歐盟電子身分識別 eIDAS 介紹

本季技術新知特別介紹由歐盟成員國愛沙尼亞主導的歐盟電子身分識別 eIDAS(electronic IDentification, Authentication and trust Services)的具體作法，以及與我國的數位身分證的比較。

一、 eIDAS 運作方式

eIDAS 方案(eIDAS solution) 係為歐盟成員國公民使用其他成員國之線上服務時，藉由電子身分識別機制與他國之身分提供者（Identity Provider）介接方式，以證明其身分。其過程如下：

1. 成員國的公民使用他國線上服務。
2. 線上服務平台傳送公民資料以進行身分驗證。
3. 在身分驗證階段判斷該公民來自哪個成員國，如為本國公民逕行身分驗證，否則發送會員國(sending Member State)將透過 eIDAS 節點(即 connector)將資料轉換為 eIDAS 協定(protocal)，並透過路由(routing)將公民相關資訊發送至該公民所在國家/地區之接收會員國(receiving Member State)之 eIDAS 節點，再傳送予該國身分識別提供者，進行身分驗證。
4. 認證結果回應予線上服務提供者。
5. 身分驗證通過後，公民即可使用線上服務。

二、 eIDAS 體系架構

eIDAS 由使用者、服務提供者、身分驗證提供者、eIDAS 節點所組成。

（一） eIDAS 節點

1. 傳送會員國(Sending Member State)之 eIDAS 連接器(connector)；當線上服務提供者接收到其他會員國的使用者服務請求時，會將公民身分資訊透過服務提供國之連接器將資料轉換為 eIDAS 協定，經由 eIDAS 路由將身分認證資料跨境傳送至接收會員國之 eIDAS 連接器，並將回傳之驗證資料回傳回服務提供者。

2. 接收會員國(Reciving Member State)之 eIDAS 連接器(connector)；該國之連接器將 eIDAS 協定資料轉換為該國身分認證格式傳送至身分驗證提供服務者，並將驗證結果及授權轉換為 eIDAS 協定資料，並透過路由回傳傳送會員國之連接器。

(二) eIDAS 介面

1. Proxy-Service：本國成員對於本國線上服務有使用者需求，由本國身分認證提供者進行身分驗證。

2. Middleware-Service：本國成員對於他國線上服務有使用需求，經由發送會員國之連接器將資料進行相關轉換及路由，送交接收會員國連接器，並由他國身分認證提供者進行身分驗證。

(三) eIDAS 協議

eIDAS 協議將不同國家身分識別相關資料轉換為會員國

認可之共同格式，使不同國家之 eIDAS 節點間進行身分驗證及權限賦予等作業得保留各國國內之身分驗證標準，不需要因為導入相關機制，而更改其國家基礎建設，能有效地擴大公民跨界使用服務之可能性和機會。

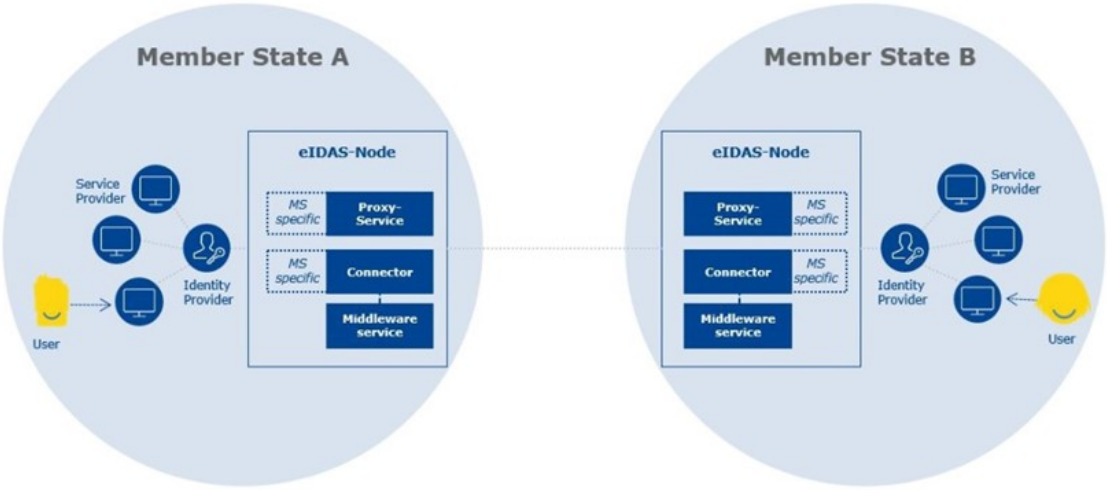

圖1　eIDAS 體系架構

三、 成功案例-比利時 itsme®數位身分應用程式

2019 年 12 月 18 日，比利時政府在《歐盟官方期刊》上發布行動 eID 方案計畫，其包括比利時政府的聯邦身分驗證服務（FAS）和 itsme®數位身分應用程式，提供 eIDAS 條例中所定義的「高度可信」(high level of identity assurance)。

為了使用多種線上服務，不同系統除非有單一登入外，其餘系統均需保留多組帳號及密碼，而 itsme®數位身分應用程式能解決此麻煩。itsme®為比利時居民提供由政府支持的單一數位身分，以利在眾多不同的跨境線上服務上登錄並執行各種交易。由國內主要的銀行和行動網絡運營商(mobile network operators)共同開發，並已得到比利時聯邦政府的正式承認，有效控制政府成本。

itsme®已迅速被比利時公民、當地公司以及公共部門組織採用。在其推出的兩年半後，該應用程序現已被比利時 30%的人口所使用，每月可促進超過 500 萬筆交易。借助 itsme®，用戶在註冊使用新的健 康保險門戶網站時可以輕鬆登錄以提交納稅申報表，簽署金融交易並驗證其身分。

任何擁有比利時的 eCard ID，SIM 卡和手機的人都可以使用 itsme®創建數位身分。itsme®主要四個大功能：

1. 註冊–提交驗證的身分資料以註冊新服務或開設帳戶。
2. 登錄–身分驗證，及授權在線服務或 IoT 裝置。
3. 確認程序–同意線上交易，例如付款和訂單。
4. 合格的電子簽名–取代紙質手寫簽名。

因此 itsme®具備七大優勢：

1. 單一的登錄應用程序
2. 簡易的操作過程
3. 不需要使用讀卡器
4. 強大而安全的身分驗證
5. 驗證的身分無需提交所有個人資料
6. 首批在智慧設備上驗證電子封裝(e-seals)和電子簽名(e-signatures)的合格信任服務提供者之一
7. 作為信任服務提供商，所有個人資料受歐盟一般資料保護規範（GDPR）的保護

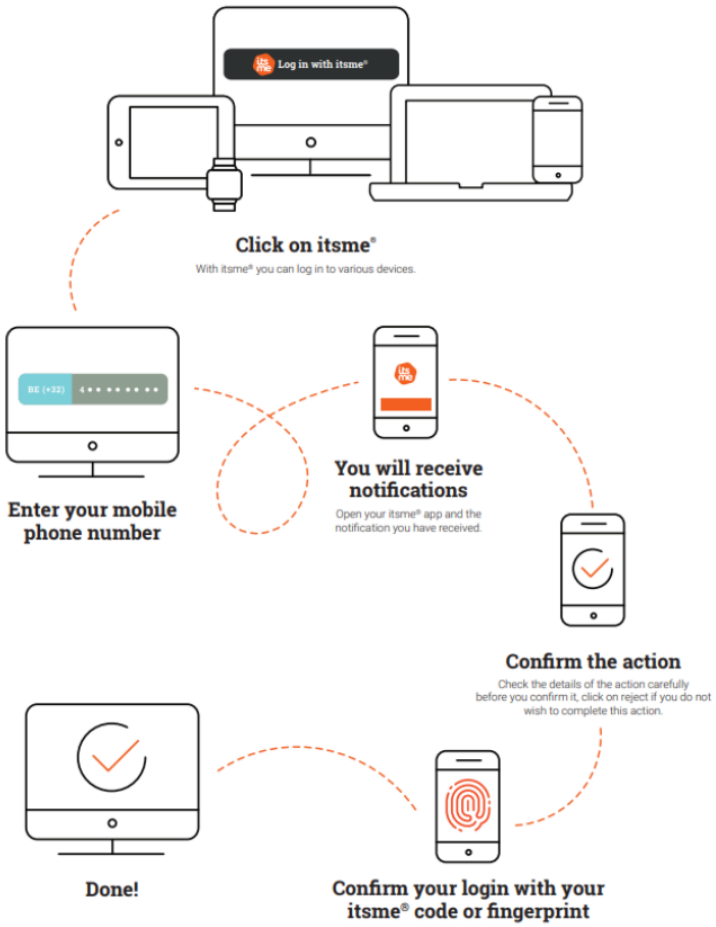

圖2　itsme®數位身分應用程式

四、 比較差異

比較本國即將推行之數位身分之差異，詳如表 1、圖 4。

表1　比較差異

國家 / 項目	台灣	比利時
服務名稱	New eID 數位身分證	itsme®數位身分應用程式
章規依據	1.ISO 29115 2.資通安全管理法 3.個人資料保護法 4.電子簽章法(自然人憑證)	1.歐盟電子身分識別及信任服務條例(eIDAS) 2.歐盟一般資料保護規範（GDPR）
驗證等級	LoA 4（Level of Assurance)	高度可信(high level of identity assurance)

型式	晶片卡	APP
參與開發者	政府	國內主要的銀行及行動網絡運營商
採用技術	1.配合最新製卡防偽技術。 2.藉由數位身分識別證串連政府所有服務及建立具安全且可信賴的 T-Road 為基礎架構。	CEF eID Building Block
跨境使用	無	有，歐盟成員國互通
跨業應用	公部門：報稅、公投聯署、申請電子病例、查詢退休金、申請津貼與補助等都可以在線上辦理。	1.公部門線上電子服務。 2.私營部門服務：保險、零售、金融、醫療照護網絡。

自行整理，參考資料來源：https://www.ris.gov.tw/documents/data/5/6/6d2ae69c-5a13-4533-81ab-42c5d9928ac8.pdf

圖3　可信安全等級

五、 面臨問題與挑戰

2019 年安全廠商 SEC Consult 的研究人員指出 eIDAS 節點軟體存在安全性漏洞。

eIDAS 節點使用安全性聲明標記語言（Security Assertion Markup Language, SAML）交換信息，惡意攻擊者透過「不會針對身分驗證提供者的公共密鑰來驗證實體簽名」的特性，迴避簽章驗證，在初始身分驗證過程中提供偽造的安全性聲明標記語言 SAML，並發送到 eIDAS 連接器進行身分驗證，一旦該身分驗證分被儲存在當地的信任資料庫(the local trust store)，就會被接受，最終達到冒充身分的目的。

歐盟 eID 負責團隊針對此問題進行修正，並釋出最新版本 2.3.1。

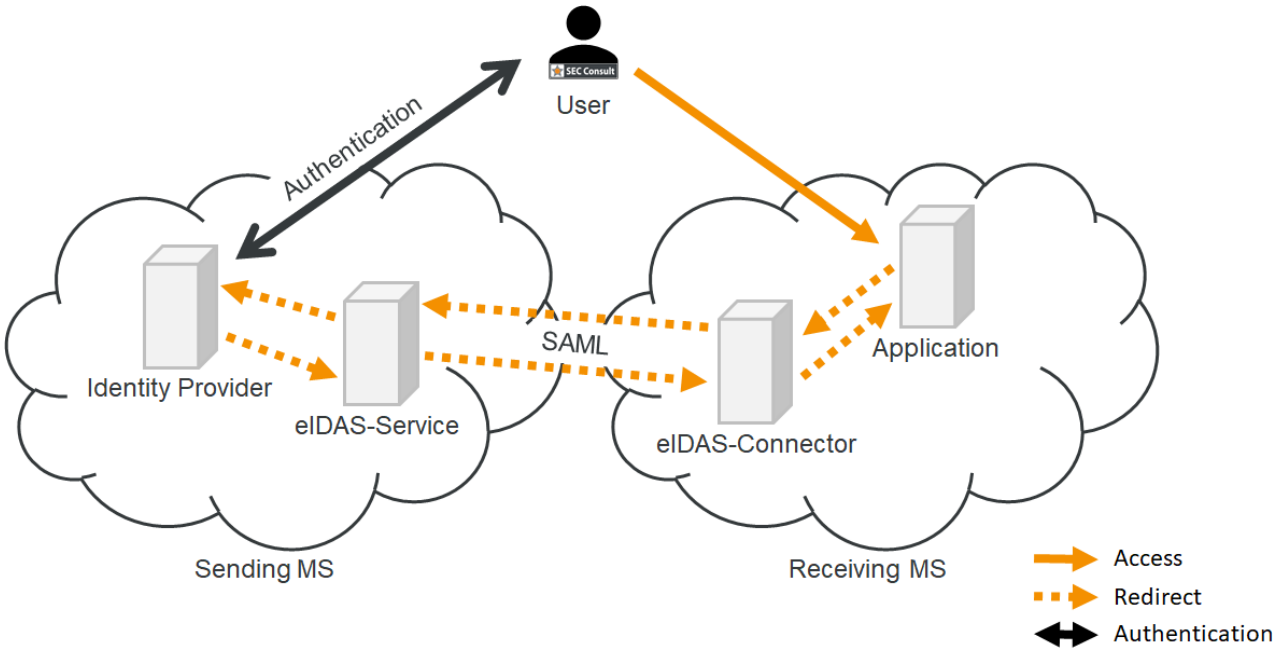

圖4 eIDAS 節點使用安全性聲明標記語言交換信息

六、 結論

eIDAS 是歐盟主導下所建構一套模板，成員國可利用其發展成自身的數位網絡，並且在歐盟龐大組織優勢下，比現今其他國家更容易實現數位

化單一市場(Digital Single Market)的理想。數位身分證可以有效改善政府與私營部門的業務流程，彼此間互利，帶動商機，itsme®便是最好的楷模。

全球電子化，數位身分證是不可逆的趨勢，許多國家已經迎向數位政府，無論何種型態、技術，現今最重要的課題是如何嚴加管控資安風險。

七、 參考資料來源

1. https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030
2. https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=227083826
3. https://epaper.ttc.org.tw/mAchievement.aspx?aQBkAA2=NAA5AA2&bgBvAA2=NgAyAA2
4. https://www.bleepingcomputer.com/news/security/europes-electronic-id-system-fixed-against-impersonation-risk/
5. https://www.zdnet.com/article/major-vulnerability-patched-in-the-eus-eidas-authentication-system/