

2020-09-14

資安問題也該超前部署吧

邱文聰／中央研究院法律學研究所研究員兼資訊法中心主任

政府部門因資訊系統外包造成資安危機，早非新聞。近日又爆發陸軍專科學校人臉辨識門禁系統廠商違規使用中國製電腦，險造成軍網被入侵事件。但外包廠違規使用明顯印著「中國製」資訊設備雖屢成問題，卻只是台灣面臨資安威脅的冰山一角。政府部門回應外界對晶片身分證之資安疑慮展現出處理資安問題的駝鳥心態，恐怕才是當前資安問題永劫回歸的最大癥結。

內政部在反對聲中執意換發晶片身分證，並號稱委由百分百國營的中央印製廠辦理卡片製作。但政府早知國內並無 PC 晶片卡與印製設備的生產製造能力，透過中央印製廠只是轉個彎，最後回到對外招標。得標的東元電機則將主要工作轉包給 IDEMIA 在境外生產 3000 萬張具防偽功能之空白晶片卡，並由另一家境外公司 Entrust Datacard 提供機器設備給中央印製廠，以便在中央印製廠內將持卡人的個資寫入空白晶片卡，並產出該張晶片卡專屬的對稱金鑰。

憂晶片身分證隱藏後門

IDEMIA 與 Datacard 被外界質疑因在中國設立亞洲唯一據點，又在中國承包多個業務而與其關係匪淺，有高度資安疑慮，例如 IDEMIA 與解放軍所屬企業合組生物辨識公司，Datacard 替港府發行新晶片身分證及港人回鄉證，卻遭爆在光復香港運動期間疑似洩漏特定人員個資的爭議。

東元、IDEMIA 與 Datacard 近日均大動作回應，聲稱轉包符合《政府採購法》、空白晶片卡製程不需接觸國人身分個資、兩家境外公司提供給台灣的合約標的將不會在中國製造，一切符合台灣法律與合約要求，並無資安疑慮。內政部與中央印製廠也出來護航，宣稱 IDEMIA 生產空白晶片卡所使用的晶圓為台積電提供，且合約已規定所有材料及設備不可來自中國，晶片身分證的安全標準堪稱已達軍事機密等級。

有趣的是，IDEMIA 與 Datacard 才分別因為替孟加拉生產晶片身分證過程涉及標案違法，曾被世界銀行在 2017 年至 2020 年間列為投標黑名單，也發生因產能不足而將原約定製造地法國改為中國深圳的狀況。IDEMIA 雖對台承諾卡片不在中國製造，但其歐洲產線長期產能不足的問題，勢將影響未來履約能力。不過，該擔憂的不僅是材料與設備製造地可能在中國的問題。長期被忽略掉的資安威脅其實來自以下諸端：

一、針對在兩岸均承包資通業務的廠商，目前並無法令或實際管控機制可禁止在兩岸提供的資通產品或服務，使用相同的系統元件，也因此無法避免一旦系統元件共用時被反向工程破解的危險。這個潛在問題不僅存在於負責提供晶片身分證硬體，卻在兩岸均有相同業務的 IDEMIA 及 Datacard，也同樣存在於負責開發晶片身分證相關應用軟體的中華電信，其子公司資拓宏宇與孫公司榮利在中國承包多家金融機構資訊系統工程。

二、在兩岸均承包資通業務的廠商，因受到中國國安法令的管轄，其人員在中國境內有被迫交出台灣資通系統參數、數位身分證專案甚或國人個資的危險。目前並無法令或實際管控機制，限制曾接觸該等機敏資料人員進出中港澳。

三、由於晶片身分證所使用的晶片模組、晶片作業系統及應用程序、印製設備均仰賴國外廠商提供，在系統設計與生產委外的情況下，即使將其中晶圓交由台積電生產，也不能擔保整體沒有隱藏後門的威脅。

竟打算靠駭客尋找漏洞

身分證的晶片化除了上述的資安問題外，還存在數位足跡該如何管控以避免監控與人格剖繪的嚴肅課題，但內政部卻打算只靠《戶籍法》中「身分證格式決定權」的一個條文，做為整個晶片化的法制基礎。針對上述根本性的資安威脅，目前政府也同樣只打算靠駭客賞金獵人，從生米煮成熟飯的晶片卡成品中尋找可能的資安漏洞。不過，把資安當國安，一切又講求超前部署的蔡政府，何以在身分證晶片化的問題上，如此地裝睡叫不醒呢？

<https://tw.appledaily.com/.../202.../LUYL6PQG2FDBVAGYO3QJ3XBZBE/>