2015 年 2 月 3 日
討論文件

立法會保安事務委員會

建議新一代智能身份證系統
保安及私隱保障特徵的補充資料

引言

本文件就新一代智能身份證系統的保安及私隱保障特徵提供進一步資料。

新晶片介面

2. 現時的智能身份證包括一張可作高度保安用途的智能晶片。該晶片於 2000 年代初研發，只可支援接觸式介面，即必須把智能身份證插入讀卡器，讓晶片直接與讀卡器接觸，方可讀取晶片資料。過去十年來，晶片硬件、操作系統和軟件技術，在處理速度、儲存量、晶片介面和保安等方面均有重大發展。晶片硬件的提升創造了機會，讓有迫切需要更新的軟件也可適時相應提升，使智能身份證能藉着科技發展，有更廣泛、更方便和更具效率的用途。

3. 建議採用的新晶片介面具有多重保安特徵（詳見下文第 4 至第 15 段），讀取資料更快捷，更耐用，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%[1]。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。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。不過，即使推出新晶片介面，我們仍需保留目前的接觸式介面作過渡用途[2]。

---

[1] 現時，每條 e-道平均每分鐘可處理 5 名旅客（60 秒／12 秒）。引入新晶片介面的新一代智能身份證後，同一 e-道平均每分鐘可處理 7.5 名旅客（60 秒／8 秒）。因此，可處理的旅客流量將提升 50%。

[2] 除了更換入境處的電腦系統外，康樂及文化事務署的圖書證服務及租訂康樂設施、

保安特徵

4. 建議的新晶片介面利用無線射頻傳輸資料，有人因而擔心日後因未經授權讀取晶片資料而令個人資料外洩甚至被追蹤的風險將會增加。下文列出新一代智能身份證的多重保障，旨在釋除相關的疑慮或誤解。

依照為保密文件所訂的 ISO 標準設計的新晶片

5. 無線射頻識別（RFID）泛指各種符合不同標準的無線通訊裝置。建議的新智能身份證將嚴格按照 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。

存取控制及雙重認證

6. 為確保晶片和閱讀器之間的無線通訊和資料傳送安全可靠，當局會顧及以下保安及私隱保障需要：

(a) 讀取晶片資料只可由持證人啟動；
(b) 在進行通訊前，必須確定晶片和閱讀器的身份，並必須經過相互認證；及
(c) 整個通訊及資料傳送過程必須加密。

7. 在顧及上述考慮的前提下，建議的新智能身份證的晶片將屬於被動型，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：

(I) 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上[3]（閱讀器），將身份證上印有「鑰匙文字

食物及衞生局及衞生署的醫健通服務系統，以及醫院管理局及私家醫生的醫療病歷互聯計劃亦需要一定時間來更換其智能身份證閱讀器（2014 年年底大約有 6 000 部，預計 2017 年年底，會增加至 17 700 部）。以上服務系統逐步採用新的非接觸式介面後，新智能身份證因使用接觸式介面而造成的損耗會明顯減少。

[3] 光學證件閱讀器是支援對證件表面進行光學掃描及讀取智能身份證晶片的裝置。

串[4]」(Key Text String)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；

(II) 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；

(III) 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；

(IV) 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。值得留意的是，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；

(V) 經過上述(I)至(IV)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。

以上步驟的示意圖載於**附件 A**。

8. 上述雙重認證過程包含多項保障措施，旨在確保晶片資料不會在「沒有持證人的同意下」或被「隔空」讀取。這些措施重點如下。

(A) 無線通訊的存取控制

9. 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 I**)，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 I**）。

[4] 「鑰匙文字串」是由印於智能身份證證件表面的某些資料組成，例如香港身份證的部分號碼加上香港身份證的簽發日期。這些資料不能用於識別個別人士的身份。

10. 以上所述的程序通常稱為基本存取控制（Basic Access Control – BAC）。這項技術在多個司法管轄區已被廣泛採用多年，行之有效。更加精密的技術，如額外存取控制（Supplemental Access Control – SAC）或密碼驗證連接建立（Password Authenticated Connection Establishment – PACE），亦不斷面世[5]。入境事務處（入境處）將確保新一代智能身份證會採用最先進及最可靠的技術。

(B) 認可的閱讀器

11. 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 II**）。

(C) 非獨一無二的鑰匙文字串

12. 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[6]，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 I 至 III**，也無法識別個別人士的身份。

(D) 實時通訊通道

13. 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 I 至 III** 後所建立）只會在該次通訊時有效。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，當同一張身份證再次靠近同一部閱讀器時，除非成功重複**步驟 I 至 III**（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。

---

[5] 某些國家已經發出支援 SAC 或 PACE 技術的身份證、電子護照等個人身份證明文件，例如德國、瑞士、科索沃共和國、摩爾多瓦、波斯尼亞和黑塞哥維那。

[6] 這項特徵與德國身份證所採用的類似，證件表面上印有非獨特的六位數字號碼作為「鑰匙文字串」。

(E)　專用通訊通道

14.　為釋除有關資料被竊聽的疑慮，透過上文**步驟 I 至 III** 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。

(F)　用於個人身份證明文件的可靠加密技術

15.　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 IV 至 V** 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 I 至 V** 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。

專家意見

16.　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。上述保安特徵的設計會在下一階段進行系統分析和設計時定案，下一次私隱影響評估將涵蓋有關設計。

17.　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，載於**附件 B**.

18. 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。

個人資料私隱保障

19. 除了上述設計保安特徵外，現行的《人事登記條例》（第 177 章）及《人事登記規例》（第 177A 章）對防止非法讀取智能身份證晶片有嚴格的規定，亦對使用及收集人事登記資料設有嚴格的規管。

禁止非法讀取晶片

20. 《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[7]。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。相關法律條文載於**附件 C**。

[7] 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。

身份證的其他可能用途

21. 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。

收集人事登記資料及儲存數據

22. 人事登記處處長嚴格按照《人事登記規例》第 4(1)(b)條的規定收集個人資料。推行新智能身份證系統不會改變有關做法，即在建議的新一代智能身份證系統和新智能身份證之下，當局收集的個人資料不會比現行的系統和身份證多。《人事登記規例》附表 1 列明智能身份證內（包括其晶片內）所儲存的資料。除取覽任何儲存於晶片內的數據的規定之外，《規例》第 12(1A)條亦規定，任何人無合法權限或合理辯解而儲存數據於晶片內、除去、取消或改動晶片的任何數據，或對該等數據作出增補或令晶片失效，亦屬犯罪，可處第 4 級罰款（港幣 25,000 元）及監禁 2 年。

其他資料

經濟合作暨發展組織國家的身份證

23. 在經濟合作暨發展組織的 34 個成員國中，有 28 個國家（82%）簽發身份證；其中 17 個成員國（佔所有經濟合作暨發展組織成員國的 50%）備有特定的法定要求，獲授權人士可要求國民出示身份證。有關資料摘要載於**附件 D**。在有簽發身份證的國家中，德國、荷蘭、智利、芬蘭及瑞典均採用了無線傳輸技術。

智能卡的耐用性

24. 於 2003 年發行的第一批香港智能身份證，到 2018 年時已使用 15 年。入境處於 2012 年委託兩間歐洲的獨立化驗所，進行一系列的

老化試驗（例如熱能、化學、濕度、紫外光及動態彎曲應力試驗），模擬正常使用的情況，從而確定現有以聚碳酸酯物料製成的香港智能身份證的可用壽命。兩間化驗所根據 ISO/IEC 24789 *識別卡—卡使用壽命*及 ISO/IEC 10373 *識別卡—測試方法*等國際標準（代表超過十年使用期）進行的測試，均未能確定智能身份證的可用壽命能超過十年。入境處將繼續密切關注市場的發展，並於下一步招標時考慮有關事項。

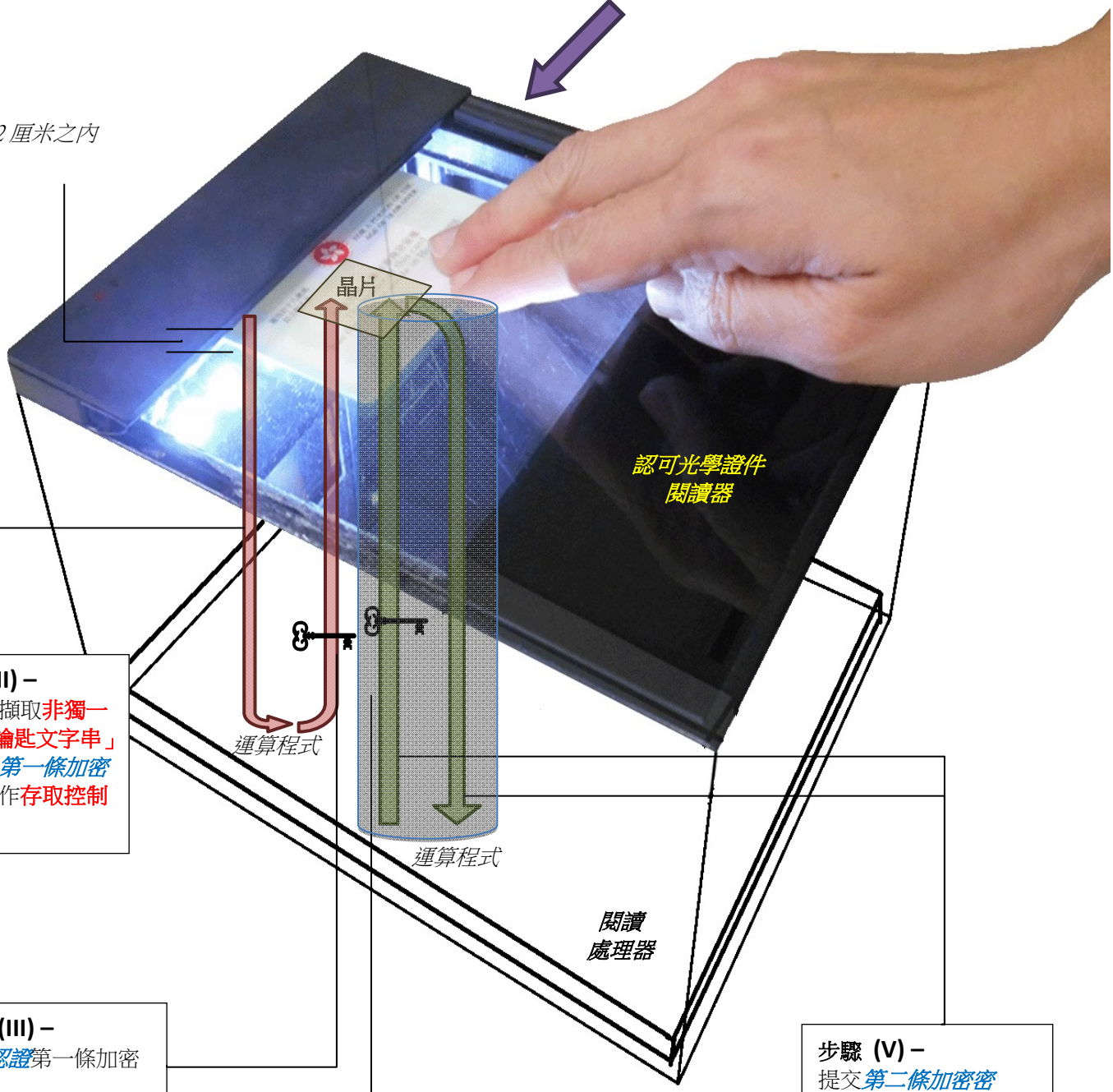
保安局
2015 年 1 月

附件 A

身份證卡面上的非獨一無二「鑰匙文字串」

步驟 (I) –
把智能身份證放在**認可光學證件閱讀器**上

2 厘米之內



步驟 (II) –
閱讀器擷取**非獨一無二「鑰匙文字串」**及產生***第一條加密密匙***以作**存取控制**之用

步驟 (III) –
晶片***認證***第一條加密密匙
(按 ISO14443 標準設計，晶片可支援約 10 厘米範圍內的通訊)

步驟 (IV) –
建立晶片和閱讀器之間的**實時**及**專用加密通訊通道**

步驟 (V) –
提交***第二條加密密匙***，利用**可靠加密技術**在成功***認證***後，開啟加密資料傳送

附件 B

新一代智能身份證系統第一份私隱影響評估
有關智能卡介面、物料及卡身防偽特徵方面的摘要

範疇	可能風險	評估結果/建議
智能卡介面	香港身份證儲存的個人資料可能會被略讀、被竊聽，或遭複製。	經審閱選定的業務系統選擇及功能規格後，我們注意到有關方面建議於讀取儲存於身份證晶片的資料時，採用以下邏輯存取保障措施，例如基本存取控制（Basic Access Control – BAC）及相互認證等。 我們注意到這些邏輯存取保障措施為有效的方法，可防止有人在未經授權下透過非接觸式或接觸式介面讀取儲存於身份證內的個人資料。 我們建議入境處在新一代智能身份證系統的較後階段，應就建議採用的邏輯存取保障措施的有效性進行評估。 我們亦建議入境處在設計和推行新一代智能身份證系統期間，繼續密切留意邏輯存取保障措施技術的最新發展。 **並無察覺違反保障資料原則的情況。**
智能卡介面	如雙重介面的身份證的非接觸式介面遭入侵，原本只可經接觸式介面讀取的敏感個人資料可能會經非接觸	由於雙重介面的身份證只使用同一套晶片，如無妥善監控，若非接觸式介面遭入侵，原本只可經接觸式介面讀取的敏感個人資料可能會經非接觸式介面外洩。 經審閱選定的業務系統選擇及功能規格後，我們注意到有關方面建議身份證晶片採用雙重介面，並採用邏輯存取保障措施，例如基本存取控制及相互認證等，以防止非接觸式

範疇	可能風險	評估結果/建議
	式介面外洩。	介面遭入侵。 我們注意到這些邏輯存取保障措施為有效的方法，可防止有人在未經授權下透過非接觸式介面讀取儲存於身份證內的個人資料。 **並無察覺違反保障資料原則的情況。**
智能卡物料／卡身防偽特徵	身份證遭偽造而令其安全性降低。	經審閱選定的業務系統選擇後，我們注意到有關方面建議於身份證的卡身上採用多種防偽特徵，以防身份證遭偽造。 <u>身份證現時已有的防偽特徵：</u> 1. 扭索式圖案 2. 光學變色油墨 3. 浮雕 4. 彩虹印刷 5. 多重激光影像 6. 縮微文字印刷 7. 紫外線圖案 8. 在持證人照片上的隱置個人圖像 <u>考慮用於新一代智能身份證系統的新防偽特徵：</u> 1. 透視窗 2. 全息圖效果 3. 透鏡狀效果 4. 彩色紫外線圖案 我們注意到建議採用的物料為可使用激光刻蝕的聚碳酸酯物料，可在卡身加上有關的防偽特徵。 我們於檢討有關智能卡物料及卡身防偽特徵的各種現有做法後，注意到德國身份證可用作基準。德國身份證於 2010 年 11 月推出，

範疇	可能風險	評估結果/建議
		卡身內置無線射頻識別(RFID)晶片。此外，有關智能卡物料／卡身的防偽特徵方面，並無發現重大問題。 我們建議在較後階段，入境處在卡身採用先進的防偽特徵(須採用多層式，及其物料能以激光刻蝕防偽特徵，例如採用可行性研究建議的聚碳酸酯物料)，並進行測試，以確保卡身已恰當地設有所需的防偽特徵。 **並無察覺違反保障資料原則的情況。**

附件 C

章：	177A	標題：	**《人事登記規例》**	憲報編號：	9 of 2003
附表：	1	條文標題：	**各式樣身分證的內容**	版本日期：	12/05/2003

[第 2(1)、4A、5、11A 及 12(1B)條]

(2003 年第 9 號第 20 條)

1. 每張身分證須包括—

(a) 申請人姓氏及個人名字的英文或中英文全寫；

(b) 中文字的商用電碼(如適用的話)；

(c) 申請人的出生日期；

(d) 作識別用途的編號；

(e) 該證的發出日期；

(f) 申請人照片(申請人不足 11 歲者除外)； (2003 年第 9 號第 20 條)

(g) 處長決定的代表本條例第 7(2A)(b)條所指的訂明資料、詳情或數據的數據、符號、英文字母或號碼；及 (2003 年第 9 號第 20 條)

(h) 以數據形式儲存於身分證內的晶片內的—

(i) 根據第 4(1)(a)條套取的申請人的拇指指紋或其他手指的指紋的模版；及

(ii) (凡申請人沒有香港居留權)根據《入境條例》(第 115 章)第 11 條就申請人施加的逗留條件(包括逗留期限)。 (2003 年第 9 號第 20 條)

章：	177A	標題：	**《人事登記規例》**	憲報編號：	9 of 2003
附表：	5	條文標題：	**第 4A 條所提述的目的、資料、詳情及數據**	版本日期：	12/05/2003

[第 4A 及 12(1B)條]

第 1 欄	第 2 欄
目的	資料、詳情及數據
1. 儲存由郵政署署長發出的《電子交易條例》(第 553 章)第 2(1)條所界定並根據該條例第 22 條獲認可的證書。	由郵政署署長發出的《電子交易條例》(第 553 章)第 2(1)條所界定並根據該條例第 22 條獲認可的證書。

(附表 5 由 2003 年第 9 號第 22 條增補)

(1A) 任何人無合法權限或合理辯解而—

(a) 儲存數據於晶片內；

(b) 取覽任何儲存於晶片內的數據；

(c) 除去、取消或改動儲存於晶片內的任何數據，或對該等數據作出增補；或

(d) 令晶片失效，

即屬犯罪。 (2003 年第 9 號第 14 條)

(1B) 就第(1A)款而言，—

(a) 身分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，而取覽儲存於該身分證的內置晶片內的附表 1 指明的數據，則他即屬有合法權限而作出該項取覽；

(b) 如附表 5 指明的數據為某目的而儲存於身分證的內置晶片內，則獲發該身分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。 (2003 年第 9 號第 14 條)

附件 D

經濟合作暨發展組織(經合組織)國家身份證政策

	簽發強制性身份證[註 2]	簽發非強制性身份證[註 3]	並無簽發身份證[註 4]
經合組織成員國[註 1]	- 比利時 - 智利[註 5] - 捷克共和國 - 愛沙尼亞 - 德國[註 5] - 希臘 - 匈牙利 - 以色列 - 韓國 - 盧森堡 - 荷蘭[註 5] - 波蘭 - 葡萄牙 - 斯洛伐克 - 斯洛文尼亞 - 西班牙 - 土耳其	- 奧地利 - 加拿大 - 芬蘭[註 5] - 法國 - 冰島 - 意大利 - 日本 - 墨西哥 - 瑞典[註 5] - 瑞士 - 美國	- 澳洲 - 丹麥 - 愛爾蘭 - 新西蘭 - 挪威 - 英國[註 6]
總數 (34)	**17**	**11**	**6**

註 1 會員國名單載於經合組織的官方網站 www.OECD.org。

註 2 **簽發強制性身份證的國家 -**

獲授權人士可在指明的情況下要求國民出示身份證。出示駕駛執照等其他身份證明文件或可接受。在不同的國家，「強制」一詞可能有不同意思和含意。（來源：維基百科）

註 3 **簽發非強制性身份證的國家 –**

這些國家的官方機構只會向主動申請身份證的國民簽發身份證，

而即使國民沒有官方身份證明文件，也不會觸犯法例。（來源：維基百科）

註 4 **並無簽發身份證的國家** –

這些國家的官方機構不會簽發身份證。如需證明身份時，國民可出示護照、由銀行等簽發的身份證，或一些主要用途不是用作證明身份的文件，例如駕駛執照等。（來源：維基百科）

註 5 **採用非接觸式介面身份證的國家**以灰色標示。這五國的身份證包含非接觸式晶片介面，支援基本存取控制及／或相關技術。

註 6 英國的《2010 年身份證明文件法令》於 2010 年實施後，終止了在該國推行身份證的措施。

參考資料

1. 歐洲聯盟部長理事會網上核證旅遊證件公眾登記冊 http://prado.consilium.europa.eu/EN/8391/docHome.html
2. 維基百科的超連結：http://en.wikipedia.org/wiki/List_of_national_identity_card_policies_by_country
3. 經濟合作暨發展組織官方網站： www.OECD.org