電話 Tel：2829 3829 傳真 Fax：2507 3581
入境事務處
Immigration Department
覆函請註明本處檔號
In reply please quote this ref ：ImmD ISPM1/6-15/3/19C
圖文傳真：3020 9867

（以傳真、郵寄及電郵發出）

香港中區
立法會道 1 號
立法會綜合大樓 917 室
莫乃光議員

莫議員：

有關新一代智能身份證系統的跟進問題

謝謝你於 2015 年 1 月 21 日致保安局局長的信，本處現獲授權回覆。

就有關新一代智能身份證系統的技術設計、機密和安全性等問題，現給你回覆，詳情請見附件。

希望上述資料有助釋除公眾對新一代智能身份證系統關於私隱和保安等的疑慮。

入境事務處處長

（周康道 代行）

2015 年 2 月 3 日

附件： 莫乃光議員有關新一代智能身份證系統的跟進問題及相關回覆

副本抄送：
保安局局長黎棟國先生
保安局副局長李家超先生

香港灣仔告士打道七號入境事務大樓二十三樓 23/F, Immigration Tower, 7 Gloucester Road, Wan Chai, Hong Kong
圖文傳真 Fax (852) 2824 1675 • 電郵地址 E-mail Address enquiry@immd.gov.hk
網址 Website http://www.immd.gov.hk/

莫乃光議員就新一代智能身份證系統的跟進問題及相關回覆

(1) 一般問題

問(1.1) 除節省成本、滿足有關入境處的業務需求和提升技術水平，採用RFID技術的必要性和對市民的具體益處為何？

答(1.1) 現時的智能身份證只支援接觸式介面，如需讀取晶片所載資料，必須把智能身份證插入讀卡器，讓晶片直接與讀卡器連接，方可讀取晶片資料。新智能身份證所採用的晶片將置有非接觸式介面，利用光學閱讀及無線射頻傳輸資料，以優化現時智能身份證的以下方面：

(1) 晶片更耐用 - 在新晶片介面下，晶片與讀卡器沒有直接接觸，因頻密讀卡而對身份證造成的損耗亦可因而減少，從而有效地提高其耐用性；以及

(2) 資料傳送速度更快 – 透過新晶片介面讀取資料將更快捷，可大幅提升出入境檢查的效率。香港居民使用e-道辦理出入境手續所需的時間，將由12秒大幅降至8秒（減少33%），相應的運算顯示，供香港居民使用的e-道可處理的旅客流量，將增加50%。香港各管制站需處理的旅客量龐大且不斷上升（在2014年，使用e-道進出香港的香港居民總數達114 400 000人次）。增加旅客流量對整體社會帶來莫大益處。

問(1.2) 能否給予市民選擇繼續使用接觸式技術的智能身份證或停用新一代智能身份證的無線傳輸功能？

答(1.2) 新智能身份證將嚴格按照國際標準化組織（International

Organization for Standardization or ISO）的 ISO 14443（A 或 B 型）標準設計。另外，建議的新晶片具備多重保安特徵，包括採用基本存取控制以及相互認證等存取保障措施。顧問及業界專家均認為，這些存取保障措施能有效防止智能身份證內的個人資料透過非接觸式介面被非法讀取。因此，市民並不會因使用新智能身份證而增加其個人資料外洩甚至被追蹤的風險。（詳見答(2.2)，及立法會 CB(2)654/14-15(03)號文件第 4 至 15 段）。

同時提供接觸式技術智能身份證或停用智能身份證的無線傳輸功能讓市民選擇，在系統技術要求和配套方面將大大增加所需開支，在人事登記和簽發身份證的過程亦將引起混亂和變得非常複雜，市民日常使用身份證時亦可能產生不少問題，故此有關建議並不切實可行。

問(1.3) 新一代智能身份證系統的硬件、軟件更新等合約會否考慮分開不同部份批出，以提高日後系統升級及更新方面的靈活性？

答(1.3) 入境處會在充分考慮各組件日後的更新、升級和兼容性等問題後，並根據政府的採購守則及有關部門的意見才制定採購策略，包括將不同組合的系統硬件、軟件分拆招標，從而鼓勵更多資訊科技公司參與投標，讓政府取得既切合要求又具競爭力的投標書，從中選擇最可取和最符合公眾利益的建議。

問(1.4) 澳門特別行政區推出第二代智能身份證時以自然淘汰方式，為居民更換非接觸式智能身份證，居民只需待身份證到期更換新證即可，並停發接觸式智能身份證。香港的新一代智能身份證為何不能採取類似方式更換？

答(1.4) 與澳門特別行政區所簽發的身份證不同，香港身份證並沒有設定有效期限，所以澳門特別行政區所採用的換證方式並不適用於香港。假如在香港採用自然淘汰的方式更換身份證，新舊兩種身份證將長期並存及流通，容易產生混亂及引起保安漏洞。

有關在新智能身份證上保留接觸式介面的原因，請參閱以下第2.4題。

(2) 技術設計

問(2.1) 建議新證採用的RFID標籤晶片、天線的技術規格為何，晶片記憶體容量比上一代智能身份(舊證)證比較提升了多少百分比，建議新證的數據加密算法、信號傳輸功率、安全協議和內部儲存區的標準為何？

答(2.1) 新智能身份證將嚴格按照國際標準ISO 14443 (A或B型)標準設計。同時智能晶片亦必須符合相關的技術規格(如信號傳輸功率等)。

新智能身份證的晶片將屬於被動型，即不附設獨立電池。其數據儲存容量(如電子抹除式可複寫唯讀記憶體，Electrically Erasable Programmable Read-Only Memory)將由現時的32/36kBytes增加至最少80kBytes。

為確保資料保密，新晶片將採用嚴格加密技術認證（包括公開密碼匙基礎建設，Public Key Infrastructure or PKI)、非對稱及對稱密匙加密算法（如RSA加密演算法、橢圓曲線密碼學，Elliptic Curve Cryptography or ECC，以及高級加密標準，Advanced Encryption Standard or

AES）。

問(2.2) 請詳細解釋新證採用的光學閱讀技術的運作與功能。閱讀器是否採用ISO 14443 A&B標準？

答(2.2) 建議的新智能身份證將嚴格按照國際標準ISO 14443（A或B型）標準設計；此標準行之有效，在國際上被廣泛應用於保密文件的智能卡晶片，支援約10厘米範圍內的近距離通訊。此標準有別於用作其他不同用途、支援可達數百米範圍內的遠距離通訊，但對儲存資料有較少甚或沒有任何保護的無線射頻識別標準，例如作物品標示（ISO 15693）、貨倉管理（ISO 18000-6）、貨櫃電子封條（ISO 18185）等用途的無線射頻識別標籤，兩者截然不同。

建議的新晶片將屬於被動型，即不附設獨立電池。晶片沒有電源，就不能自行傳送任何訊號。換言之，其無線資料傳送功能將長期處於關閉狀態。只有在成功完成下列所有步驟後，才能通過無線資料傳送功能讀取晶片資料：

(1) 把智能身份證直接放在獲證書授權及配備特定運算程式的認可光學證件閱讀器（閱讀器）上，將身份證上印有「鑰匙文字串」的一面面向閱讀器，令閱讀器可擷取「鑰匙文字串」，繼而產生一條隨機加密密匙；

(2) 如認可閱讀器成功擷取「鑰匙文字串」（一如電腦掃描器擷取資料），閱讀器就會根據所擷取的「鑰匙文字串」以及認可閱讀器的特定運算程式產生一條實時的一次性加密密匙；

(3) 閱讀器產生的加密密匙將由晶片認證，並要求晶片建立一對一的專用加密通訊通道；

(4) 只有在加密密匙獲得晶片認證後，晶片和閱讀器之間的加密通訊通道才能建立。即使該加密通訊通道已被成功建立，晶片的無線資料傳送功能仍處於關閉狀態，即儲存在智能身份證晶片中的資料不會傳送到閱讀器。資料傳送功能只有在進一步認證後才會啟動；

(5) 經過上述(1)至(4)的步驟建立加密通訊通道後，閱讀器須向晶片提交第二條不同的加密密匙以作認證。只有在第二條密匙成功認證後，資料傳送功能才會開啟，閱讀器方可從智能身份證的晶片讀取資料；否則資料傳送功能會一直保持關閉。

使用認可的閱讀器成功擷取印在證件表面的「鑰匙文字串」(上文的步驟(1))，是啟動晶片無線通訊功能的「先決條件」。否則，晶片不會回應任何通訊要求。持證人可全權掌控，是否把證件直接放在認可的閱讀器上以啟動認證過程。換言之，若證件存放在銀包、手袋或衣物內，或是以其他任何方法隱藏起來，無線資料傳送功能會保持關閉，與晶片之間的通訊將不會啟動。事實上，即使證件被拿出來，但如未有正確地擺放（例如「鑰匙文字串」並非面向閱讀器）並在距離認可閱讀器2厘米之內，「鑰匙文字串」仍然無法被成功擷取，而加密過程及隨後的無線通訊亦不會啓動（即停留在上文的步驟(1)）。

為提供額外保障，新一代智能身份證系統下，只有認可的光學證件閱讀器（即獲證書授權及配備特定運算程式，可從身份證表面經光學擷取的「鑰匙文字串」產生

一個隨機加密密匙的閱讀器），方能啟動無線資料傳送過程。即使有人取得某張香港身份證上的「鑰匙文字串」（例如從該香港身份證影印本取得），但在沒有認可閱讀器的情況下，該人仍無法啟動任何無線資料傳送（停留在上文的步驟(2)）。

為了確保個別人士不會因未獲授權的無線資料傳送而有被追蹤的可能，入境處將參考德國身份證所採用的模式（與德國身份證所採用的類似），印在香港身份證上的「鑰匙文字串」將不會是獨一無二的文字串。換言之，即使在極不可能發生的假設情況下，有人非法取得「鑰匙文字串」及認可閱讀器並成功完成上文的步驟(1)至(3)，也無法識別個別人士的身份。

智能身份證晶片與閱讀器之間建立的每條一對一專用加密通訊通道（在成功完成上文的步驟(1)至(3)後所建立）只會在該次的通訊時有效。當智能身份證晶片從閱讀器移開，該通訊通道將會消失。換言之，即使某張身份證曾經與某部閱讀器成功建立過加密通訊通道，在該通道消失後，當同一張身份證再一次靠近同一部閱讀器時，除非成功重複步驟(1)至(3)（即持證人再次取出身份證並放在閱讀器上），否則加密通訊通道將不會自動再次建立。

另外，為釋除有關資料被竊聽的疑慮，透過上文步驟(1)至(3)相互認證所建立的加密通訊通道將會是一對一及專用的通道。換言之，只有成功認證的閱讀器方能讀取晶片。在通道建立後，即使將其他閱讀器放在晶片附近，其他閱讀器也不能夠讀取晶片。

為確保資料保密，成功完成（第二重）嚴格加密技術的認證（包括公開密碼匙基礎建設、非對稱及對稱密匙加

密算法（如 RSA 加密演算法、橢圓曲線密碼學，以及高級加密標準）），方可進行上文步驟(4)至(5)讀取晶片內的資料。有關技術又名延伸存取控制（Extended Access Control）或相互認證，是一項極可靠的保安特徵，在多個司法管轄區區已被廣泛採用，包括德國的身份證，以及德國、捷克、瑞士及意大利的電子護照等。只有透過認可的閱讀器才可以讀取智能身份證晶片內的個人資料，資料不可能被略讀或被竊聽。換言之，即使有其他人在晶片進行無線資料傳輸進行時（在成功完成上文步驟(1)至(5)後）近距離偵測到訊號，他亦只能夠偵測到經擾亂、沒有意義的訊號。

問(2.3) **建議新證表面供光學證件閱讀器擷取，以啟動傳輸的「某些獨特的資料」及其使用壽命為何，會否因為證件磨損而失效，出現無法讀取或錯誤啟動傳輸的情況？在甚麼情況下，建議新證會否未經光學認證而啟動傳輸？**

答(2.3) 近年，製造智能身份證物料的技術已進步不少。新的聚碳酸不碎膠 Polycarbonate (PC) 物料提高了身份證對防禦磨損、屈曲，以及化學物品和熱力侵害的能力，使其更耐用，更不容易被刮花。此外，新物料中的碳粒子成份和密度較高，所以以激光把資料刻蝕於身份證上的質素和效率亦有所提升。由於以激光刻蝕的資料深入身份證的內層，因此在正常使用情況下，一般不會出現因表面磨損而導致無法擷取資料或錯誤啟動傳輸的情況。

在新晶片下，以非接觸式介面讀取晶片資料是必須經指定步驟進行（詳見答(2.2)）。若在過程中不能成功認證，無線資料傳送功能仍處於關閉狀態，故此不可能錯誤啟動傳輸。

問(2.4) 建議新證是否保留接觸式晶片作為其中一種傳輸方式，若是原因及理據為何？該接觸式晶片的物料、其使用壽命為何，在甚麼情況下會導致失靈？接觸式傳輸是否需要經過光學認證啟動傳輸？

答(2.4) 顧問建議新智能身份證引入無線傳輸介面，亦同時保留接觸式介面，以作過渡用途。目前，政府部門以智能身份證提供的非入境事務應用包括，公共圖書館服務、康體通自助服務站、醫健通系統、以及公私營醫療合作—醫療病歷互聯試驗計劃和儲存電子證書。這些政府部門以接觸式介面運作的讀卡器將會由現時約6 000部增至於2017年底約17 700部。

現時智能身份證所採用的接觸式晶片，在一般使用情況下，供應商的使用期保證為十年。入境處會密切留意市場上的發展，於在新智能身份證招標時盡可能要求供應商提供更長的使用期保證。

以接觸式介面讀取新智能身份證晶片所儲存的資料，必須把智能身份證插入讀卡器（而並非光學證件閱讀器），讓晶片直接與讀卡器接觸，方可讀取晶片資料。讀卡器和晶片亦必須經認證成功後才能讀取晶片資料。

問(2.5) 第一代智能身份證是採用接觸式晶片技術，如輸入的密碼是容許有五次的錯誤；在新一代智能身份證，如何避免如有人以 RFID 讀卡器在近距離強行讀取晶片上的資料而輸入五次密碼而使智能身份證失效？

答(2.5) 在新晶片下，引入基本存取控制及雙重認證之後，以非接觸式介面讀取晶片資料是必須經指定步驟進行（詳見答(2.2)）。若在過程中不能成功認證，無線資料傳送功能

仍處於關閉狀態，故此不可能錯誤啟動傳輸。

現時，根據香港郵政關於載入第一代智能身份證內的電子證書的指引，如電子證書密碼被錯誤地輸入超過五次，證書將會被鎖上，需要向香港郵政提出重設密碼。除電子證書之外，智能身份證上的其他入境事務及多用途智能身份證應用均無需輸入密碼啟動。政府資訊科技總監辦公室現正另行進行技術研究，檢討智能身份證在多用途智能身份證計劃下其他可能的用途，以及現有智能身份證使用上之過渡安排和遷移策略。

(3) 機密和安全性

問(3.1) 建議新證是否支援遙距資料傳輸，最長傳輸距離及達至最長傳輸距離所需的器材配置規格為何？目前有否方法可繞過光學認證啟動傳輸，若有詳情為何？

答(3.1) 詳見答(2.2)。

問(3.2) 建議新證是否容許多重傳輸，在一方完成光學認證或進行接觸式傳輸的同時，被其他閱讀器在未經認證的情況下讀取資料，相關的保安細節詳情為何？

答(3.2) 詳見答(2.2)。

問(3.3) 系統核實所需的密匙如何管理，讀取資料一方如何取得密匙，如何確保密匙不會被第三方獲取？

答(3.3) 入境處已制定了一套嚴密的密匙管理保安規章及程序，

監管密匙的製造、傳輸、應用和棄置，並要求相關授權的同事嚴格遵守，以確保密匙不會被未經授權人士獲取。有關人員亦受《官方機密條例》(第521章) 的監管。

密匙的製作過程是需要經過特別安排及嚴緊的保安程序，已製作的密匙只可按既定程序存放於高安全性的保密儀器(Hardware Security Module 硬體安全模組) 內，當完成存放後就不能被取出。這些儀器本身備有多重保安設計和感應器，在受到不正常外部的攻擊時會自動刪除所儲存的密匙。而且，此保安系統的安全策略、運作程序和所有的活動日誌亦會被定期審查，以確保系統安全。

問(3.4) 甚麼政府人員擁有存取加密密匙的權限，其適用範圍及功能為何，能否存取建議新證上的個人資料，詳情為何？

答(3.4) 入境處會採取嚴格的保安技術架構，以防密匙被存取。入境處亦會參考市場上最新的科技發展，按照政府的保安條例和指引，採用最穩妥而合適的保安技術和措施，確保存取密匙的安全性。密匙的製作過程是需要經過特別安排的保安程序，我們會使用專門針對儲存與保護密匙運算的高安全性的保密儀器(Hardware Security Module 硬體安全模組)，經既定程序把密匙儲存，確保參與密匙製作的人員不能從中知悉或擷取密匙的數值。密匙一經儲存在這些儀器內是不能被取出。這些儀器本身備有多重保安設計和感應器，在受到不正常外部的攻擊時會自動刪除所儲存的密匙，確保密匙在任何情況下也不能被任何人存取。存取晶片資料亦需要透過這些保密儀器進行。

問(3.5) 文件指新證設計能保障接觸式/無線閱讀器不能同時讀取和收集多張智能身份證上的資料，相關的保安細節詳情為何？

答(3.5) 不論以接觸式或非接觸式的介面進行資料傳輸，閱讀器是需要根據特定的傳輸協定設計，以加密通訊通道向晶片提供密匙作相互認證。只有經過成功認證後才能啟動資料傳送功能，以讀取晶片資料；否則，資料傳送功能仍然保持關閉。由於整個資料傳送過程是在一對一及專用的加密通訊通道中進行，同一時間內光學證件閱讀器並不能與其他晶片進行相互認證，故不可能同時讀取和收集多張智能身份證上的資料。詳見答(2.2)。

問(3.6) 文件指新證設計能保障晶上部份敏感個人資料不被無線傳輸讀取，相關的保安細節詳情為何？

答(3.6) 詳見答(2.2)。

問(3.7) 政府會否主動公開新智能身份證系統的技術細節(包括晶片所儲存的資料、通訊協定和密碼學協定等)以供公眾審視？

答(3.7) 保安事務委員會於2015年1月6日會議上，有委員要求當局就新一代智能身份證的保安及保障私隱方面的詳情提供進一步資料。按此要求，當局已向委員會提供補充文件，詳見立法會CB(2)654/14-15(03)號文件。

另外，現時智能身份證晶片內儲存的資料項目已於香港政府一站通網站供市民參閱，新智能身份證亦會參照現時做法。

問(3.8) 政府會否在負責執行整個項目的主要承辦商之外委託一家獨立顧問/公司進行資訊及保安系統設計，以確保保安標準和要求不會『價低者得、因貨就價』而下降？

答(3.8) 入境處一向嚴格遵守保障資料原則及一切有關的政府系統保安規定。在招標的過程中，入境處會把相關的保安標準和要求加入標書內，對投標的承辦商進行嚴謹的技術審查，以確保相關的保安標準和要求必須達到，因此不會構成『價低者得、因貨就價』的情況。

與推行現行智能身份證系統時一樣，入境處將委聘外間的顧問，在推行新一代智能身份證系統的不同階段進行私隱影響評估，然後將每份私隱影響評估報告提交個人資料私隱專員，讓專員就報告內容提供意見。入境處會採納顧問和專員的建議，令推行新一代智能身份證系統的工作更為妥善。

除進行私隱影響評估外，入境處亦會委聘獨立的審計人員，在推行新一代智能身份證系統的不同階段，包括系統分析和設計階段，以及在新一代智能身份證系統推行前和推行後，進行資訊科技保安風險評估及保安審計，以確保新一代智能身份證系統及香港智能身份證的保安措施能有效保護個人資訊。

(4) <u>保障私隱</u>

問(4.1) 當局如何保障，建議新證上的個人資料不被竊取，例如數據傳遞過程中截取讀寫器或標籤發出的資料、複製標籤使防偽失效等，或資料在未經當時人同意下被儲存？

答(4.1) 詳見答(2.2)。

問(4.2) 當局提交文件指出，為配合建議新證推行將會分階段為本港市民更換建議新證，估計需要額外設立9個換證中心；就此在更換建議新證時，市民需要額外提供甚麼資料以完成換證程序，當局會如何處理有關資料，會以甚麼方式儲存有關資料，如何確保資料不會外洩？

答(4.2) 現時申請人在申請登記身份證時，須按照《人事登記規例》(第177A章)第4(1)條的規定向人事登記處提供其個人資料。在推行換證計劃時，申請人將按相同的法定要求提供資料，跟現時並無兩樣。有關資料的儲存、使用和披露亦將繼續嚴格依照《個人資料(私隱)條例》(第486章)、《人事登記條例》(第177章)及《人事登記規例》(第177A章)的規定而執行。

與推行現行智能身份證系統時一樣，入境處將委聘外間的顧問，在推行新一代智能身份證系統的不同階段進行私隱影響評估，然後將每份私隱影響評估報告提交個人資料私隱專員，讓專員就報告內容提供意見。

除進行私隱影響評估外，入境處亦會委聘獨立的審計人員，在推行新一代智能身份證系統的不同階段，包括系統分析和設計階段，以及在新一代智能身份證系統推行前和推行後，進行資訊科技保安風險評估及保安審計，以確保新一代智能身份證系統及香港智能身份證的保安措施能有效保護個人資料。

問(4.3) 據私隱專員公署通訊第30期及政府2008年2月發出的《射頻識別(RFID)保安》文件，無線射頻識別(RFID)

會帶來私隱風險，例如不能主動關閉傳輸，相對容易在未經持有人同意下被讀取，有可能被竊聽(或側錄)和仿冒、亦有可能以RFID 晶片的識別碼來追蹤位置，以及收集持有人資料的風險；當局會如何減低這些風險，詳情為何？

答(4.3) 詳見答(2.2)。

問(4.4) 新系統有什麼機制確保只有獲授權的政府部門/機構可存取身份證所儲存的資料？新系統會否限制各個獲授權的政府部門/機構只能讀取必須的部份資料(on a need-to-know basis)？如會，詳情為何；如否，原因為何？

答(4.4) 《人事登記規例》第12(1B)(a)條規定，身份證所關乎的人如藉使用由政府提供或獲政府批准提供的設施，而取覽儲存於該身份證內置晶片的（該規例）附表1指明的數據，則他即屬有合法權限而作出該項取覽。現時，上述設施包括（由入境處全權控制的入境事務設施）e-道、申請電子護照自助服務站、澳門e-道自助登記服務機、智能身份證系統自助服務站，以及（在多用途智能身份證計劃下利用卡面資料的非入境事務設施）公共圖書館服務、康體通自助服務站、醫健通系統，以及公私營醫療合作－醫療病歷互聯試驗計劃。持證人如欲使用以上所有設施，必須把身份證放入讀卡機取覽晶片，按照《人事登記規例》第12(1B)(a)條所授權閱讀晶片內的資料，並向上述所指的相應設施提交這些資料，以使用不同公共服務。

此外，《人事登記規例》第12(1B)(b)條亦規定，如（該規例）附表5指明的數據為某目的而儲存於身份證的內置晶片內，則獲發該身份證的人如只為該目的而取覽

該等資料，即屬有合法權限而作出該項取覽。現時，該等資料只包括電子證書。《人事登記條例》、《人事登記規例》或任何香港法例的其他條文，均沒有賦予任何人同樣的合法權限取覽儲存於身份證的內置晶片內的數據。

根據《人事登記規例》第12(1A)(b)條，任何人無合法權限或合理辯解而取覽任何儲存於（香港智能身份證）晶片內的數據，可處第4級罰款（港幣25,000元）及監禁2年。建議中新香港智能身份證的新晶片介面，與上述法律規定相符。

另外，多用途智能身份證計劃讓智能身份證可用作更多其他應用功能，以便利市民。增加這些應用功能時，均須符合《個人資料（私隱）條例》（第486章）及得到持證人同意。依照同樣原則，政府資訊科技總監辦公室現正另行進行技術研究，檢討智能身份證在多用途智能身份證計劃下其他可能的用途。當局在推出任何新應用功能之前，會確保建議的應用功能在讀取卡面資料時符合法例要求，並就卡面資料的用途諮詢立法會相關事務委員會。如有需要，會修訂有關的法例或規例，以及籌劃和實行保護數據及保障私隱的措施。

問(4.5) 政府會否按個人資料(私隱)條例要求，提供方法讓持卡人查閱新一代智能身份證所儲存的所有資料，並且檢視身份證的存取紀錄？如會，詳情為何；如否，原因為何？

答(4.5) 與人事登記有關個人資料的收集、儲存、使用、保安、查閱及改正均按照《個人資料（私隱）條例》（第486章）、《人事登記條例》（第177章）及《人事登記規例》（第177A章）的規定來處理。

身份證持有人如需查閱智能身份證晶片所儲存的資料，可利用設置於各人事登記辦事處、灣仔入境處總部及出入境管制站的自助服務站，把智能身份證插入站內閱讀機，以查閱晶片內的資料。另外，根據《個人資料（私隱）條例》，任何個人均有權要求資料使用者告知是否持有他/她的個人資料，並要求索取一份該等資料的複本。入境處已制定相關的指引，按照《個人資料（私隱）條例》的規定來處理查閱個人資料的要求。

問(4.6) **文件提及政府會在項目不同階段聘請獨立顧問進行私隱影響評估(Privacy Impact Assessment)，內容為何？會否在項目不同階段聘請獨立顧問進行資訊安全審核(Information Security Audit)，核實系統的程式碼，以確保系統實作和政府公佈的設計一致？**

答(4.6) 入境處已就新一代智能身份證系統委聘顧問進行了第一次私隱影響評估。據報告指出，新一代的智能身份證系統，無論在設計上或運作程序上，均符合《個人資料(私隱)條例》（第486章）下的保障資料原則及其他規定。就晶片介面方面，顧問認為採用基本存取控制以及相互認證等存取保障措施，能有效防止智能身份證內的個人資料透過非接觸式介面被非法讀取。根據顧問建議，入境處會在推行新一代智能身份證系統的較後階段（包括系統分析和設計），評估有關措施的成效。

私隱影響評估報告亦已提交個人資料私隱專員公署以徵詢其意見。入境處會在日後新系統設計階段及推出前後會再委託合資格的獨立顧問進行私隱影響評估，確保新系統在運作上可全面地保障個人資料私隱。

此外，為確保新一代智能身份證系統及香港智能身份證

的保安措施能有效保護個人資料，入境處亦會於往後的不同階段（包括系統分析和設計、推行前及推行後等）委聘獨立的審計人員進行獨立資訊科技保安風險評估及保安審計。

問(4.7) 會否公佈私隱影響評估和安全審核的報告？如會，詳情為何；如否，原因為何？

答(4.7) 新一代智能身份證系統的私隱影響評估報告，是從保障私隱的角度對推行新一代智能身份證系統所提出的建議包括系統設計、保安技術及審批新一代香港智能身份證的詳細工作流程等進行評估，並提出相關建議。資訊科技保安風險評估及保安審核則會評估包括系統與智能身份證的保安措施是否有效。

新一代智能身份證系統第一次私隱影響評估經已完成，顧問認為採用基本存取控制以及相互認證等存取保障措施，能有效防止智能身份證內的個人資料透過非接觸式介面被非法讀取。根據顧問建議，入境處會在推行新一代智能身份證系統的較後階段（包括系統分析和設計），評估有關措施的成效。顧問在第一次私隱影響評估中，就身份證介面、物料和證件保安特徵等方面的評估和建議的摘要，請參閱立法會CB(2)654/14-15(03)號文件的附件B。

(5) 普及應用

問(5.1) 當局有否評估建議新證的新增功能如何提升智能身份證的普及應用，舊證推出時建議的『多用途智能身份證計劃』中提供的服務當中，有否服務從未推出，分別為何？

答(5.1) 在多用途智能身份證計劃下利用卡面資料的非入境事務設施，已推出的包括公共圖書館服務、康體通自助服務站、醫健通系統，以及公私營醫療合作－醫療病歷互聯試驗計劃。其他曾經討論但未有推出的服務包括應用智能身份證作駕駛執照、電子錢包及個人識別密碼。

政府資訊科技總監辦公室現正另行進行技術研究，檢討智能身份證在多用途智能身份證計劃下其他可能的用途。

問(5.2) 請具體列出建議新證的功能支援的可行用途，各政府部門會如何利用這些功能開發服務，相關計劃的詳情及時間表為何？當局會如何協助有關部門推行應用建議新證的服務，另外當局有否計劃提升現有個別部門推出的電子服務，例如「稅務易」平台，兼容建議新證提供的功能，如有詳情及時間表為何？

答(5.2) 政府資訊科技總監辦公室現正另行進行技術研究，檢討智能身份證在多用途智能身份證計劃下其他可能的用途。

問(5.3) 得悉當局即將推行「電子支票」，將會應用到電子證書，然而在舊證推出至今電子證書的使用率持續偏低，當局會如何在推行建議新證的同時協助提升電子證書的使用率，以便推廣相關應用？

答(5.3) 詳見答(5.2)。

問(5.4) 澳門居民可以利用澳門第2代智能身分證在身分證明局

的自助櫃台上申請更換新的智能身分證、使用香港的e道過關、更改個人聯絡資料、申請無犯罪記錄證明書、打印醫療券及登記生存證明書。新一代智能身份證將儲存甚麼種類的個人資料，新證會否開放儲存區予其他機構儲存資料及提供類似增值服務，如會，機構申請提供服務的詳情為何？

答(5.4) 詳見答(5.2)。

問(5.5) 市民能否選擇加入或退出(opt-in / opt-out)這些服務？

答(5.5) 詳見答(5.2)。

- 完 -