政府零信任架構說明

國家資通安全研究院

112年6月16日

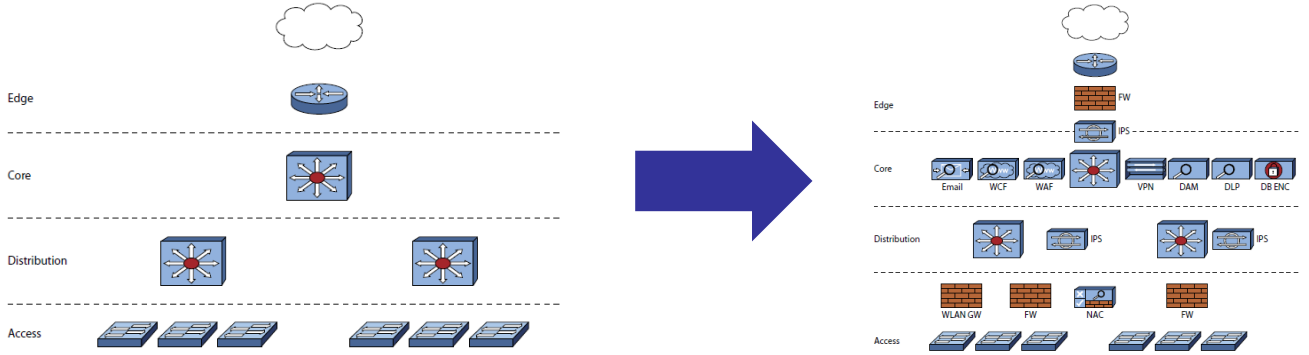
大綱

- 緣起與零信任簡介
- 政府零信任架構說明
- 推動商用產品投入發展
- 結語

緣起與零信任簡介

傳統網路模型的資安窘境

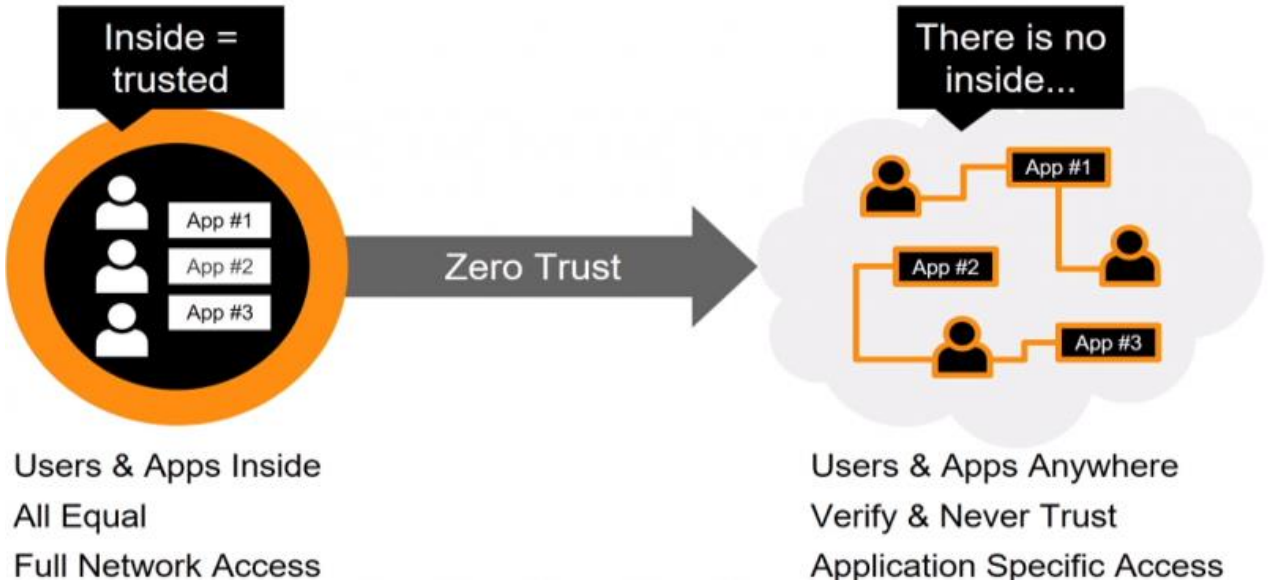
- 隨著資料/服務雲端化、使用者移動化及存取設備多元化，傳統網路模型已現資安窘境
  - 傳統網路建構是先建置階層式網路，再添加資安控制，資安思維受限於階層式網路架構



  - 傳統奉行基於信任邊界的網路威脅模型，邊界內存取受信任、邊界外存取不受信任，惟許多攻擊直接或間接來自信任邊界內，且面對複雜的網路環境變化，邊界的形成越發困難

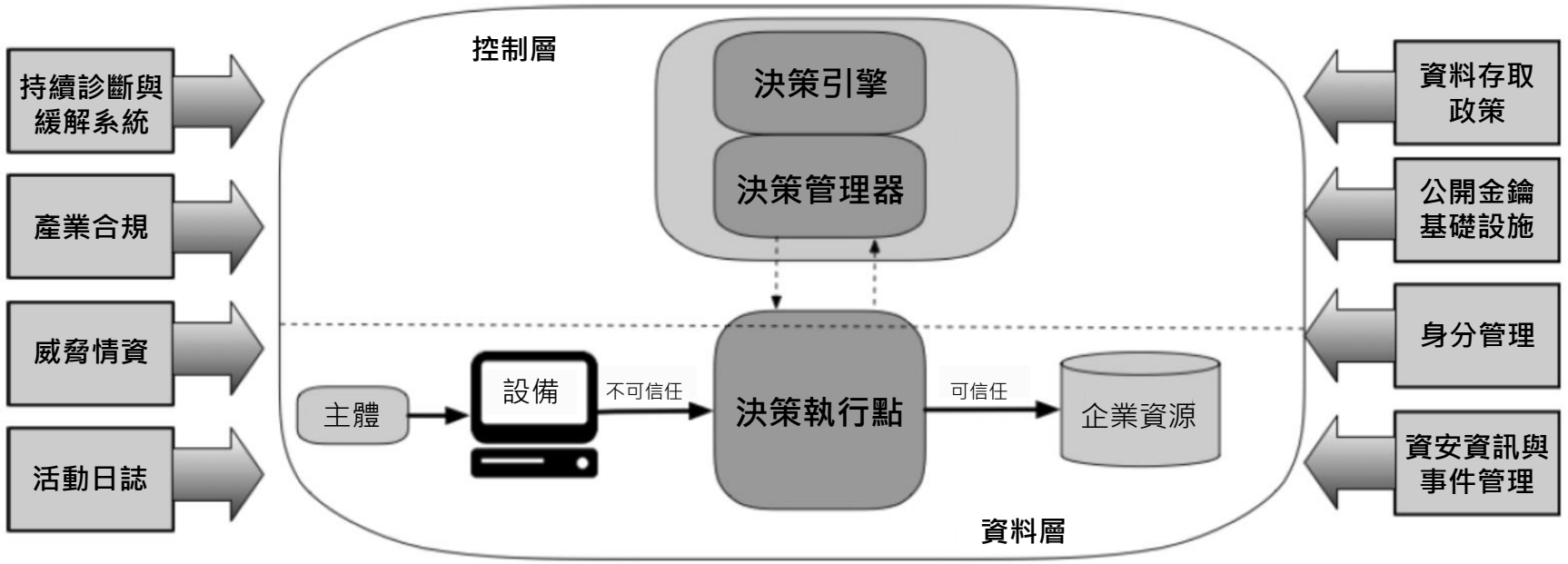
零信任概念

- 突破傳統網路模型之資安窘境，保護資料存取
  - 非保護網路存取，聚焦保護資料/應用存取
  - 無具體邊界，使用者/設備與資料/應用無處不在
  - 任何資料存取永不信任且必須驗證



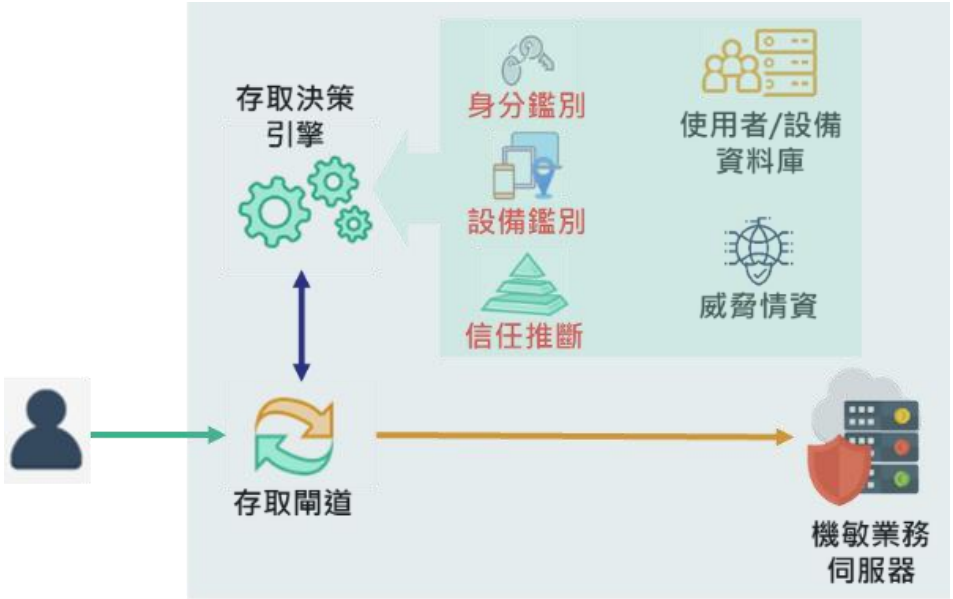
NIST ZTA

- 2020年美國國家標準技術研究院(NIST)正式頒布標準文件NIST SP 800-207，將零信任架構分成核心組件與支援組件
  - 核心組件：執行鑑別、決定授權及管理連線
  - 支援組件：支援存取決策的資訊與系統



NIST零信任推動建議

- 零信任架構以決策引擎為核心，包含身分鑑別、設備鑑別及信任推斷3大關鍵技術
- 實施零信任會是一段過程，而不是一次大規模替換基礎架構，且與傳統模式會同時混合運作



零信任架構

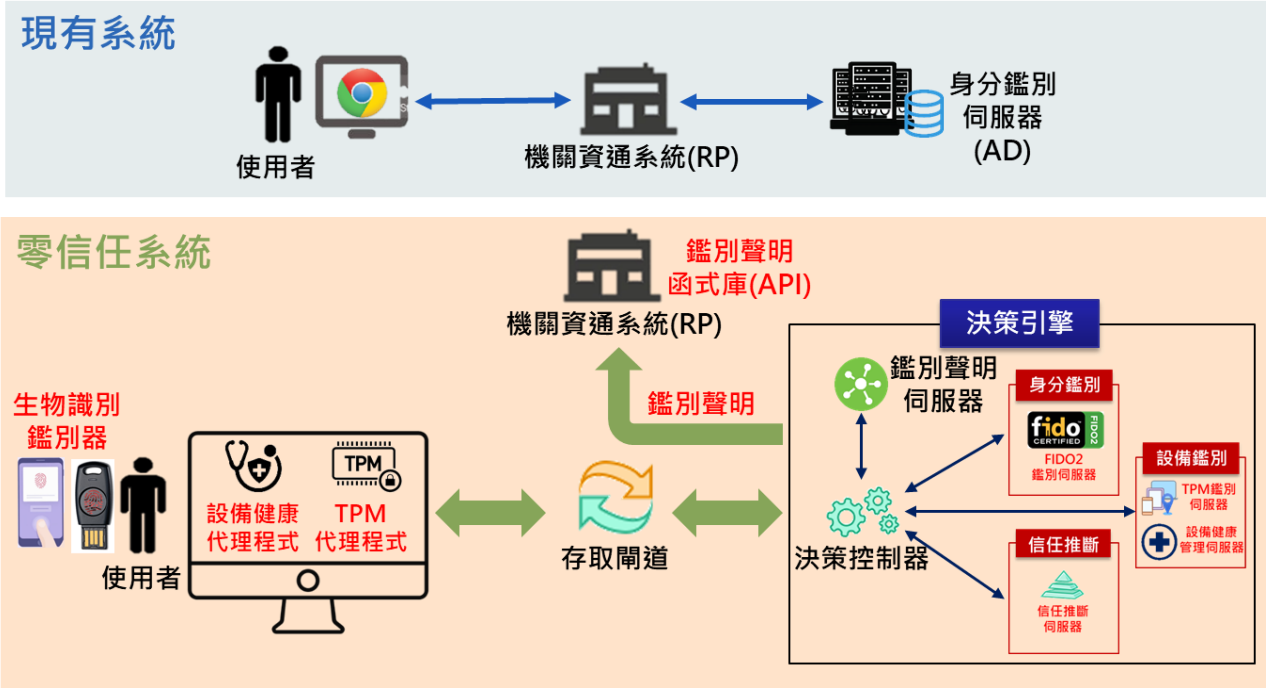
政府零信任架構說明

政策依據

- 依據
  - 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， 藉由發展主動式防禦技術，推動政府機關導入零信任架構，完善政府網際服務網防禦深廣度
- 推動規劃
  - 數位發展部資通安全署規劃投入經費，優先推動A級公務機關導入零信任架構

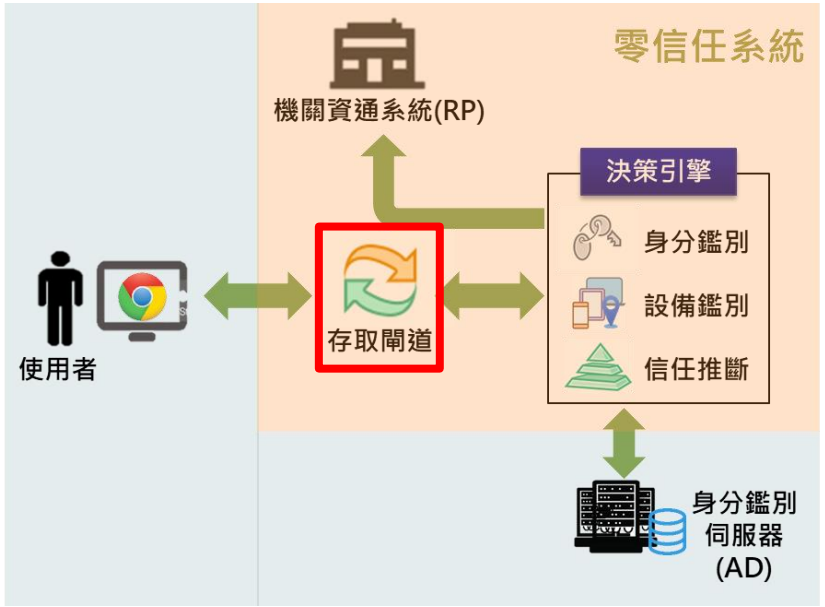
政府零信任架構

- 參考NIST零信任架構，採取資源門戶之部署方式(Resource Portal-Based Deployment)，包含3大核心機制：
  - 身分鑑別：多因子身分鑑別與鑑別聲明
  - 設備鑑別：設備鑑別與設備健康管理
  - 信任推斷：使用者情境信任推斷機制



存取閘道

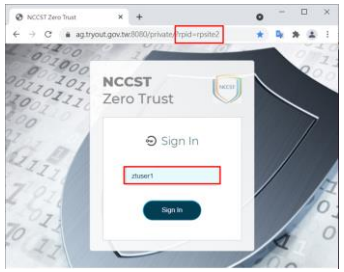
- 存取閘道為資源控管門戶
  - 調整防火牆使任何對資通系統之存取皆須透過存取閘道
  - 透過反向代理(Reverse Proxy)技術，隱藏內部伺服器與機關資通系統之網路路徑

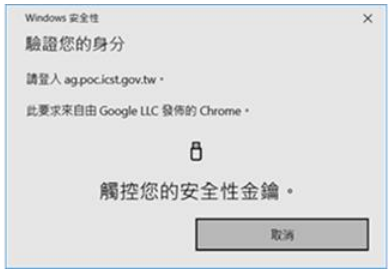


鑑別前後皆隱藏真實路徑

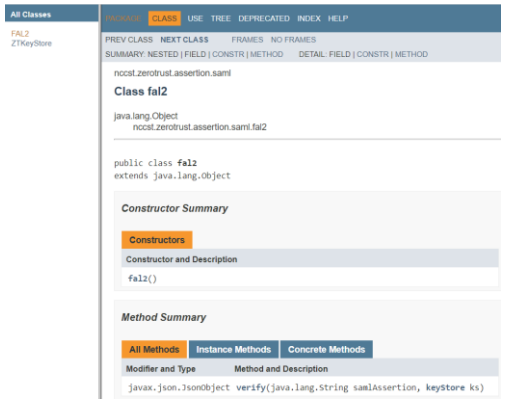
身分鑑別

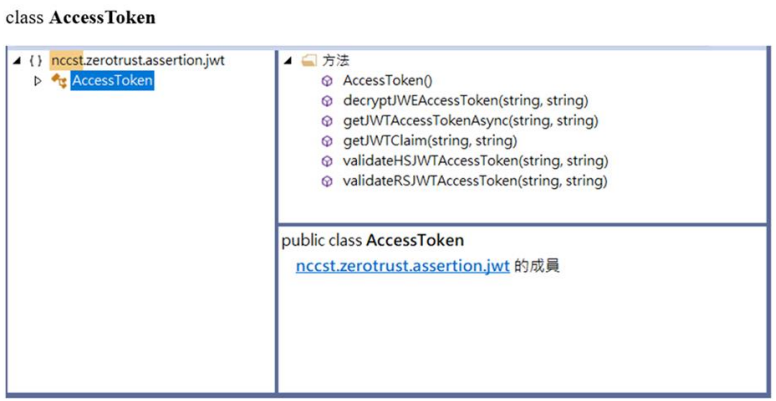
- 以無密碼雙因子方式達成身分鑑別
  - 運用如FIDO2相關技術鑑別使用者之身分





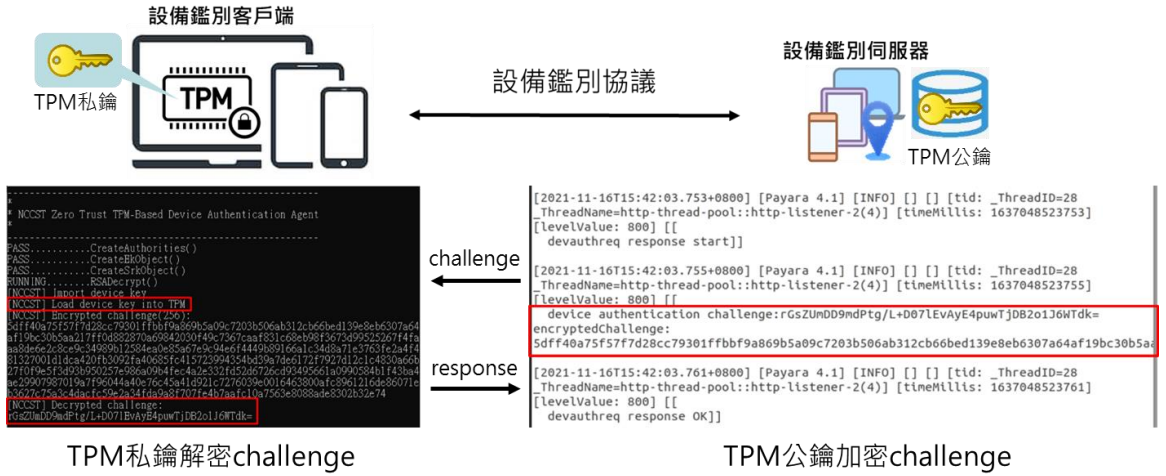
- 提供具備簽章與加密之鑑別聲明
  - 提供API函式庫，使機關之資通系統(RP)可解密並驗證鑑別聲明以確保其機密性與完整性



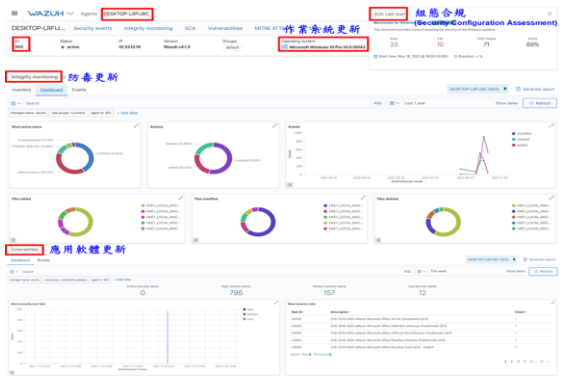


設備鑑別

- 基於公開金鑰技術之設備鑑別方法
  - 透過TPM或Agent產生金鑰與憑證，完成設備註冊與鑑別



- 設備健康管理
  - 持續性設備健康狀態監控
  - 依設備健康狀態計算設備健康信任等級

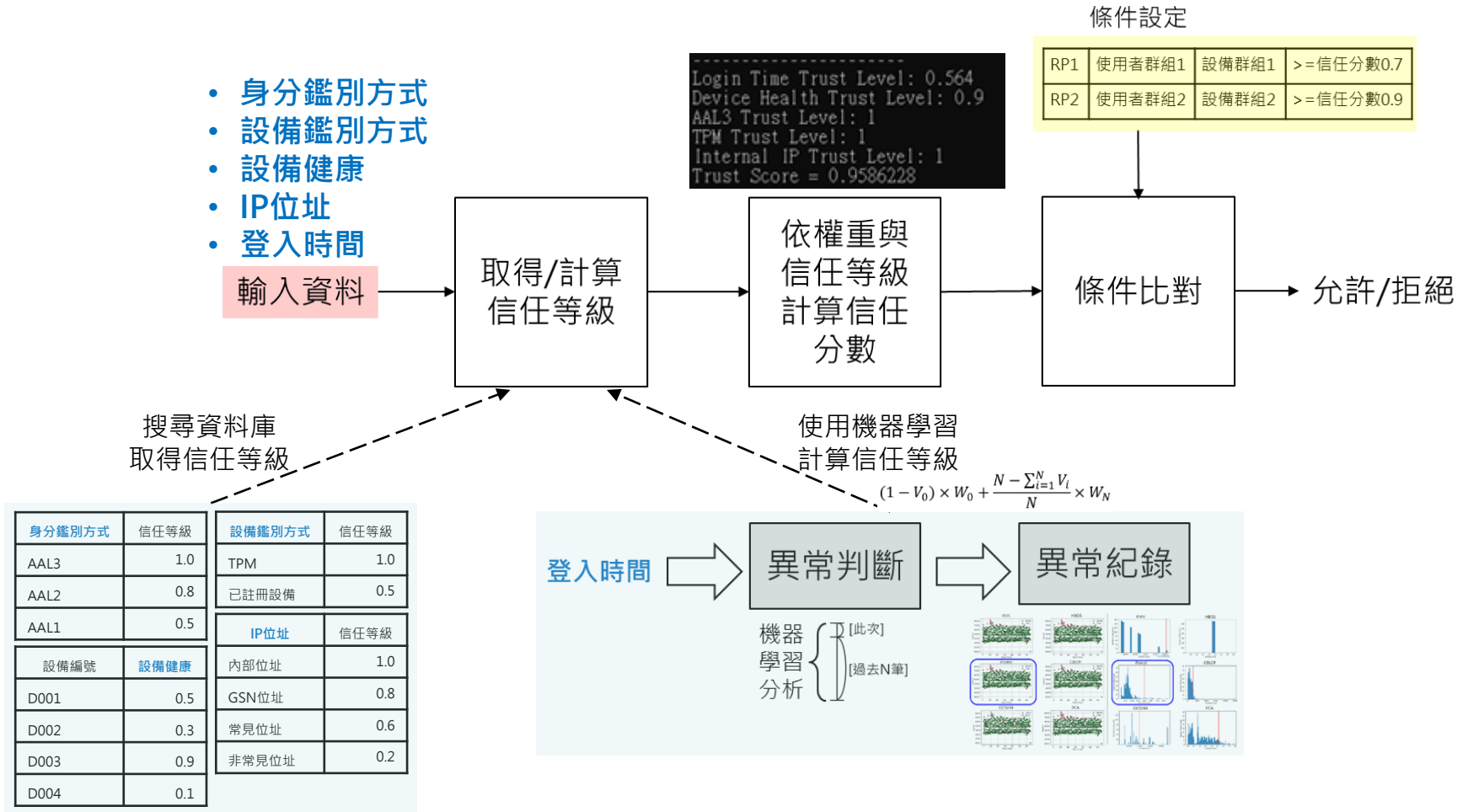


設備編號	設備健康狀態	信任等級
D001	AD	0.5
D002	CD	0.3
D003	ABC	0.9
D004	D	0.1

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

信任推斷

- 基於信任推斷機制決定存取權限
  - –依使用情境計算每次存取之信任分數作為判斷依據



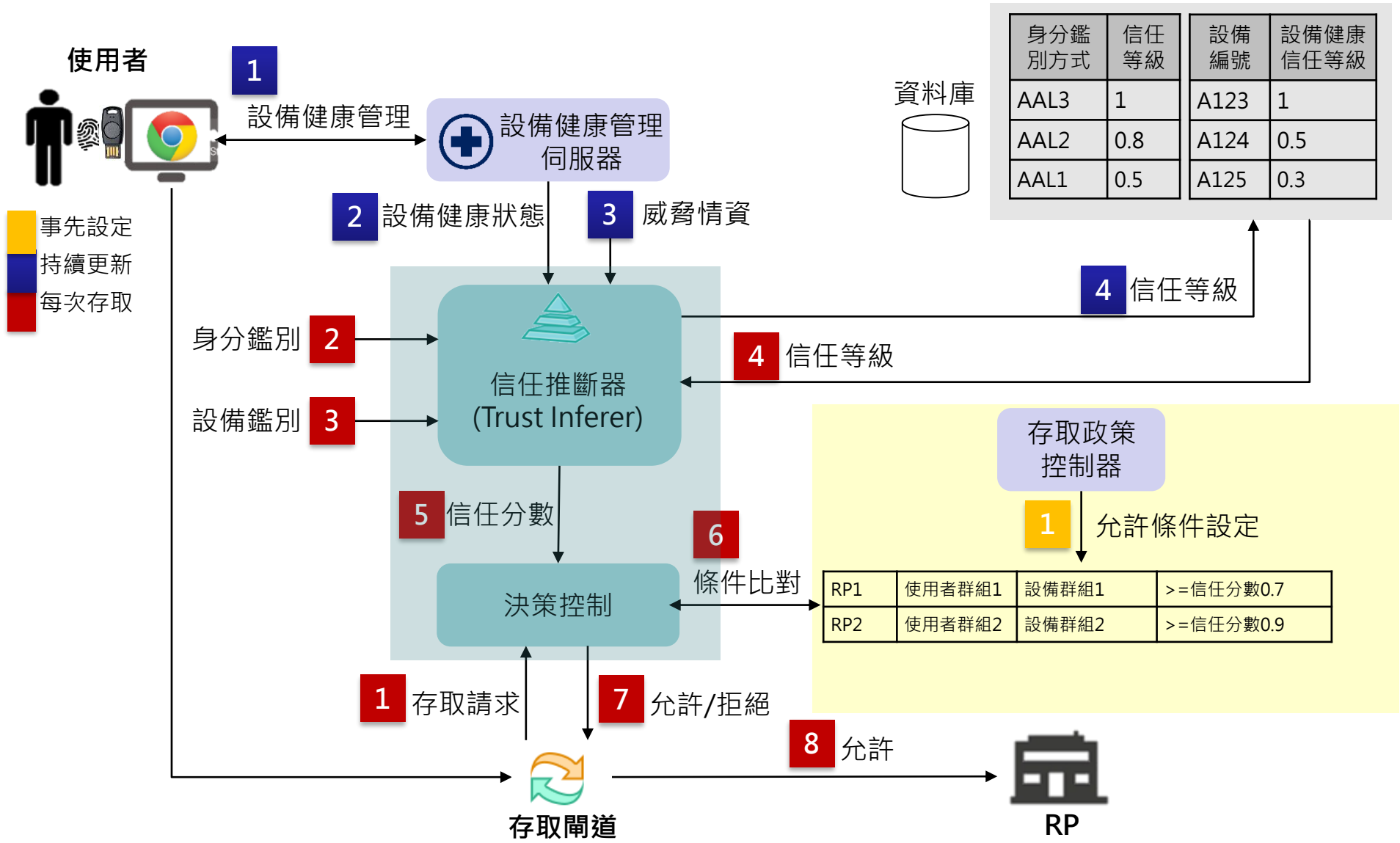
身分鑑別方式	信任等級
AAL3	1.0
AAL2	0.8
AAL1	0.5

設備鑑別方式	信任等級
TPM	1.0
已註冊設備	0.5

IP位址	信任等級
內部位址	1.0
GSN位址	0.8
常見位址	0.6
非常見位址	0.2

設備編號	設備健康
D001	0.5
D002	0.3
D003	0.9
D004	0.1

完整零信任登入流程


使用者
1
設備健康管理
設備健康管理伺服器
資料庫
身分鑑別方式 | 信任等級 | 設備編號 | 設備健康信任等級
AAL3 | 1 | A123 | 1
AAL2 | 0.8 | A124 | 0.5
AAL1 | 0.5 | A125 | 0.3
事先設定
持續更新
每次存取
2 設備健康狀態
3 威脅情資
4 信任等級
4 信任等級
身分鑑別 2
設備鑑別 3
信任推斷器
(Trust Inferer)
存取政策控制器
1 允許條件設定
RP1 | 使用者群組1 | 設備群組1 | >=信任分數0.7
RP2 | 使用者群組2 | 設備群組2 | >=信任分數0.9
5 信任分數
6 條件比對
決策控制
1 存取請求
7 允許/拒絕
8 允許
存取閘道
RP

推動商用產品投入發展

推動資安產業投入

- 美國NCCoE與Microsoft等24家技術公司簽署合作研發協議，規劃利用商用技術建立零信任架構

AWS	f5	Lookout	Palo Alto Networks	Tenable
Appgate	Forescout	Mandiant	PC Matic	VMware
Broadcom	Google Cloud	McAfee	Ping Identity	Zimperium
Cisco	IBM	Microsoft	Radiant Logic	Zscaler
DigiCert	Ivanti	Okta	SailPoint	

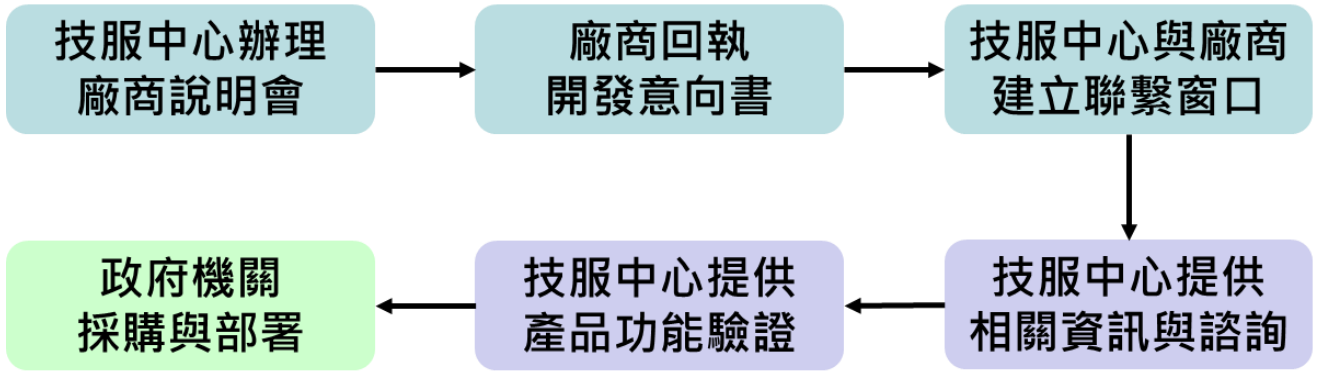
美國零信任架構落地合作廠商

資料來源：https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

- 參考美國作法，推動國內廠商參與開發與整合符合政府零信任架構需求之解決方案，提供多元建置方式，強化資安韌性

辦理零信任廠商說明會

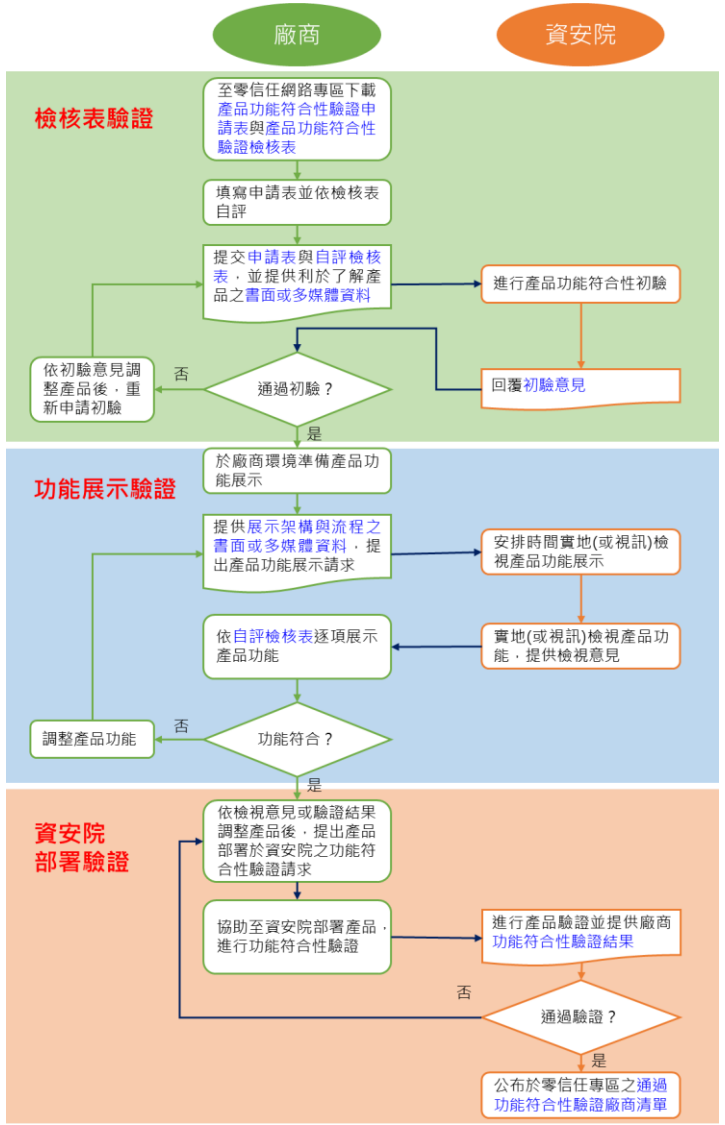
- 111年7月14日由前技服中心辦理「政府零信任架構廠商說明會」
  - 因應後續擴大推動機關導入之政策，透過前行政院資安處發文，廣邀國內資安廠商與會，說明政策規劃、開發需求及參與流程



制訂零信任產品功能驗證與流程

- 逐年發展功能驗證檢核表
  - 驗證資安廠商所開發之產品具備零信任架構之必要功能(Baseline)
- 功能驗證流程分為3個階段
  - 檢核表驗證
    - ➢ 廠商依檢核表自評
  - 功能展示驗證
    - ➢ 廠商依檢核表Demo各項功能
  - 資安院部署驗證
    - ➢ 廠商至資安院之測試環境部署產品

零信任網路身分鑑別								
編號	名稱	說明	驗證項目		適用性	符合	未符合	備註
ZTUA-3	鑑別器保證等級(AAL)	身分鑑別系統應滿足AAL3等級	1	身分鑑別機制須使用雙因子身分鑑別協定	必要	√		使用FIDO雙因子身分鑑別協定
			2	身分鑑別機制須使用實體安全金鑰	必要	√		使用實體安全金鑰或手機鑑別器



結語

- 導入零信任架構為政府強化資安防護之既定政策，除依國家資通安全發展方案進程逐年推動，近期數位發展部亦已規劃資安責任等級A級之政府機關開始導入零信任架構
- 後續將持續鼓勵並引導資安廠商參與零信任相關產品開發並納入共同供應契約，為擴大推動做好萬全準備

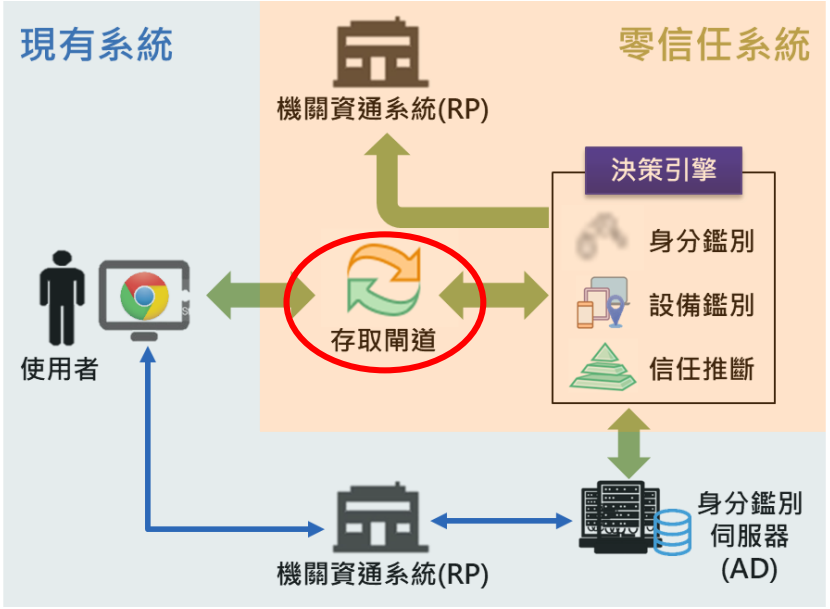
報告完畢
敬請指教

附錄

政府零信任架構需求
補充說明

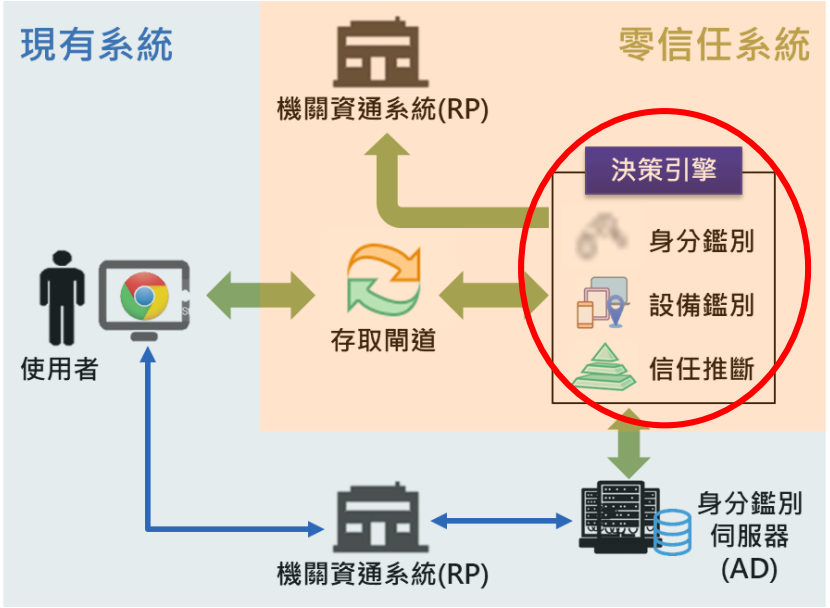
存取閘道

- 存取閘道(Access Gateway)負責網路導向與連線，為機關資通系統(RP)之存取門戶
  - 不論來自內部或外部網路之存取，必須且唯一經由存取閘道
  - 為唯一公開存取之組件，存取全程必須隱藏內部網路路徑(如利用反向代理技術)
  - 必須實施負載平衡機制以避免效率瓶頸
  - 必須實施可有效防止阻斷服務攻擊之機制



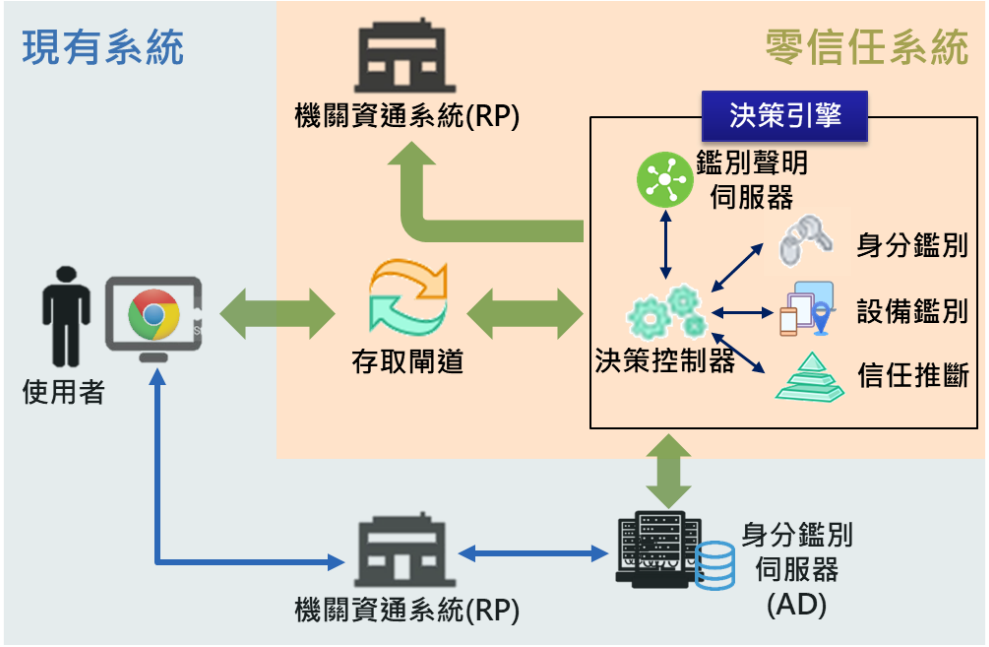
決策引擎

- 決策引擎(Decision Engine)負責存取決策，包含身分鑑別、設備鑑別及信任推斷3大核心機制
  - **身分鑑別**：以實體安全金鑰或手機APP進行無密碼雙因子身分鑑別(FIDO2)，並可與現有AD共存與同步
  - **設備鑑別**：可確認使用者設備為受機關管理之設備，且在可接受之資安狀態，可因應遠距與居家辦公之資安需求
  - **信任推斷**：可隨時依使用者行為與設備狀態，偵測異常存取



決策引擎組件

- 決策引擎負責接收存取請求、決定允許與否及授予存取憑據，其組件包含：
  - **決策控制器**：負責控制存取決策之流程，包含設定存取允許條件、接收存取請求、驅動3大核心機制及授予鑑別聲明
  - **3大核心機制**：由身分鑑別、設備鑑別及信任推斷進行驗證與評估，並將結果回饋給決策控制器
  - **鑑別聲明伺服器**：針對獲得允許之存取，發行鑑別聲明，做為存取RP之憑據

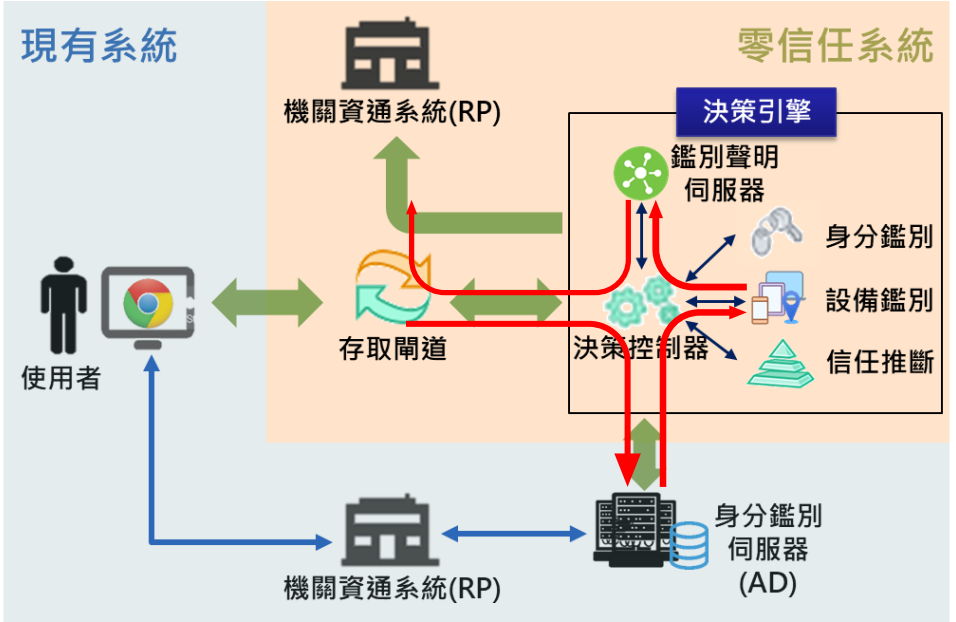


決策控制器

- 存取條件管理
  - 可設定存取允許之條件，做為存取允許或拒絕之依據

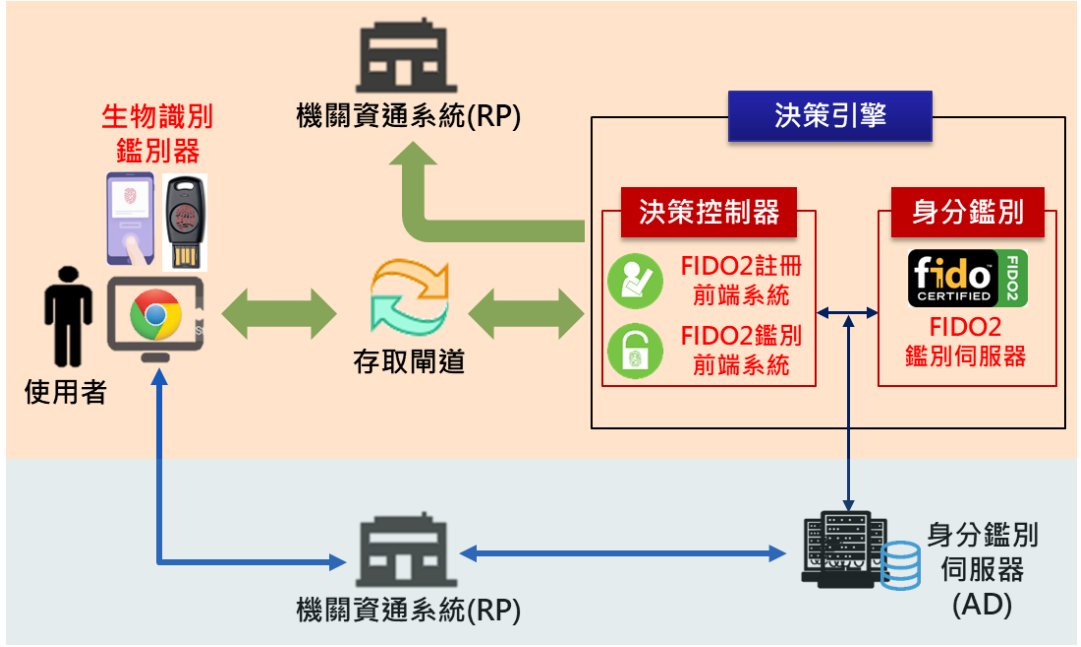
RP1	使用者群組	設備群組	FIDO2身分鑑別
RP2	使用者群組	設備群組	FIDO2身分鑑別 & TPM設備鑑別
RP3	使用者群組	設備群組	>=信任分數0.8

- 存取請求介面
  - 建置3大核心機制所需之前端系統，包含身分註冊網頁、登入網頁、設備鑑別代理程式驅動模組、情境資料擷取等
- 決策流程控制
  - 接收存取請求
  - 與現有系統協作
  - 驅動3大核心機制
  - 確認是否滿足存取允許條件
  - 驅動鑑別聲明產生
  - 進行RP存取導向



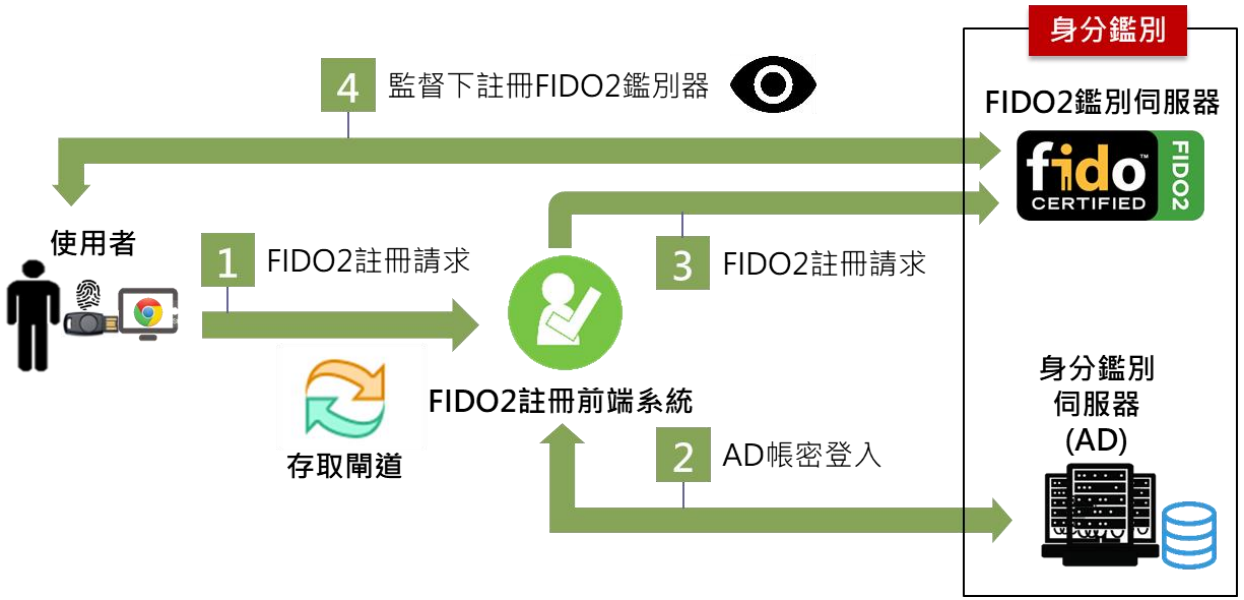
身分鑑別

- 無密碼雙因子身分鑑別
  - 建置FIDO2鑑別伺服器，並與現有身分鑑別伺服器(如AD)維持帳號狀態一致
  - 建置FIDO2註冊前端系統與FIDO2鑑別前端系統，提供使用者身分註冊與登入網頁
  - 使用者以生物識別鑑別器(實體安全金鑰或手機APP)進行身分鑑別

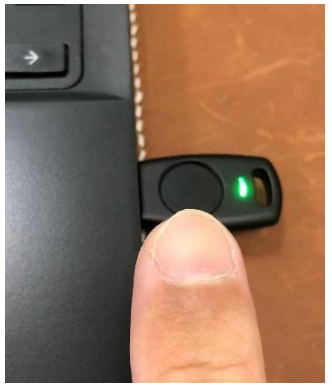


身分鑑別流程-註冊階段(IAL3)

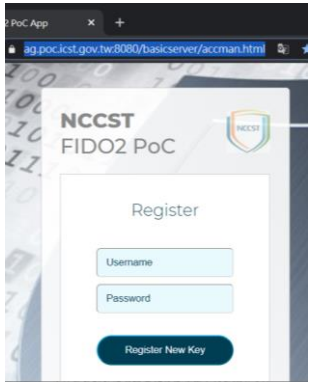
- 使用者先具備現有AD帳號，再以該帳號註冊(綁定)FIDO2鑑別器



IAL3註冊流程



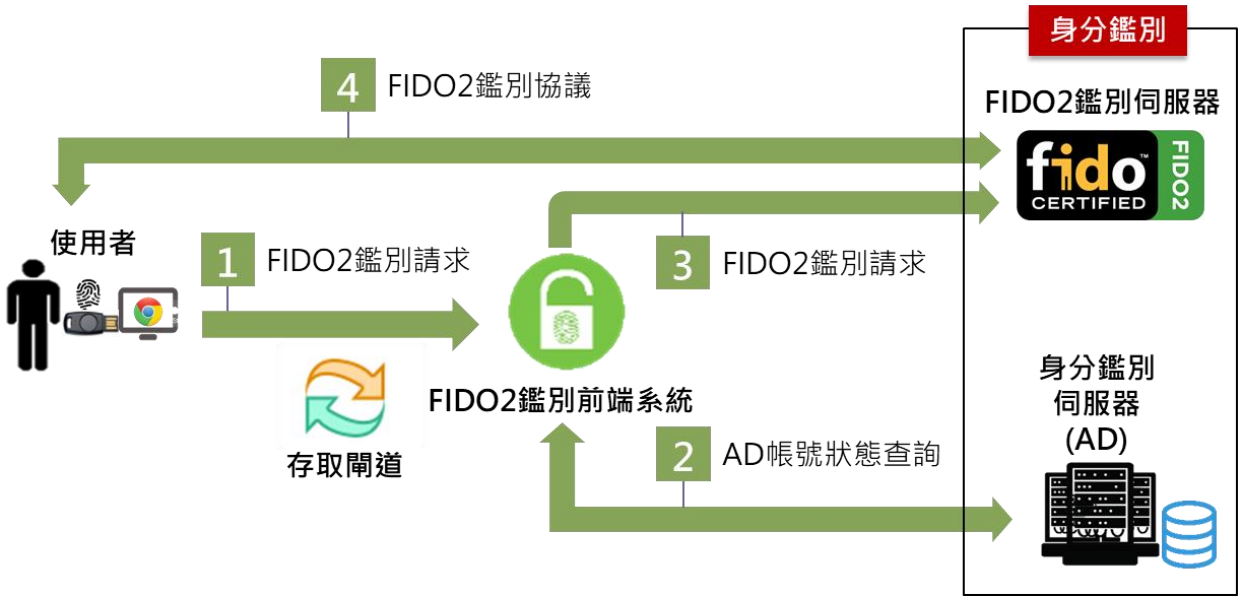
註冊FIDO2鑑別器



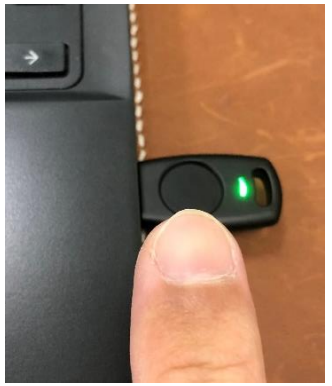
以現有AD帳密登入

身分鑑別流程-鑑別階段(AAL3)

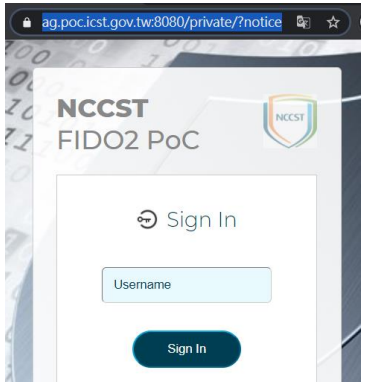
- 以FIDO2帳號與鑑別器進行身分鑑別，惟鑑別前先檢查AD帳號是否已停用或鎖住



AAL3鑑別流程



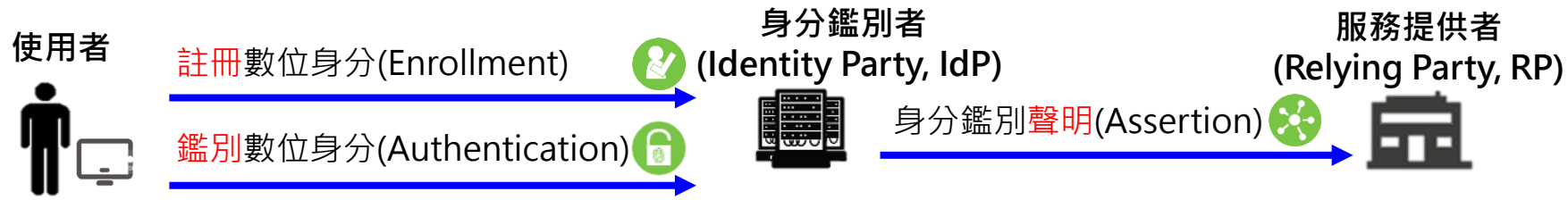
按壓FIDO2鑑別器



以FIDO2帳號登入

身分鑑別保證等級

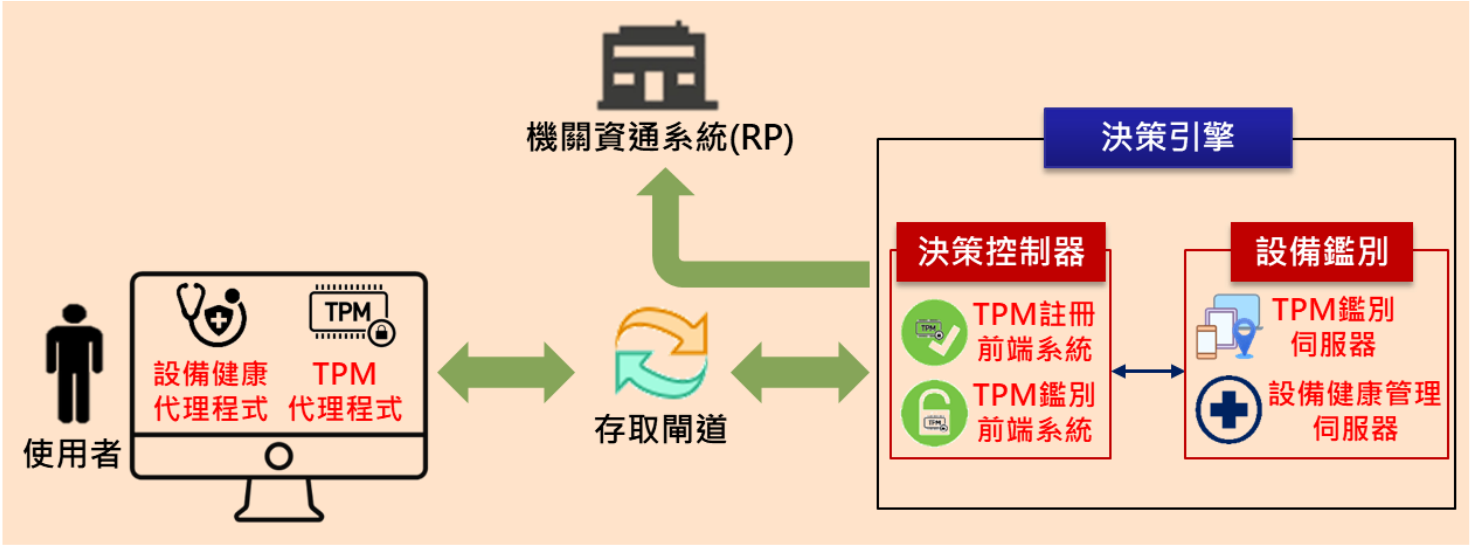
- NIST SP 800-63-3依註冊、鑑別及聲明3階段將身分鑑別分為身分保證等級(IAL)、鑑別保證等級(AAL)及聯邦保證等級(FAL)3個類別，各類別定義3個等級
- 政府機關導入零信任架構應至少達到IAL2/AAL3/FAL2等級



	身分保證等級(IAL) Identity Assurance Level	鑑別保證等級(AAL) Authenticator Assurance Level	聯邦保證等級(FAL) Federation Assurance Level
說明	使用者用來證明自己身分之強度	鑑別過程之防護強度	身分鑑別者(IdP)傳遞給服務提供者(RP)之身分鑑別聲明(Assertion)之防護強度
等級1	自己宣稱之身分便具有效力	至少需要單因子身分鑑別	身分鑑別聲明須經過IdP簽章
等級2	需親自提供證據進行身分證明	• 需要2種不同之鑑別因子 • 鑑別過程之通訊，需使用加密技術	身分鑑別聲明須簽章與加密
等級3	需在監督下親自提供證據與生物特徵進行身分證明	• 透過密鑰(key)進行鑑別 • 需要硬體加密鑑別器	身分鑑別聲明須簽章與加密，且使用者應向RP證明，擁有與身分鑑別聲明對應之密鑰

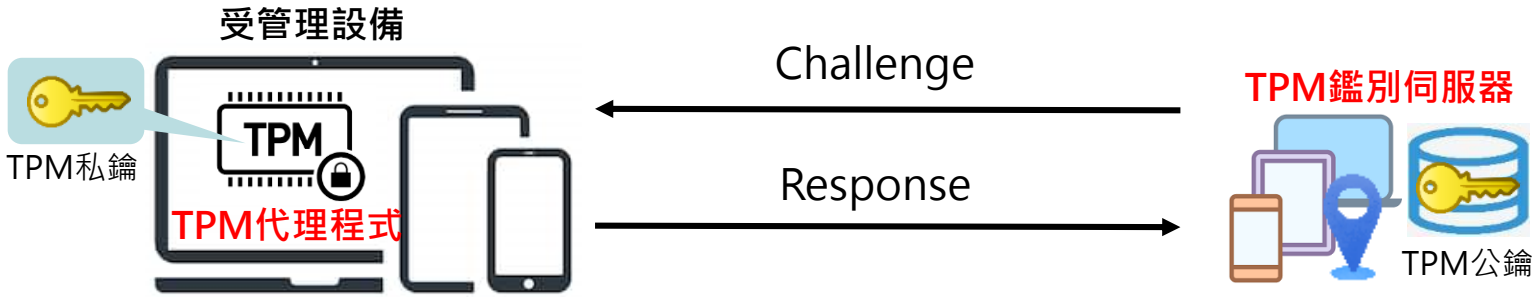
設備鑑別

- 設備TPM鑑別
  - 使用者設備須具備信任平台模組(TPM)
  - 執行基於TPM私鑰之鑑別協議，以驗證使用者設備是受管理設備
    - Client：部署TPM代理程式，負責TPM之輸入與輸出
    - Server：建置TPM鑑別伺服器，負責TPM鑑別協議之驗證，並建置TPM註冊前端系統與TPM鑑別前端系統，負責驅動TPM代理程式進行設備之TPM註冊與鑑別作業
- 設備健康管理
  - 使用者設備部署設備健康代理程式，提供作業系統與病毒保護等設備健康資訊，並進行必要之設備健康修補
  - 建置設備健康管理伺服器，隨時匯整使用者設備健康資訊，監控設備健康狀態，並分析設備健康信任等級，以提供存取決策依據



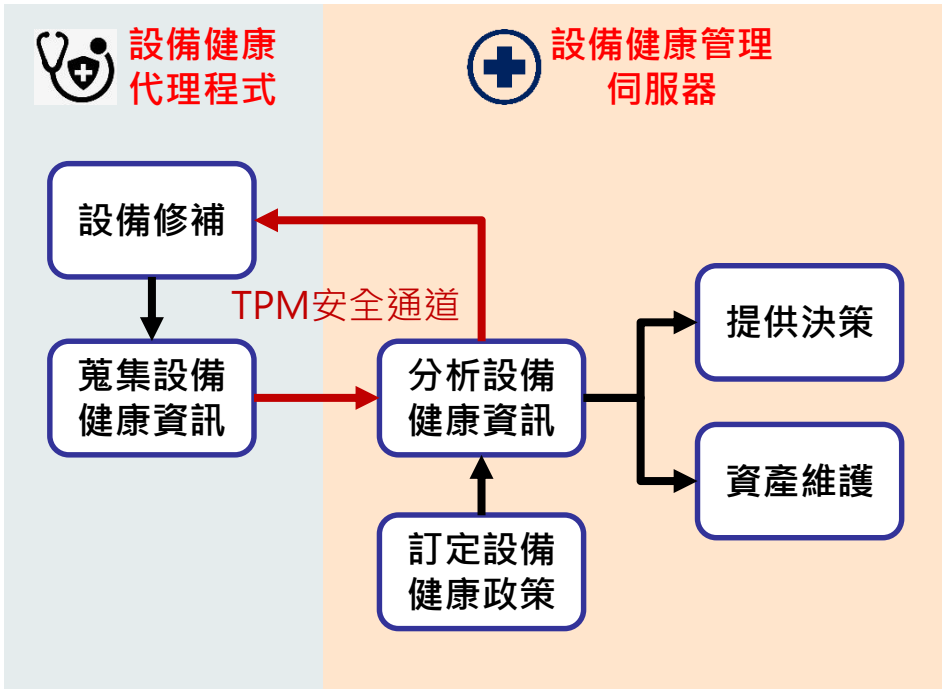
設備TPM鑑別

- 註冊階段
  - –系統管理者於受管理設備初始化TPM金鑰對
  - –於TPM鑑別伺服器註冊受管理設備之TPM公鑰
- 鑑別階段
  - –TPM代理程式驅動TPM進行私鑰運算，並與TPM鑑別伺服器完成TPM鑑別協議



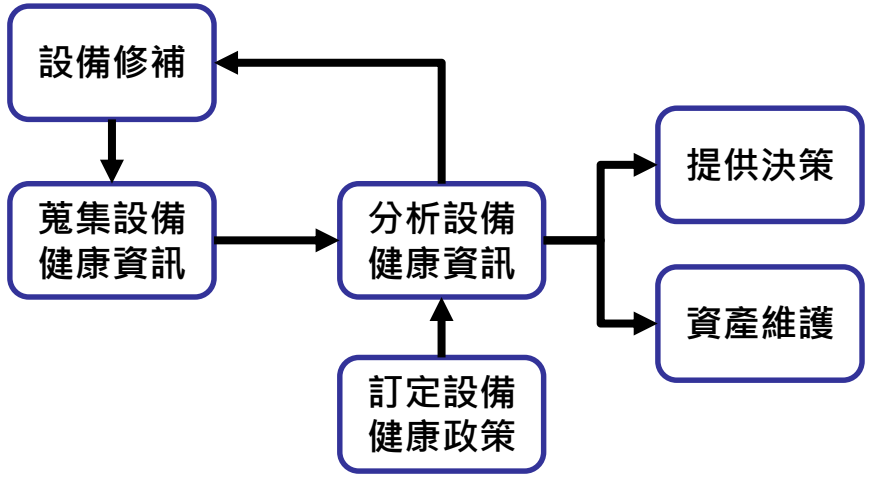
設備健康管理

- 透過設備健康管理流程，維持受管理設備在可接受之資安狀態
- 設備健康代理程式與設備健康管理伺服器之通訊須使用TPM安全通道



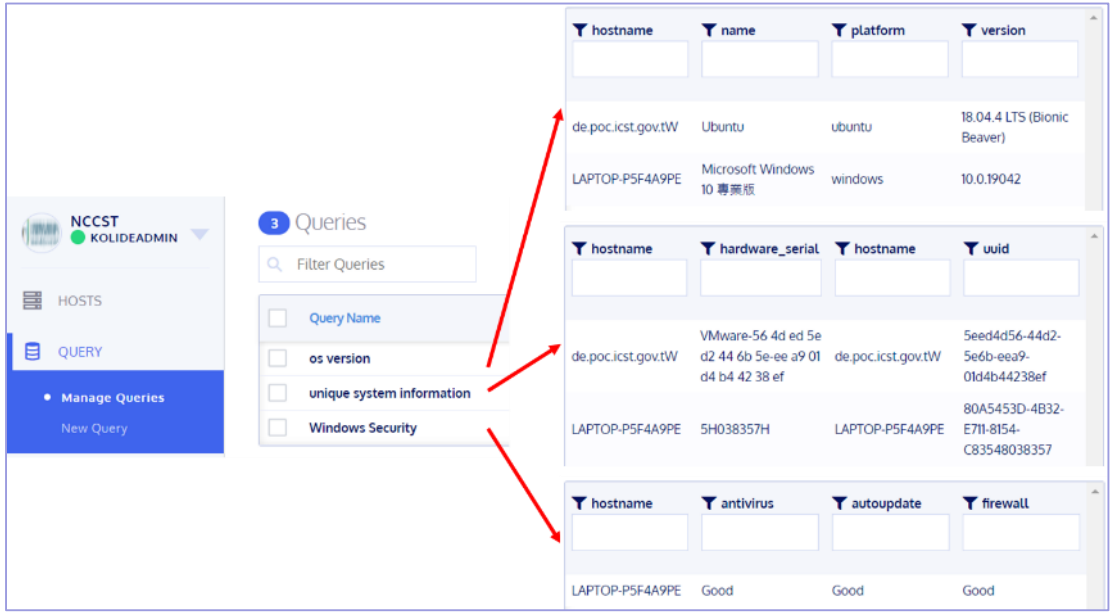
設備健康管理流程

- 訂定設備健康政策
  - 定義可接受之資安規則/狀態
- 蒐集設備健康資訊
  - 設計與執行蒐集指令
  - 排程蒐集腳本
- 分析設備健康資訊
  - 依設備健康政策檢驗設備健康狀態
  - 健康資訊分析與異常偵測
- 設備修補
  - 針對健康狀態不合格之設備，進行組態調整或軟體更新
- 提供決策
  - 依健康狀態分析健康信任等級，以進行信任推斷與存取決策
- 資產維護
  - 依健康狀態，維護設備資產管理資料庫紀錄

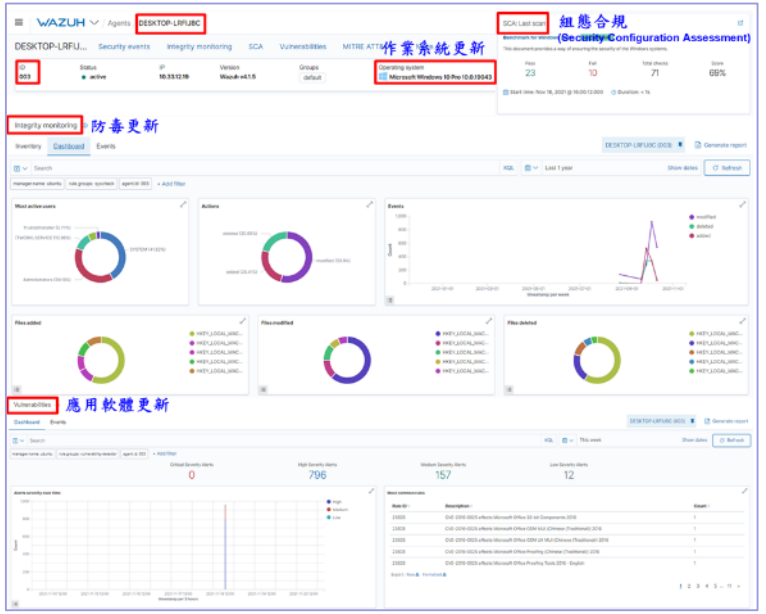


設備健康管理示例(1/2)

- 設備健康代理程式與設備健康管理伺服器示例
  - 示例1：osquery + Kolide Fleet
  - 示例2：Wazuh Agent + Wazuh Server



示例1：osquery + Kolide Fleet



示例2：Wazuh Agent + Wazuh Server

設備健康管理示例(2/2)

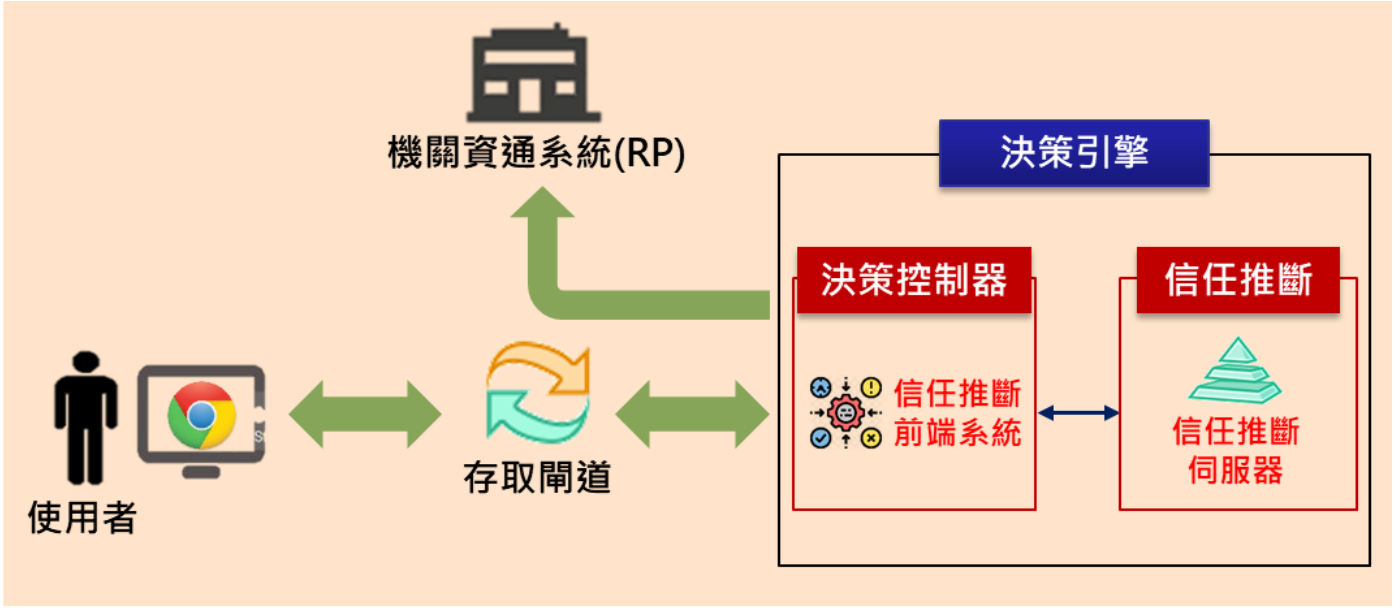
- 設備健康管理伺服器須依設備健康狀態，隨時分析設備健康信任等級，以提供信任推斷
  - 設備健康信任模型示例(加權總和模型)
    - 設定設備健康狀態採計項目
    - 設定權重
    - 加權信任等級

編號	設備健康狀態採計項目	權重分配
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

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

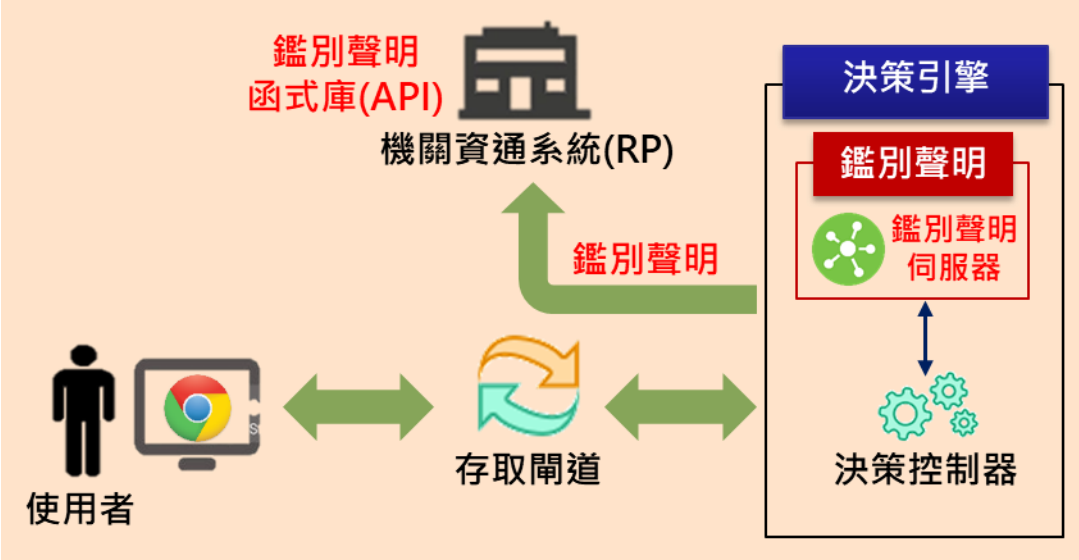
信任推斷

- 基於分數與情境之信任推斷機制
  - 建置信任推斷前端系統，匯整各類輸入資料，透過信任推斷伺服器，進行(智慧)評估與計算，輸出信任分數
    - 輸入：身分鑑別方式、設備鑑別方式、設備健康信任等級、及使用者情境(IP位址、登入時間、瀏覽器等)
    - 輸出：信任分數，供決策控制器做存取決策



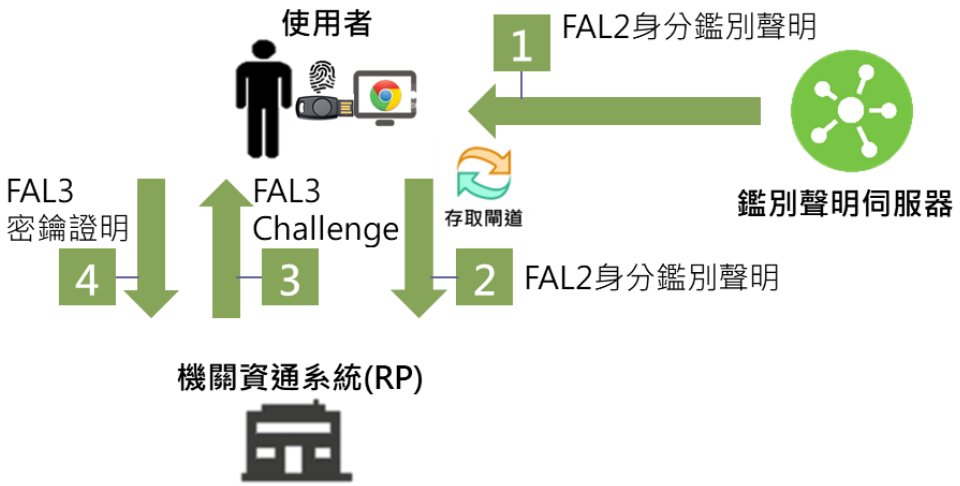
鑑別聲明

- 機關資通系統(RP)存取控制
  - 建置鑑別聲明(Assertion)伺服器，於使用者獲得存取允許後，發行鑑別聲明(JWT與SAML標準格式)
  - 提供鑑別聲明函式庫(API)，以供機關資通系統(RP)介接時取得與驗證鑑別聲明



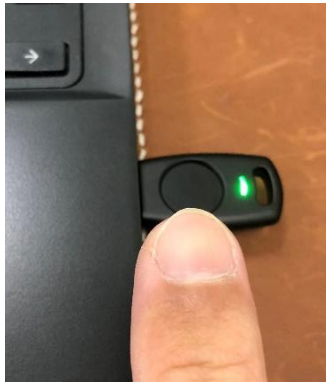
鑑別聲明流程(FAL2/FAL3)

- 鑑別聲明伺服器發行具簽章與加密之FAL2身分鑑別聲明
- 機關資通系統(RP)透過API取得與驗證鑑別聲明
- 機關資通系統(RP)可再針對特定服務，延伸要求FAL3之使用者密鑰證明



FAL3聲明流程

管理介面須FAL3



按壓FIDO2鑑別器

進入管理介面