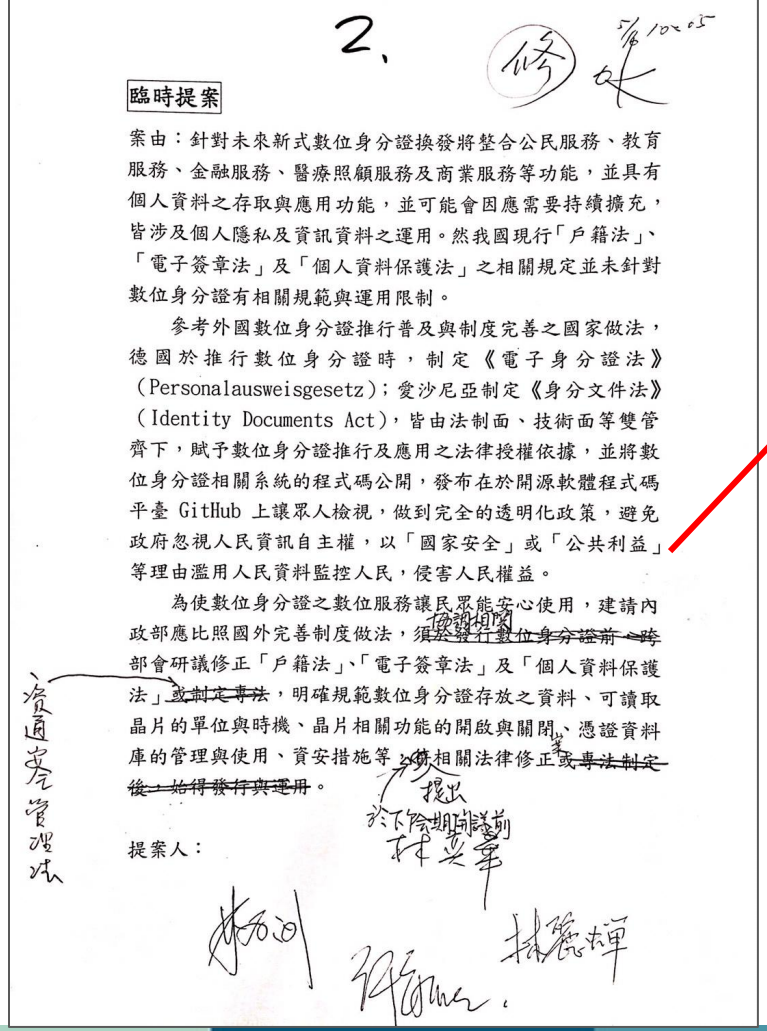
Hsu Yu Jen

內政委員會質詢

立法委員許毓仁國會辦公室

2019.09.25

Hsu Yu Jen



2.

臨時提案

案由：針對未來新式數位身分證換發將整合公民服務、教育服務、金融服務、醫療照顧服務及商業服務等功能，並具有個人資料之存取與應用功能，並可能會因應需要持續擴充，皆涉及個人隱私及資訊資料之運用。然我國現行「戶籍法」、「電子簽章法」及「個人資料保護法」之相關規定並未針對數位身分證有相關規範與運用限制。

參考外國數位身分證推行普及與制度完善之國家做法，德國於推行數位身分證時，制定《電子身分證法》（Personalausweisgesetz）；愛沙尼亞制定《身分文件法》（Identity Documents Act），皆由法制面、技術面等雙管齊下，賦予數位身分證推行及應用之法律授權依據，並將數位身分證相關系統的程式碼公開，發布在於開源軟體程式碼平臺 GitHub 上讓眾人檢視，做到完全的透明化政策，避免政府忽視人民資訊自主權，以「國家安全」或「公共利益」等理由濫用人民資料監控人民，侵害人民權益。

為使數位身分證之數位服務讓民眾能安心使用，建請內政部應比照國外完善制度做法，~~須於發行數位身分證前，跨~~部會研議修正「戶籍法」、「電子簽章法」及「個人資料保護法」~~或制定專法~~，明確規範數位身分證存放之資料、可讀取晶片的單位與時機、晶片相關功能的開啟與關閉、憑證資料庫的管理與使用、資安措施等，~~並~~相關法律修正~~或專法制定後，始得發行與運用~~。

提案人：

內政委員會臨時提案，eID專報，2019.05.16。

「....然我國現行『戶籍法』、『電子簽章法』、『個人資料保護法』之相關規定未針對數位身分證有相關規範與運用限制.....

內政部應....協調相關部會研議 ....，於**下會期開議前提出相關法律修正案。**」

- **2年前內政部戶政司本來有要修戶籍法？為什麼後來中止？**

- "因此，參考他國晶片身分證法令，**戶政司也計畫修訂《戶籍法》，以及《國民身分證及戶口名簿製發相片影像檔建置管理辦法》，並公布了增修要點，修正重點在於加強臺灣民眾對於該卡的使用自主權**，例如，晶片身分證的存取、儲存使用必須經過該持卡人的同意。而服務提供者提供之服務，不得強制讀取晶片身分證，未經過法院、當事人同意，服務提供者亦不能對外提供當事人的使用紀錄。"
(iThome 報導，文/王立恒 | 2017-09-23發表)

內政部到立法院報告eID案的執行程序

規劃案
- 4月11日戶政司委託給國巨管理顧問公司
- 為期半年

規劃案成果公開閱覽 (RFI)
- 預期9月份規劃案成果出來後，將規格公開閱覽
- 目前進度只交了2份報告(共3份報告)。

建置案 (RFP)
- 預計RFI階段過後，10月份展開RFP的相關作業

被人爆料戶政司偷偷地委託給中央印製廠，並且在規劃標結案以前，打算直接招標。

6月24日以限制性招標的方式，委託給「中央印製廠」：『數位身分識別證(New eID)印製案』

疑雲？

中央印製廠8月26日以『PC晶片卡及印製設備乙式』發布公開閱覽公告(RFI)，準備招標。

預算金額**新臺幣 33億元**。
(一) PC晶片卡3,000萬張新臺幣【29億4千3百萬】元。
(二)印製設備（含系統）乙式新臺幣【3千5百萬】元。

Hsu Yu Jen

Hsu Yu Jen

(三)晶片規格

廠商應提供 2 顆晶片規格（詳(九)相容性），二者皆應符合下列規範。

1.基本要求

廠商所提供晶片模組，須符合 Dual Interface 使用需求。

(1)接觸式介面：需符合 ISO/IEC 7816 Part3 T=1 的規範，工作頻率在 3.579MHz 下，傳輸速度至少須能支援 115200 b/s(含)以上。

(2)非接觸式介面：需符合 ISO /IEC 14443 第 2-4 部分，支援 Type A or Type B 規範的 T=CL 傳輸協定，工作頻率 13.56MHz±7KHz，無線讀取距離：Type A 及 Type B 均為 6 cm 以內。

(3)晶片容量：晶片微處理器至少 8 位元（含）以上，可儲存或使用之記憶體(EEPROM 或 NVM)至少 120KB（含）以上。

(4)晶片加解密安全功能：支援 HRNG 或 TRNG 亂數生成器、DES、RSA、ECC、3DES 及 AES 硬體加速器，以及相關各式演算法（如 SHA 等）。

(5)溫度：－20℃～65℃

(6)傳輸速度：Type A 或 Type B 傳輸速度均可支援 106、212、424 Kbps（含）以上。

(7)射頻頻率：依 13.56MHz±7KHz 要求設定，並符合 ICAO MRTD Technical Report Annex J、Annex K 及 InterFest 國際共通性測試。

(8)晶片壽命：可讀寫次數不低於 500,000 次及資料保存可達 15 年（含）以上。

(9)其他：支援防衝突設計（Anti-Collision），以避免晶片重疊之干擾。

A120

非接觸介面 ISO 14443

(出自中央印製廠 CEPP,「PC 晶片卡及印製設備乙式」購案, 招標規範, 頁數 A120)

Hsu Yu Jen

非接觸介面 ISO 14443 即是RFID

Frequency range	Commonly associate applications	ISO (and ISO/IEC) standards
LF <135 kHz	Animal identification, access control, car ignition keys	ISO/IEC 18000-2
HF 13.553-13.567 MHz	Smart card applications, access control, financial cards, national ID cards, passports, ticketing	ISO/IEC 18000-3, ISO/IEC 14443, ISO/IEC 15963, ISO/IEC 18092, ISO/IEC 21481
UHF 433 MHz	Active RFID for cargo handling and military logistics in the USA & NATO countries	ISO/IEC 18000-7
UHF 840 – 960 MHz	Materials handling, asset tracking, logistics supply chain, item-level tracking, RFID/electronic article surveillance (EAS) tags, cargo handling, airline baggage, transportation	ISO/IEC 18000-6, ISO/IEC 29143
UHF 2.45 GHz	Item management	ISO 18000-4
UHF 2.45 GHz	Real Time Locating Systems (RTLS)	ISO/IEC 24730-2, ISO/IEC 24730-5

Table 2 – *Common frequency ranges for RFID applications driven by ISO standards.*

Hsu Yu Jen

(六)安全規範

廠商交付之卡片，應先行檢查晶片內是否內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）及隱密通道（covert channel）。

得標廠商第一批交貨時須提供保證函與該批原廠(晶片廠)檢測報告，後續各批次交貨提供保證函。

且廠商必須於投標時就晶片製程、晶片資料存取、資料傳輸、金鑰交換更新、Java 作業系統及多重應用程序設計架構提供所採用之安全防

中央印製廠,「PC晶片卡及印製設備乙式」購案，招標規範，**2019-0826-第一次閱覽。**

作業系統之安全考量必須包含以下內容：

1.**晶片**內所有 EF 及 DF 資料欄位均可以設定各自安全存取權限。

2.作業系統必須具備支援「生命週期安全管理」機制。

3.具備支援 Random UID 功能，以保障持卡人之**個人行蹤**安全。

4.**具備追蹤機制**，此機制須經內政部授權，**方可進行晶片之追蹤。**

5.**可追蹤之資料（UID）**必須儲存於晶片唯讀記憶體（ROM 或 OTP）內，以確保資料確實無法遭任意竄改。

(中央印製廠/CEPP,「PC 晶片卡及印製設備乙式」購案，招標規範，頁數：A117)

(六)安全規範

廠商交付之卡片，應先行檢查晶片內是否內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）及隱密通道（covert channel）。廠商第一批交貨時須提供保證函與該批原廠（晶片廠）檢測報告，後續各批次交貨提供保證函。

廠商提供之晶片、作業系統及 Applet 等，若經內政部進行相關

中央印製廠,「PC晶片卡及印製設備乙式」購案，招標規範，**2019-0917-第二次閱覽。**

作業系統之安全考量必須包含以下內容：

1.**晶片**內所有 EF 及 DF 資料欄位均可以設定各自安全存取權限。

2.作業系統必須具備支援「生命週期安全管理」機制。

3.具備支援 Random UID 功能，隨機亂數序號產生機制，以**保障持卡人之個人隱私安全**。

4.**具備生產溯源機制**，此機制須經內政部授權，方可於**印製過程執行卡片履歷管理**。

5.**UID** 必須儲存於晶片唯讀記憶體（ROM 或 OTP）內，以確保資料確實無法遭任意竄改。

(七)加解密功能及規範

加密演算法應採用公開、國際機構建議安全且未遭破解之演

Hsu Yu Jen

X 錯誤！

內政部新聞稿

有關中央印製廠招標公告所載晶片追蹤的議題，內政部解釋，New eID是一張晶片卡，就像晶片護照、信用卡、健保卡、悠遊卡、手機晶片卡一樣，是不會主動發送訊號，所以不會洩漏位置，無法追蹤。

戶籍法

第 51 條

國民身分證用以辨識個人身分，其效用及於全國。

第 56 條

國民身分證應**隨身攜帶**，非依法律不得扣留。

【目前內政部的設計】

「自然人憑證的功能」可以取消。

新版卡片上面埋有RFID線圈，**無法取消RFID的追蹤辨識功能**！

強迫把RFID晶片放在人民身上！

- RFID商業應用很多，但**沒有一張卡片像身分證一樣有法律上強制攜帶的要求**！
- 請問部長哪一條法律有授權內政部規定**人民一定得領取有RFID功能的身分證？(強制發卡)**
- 第一階段就是在人民身上放有追蹤功能的晶片卡，第二階段就是要廣設掃描機了嗎？

資安疑慮誰負責？

- 2017年，愛沙尼亞的eID發生資安事件，花了約2個月做緊急處置。(全國130萬人，清查後，證實**有問題的卡片40萬張**)
- **目前內政部的編制可以負擔全國2300 萬張晶片卡身分證的資訊安全事務？**
- 晶片身分證開啟外界系統性、全面性的數位攻擊管道。
- 台灣公部門目前每個月平均有2000至4000萬筆的駭客攻擊事件！

Hsu Yu Jen

Hsu Yu Jen

應修正的法律

- 戶籍法修正(#56):應隨身攜帶身分證
- 新式身分證應該要有「無RFID 功能」的選擇
- 戶籍法上應清楚規範eID專責處理機構及相關程序
  - 人民使用政府網站所產生的數位足跡, 應能查詢並刪除
  - 晶片身分證的存取、儲存使用必須經過該持卡人的同意。而服務提供者提供之服務, 不得強制讀取晶片身分證, 未經過法院、當事人同意, 服務提供者亦不能對外提供當事人的使用紀錄。

質詢結束，謝謝