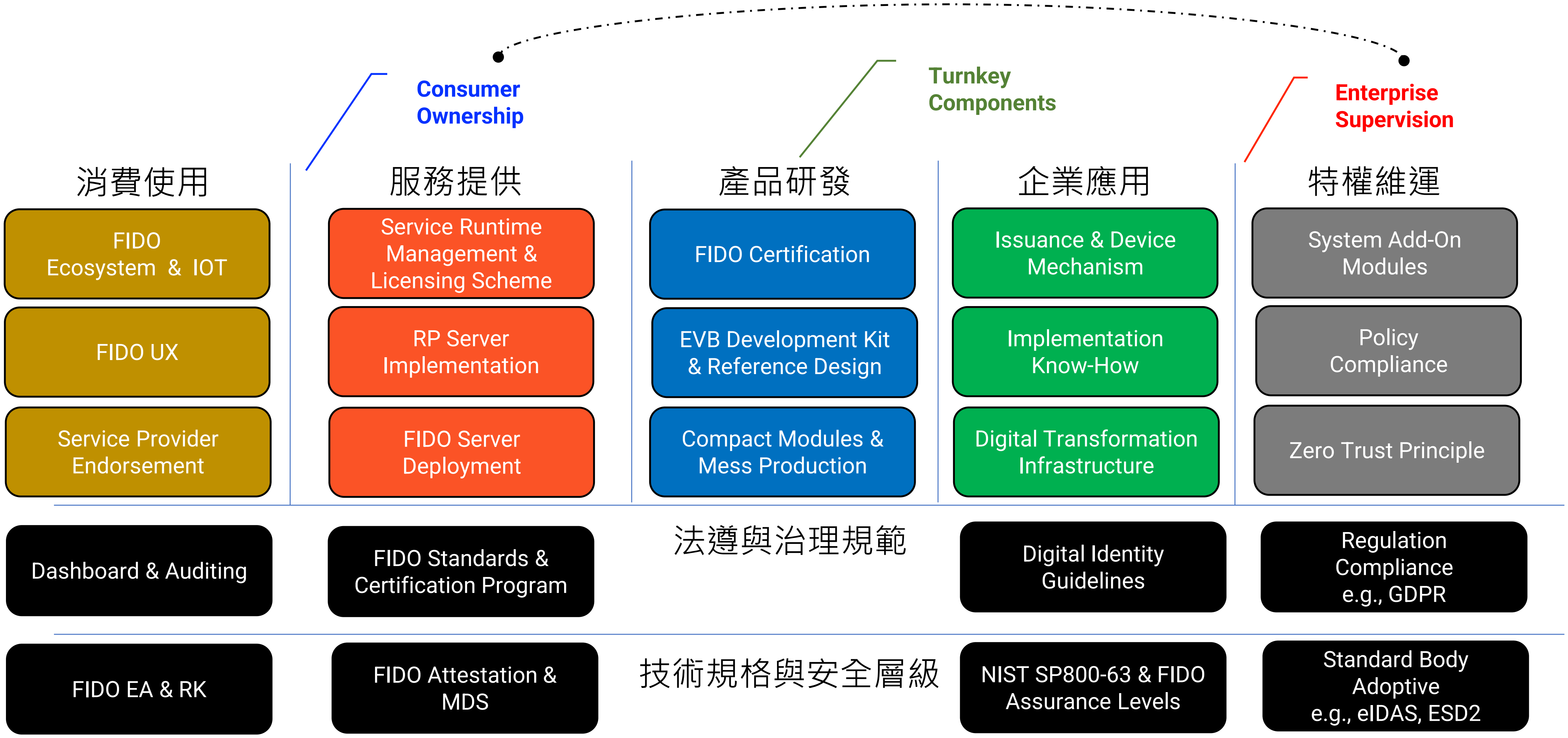
FIDO2 Mobile APP Package

OEM/ODM Services

Mess Production Solutions

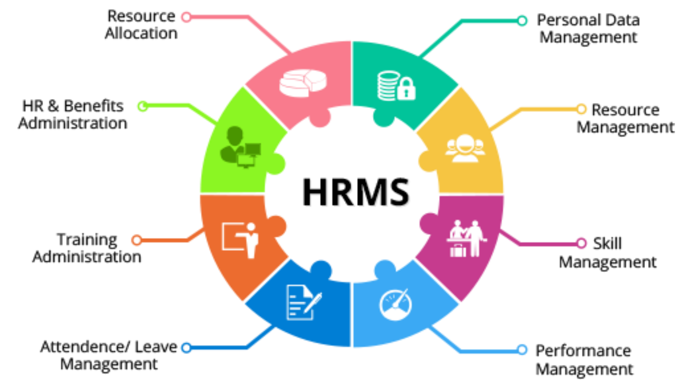
FIDO Enabled Applications

匯智安全科技 | 匯智安全 FIDO 生態系 FIDO解決方案 需求構面



消費使用	服務提供	產品研發	企業應用	特權維運
FIDO Ecosystem & IOT	Service Runtime Management & Licensing Scheme	FIDO Certification	Issuance & Device Mechanism	System Add-On Modules
FIDO UX	RP Server Implementation	EVB Development Kit & Reference Design	Implementation Know-How	Policy Compliance
Service Provider Endorsement	FIDO Server Deployment	Compact Modules & Mess Production	Digital Transformation Infrastructure	Zero Trust Principle
Dashboard & Auditing	FIDO Standards & Certification Program	法遵與治理規範	Digital Identity Guidelines	Regulation Compliance e.g., GDPR
FIDO EA & RK	FIDO Attestation & MDS	技術規格與安全層級	NIST SP800-63 & FIDO Assurance Levels	Standard Body Adoptive e.g., eIDAS, ESD2

企業 FIDO 導入實例



Password-less Strong Authentication

Backoffice, Front Desk, CSR Console, Vendor Portal

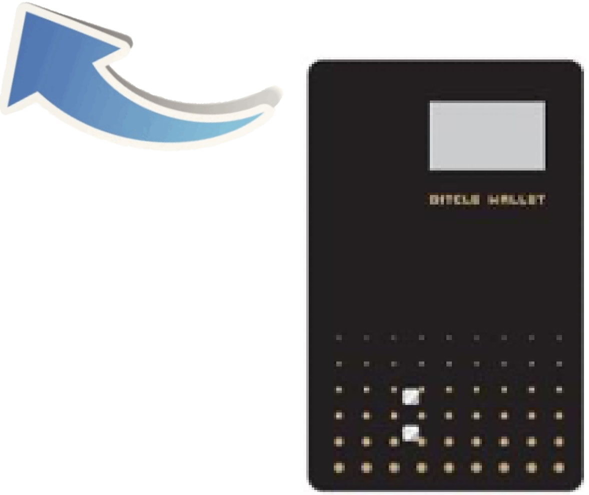
Source:
https://www.flaticon.com/premium-icon/bank_2887334?term=branch&page=1&position=39&page=1&position=39&related_id=2887334&origin=tag
https://hazentech.com/best-litigation-support-services-for-legal-case-correspondence/
https://www.indiamart.com/proddetail/multi-vendor-e-commerce-website-development-21349541455.html
https://vendorbali.com/index.php/software-aplikasi-bali/jual-aplikasi-hr-system-di-bali/aplikasi-hr-bali.html

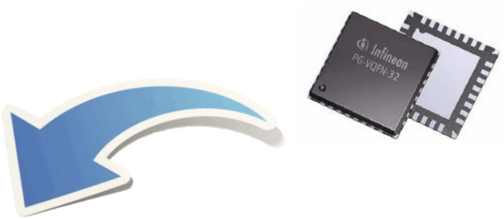
Product by FIDO Featured Security Chip

Evaluation Board & SDK

1. Interface Spec
2. FIDO API
3. Library on MCU
4. Sample Code
5. EVB
6. Engineering Sample Chip
7. Testbed
8. Conformance Tool

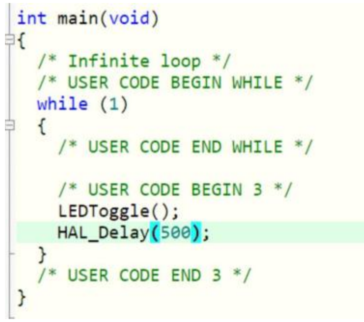
10. FIDO Authenticator Certification Application





9. Production Materials & MP Script

Sample Code

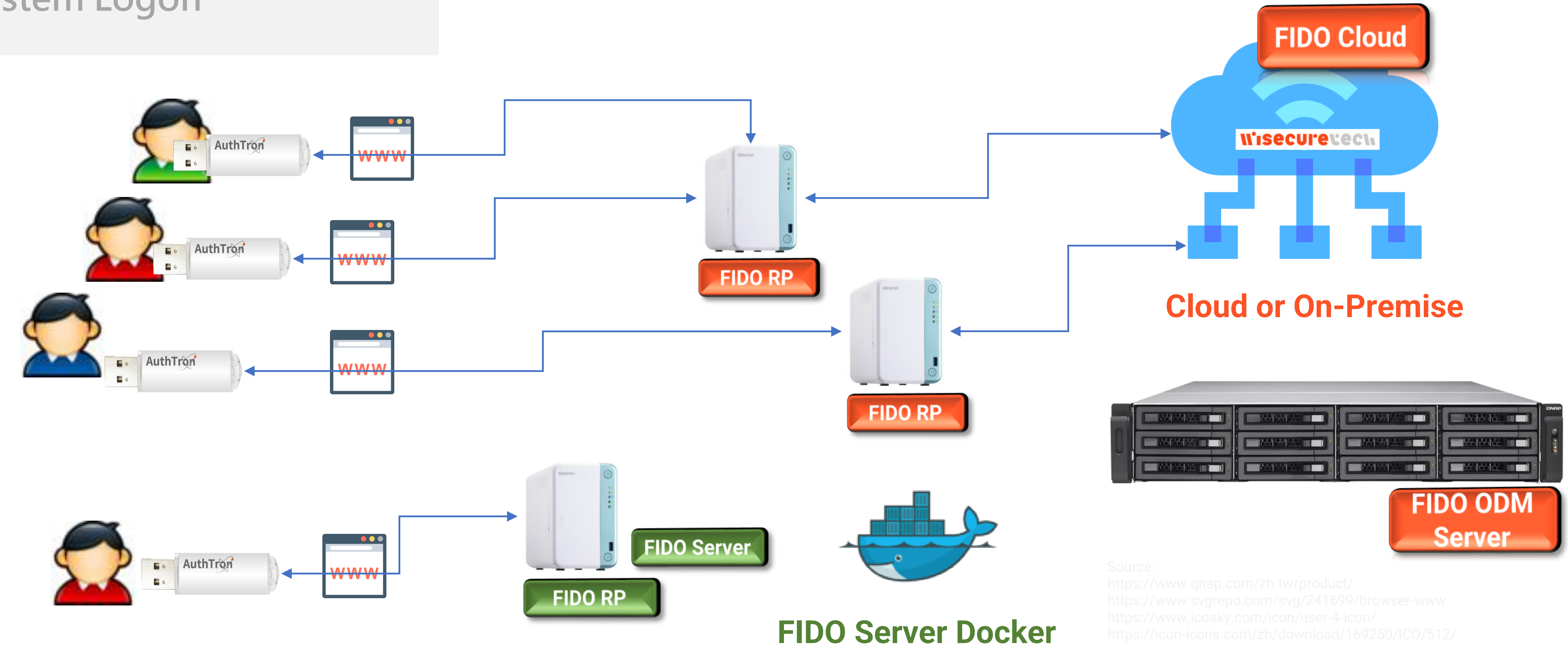


```
int main(void)
{
  /* Infinite loop */
  /* USER CODE BEGIN WHILE */
  while (1)
  {
    /* USER CODE END WHILE */

    /* USER CODE BEGIN 3 */
    LEDToggle();
    HAL_Delay(500);
  }
  /* USER CODE END 3 */
}
```

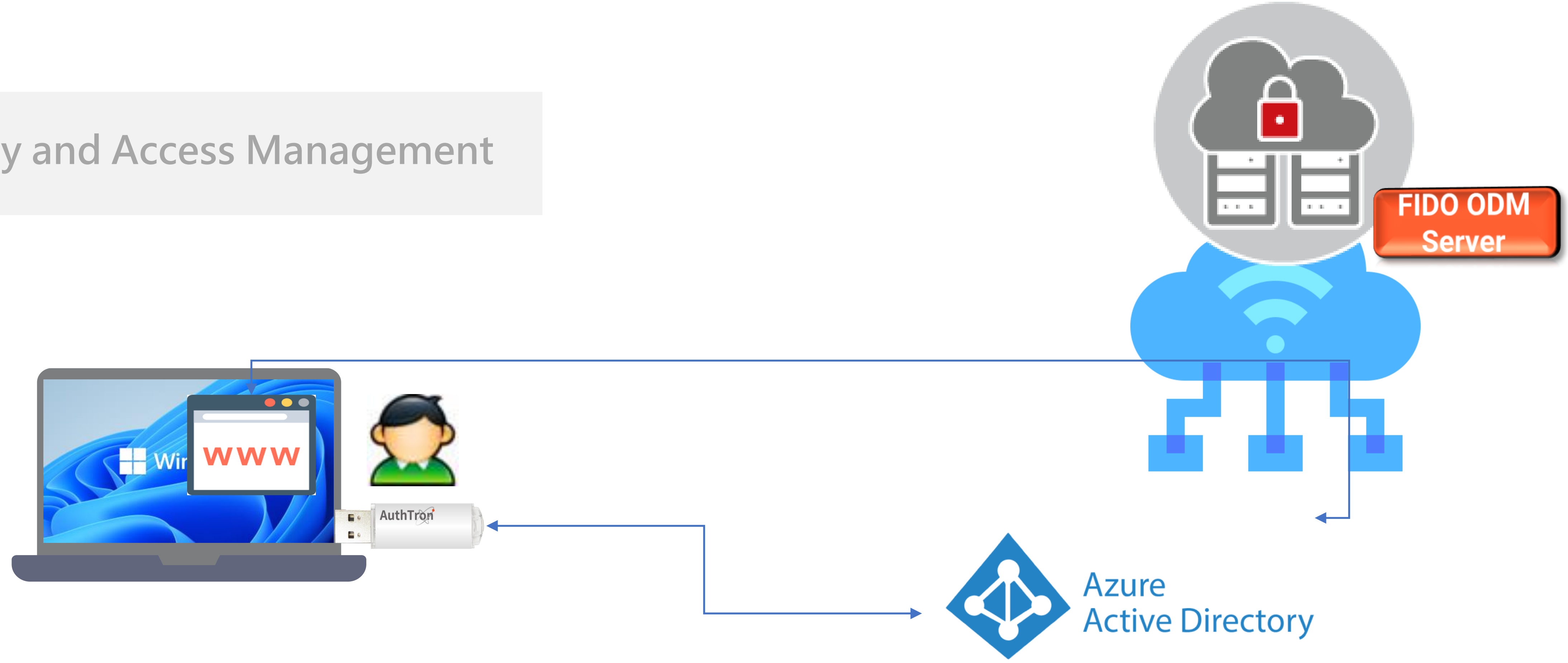
Source: http://www.summit-tech.com.tw/si-wafer.html

Password-less Embedded System Logon



Source:
https://www.qnap.com/zh-tw/product/
https://www.svgrepo.com/svg/241699/browser-www
https://www.icosky.com/icon/user-4-icon/
https://icon-icons.com/zh/download/169250/ICO/512/

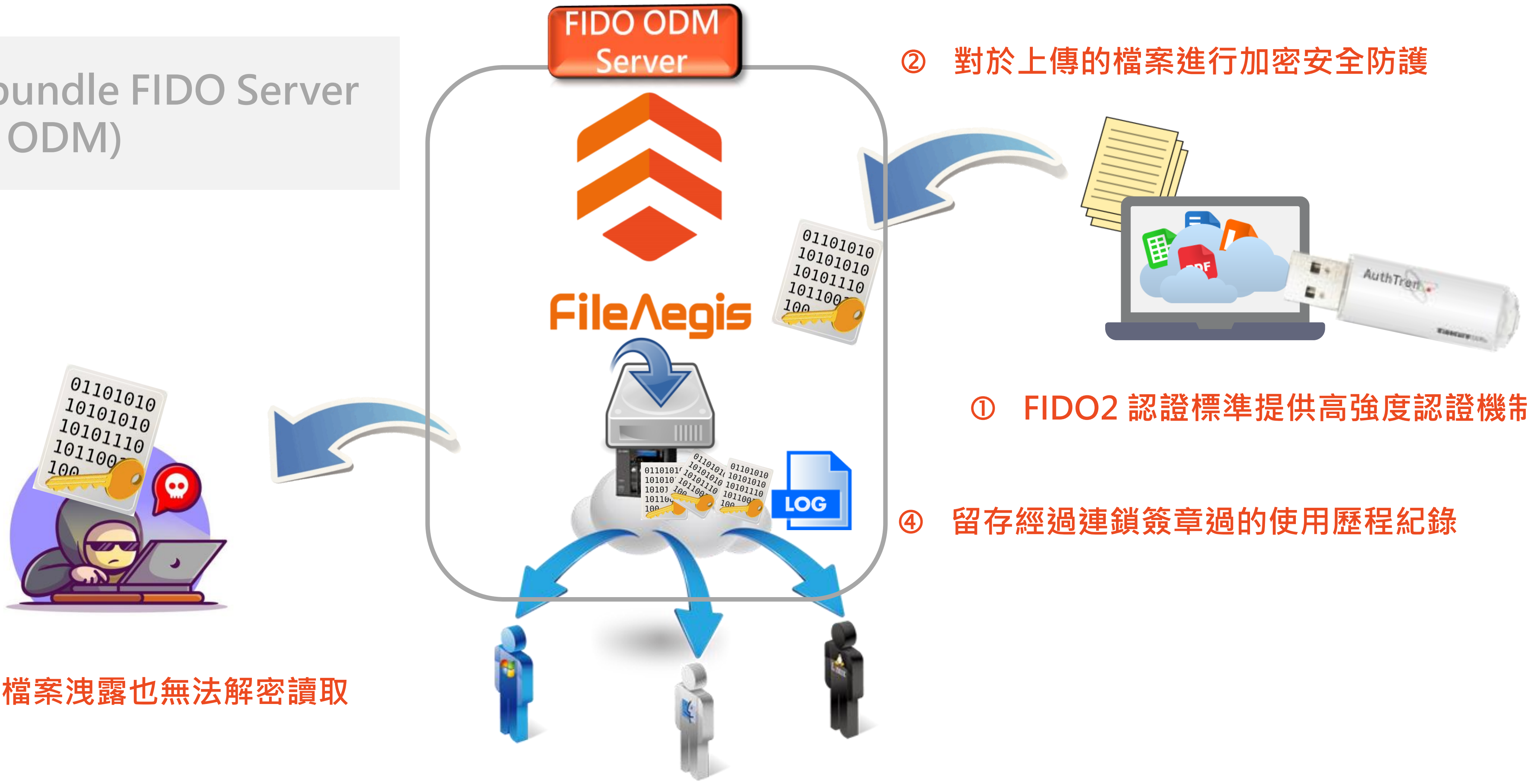
Identity and Access Management



Microsoft Certified FIDO Authenticator for Windows Logon

Source:
https://www.qnap.com/zh-tw/product/
https://www.svgrepo.com/svg/241699/browser-www
https://pki.ares.com.tw/products/uiam/
https://support.microsoft.com/zh-tw/windows/%E8%A3%9D%E7%BD%AE%E5%8A%A0%E5%AF%86windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d

Application bundle FIDO Server (FIDO Server ODM)



① FIDO2 認證標準提供高強度認證機制

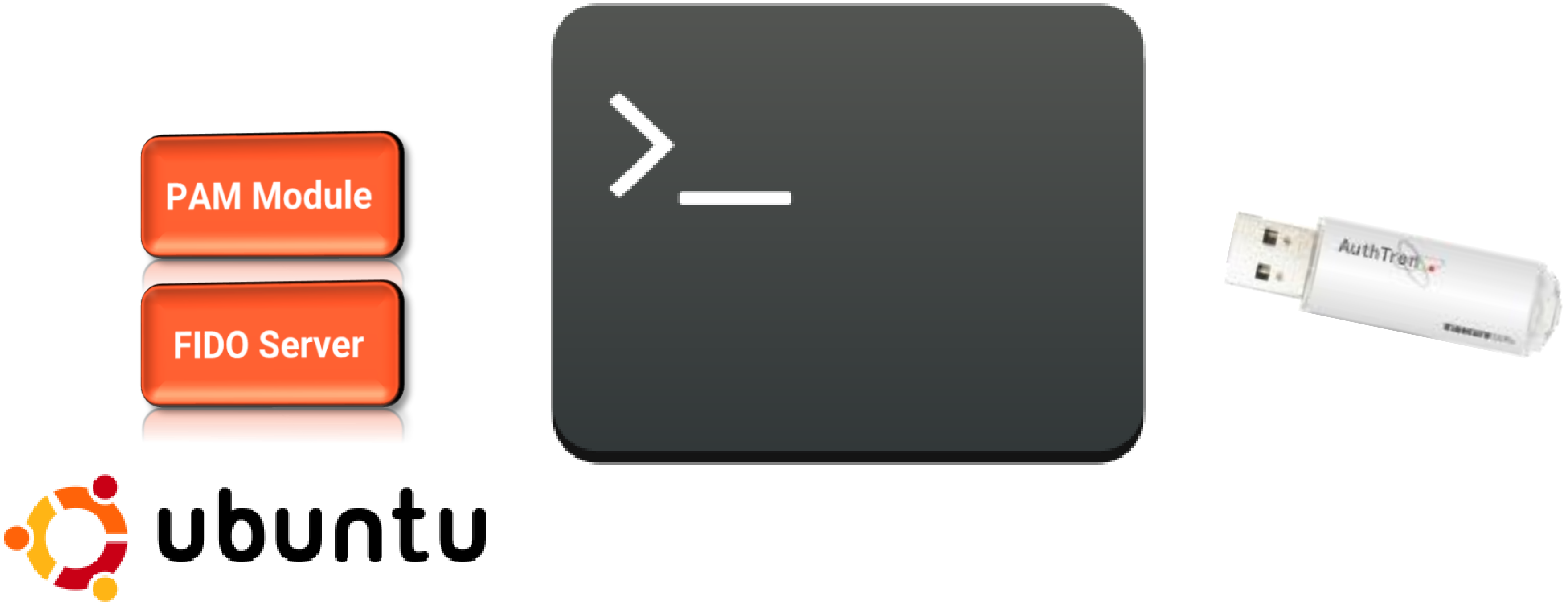
② 對於上傳的檔案進行加密安全防護

③ 提供以金鑰為基礎的高安全分享機制

④ 留存經過連鎖簽章過的使用歷程紀錄

⑤ 即使加密檔案洩露也無法解密讀取

FIDO for Linux Pluggable Authentication Modules (PAM)

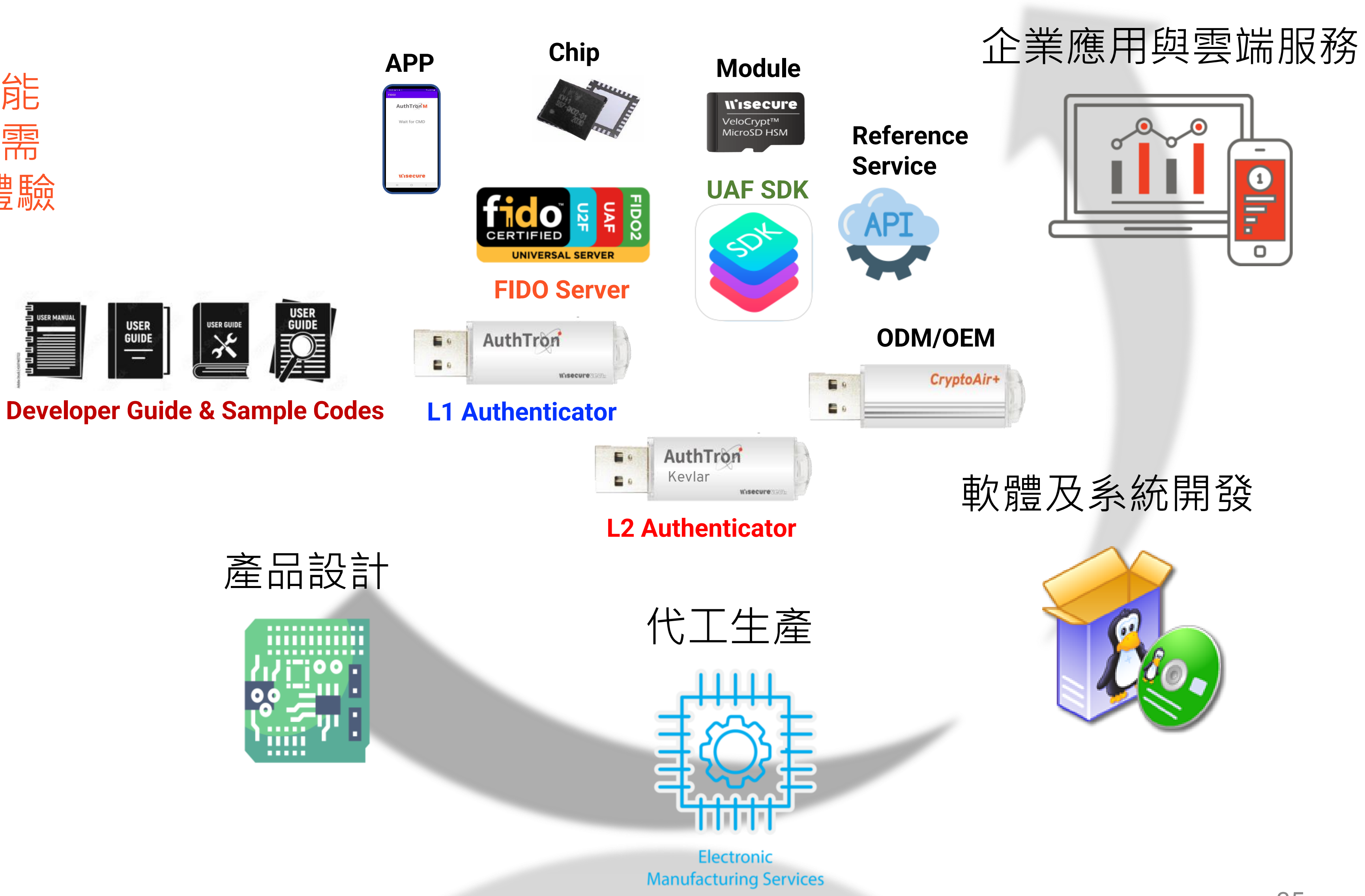


PAM Module

FIDO Server

匯智安全 FIDO 生態系 FIDO 解決方案 滿足各類需求

- ✓ 提供軟硬體模組加值功能
- ✓ 滿足各類應用情境之所需
- ✓ 確保FIDO使用者完美體驗



企業應用與雲端服務

APP

Chip

Module

UAF SDK

Reference Service

FIDO Server

Developer Guide & Sample Codes

L1 Authenticator

ODM/OEM

L2 Authenticator

軟體及系統開發

產品設計

代工生產

Electronic Manufacturing Services

Source:
https://sbsepos.co.uk/modules/back-office-software/
https://www.parsec.co.za/company/products-services/
https://findicons.com/search/software
https://www.flaticon.com/free-icon/pcb_2399658
https://www.flaticon.com/free-icon/api_2165004
https://stock.adobe.com/tw/images/

35

匯智安全科技FIDO解決方案

Beyond the FIDO solution provider,

Being a FIDO enabler.

Thank You !

Your advice is highly appreciated !

WiSECURE Technologies (WiSECURE) was founded in 2019, aiming to design standardized hardware security modules in various form factors, including PCIe cards, microSD cards, USB tokens, etc. WiSECURE specializes in cryptographic implementation and key management, which are fundamental in storage encryption, authentication, emerging digital assets, industrial control, IoT, WFH (Working from home), digital rights managements (DRM) and other innovative services and applications.

匯智安全科技