中華電信零信任網路系統
xTrust

中華電信
Chunghwa Telecom

Chunghwa Telecom
xTrust

中華電信 Chunghwa Telecom

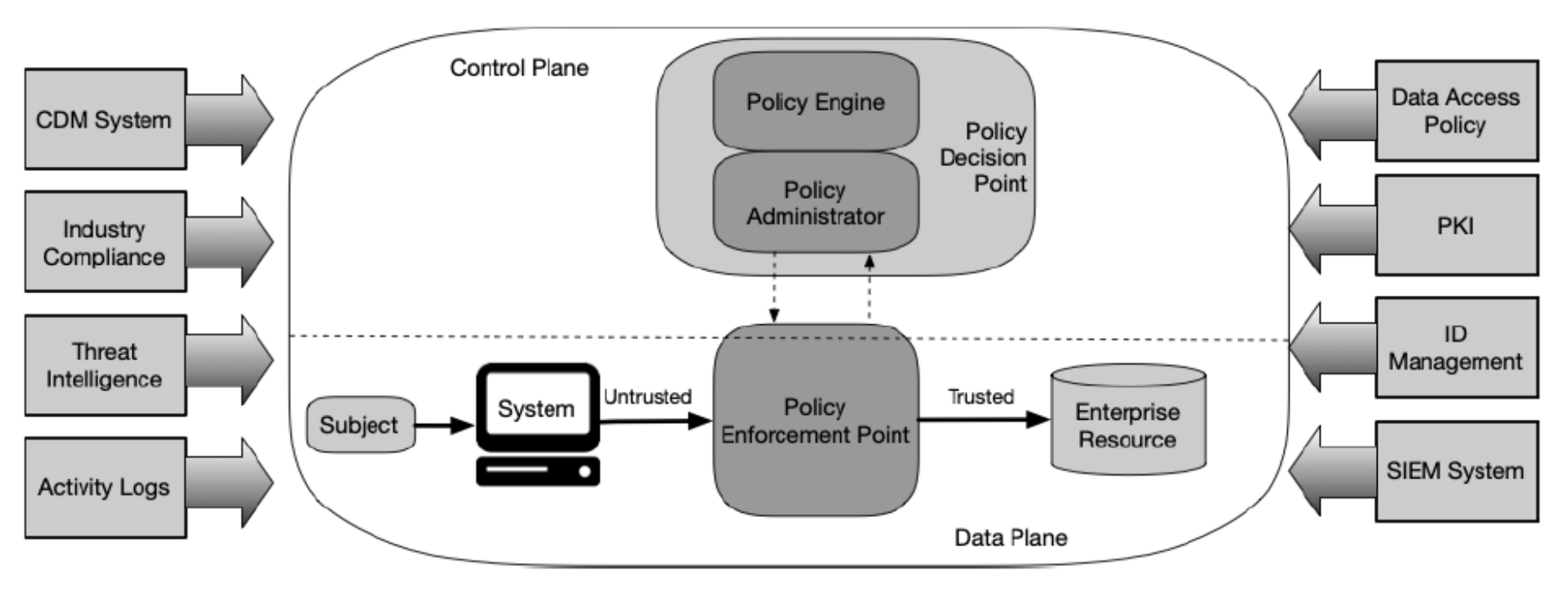
創新
當責
客戶導向
誠信

Agenda

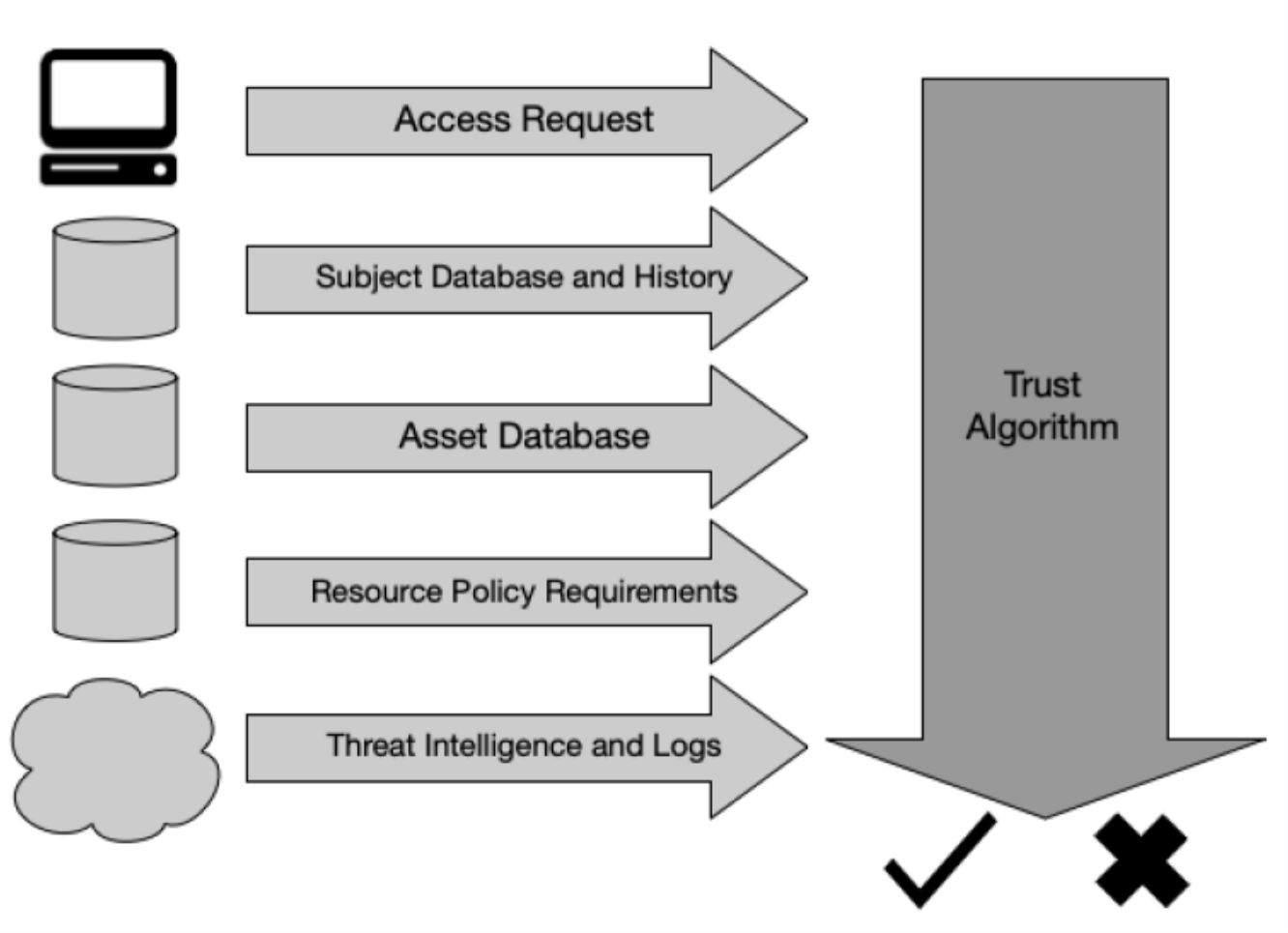
1. 零信任概念
2. 各國零信任網路發展
3. 中華電信零信任網路系統 xTrust
4. Q&A

1. 零信任概念

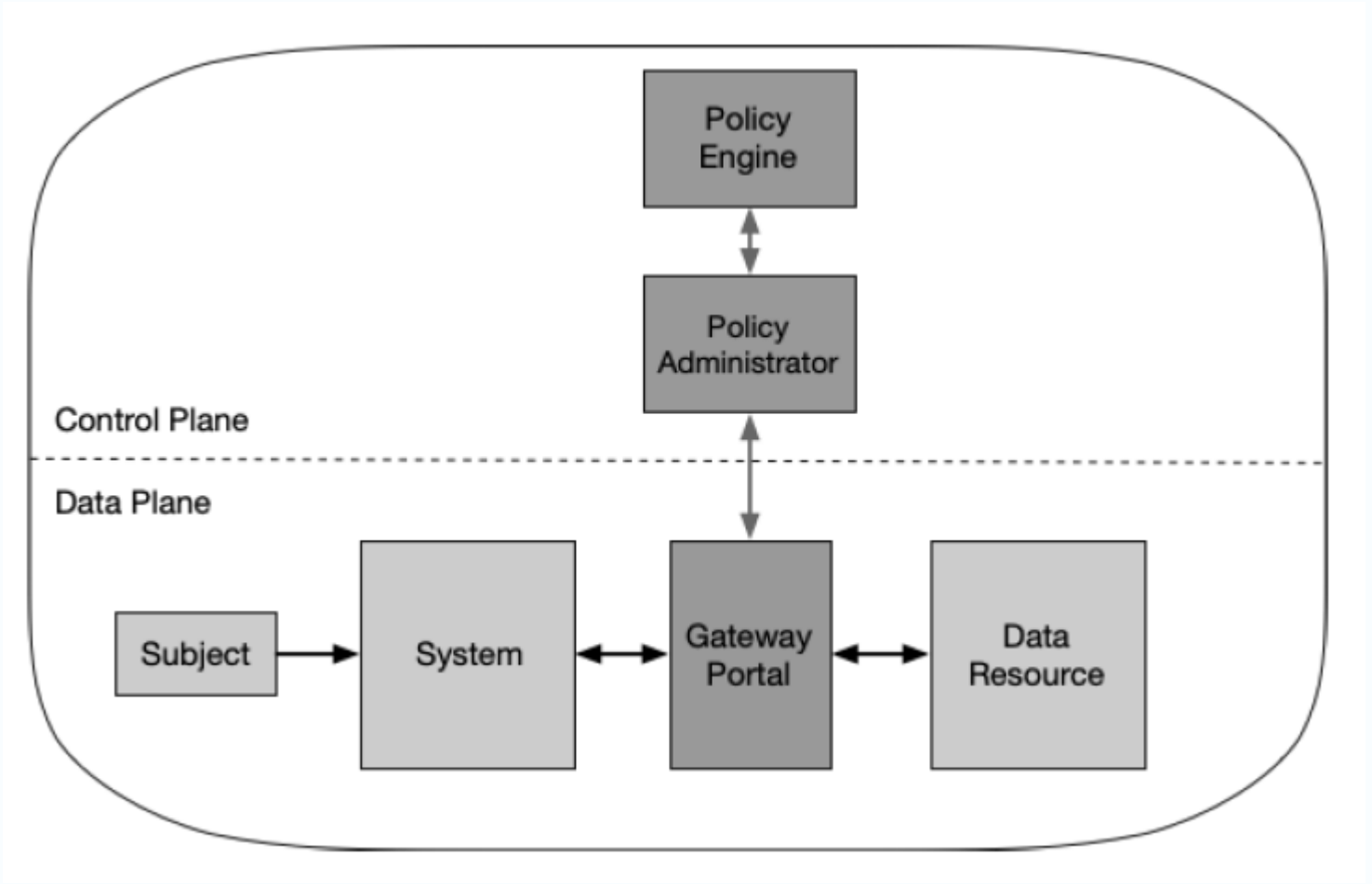
- NIST SP 800-207 : **Logical Components of Zero Trust Architecture**



- NIST SP 800-27 : **Trust Algorithm**



- NIST SP 800-27 : **Resource Portal Model**



2. 各國零信任網路發展

各國零信任網路說明

創新 當責 客戶導向 誠信

國外標準

- 零信任概念歷經10幾年發展，2020年美國國家標準技術研究院(NIST)正式頒布標準文件**SP 800-207**：零信任架構(Zero Trust Architecture, ZTA)，成為各界採用基礎
- SP 1800-35 Implementing a Zero Trust Architecture (2022)
- USA CISA Zero Trust Maturity Model (https://www.cisa.gov/zero-trust-maturity-model) (2022)
- USA DoD Zero Trust Reference Architecture (2022)

國內政策

第六期「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，將**發展零信任網路資安防護環境，推動政府機關導入零信任網路，完善政府網際服務網防禦深廣度**

數位發展部**優先推動A級公務機關導入零信任網路**

為推動六大核心戰略產業，**厚植台灣資安產業自主研發能力**，貫徹「**資安即國安**」戰略，政府將透過零信任網路之資安供需合作，**支持資安公司發展零信任網路資安產業鏈**

2020年建立歐盟網路安全戰略，提出標準框架，協助成員國轉型

2024年前聯邦網路完成初步遷移，國防部規劃2027年完成零信任的部署

2021年發布網路安全戰略，將零信任網路安全策略列為發展重點

2022年發布零信任架構適用方針，指引政府機關進行零信任部署

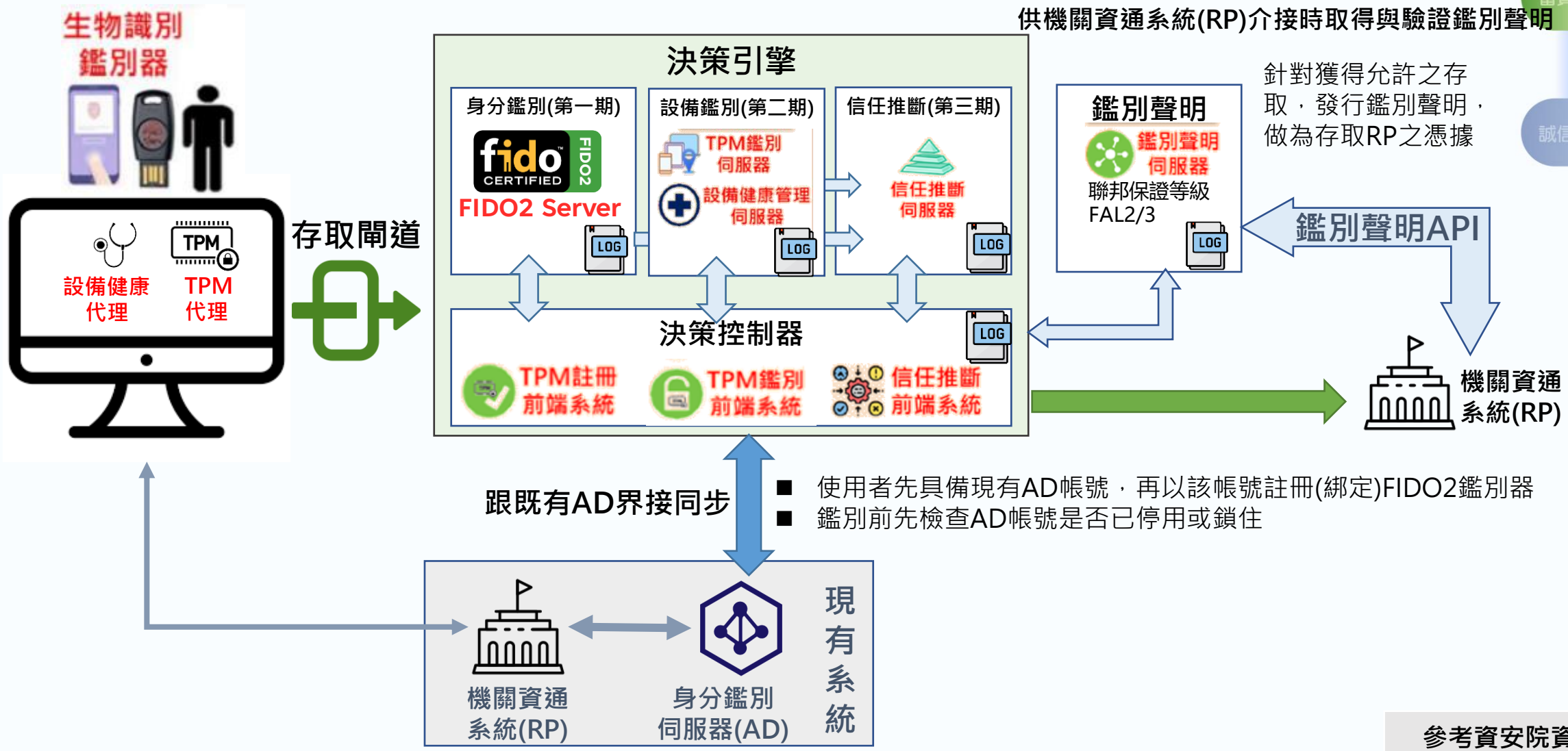
政府零信任網路推動進程

政府機關 –111年起遴選機關逐年導入零信任網路之**身分鑑別、設備鑑別及信任推斷3大核心機制** –後續於資通安全責任等級A級公務機關推動導入

商用產品–配合111~113年之機關導入，推動**廠商開發符合政府零信任網路部署架構、部署原則及核心機制之商用產品**，以因應後續A級公務機關之導入

參考資安院資料

零信任網路架構圖



參考資安院資料

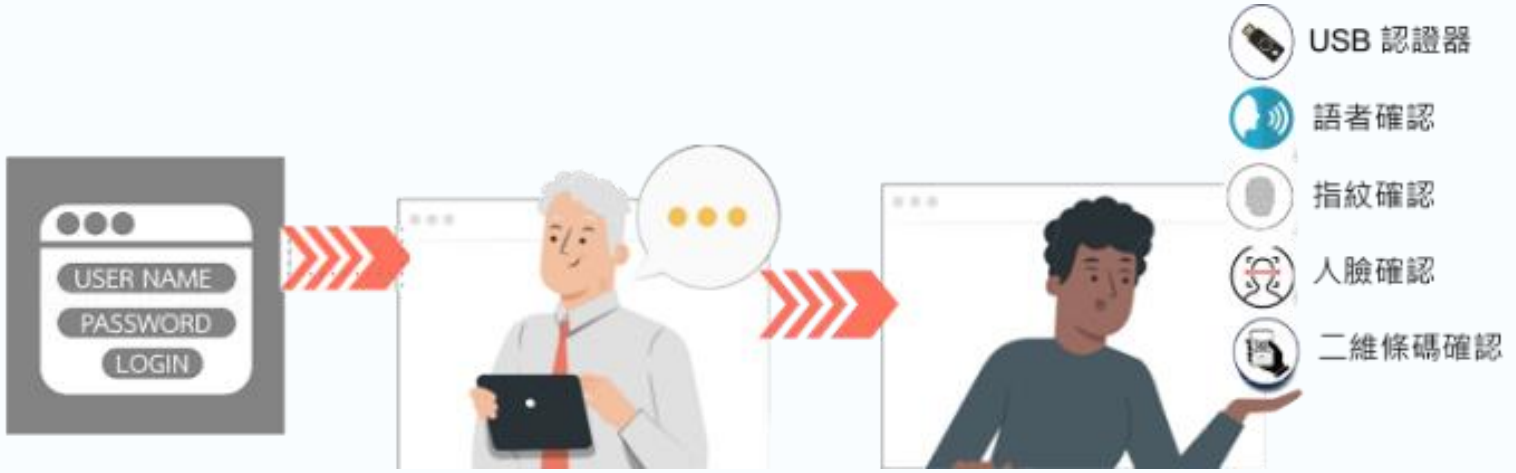
身分鑑別

➢基於FIDO2之身分鑑別方法

- 國際FIDO聯盟制訂的共通安全規範，解決使用者需記憶複數組合帳號/密碼之沉重負擔。
- FIDO2使用PKI來實現身份驗證，避免了傳統密碼的弱點，如社會工程學攻擊、密碼盜竊和重放攻擊。

帳密 → 多因子 → FIDO2

身分鑑別技術演進



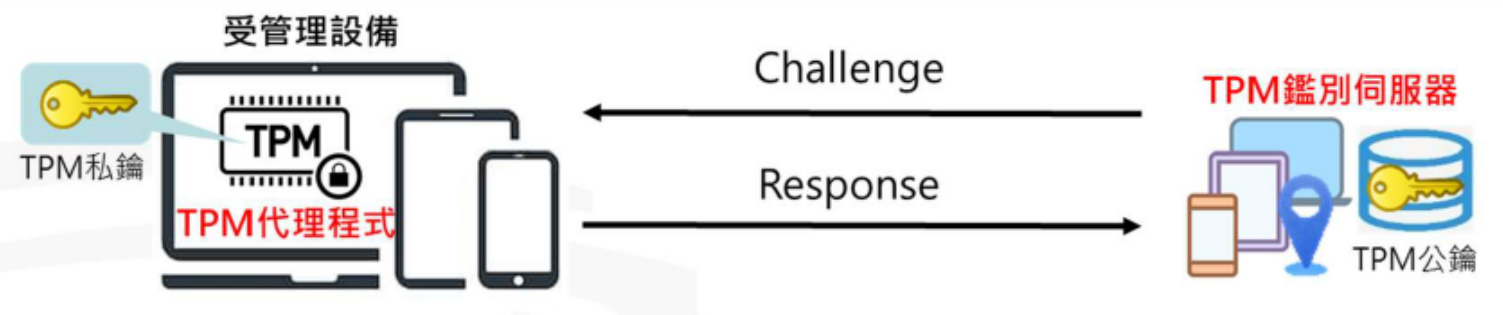
https://fidoalliance.org/fido2/

設備鑑別

創新 當責 客戶導向 誠信

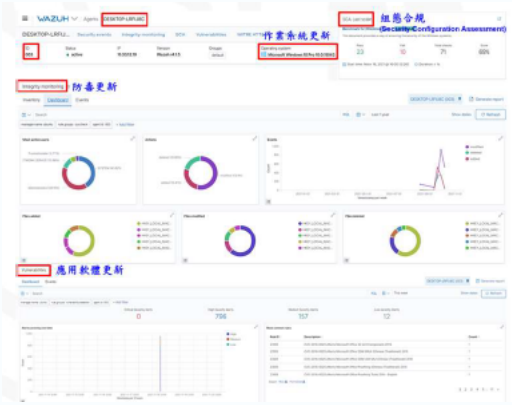
➢基於信任平台模組(TPM)之設備鑑別方法

- TPM代表 Trusted Platform Module，是一種安全晶片，可以用於存儲和保護數位憑證、密鑰和其他機密資料



➢設備健康度管理

- 持續更新設備健康狀態
- 依設備健康狀態隨時換算設備健康信任等級



設備編號	設備健康狀態	信任等級
D001	AD	0.5
D002	CD	0.3
D003	ABC	0.9
D004	D	0.1

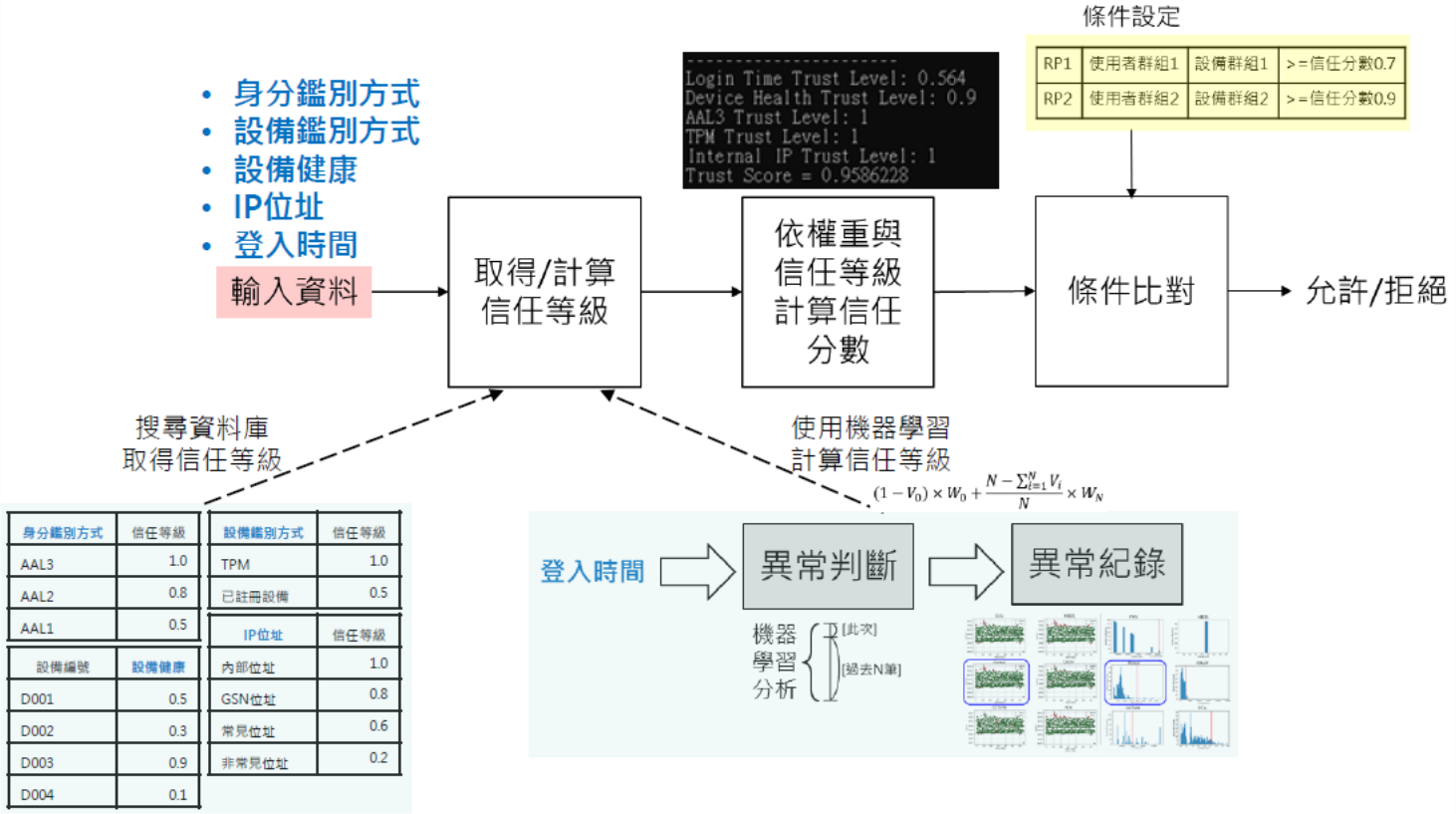
健康狀態/等級分配
(A)作業系統更新：0.4
(B)防毒更新　　：0.3
(C)應用軟體更新：0.2
(D)組態合規　　：0.1

參考資安院資料

信任推斷

創新
當責
客戶導向
誠信

- 信任推斷依各類輸入資料(身分鑑別結果、設備鑑別結果、設備健康信任等級及使用者情境Time, Location等)，進行評估與計算，輸出信任分數以提供存取決策。

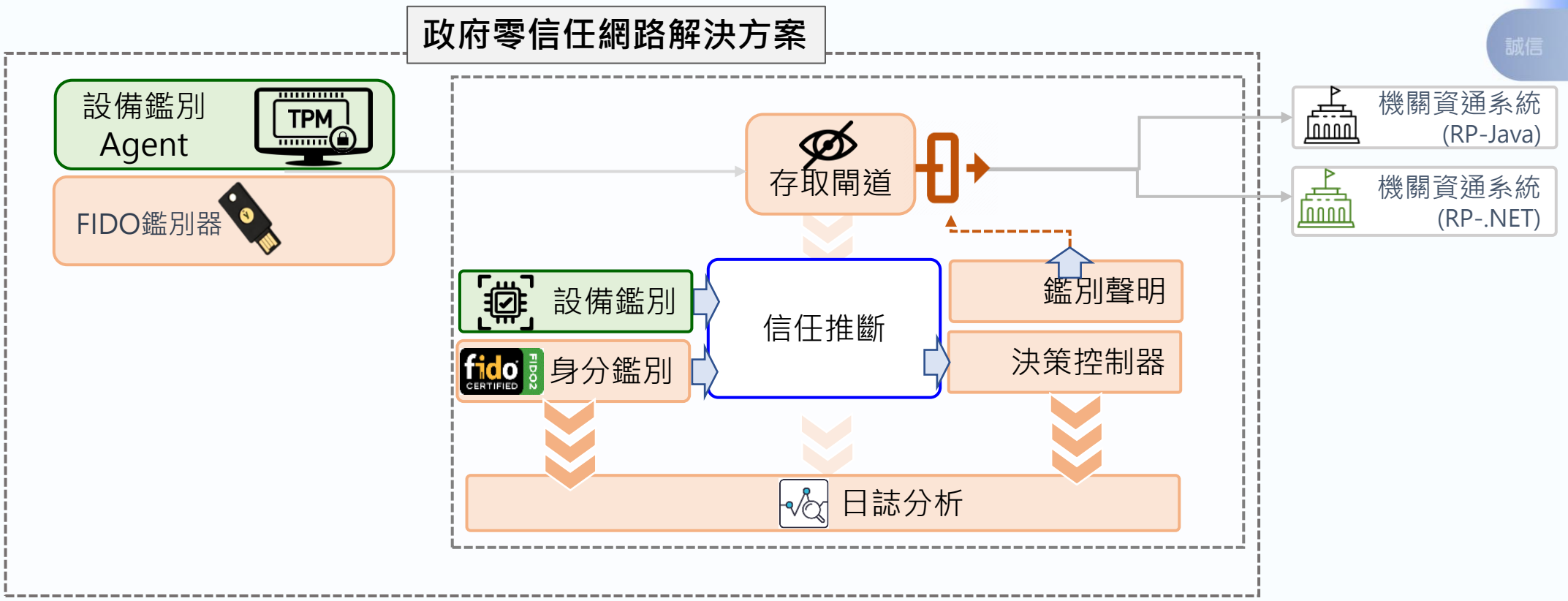


參考資安院資料

3. 中華電信零信任網路系統 xTrust

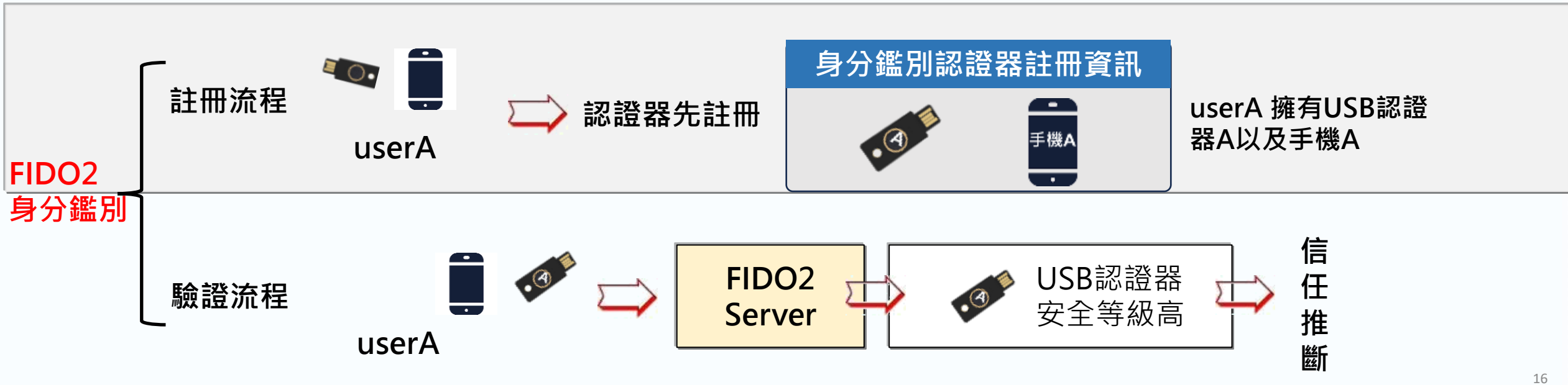
中華電信零信任網路系統 xTrust

系統架構

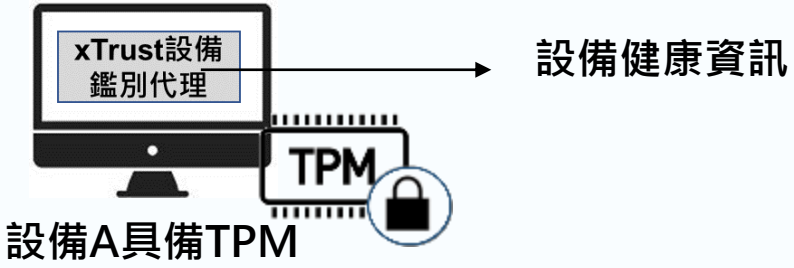


xTrust決策引擎-身分鑑別

FIDO (Fast IDentity Online) **聯盟**所訂定的一套網路識別標準，以解決使用者需記憶複數組合帳號/密碼之沉重負擔，**各大作業系統與瀏覽器均支援**



xTrust決策引擎-設備鑑別



設備鑑別

設備註冊流程

userA

設備註冊資訊

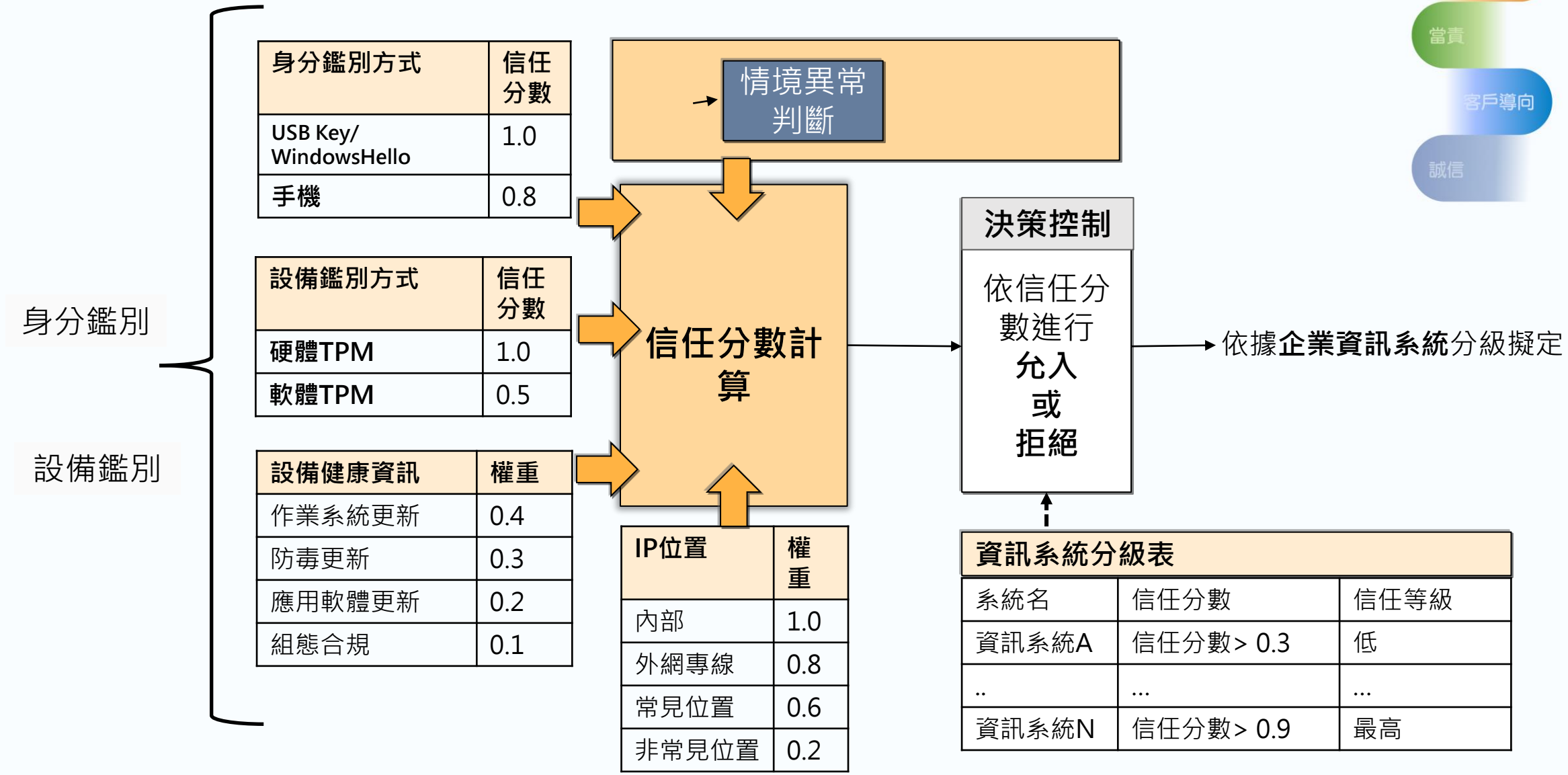
設備A TPM　　設備B　軟體TPM

設備鑑別流程

userA

設備確認 → 設備健康資訊 → TPM ：安全等級高 → 信任推斷

xTrust決策引擎-信任推斷

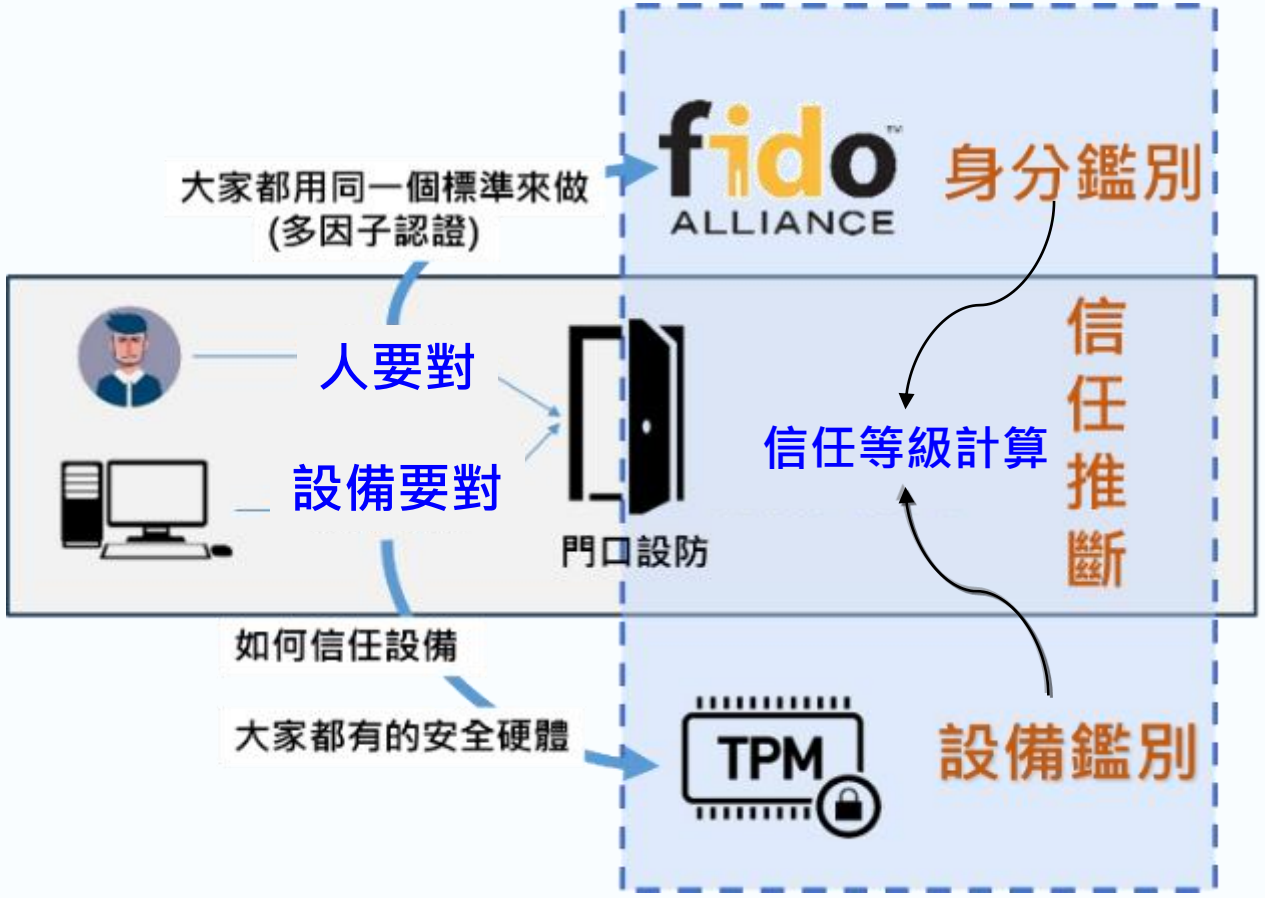


中華電信零信任網路系統 xTrust特點

創新 當責 客戶導向 誠信

Chunghwa Telecom xTrust

決策引擎(身分鑑別、設備鑑別及信任推斷)三大核心



自主研發，通過國際/ 國家認證的身分鑑別

fido CERTIFIED FIDO2 國家資通安全研究院 National Institute of Cyber Security

自主研發信任推斷引擎

AI 行為分析

自主研發千錘百鍊的設備鑑別

IRMAS ✚ 硬體安全晶片

4. Q&A

中華電信
Chunghwa Telecom

謝謝聆聽

THANK YOU