政府零信任網路說明

行政院國家資通安全會報技術服務中心

111年7月14日

【內部公開】

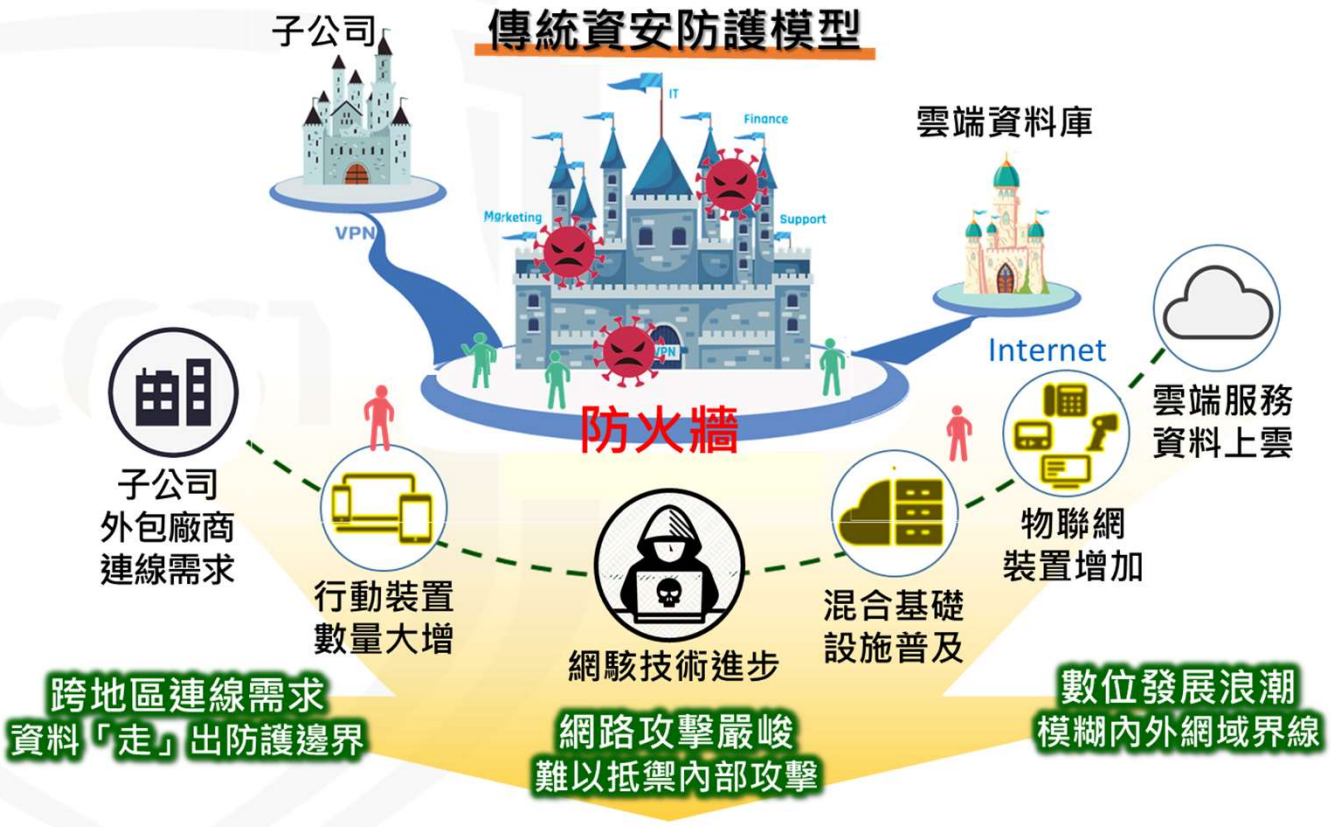
大綱

- 零信任網路簡介
- 國際推動現況
- 我國政策與推動規劃
- 政府零信任網路需求
- 後續作業與展望

零信任網路簡介

傳統網路模型的資安窘境

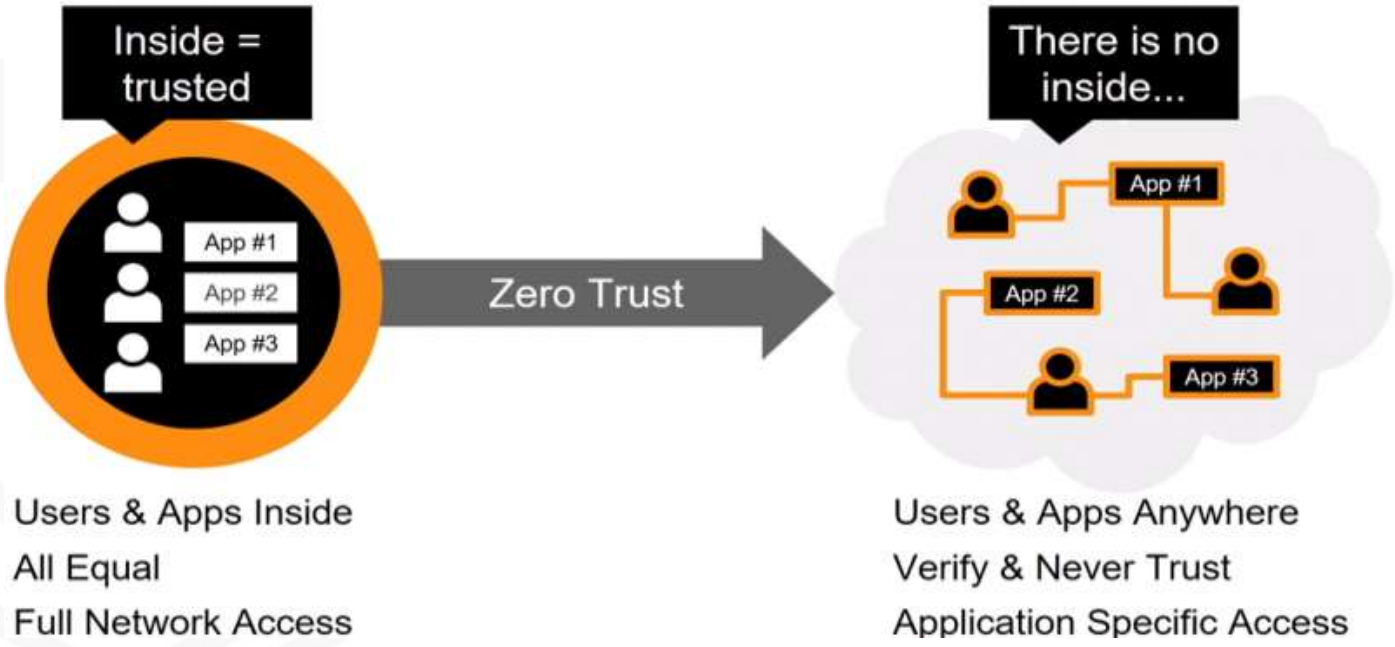
- 隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型已現資安窘境，難以滿足新形態工作需求



資料來源：國家安全局

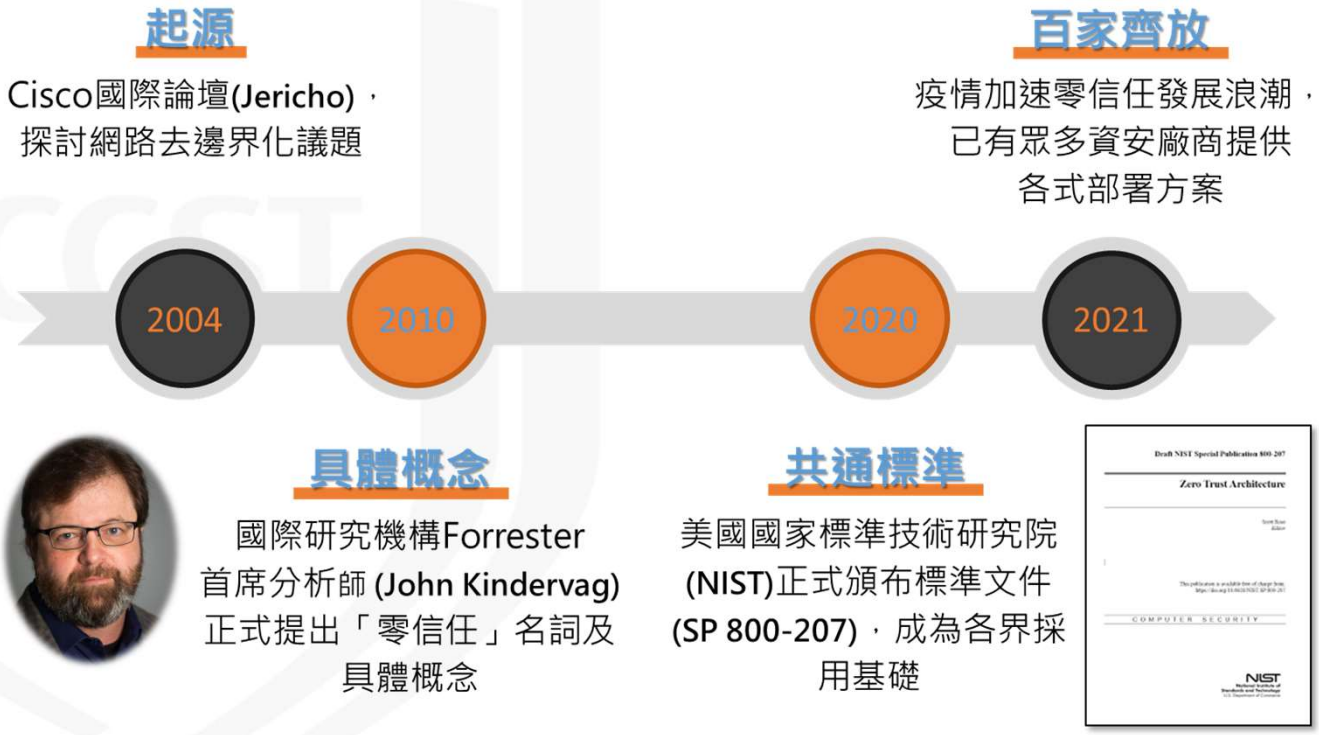
零信任概念

- 零信任希望突破傳統網路模型的資安窘境，並能保護資料存取
  - 不是保護網路存取，而是保護資料/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



零信任演進

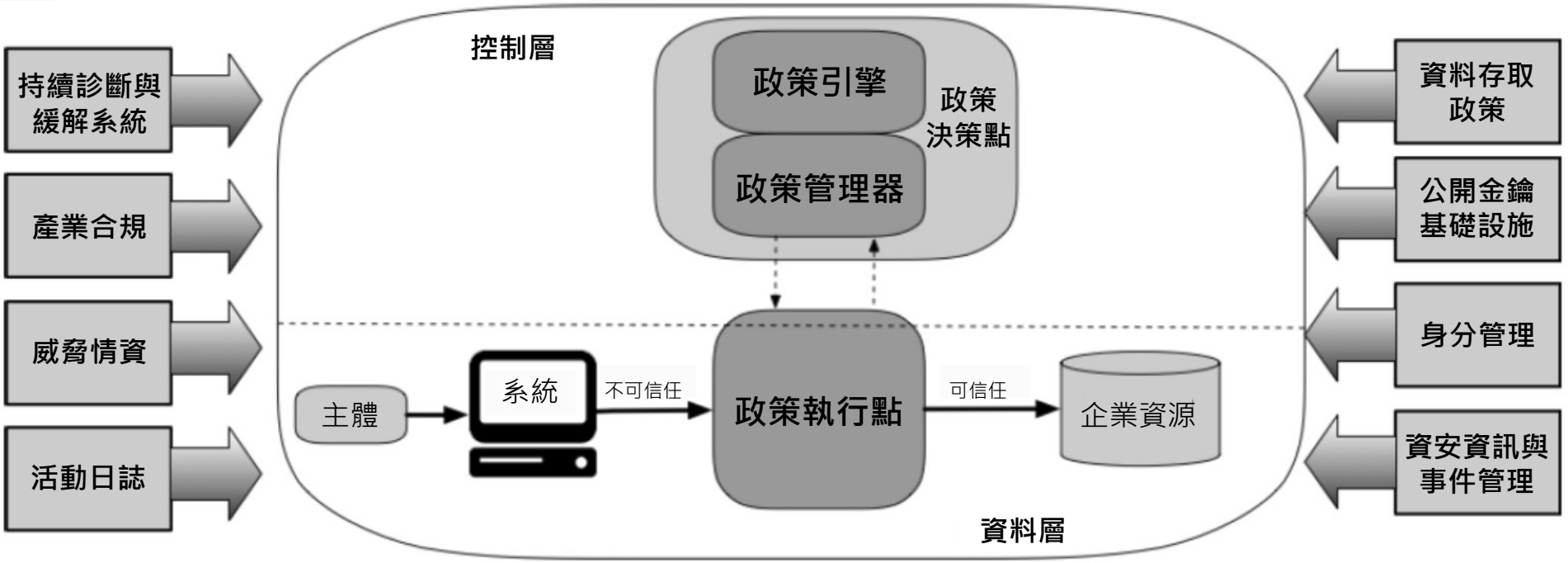
- 零信任概念歷經10幾年發展，2020年美國國家標準技術研究院(NIST)正式頒布標準文件SP 800-207：零信任架構(Zero Trust Architecture, ZTA)，成為各界採用基礎



資料來源：國家安全局

NIST ZTA

- 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



支援組件　　核心組件　　支援組件

國際推動現況

世界重要國家政府推動規劃

- 零信任已從概念探討階段進入實務部署規劃，世界重要國家之政府紛紛建立國家零信任網路安全戰略

美國

具體規劃2024年前聯邦網路完成初步遷移。

歐盟

2020年建立歐盟網安戰略，提出標準框架，協助成員國轉型。

中國

發布國家級標準，建立「零信任聯盟」規劃轉型。

新加坡

2021年10月網路安全戰略，定為國家網安框架。

資料來源：國家安全局

美國零信任架構落地

- 美國是目前規劃最具體之國家，除了有明確政策與時間表之外，並透過國家資安卓越中心(NCCoE)推動商用產品符合NIST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

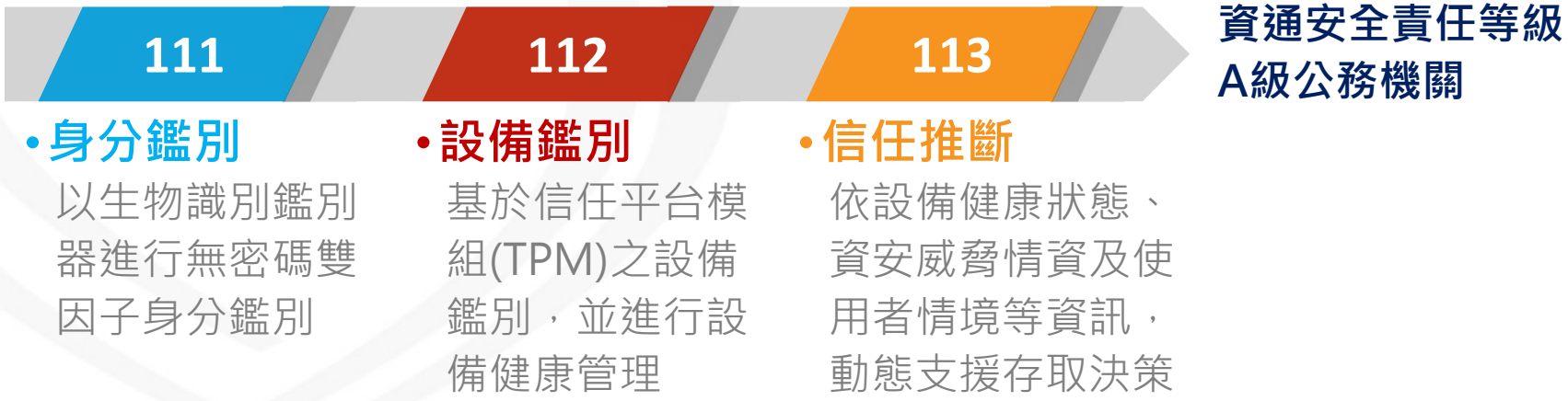
我國政策與推動規劃

政策

- 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，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
- 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

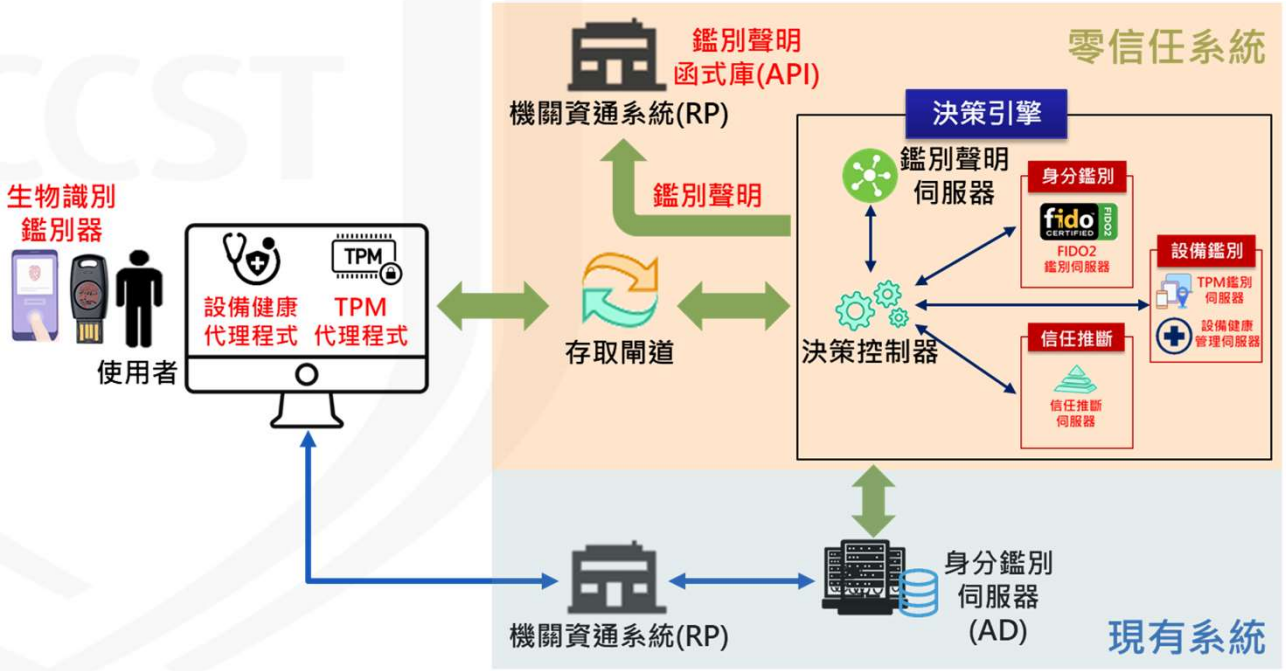
- 政府機關
  - 111年起遴選機關逐年導入零信任網路之身分鑑別、設備鑑別及信任推斷3大核心機制
  - 後續於資通安全責任等級A級公務機關推動導入
- 商用產品
  - 配合111~113年之機關導入，推動廠商開發符合政府零信任網路部署架構、部署原則及核心機制之商用產品，以因應後續A級公務機關之導入



政府零信任網路需求

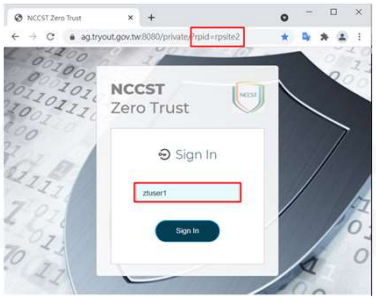
政府零信任網路架構

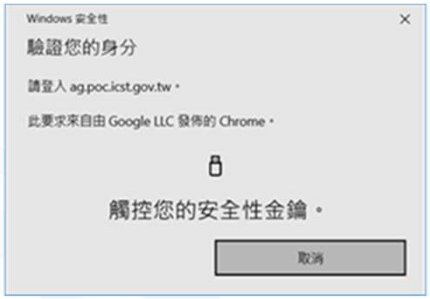
- 參考NIST零信任架構，結合向上集中防護需求，政府零信任網路採存取門戶部署方式，具備身分鑑別、設備鑑別及信任推斷3大核心機制
  - 身分鑑別：FIDO2身分鑑別與鑑別聲明
  - 設備鑑別：TPM設備鑑別與設備健康管理
  - 信任推斷：基於分數與情境之信任推斷機制



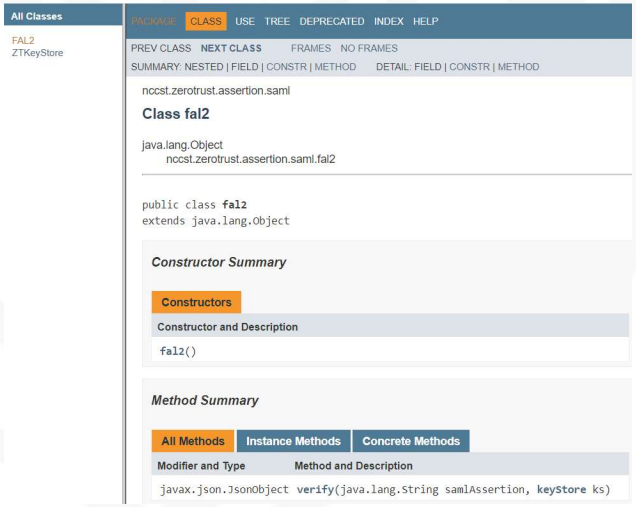
身分鑑別

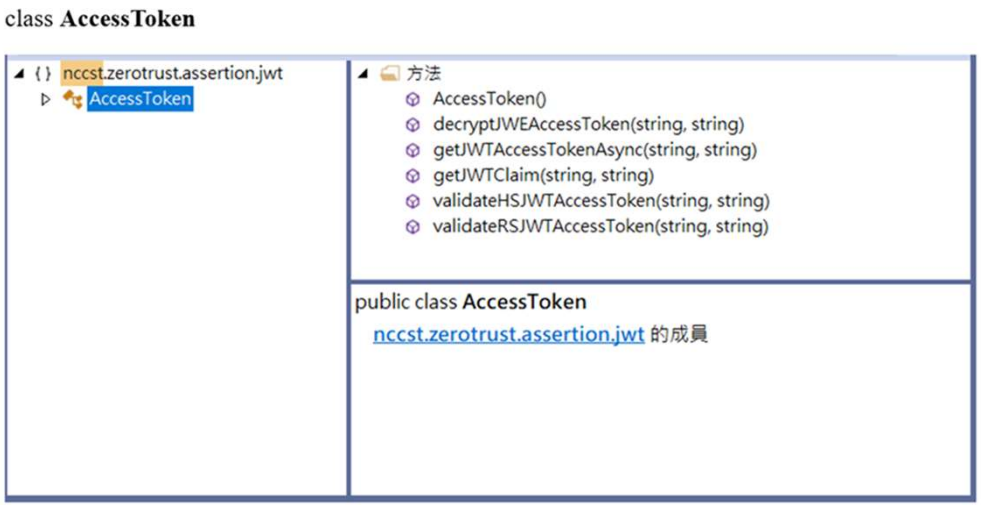
- FIDO2無密碼雙因子身分鑑別
  - 通過FIDO聯盟驗證之FIDO2伺服器與生物識別鑑別器





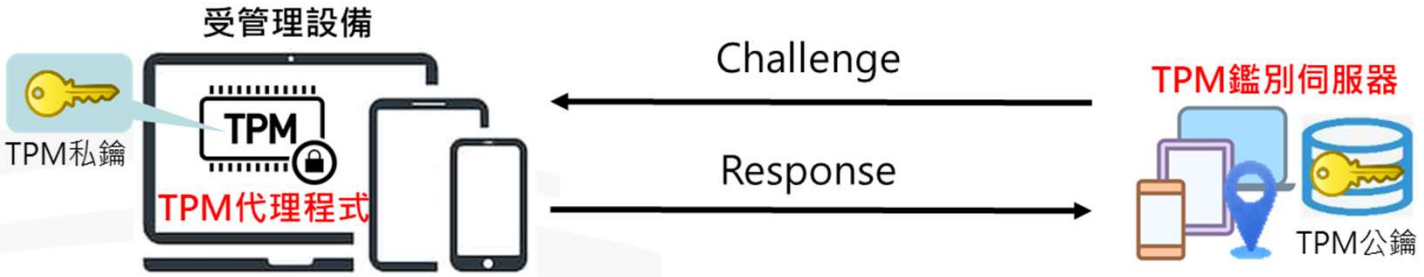
- 簽章與加密之身分鑑別聲明
  - 提供JWT與SAML 2種標準格式之函式庫，以供機關資通系統(RP)介接時取得與驗證鑑別聲明



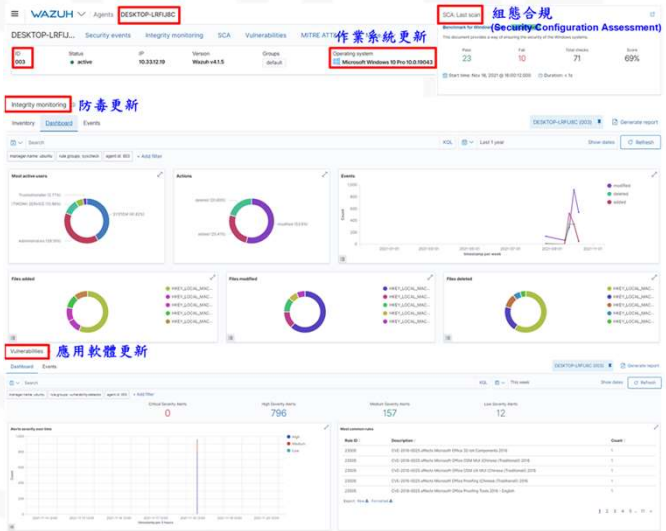


設備鑑別

- 基於信任平台模組(TPM)之設備鑑別方法
  - 執行基於TPM內私鑰之公開金鑰密碼系統鑑別協議



- 設備健康管理
  - 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

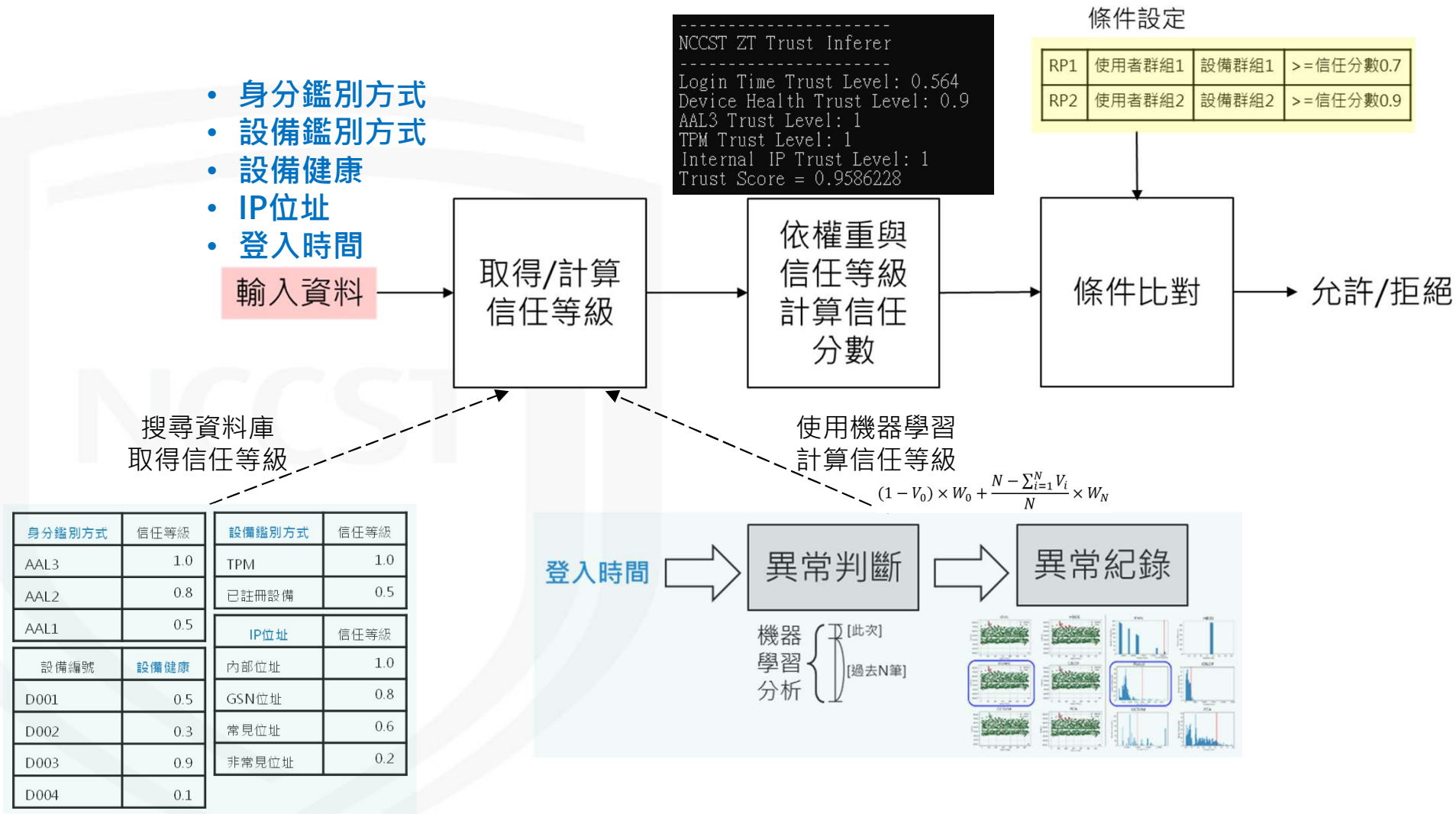


設備編號	設備健康狀態	信任等級
D001	AD	0.5
D002	CD	0.3
D003	ABC	0.9
D004	D	0.1

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

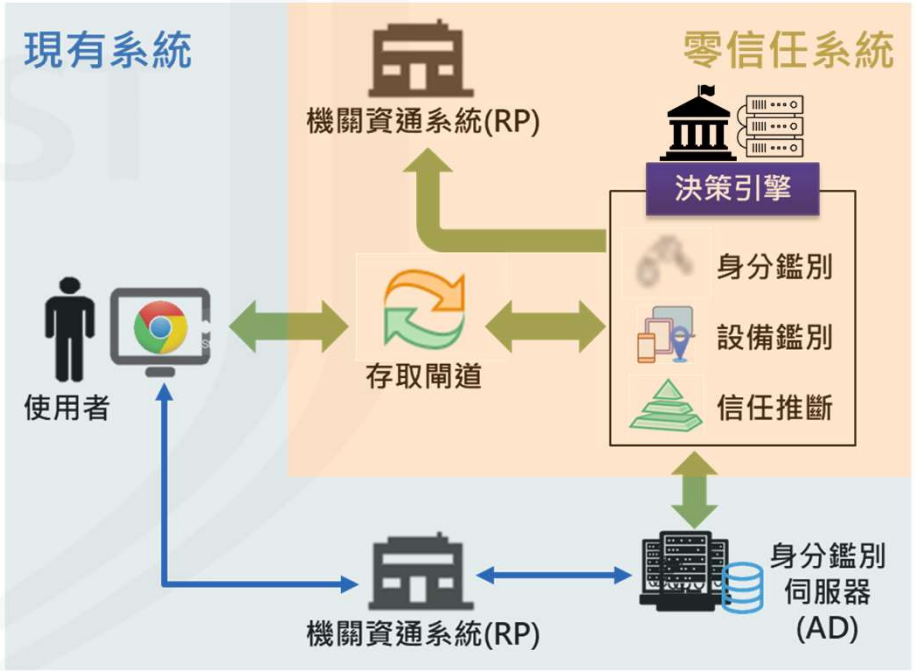
信任推斷

- 基於分數與情境之信任推斷機制



部署原則

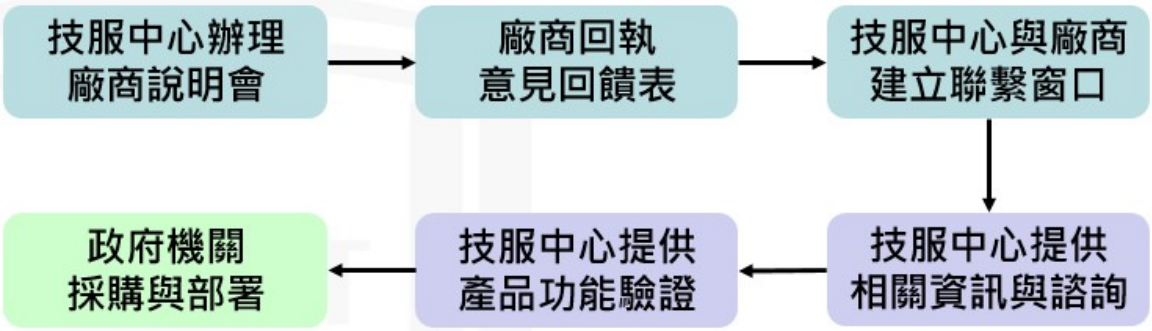
- 政府機關導入零信任網路會是一段過程，而不是一次大規模替換基礎架構，相關組件之部署須具備能與現有系統同時混合運作之能力
- 政府零信任網路相關組件之部署優先考量部署於政府機關維運之地端(On-Premises)環境

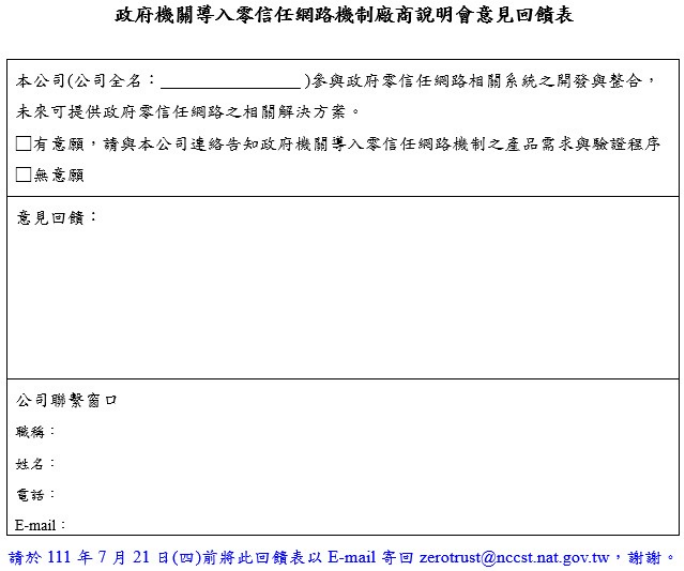


後續作業與展望

後續作業

- 廠商參與流程





政府機關導入零信任網路機制廠商說明會意見回饋表

本公司(公司全名：_____)參與政府零信任網路相關系統之開發與整合，未來可提供政府零信任網路之相關解決方案。

□有意願，請與本公司連絡告知政府機關導入零信任網路機制之產品需求與驗證程序

□無意願

意見回饋：

公司聯繫窗口

職稱：

姓名：

電話：

E-mail：

請於 111 年 7 月 21 日(四)前將此回饋表以 E-mail 寄回 zerotrust@nccst.nat.gov.tw，謝謝。

- 零信任網路專區
  - 技服中心建立零信任網路專區網頁，提供相關資訊

未來展望

- 零信任網路導入為政府強化資安防護之既定政策，將優先於資通安全責任等級A級公務機關推動導入
- 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

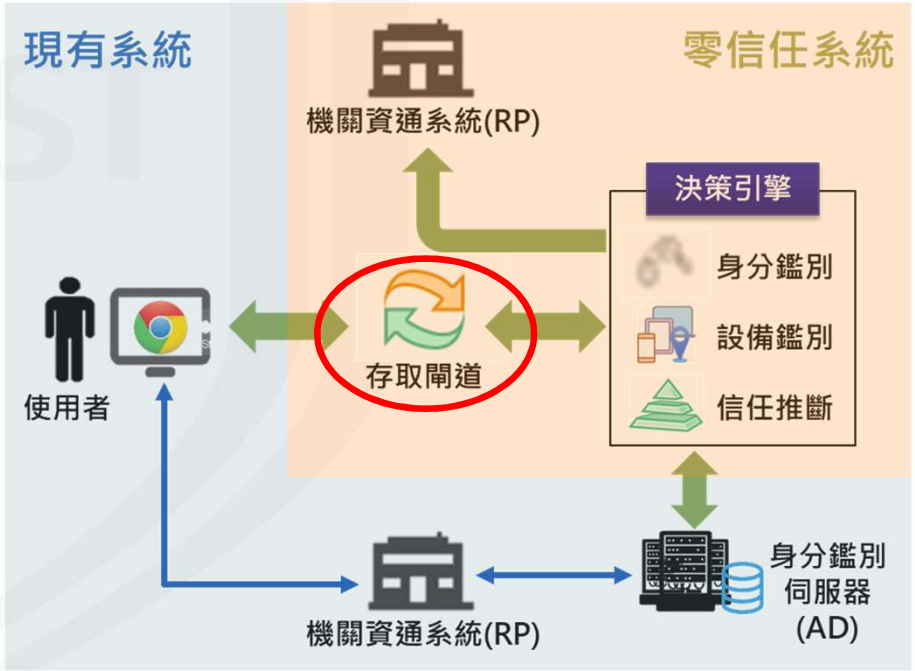
報告完畢
敬請指教

附件

政府零信任網路需求
補充說明

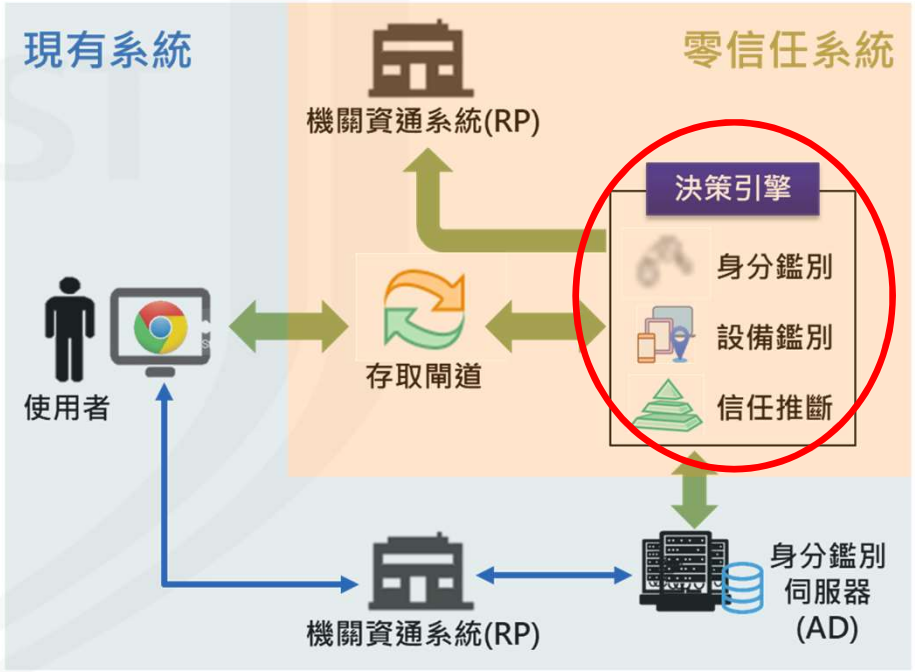
存取閘道

- 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



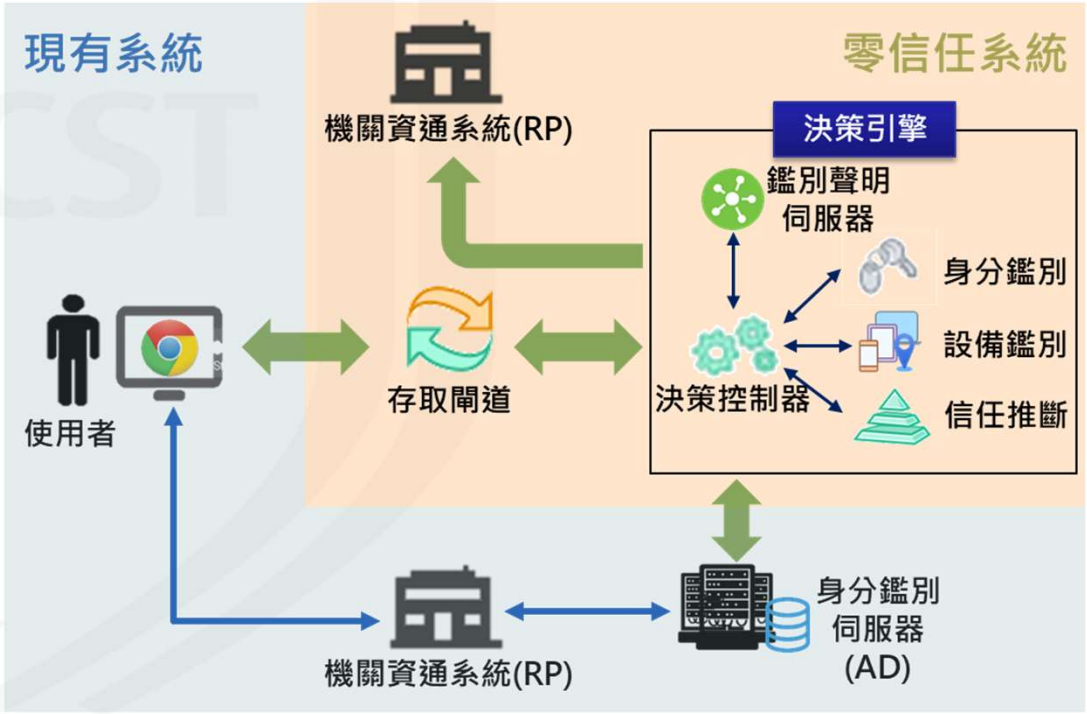
決策引擎

- 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

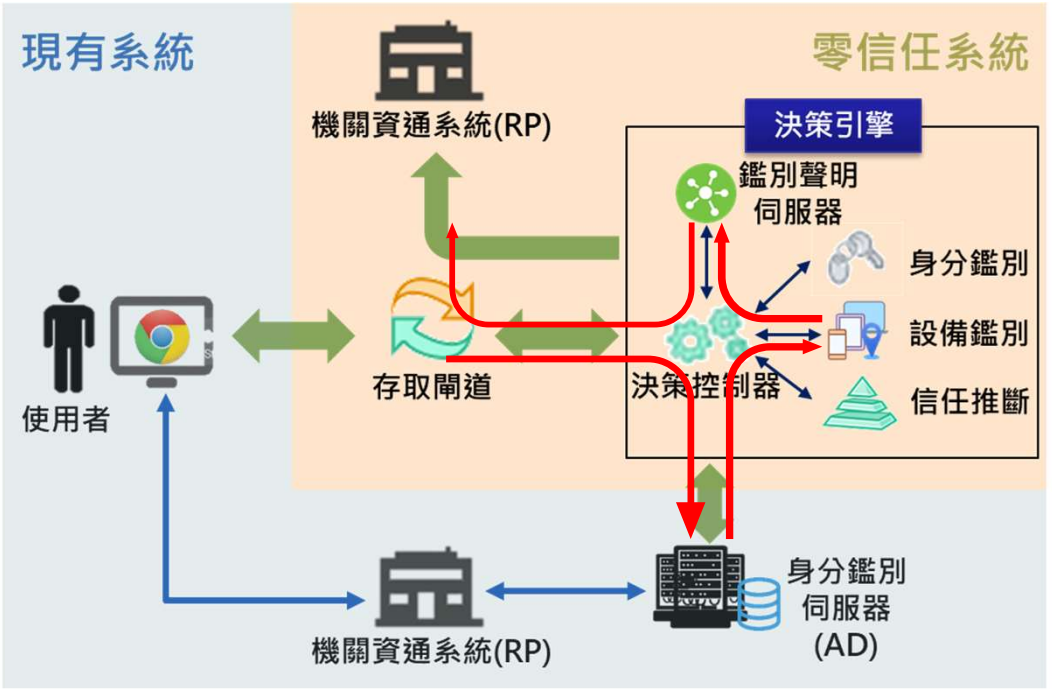


決策控制器

- 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

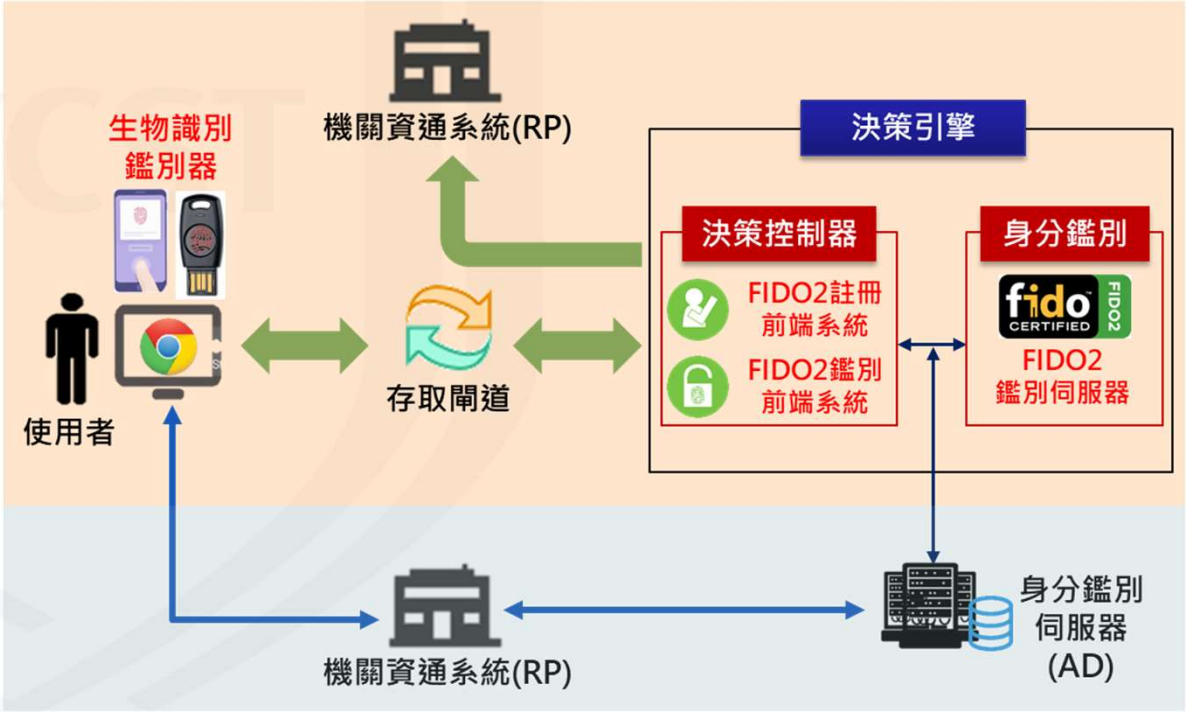
RP1	使用者群組	設備群組	FIDO2身分鑑別
RP2	使用者群組	設備群組	FIDO2身分鑑別 & TPM設備鑑別
RP3	使用者群組	設備群組	>=信任分數0.8

- 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



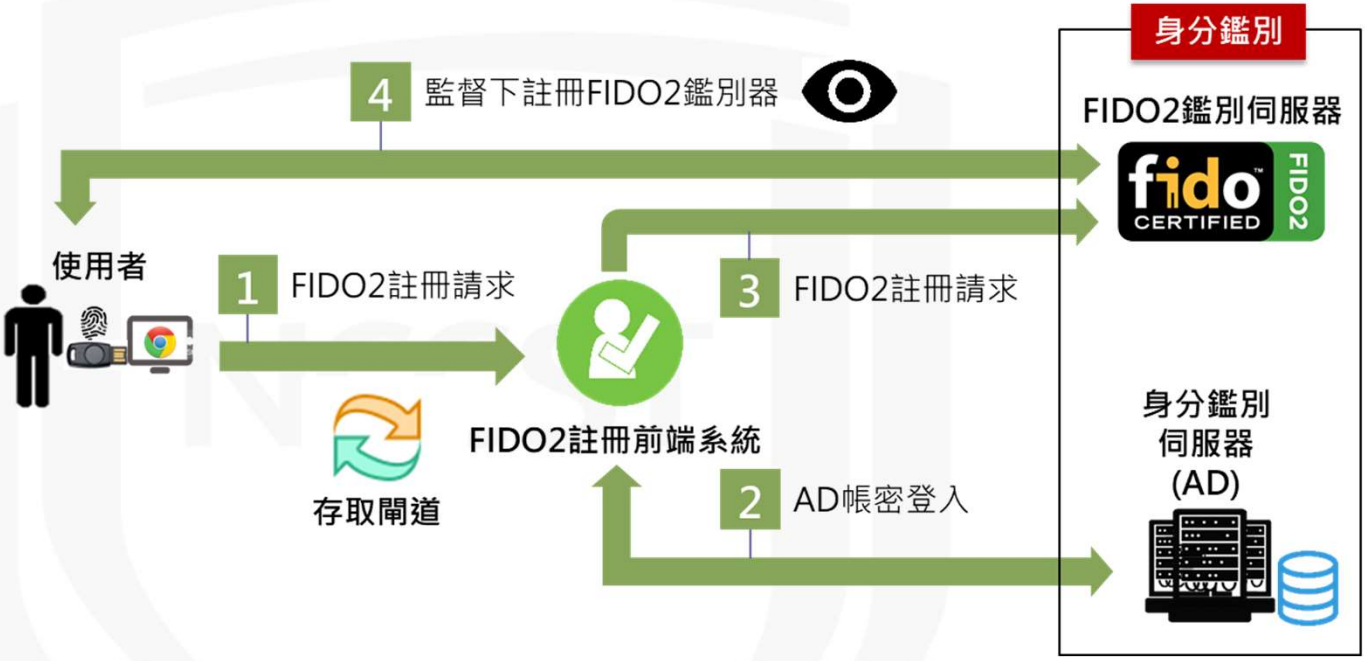
身分鑑別

- 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

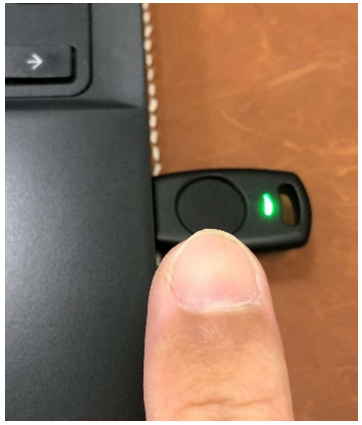


身分鑑別流程-註冊階段(IAL3)

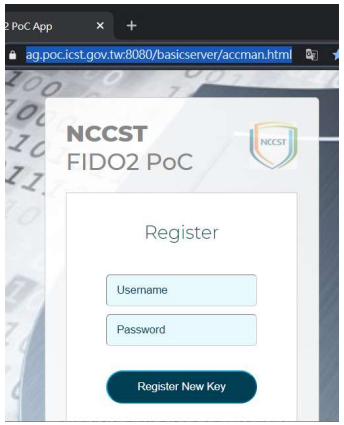
- 使用者先具備現有AD帳號，再以該帳號註冊(綁定)FIDO2鑑別器



IAL3註冊流程



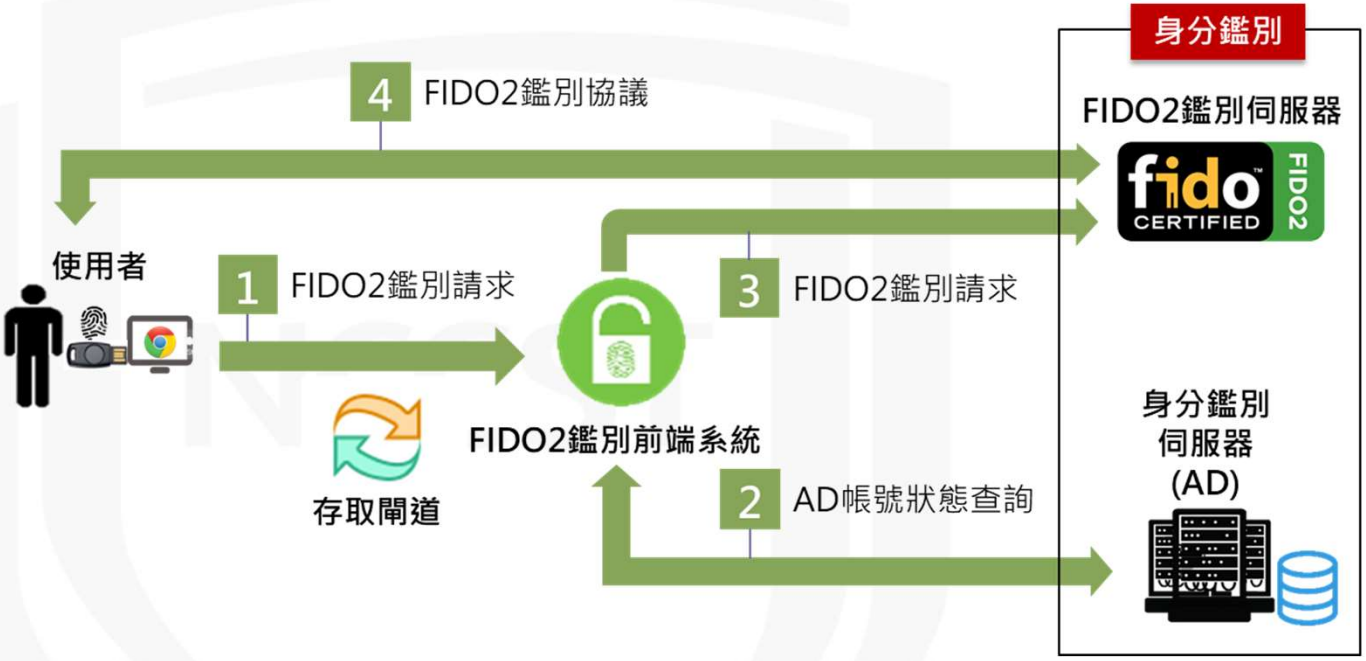
註冊FIDO2鑑別器



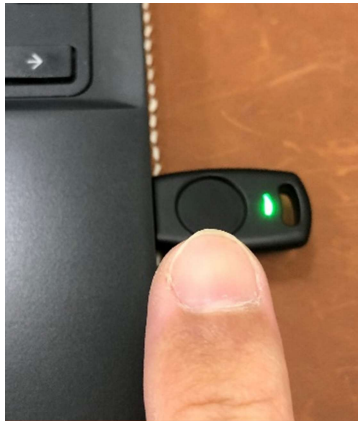
以現有AD帳密登入

身分鑑別流程-鑑別階段(AAL3)

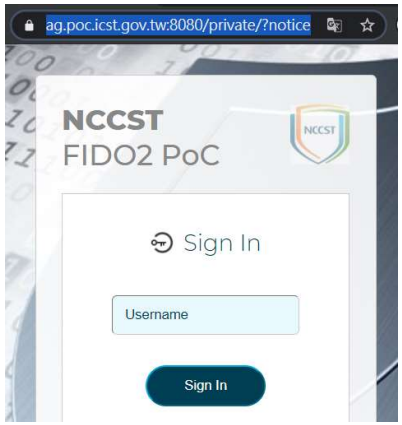
- 以FIDO2帳號與鑑別器進行身分鑑別，惟鑑別前先檢查AD帳號是否已停用或鎖住



AAL3鑑別流程



按壓FIDO2鑑別器



以FIDO2帳號登入

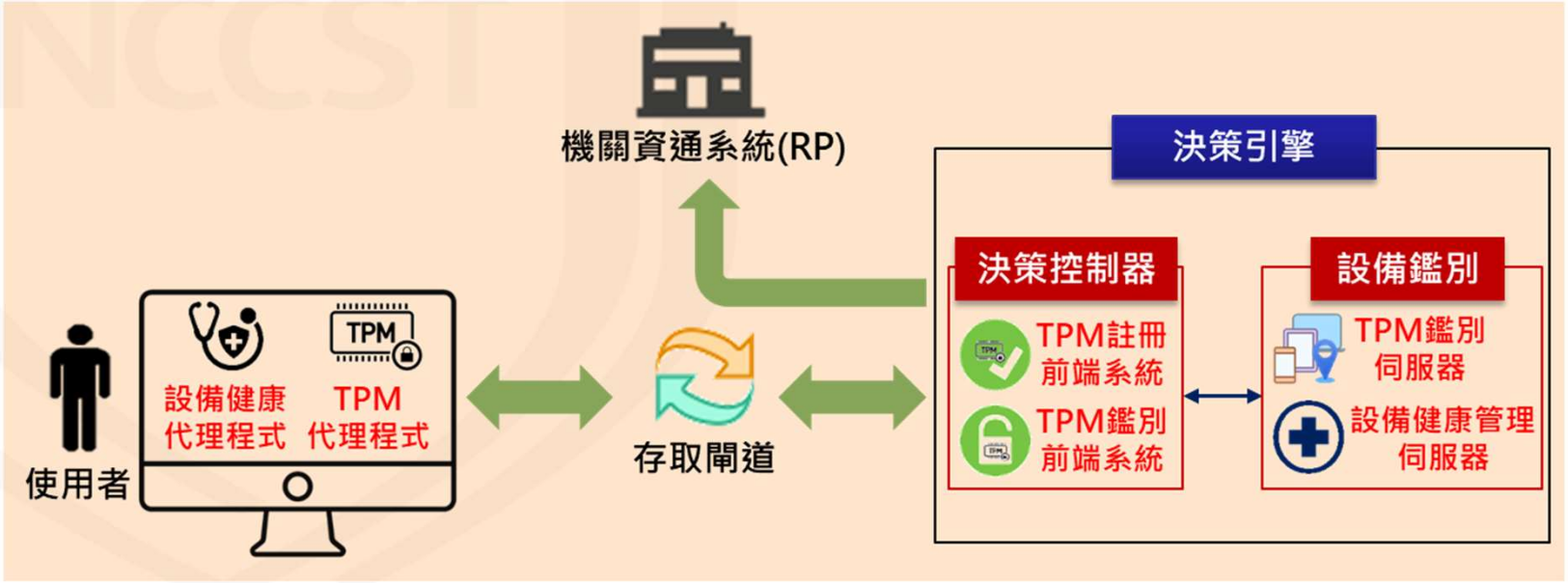
身分鑑別保證等級

- 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網路應至少達到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

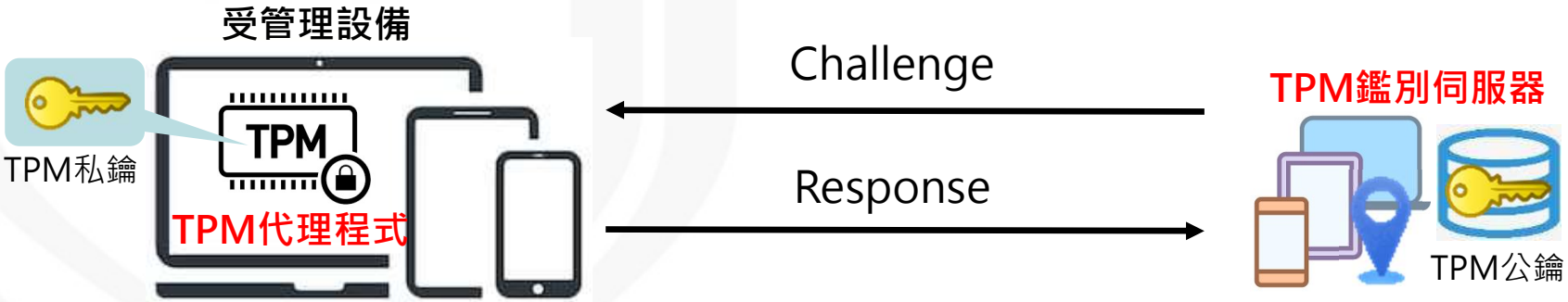
設備鑑別

- 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



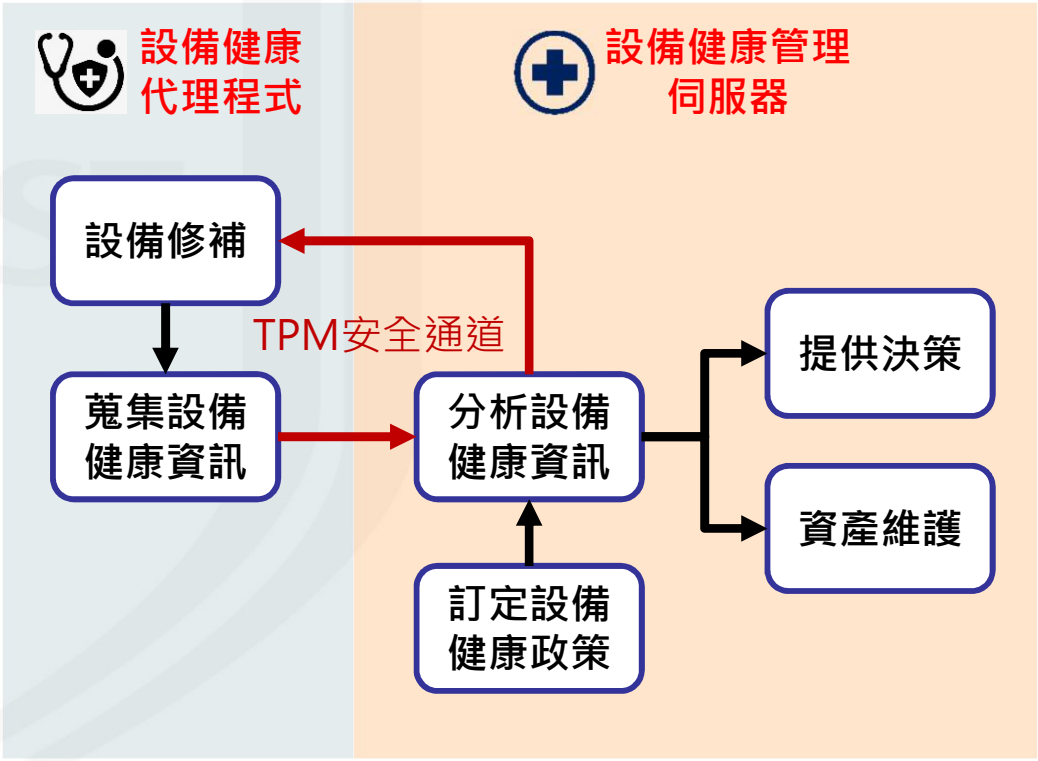
設備TPM鑑別

- 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



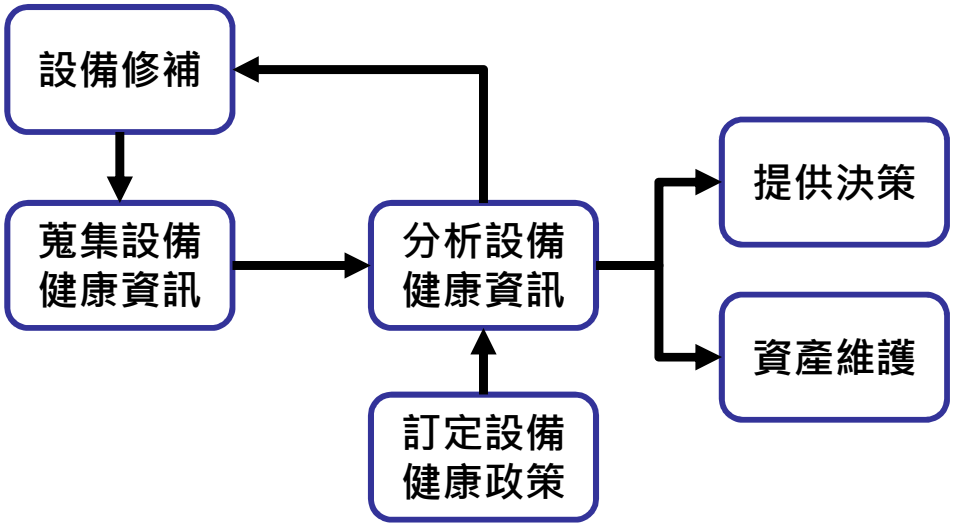
設備健康管理

- 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



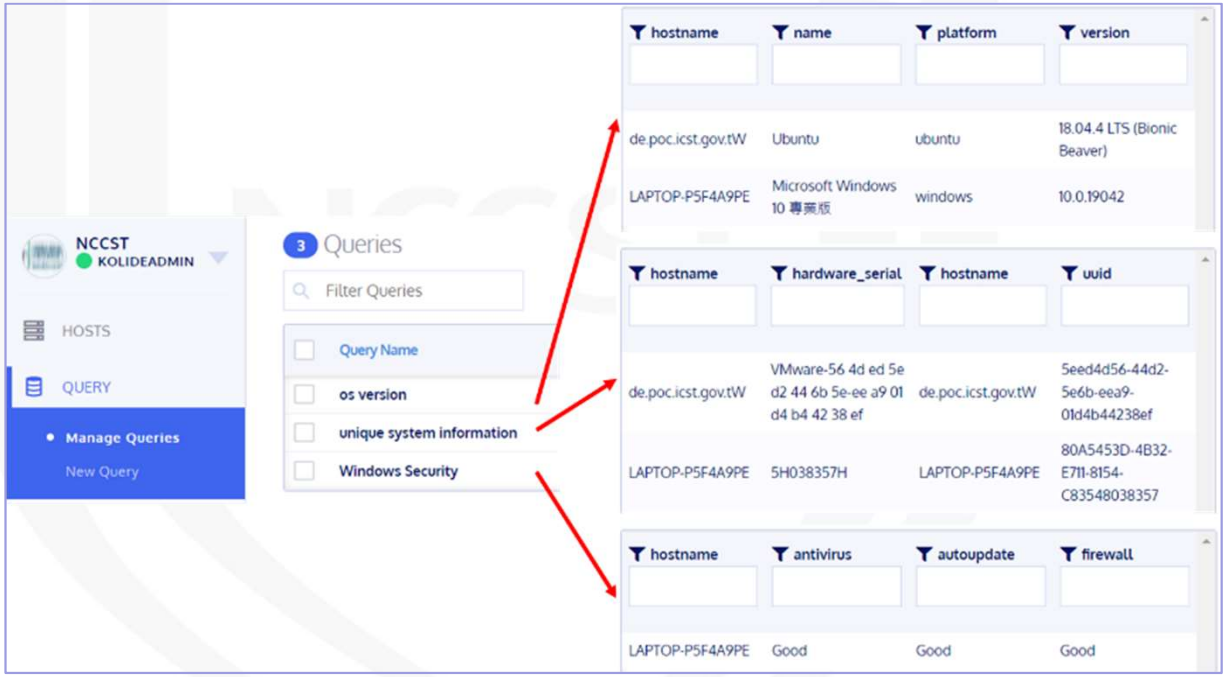
設備健康管理流程

- 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

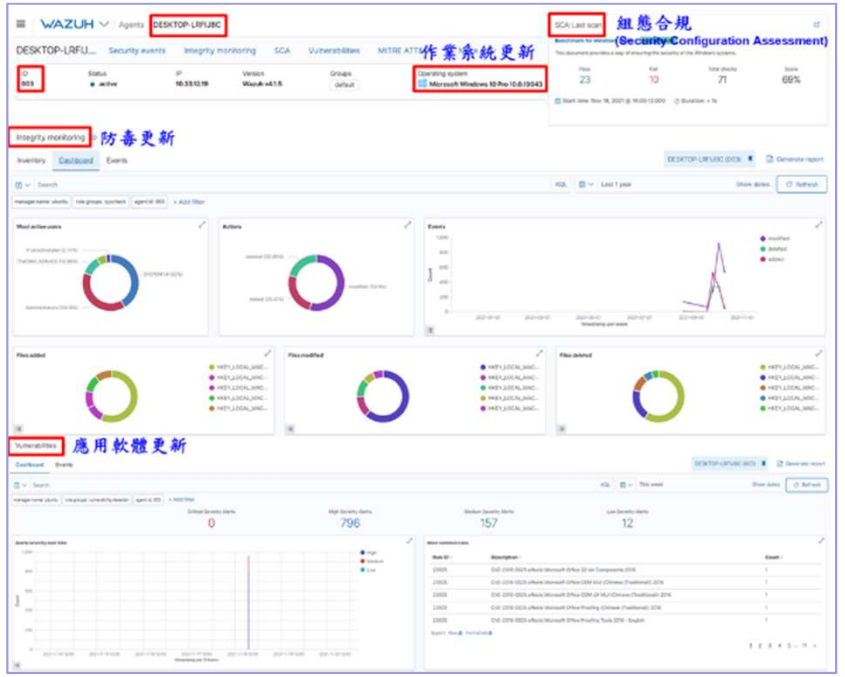


設備健康管理示例(1/2)

- 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)

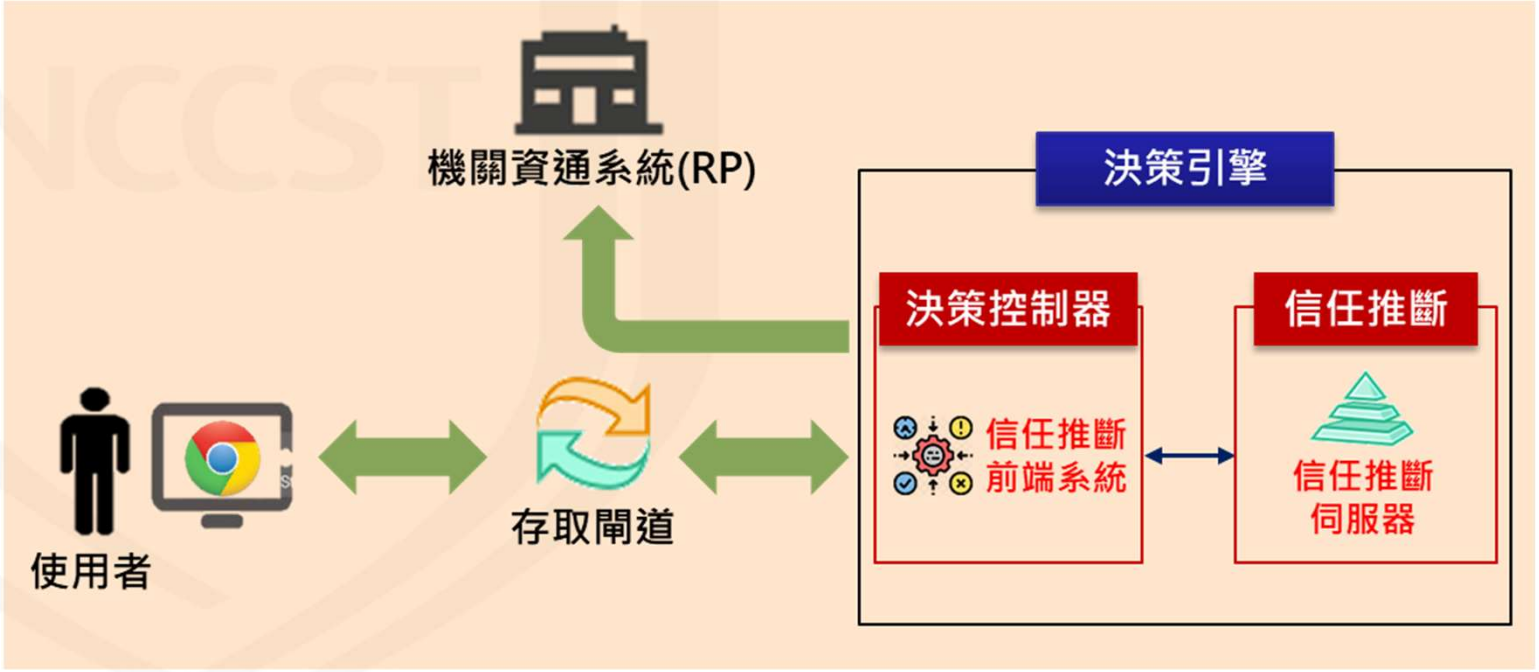
- 設備健康管理伺服器須依設備健康狀態，隨時分析設備健康信任等級，以提供信任推斷
  - 設備健康信任模型示例(加權總和模型)
    - 設定設備健康狀態採計項目
    - 設定權重
    - 加權信任等級

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

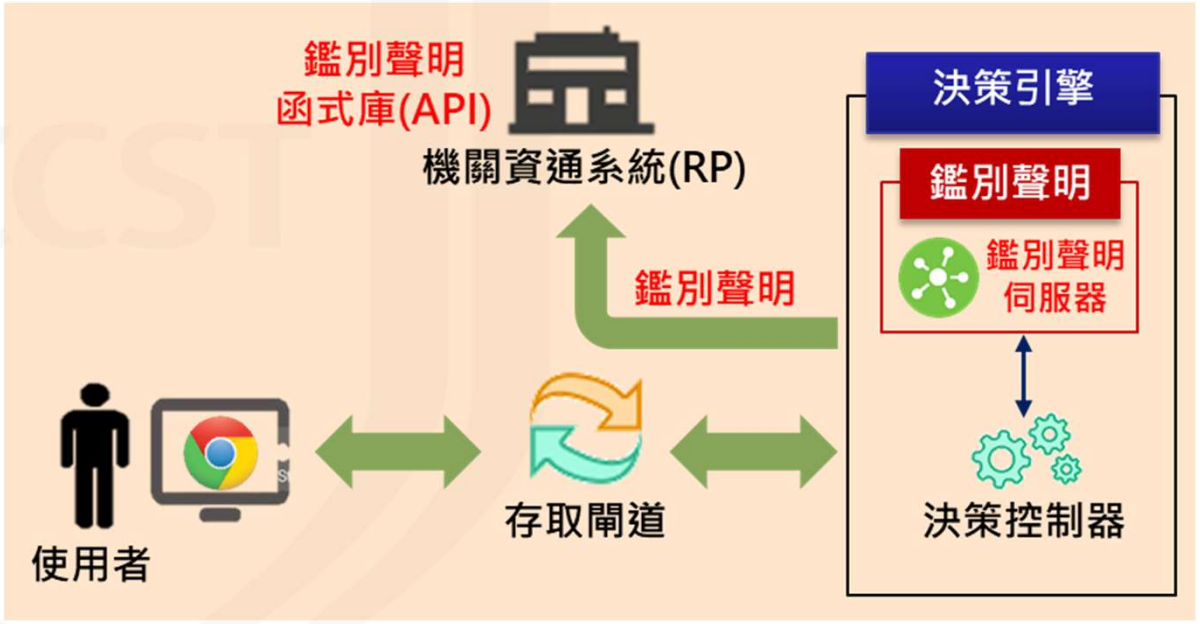
信任推斷

- 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



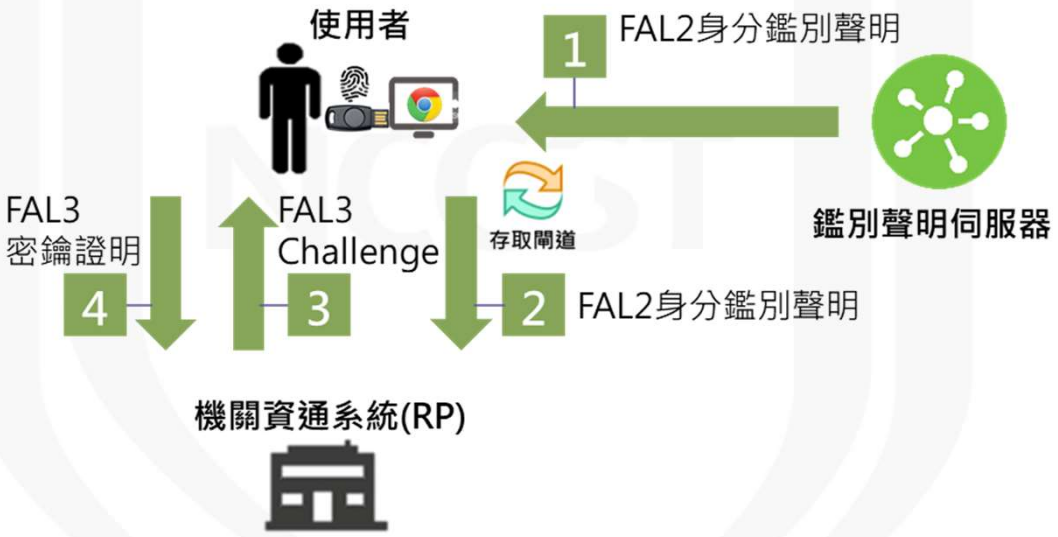
鑑別聲明

- 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



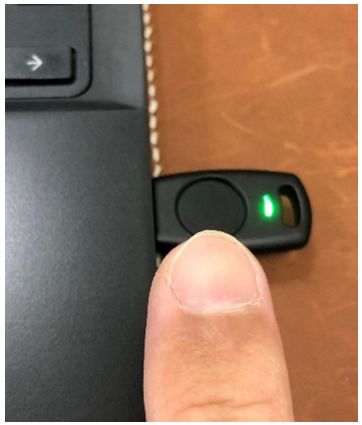
鑑別聲明流程(FAL2/FAL3)

- 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