有關全面換發晶片身分證（eID）之建議

台灣人權促進會、台灣守護民主平台

有關政府近年來所推動的全面免費換發晶片身分證政策（按內政部2019年2月27日「新一代國民身分證換發規劃案」的建議書徵求說明書，頁5），我們的建議如下：

1. 保留領取紙本身分證的可能，不全面換發晶片身分證

晶片身分證的使用固然可能提供某種生活上的便利，但其在個資保護上，涉及額外數位足跡的蒐集、處理、利用，及個人被潛藏的隱性資料標註的風險；在資訊安全上，涉及個別人民的防衛意識是否良好，及政府整體的防護機制是否完善；在長久民主社會的維繫上，也涉及國家是否能建置可大範圍蒐集人民資料的工具。按大法官釋字第603號解釋，人民自主控制其資訊的權利是受憲法保障的權利，因此我們建議，在各式風險難以悉數避免的前提下，應讓人民保有領取紙本卡或晶片卡的選擇，不應強迫所有國民都領取晶片身分證。

此外，內政部過往認為須全面換發晶片身分證的另一理由為「防偽」，然按內政部建議書徵求說明書（頁2）說明，紙本已提供21道防偽機制，具備高難度的防偽變造，「防偽」顯然也非「必須」全面換發晶片身分證的理由。

綜上，我們強烈建議，應保留人民領取紙本身分證的可能，確保人民權益不致因國家的行政便利而受損。

2. 應立專法保護晶片身分證使用者權益

現行有關換發身分證的法律為《戶籍法》。戶籍法雖授權行政機關可制定全面換發或身分證格式的作業規定（如《國民身分證及戶口名簿至發相片影像建置管理辦法》），但「晶片」身分證因其晶片上的存放資料可變，且亦攸關使用者的資料保存、資訊安全、使用範圍等人民基本權益範疇，除現行並無法律就上開項目進行規範外，本即不適合以行政規則的方式處理。因此我們建議應修正戶籍法，並另立專法，確保晶片身分證使用者的權益。

有論者或許認為我國已有《個人資料保護法》及《資通安全法》，分別掌管個資保護或資訊安全；但此二法並非逐一規範晶片身分證的個資保護與資安措施的法律，而身分證又為國民生活必備文件，僅以不明確、解釋空間廣泛的法律規範為依據，將置人民權益於受侵害的風險中。

內政部曾出訪德國、比利時、愛沙尼亞等國考察晶片身分證，這些國家皆有個資法或資安法，但除此之外，它們仍為晶片身分證或數位身分的發行訂立專法，以限定晶片身分證的資料傳輸、資料利用、資料蒐集單位等。因此我們建議，應訂定專法，具體保障晶片身分證領卡人的權利。

3. 明確限制晶片身分證的用途、資料蒐集樣態

科技產品的使用逸脫出原先所設想的目的，是科技應用上十分常見的事。晶片身分證具遠端認證、存放不同用途憑證、或需使用數位設備方能讀取等特性，倘無適當限制，除人民使用晶片身分證所產生的數位足跡恐在未來遭大量蒐集，從而其日常動態或喜好被一覽無遺外；身分證本身所儲存之個資，是否可能於數位認證的過程中，一併遭到公、私部門的蒐集，都應是政策

構思時應考量的資訊。因此我們建議，應要在法律中明確限制晶片身分證的用途，以及資料蒐集的態樣。

4. 明定重要的公、私服務，仍須提供暢通的實體服務管道

晶片身分證為政府提供人民方便取用政府電子化服務的工具。但考量我國國民在操作數位工具的熟稔程度不一、信任程度也不一，以及數位管道可能因其軟硬體的影響及資安風險，而有被迫中斷的風險，因此我們建議，在未來仍須以法律明定，凡是公、私部門所提供的重要服務，需一併提供實體（臨櫃）、非數位方式驗證身分的服務管道，確保人民權益在必要時仍得以被遂行。

5. 提供可被驗證的資訊安全機制及強化資安教育

資訊安全是規劃晶片身分證的關鍵因素。內政部應提供可被外部專家檢視的資訊安全機制，確保個人資訊不會在卡片使用或資料傳輸時被任意截取或外洩，甚至電腦資訊不會被任意竄改(我國報稅程式近來才被發現會自行修改電腦內的Hosts檔）。另外也應該採用國際行之有年的相關標準，避免自訂標準或延伸。

要提供可供驗證的資訊安全機制，我們建議可採用開放原始碼的方式，揭露讀卡機及相關認證介面的程式碼，以確保使用者的資訊安全。這也符合國際上 “Public Money, Public Code”（納稅人出資開發的軟體，其原始碼應該公開）的呼籲。

我們也要再次強調，開放原始碼「不會」因公開了系統運作方式，而降低資訊防護的強度。良好資訊安全系統的安全性不應仰賴運作方式的不透明，而應依賴系統中「密鑰」的安全保存及強度。最安全的系統，不是從未被攻擊、未經檢驗的系統，而是屢次被研究、被攻擊，卻未被發現弱點的系統。開放原始碼可以促進系統受到充分的檢驗。

此外，未來政府期待將自然人憑證之用途整合進晶片身份證當中。但過去的自然人憑證系統不僅曾有憑證公、私鑰（Public Key / Private Key）的產生方式遭外界發現嚴重安全弱點的前科，且在安全性弱點被研究披露之後，內政部更已不允許公開存取其憑證公鑰資料庫（判斷公鑰的產生方式和強度，必須要從此資料庫獲得公鑰），導致外界無從確認目前公鑰產生的安全。晶片身分證同樣有其公私鑰系統，我們建議內政部應在晶片身分證的公私鑰系統持更開放的態度，比照一般公、私鑰加密技術的運作方式，公開公鑰資料庫，確保外部專家檢視的可能。

在資訊安全機制之外，內政部亦應提出強化國民資安教育的政策，確保晶片身分證領卡人清楚其使用卡片的資安風險（例如設置過於簡單的PIN碼，或任意將PIN碼交付他人等），以降低外洩個資或遭身分盜用的情形。

6. 公開、完整揭露研究成果及規劃資訊，並給予社會一定時間討論及修正

內政部於2017年7月至2017年9月間，曾舉行數場的論壇及公民審議（委託政大公共行政學系黃東益老師舉辦開放決策工作坊），並製成會議紀錄及報告，以了解各界專家、公民對此議題的態度。內政部亦有自行製作晶片身分證Q&A，以回答人民的疑慮。

但這些本來放置於內政部網站，可供下載檢視的會議紀錄、成果、以及Q&A，自內政部網站改版後，已悉數遭到移除，再也無法存取。因此我們建議，內政部應重新將過去的研究成果及規劃資訊上架，讓人民能在過去的基礎上，更深入理解晶片身分證這個議題。

此外，內政部2019年2月27日發包的規劃案，最終由「國巨管理顧問股份有限公司」得標。按先前內政部的說明，細部規畫將於2019年8月完成。我們也建議，內政部應承諾在細部規劃完成後，完整揭露規劃內容，並給予社會一定時間討論及修正，方能開始執行，以確保晶片身分證的製作是在取得國人的信任下完成。

相關連結

本文件原始連結 https://reurl.cc/bxLxE	內政部「新一代國民身分證換發規劃案」文件 https://reurl.cc/GD9lD	內政部2017年委託政治大學進行之公民審議 https://reurl.cc/kvR2q
台權會過往發言 https://www.tahr.org.tw/issues/privacy/eid	【德國】 身分證及電子身分法 https://reurl.cc/qXxA3	【愛沙尼亞】 身分文件法 https://reurl.cc/WW5mO