

從eID看國家數位轉型 與智慧政府的推動



郭耀煌

國立成功大學資訊工程系 特聘教授
數位生活科技研發中心 主任

109年7月30日





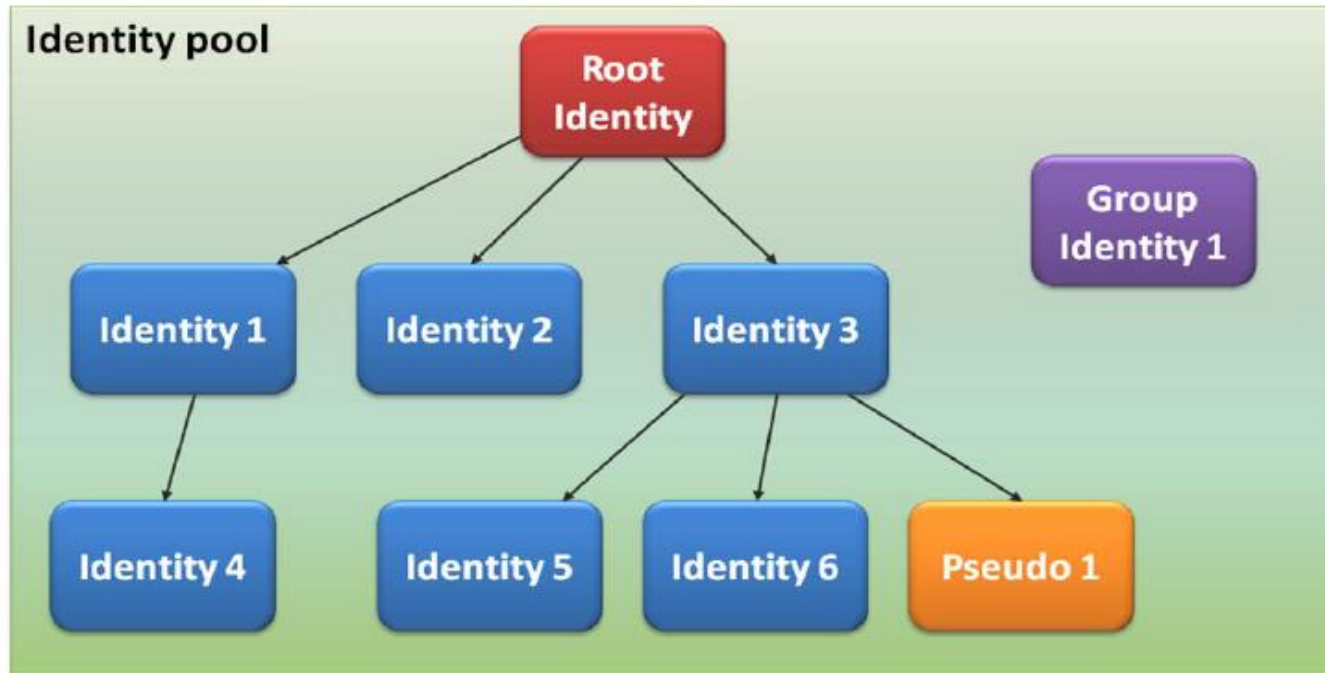
大綱

- 對eID的提問
- eID與政府數位轉型
- 可課責的智慧政府
- 結語

對eID的提問

- 萬物聯網下的智慧政府需要什麼身分管理策略？
- 使用eID（自然人憑證）接取服務之適用範圍？如何規範？
- eID對推動智慧政府的關鍵性為何？配套措施？
- 政府對eID應用的風險管控與課責機制？
- eID依據個資法、資通安全管理法、電子簽章法，但它們可以處理eID各種應用可能發生的狀況嗎？
- 相關修法及設立專責機關的明確進程？
 - 尚未修正”國民身分證及戶口名簿製發相片影像檔建置管理辦法”？

萬物聯網時代的Identity Management



- A user can use different identities or pseudonyms for accessing different services
- All subject identities should provide accountability.

GDPR與我國個資法比較 (1/2)

- 歐盟GDPR個資定義**範圍較廣**，納入**數位活動資料(如cookie)**
- 歐盟GDPR是目前國內外**最嚴格**且**罰則最重**的個資保護法
- 我國跨國傳輸採**負面表列**，不同於歐盟**正面表列**，須事前申請獲准。
且對於**轉送傳輸**規定較為寬鬆，無有效保護機制，風險較大

	GDPR	台灣個資法
個資定義	• 任何可識別自然人的資料 • 包括數位活動的資料如:網路IP位址 • 包括：民族或種族、政治見解、宗教、世界觀、所屬公會...	• 基本個資定義相仿 • 可直接或間接識別個人之資料(但未包括數位活動資料)
適用範圍	• 蒐集、處理歐盟民眾個資 • 控制者或處理個資者就算未在歐盟境內設點，但提供服務或貨物之公司亦適用	• 蒐集中華民國國民個資 • 在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用
個資去連結與去識別化	確保個資去識別化及去連結	個資以代碼匿名、隱藏部份資料

GDPR與我國個資法比較 (2/2)

	GDPR	台灣個資法
機器學習或大數據自動化分析處理個資限制	- 須明確通知當事人 - 當事人得行使拒絕權，不被分析，可要求刪除分析衍生的隱私資料 - 須有人為干預機制(中止)	無規範
個資違反通報	- 通報主管機關，必要時通報當事人 - 不得有不當遲延 - 最晚72小時	- 但規定適當方式通知當事人 - 只有主管機關或法規要求說明時，才須向主管機關通報
國際傳輸的限制	原則不允許，只有經執委會認定可提供個資適當保護的國家或企業才可以進行國際傳輸(台灣不在允許轉送傳輸名單內)	原則允許，只有涉及國家重大利益、國際條約禁止或其他限制者才不行
罰則	最高處 2000萬歐元 或全球營業額4%	5年 以下有期徒刑，或 100萬元罰金

eID與政府數位轉型 (1)

● 政府數位轉型的目的

(參考美國數位政策辦公室 (Office of Digital Strategy) 任務)

- 運用數位工具拉近政府與人民的關係
- 運用數位工具優化人民的生活方式
- 運用數位工具增進公民權，落實民主的意涵

● eID是打開智慧政府的關鍵鑰匙 (內政部張司長所言)

→ eID驅動的智慧政府藍圖和進程？

eID與政府數位轉型 (2)

● 政府數位轉型的核心價值

- 民眾為本：eID是否兼顧了不同價值觀、不同使用習慣的國民之需求？
- 政府效能：eID如何在國民信賴下，提供安全便捷的服務？
- 民主深化：eID可能的貢獻是什麼？
- 生態鏈結：eID如何以安全可靠的方式變成串連跨界服務的關鍵鑰匙？
- 國富民強：eID相關應用如何開創社會或經濟效益？

可課責的智慧政府 (1)

- eID是打開智慧政府的關鍵鑰匙，面對可能衍生的風險及損害，政府應有課責的法規依據及執法機制
 - 風險評估是否侷限於eID端，或者該整體看待智慧政府
- 可課責性之前要先建立可信賴度及透明度
- 可信賴智慧政府之基礎
 - 智慧政府服務的品質保證
 - national cybersecurity防護力
 - data governance落實度
 - privacy preserving妥善性

可課責的智慧政府 (2) – 高效能數位治理組織

資料治理與 網際防護體系

協助關鍵資通基礎設施（通訊傳播、交通事業、金融服務、科技園區、衛生醫療、能源及水資源等）、政府數位服務、數位內容流通與加值之主管部會落實資安防護

行政院國家資通安全會報

數位發展部會

數位治理與 資訊安全局

行政法人

產業與社群 發展體系

搭配經濟部強化資安產業實力，並結合大學、研究法人及民間專業社群構成具活力的資安生態體系

犯罪偵察與 防治體系

搭配內政部、法務部及通傳會，執行犯罪偵防

人才與科技 發展體系

搭配科技部、教育部及經濟部，建立資安科技研發網絡，並擴大大學之資安人才培育規模，也協助在職人士學習資安技能

搭配外交部、科技部及經濟部等部會，加強國際官方或半官方合作，也透過民間法人機構或社群，擴大非官方合作關係。

國際關係
發展體系
Center for Research of E-life Digital Technology
數位生活科技研究中心

可課責的智慧政府 (3)

● 完備可行的法制及配套措施

- 韓國2020年修訂了《數據三法》，即《個人資訊保護法》、《信用資訊法》、《資訊通信網法》
- 台灣離GDPR有多遠？

● 可信賴且獲落實的作業準則

- 隱私性、透明性、公平性、穩建性與可課責性

● 透明而積極的社會溝通

可課責的智慧政府 (4)

● 持續的服務創新

- 流程改善
- 體驗創新
- 資料加值
- 品質保證：availability, reliability, security
- universal access

結 語

- 快捷便利與安全可靠之間涉及不同的衡量與選擇，
eID是否可以有更多元的選擇或有較長的適應期？
- 可信賴度與可課責性是推動(eID)智慧政府之關鍵，
此牽涉法規配套及政府服務品質，也牽涉國民長期的
體驗及觀感，政府宜有更具說服力的社會溝通。
- 兼顧cybersecurity, data safety及privacy
preserving之數位治理體制是推動智慧政府的基礎