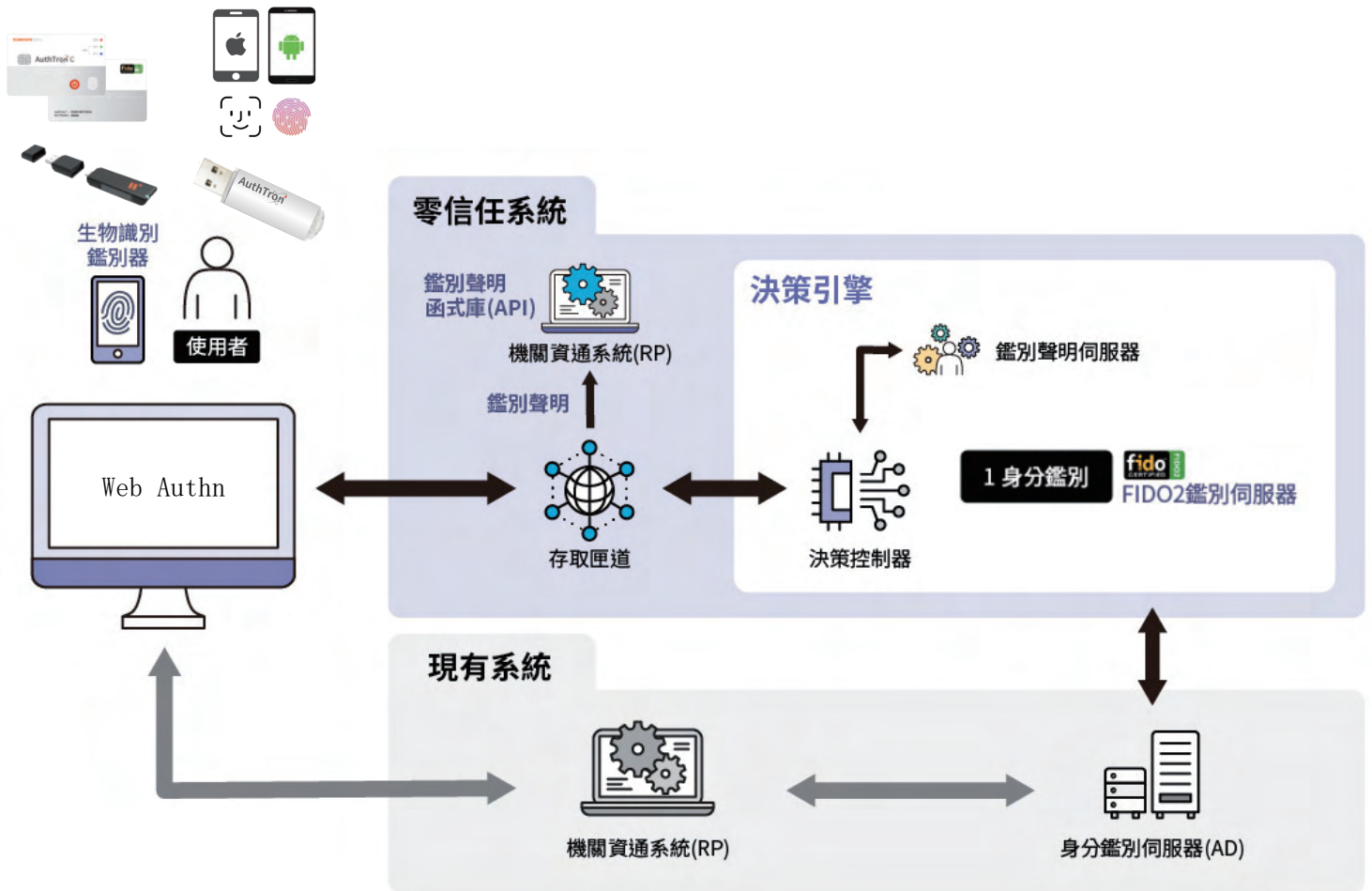


ZTA零信任身份識別-Core (含決策控制器、鑑別聲明伺服器)



身份鑑別 (Core) 功能:

- 零信任架構之核心組件: 決策控制器、FIDO2身分鑑別伺服器、存取閘道、管理後台
- 實體安全金鑰: AuthTron USB 安全金鑰 (通過FIDO2 L2認證)、支援使用 Passkeys
- 零信任架構部署方式符合 NIST 資源門戶部署方式
- 決策引擎各組件之間之網路通訊使用 TLS 加密安全通道
- 滿足 IAL2/AAL3 等級需求之匯智安全 FIDO2 身分鑑別伺服器 (通過FIDO認證)
- 提供 FIDO2 身分鑑別伺服器與 Microsoft AD 身分資料同步機制
- 提供身分註冊與身分鑑別前端介面與後台圖形化管理功能, 包含身分註冊、刪除及鑑別等功能
- 提供日誌紀錄與相關查詢功能
- 使用者端實體安全金鑰, 通過國際標準驗證之 FIDO2 鑑別器
- 身分鑑別機制使用實體安全金鑰 (FIDO 雙因子身分鑑別協定)或手機鑑別器
- 決策引擎依據匯智安全零信任網路解決方案FIDO2身分鑑別伺服器鑑別結果決定接收或拒絕存取請求
- 身分鑑別聲明伺服器滿足FAL2等級
- 鑑別聲明以單會期(per-session)為原則, 並訂定效期
- 鑑別聲明使用匯智安全零信任網路解決方案決策引擎之私鑰簽章並使用公鑰加密
- 存取閘道具備反向代理功能並提供設定介面
- 瀏覽器之URL於存取全程必須僅呈現存取閘道之網域網址, 資通系統(RP)之存取皆經由存取閘道轉址
- 存取閘道依決策引擎鑑別結果執行接受或拒絕連線請求
- 存取閘道具備日誌紀錄與相關查詢功能
- 存取閘道安全通訊使用 TLS 加密安全通道
- 資通系統存取控制之驗證功能, 提供 JAVA 與 .NET 2 種版本之 JWT 鑑別聲明函式庫
- 資通系統透過匯智安全零信任網路解決方案 JWT 鑑別聲明函式庫解密身分鑑別聲明
- 資通系統透過匯智安全零信任網路解決方案 JWT 鑑別聲明函式庫驗證身分鑑別聲明之簽章
- 資通系統解析身分鑑別聲明之格式, 並驗證身分鑑別聲明所記載屬性之有效性