財務委員會討論文件

2015 年 4 月 17 日

基本工程儲備基金
總目 710－電腦化計劃
入境事務處
新分目「新一代智能身份證系統」

請各委員就新一代智能身份證系統批准一筆為數 1,448,786,000 元的新承擔額。

問題

入境事務處(下稱「入境處」)需要開發一套新的電腦系統，即「新一代智能身份證系統」，以取代日漸老化的現有電腦系統，及更有效地支援簽發香港智能身份證(下稱「智能身份證」)的工作。

建議

2. 入境處處長建議就新一代智能身份證系統開立一筆為數 1,448,786,000 元的新承擔額。保安局局長和政府資訊科技總監均支持這項建議。

理由

採用新系統的需要

3. 政府在 2003 年引入現行智能身份證系統。與其他電腦系統一樣，智能身份證系統的設計最佳使用年期約為 10 年。系統在 2000 年代初開發，其軟、硬件快將過時。市場上對過時技術的供應及支援不斷減少，進行系統保養和技術支援越見困難。支援智能身份證系統的核心軟件亦已過時，廠商提供的支援已結束。最近，系統保養服務合約的

期限，已由原來的 2013 年 12 月延長至 2018 年年底。長時間使用過時的技術，將難以確保系統穩健，因此再次延長系統保養服務合約，並不可取。

4. 在缺乏適當及持續的保養與技術支援的情況下，因系統故障而導致主要公共服務(包括登記及印製智能身份證、核實香港特區護照申請人的身份等)出現嚴重而大規模中斷情況的風險將持續增加。我們需要盡快更換現有系統，以確保主要公共服務得以維持正常運作；此舉亦可提供機會滿足將來對新公共服務的需求(例如優化人事登記程序等)。

採用新智能身份證的需要

5. 現時的智能身份證並無有效期限[1]，但按承造商的保證，以及其後由入境處委託進行的獨立測試所確認，身份證物料在正常使用情況下的可使用年期為 10 年。入境處在 2012 年委託兩間歐洲的獨立化驗所，以確定現有智能身份證的可使用年期[2]。兩間化驗所根據國際標準[3]所進行 (即超過 10 年使用期) 的測試，均未能確定智能身份證的可使用年期能超過 10 年。這表示在 2003 年至 2007 年間發出的智能身份證，其可使用年期將在 2013 年至 2017 年間屆滿。雖然這並不代表現有的智能身份證在 10 年可使用年期屆滿時必定會立即損壞或發生故障，但這些智能身份證需要更換的可能性將會隨時日增加。引進新智能身份證以取代所有現有的智能身份證，可避免須應付大批智能身份證在短時間內同時出現故障的情況。否則，入境處未必能在服務承諾訂明時限內處理所有換證申請，為公眾帶來不便。

6. 雖然近年查獲的偽造智能身份證數目維持在低水平，但歐洲已出現類似現有智能身份證物料和防偽特徵的偽造身份證被檢獲的個案。我們預期隨着科技不斷進步，倘若不加入新的防偽特徵和晶片建構技術，偽造智能身份證的個案將可能上升。

---

[1] 德國、比利時、馬來西亞和澳門特別行政區等有關當局所發出的同類型身份證，基於要確保身份證持久耐用等不同原因，均規定須在發出後 5 至 10 年內更換。

[2] 兩間化驗所進行了一系列的老化試驗(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。

[3] 例如為模擬卡使用壽命的方法及有關做法提供指引的「ISO/IEC 24789 識別卡—卡使用壽命」標準，以及為識別卡特徵界定測試方法的「ISO/IEC 10373 識別卡—測試方法」標準。

新一代智能身份證系統的特色

優化人事登記程序

7. 跟現有系統一樣，新一代智能身份證系統將繼續支援智能身份證的登記及印製工作(包括接受申請、進行記錄核查及個案審批、個人資料印製，以及簽發身份證)，以及入境處的其他服務(例如核實香港特區護照申請人的身份)。此外，系統亦可處理其他政策局、政府部門或公營機構按法例規定提出核實個人資料以作指定用途的要求。視乎詳細系統設計而定，新一代智能身份證系統將優化人事登記程序，為公眾帶來更大的方便。藉着引入新系統，部門可推出新措施[4]如網上填表服務、審批申請中的自動記錄查核及設有電子儲存櫃的自助領取證件服務站等。

加強身份證的防偽特徵

8. 新智能身份證將採用最先進的聚碳酸不碎膠物料，以確保外觀更佳，提高文字印刷質素，並提升智能身份證在正常使用情況下的耐用程度。隨着科技進步，我們亦會把握機會，加強卡面防偽特徵，使新智能身份證保持低偽證率[5]。

9. 現有的智能身份證只可支援接觸式介面，使用者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。利用經驗證的晶片技術，令資料讀取更快捷，晶片損耗亦更少，故政府建議推出額外的「非接觸式」晶片介面(晶片無需直接與讀卡器接觸)。有關介面採用近距離無線傳送技術，並具有多重保安特徵。

---

[4] 網上填表服務讓申請人能在任何地點通過互聯網填妥智能身份證的申請表格，而無須親身前往人事登記辦事處或換證中心填寫表格。這能縮短申請人於人事登記辦事處或換證中心辦理申請時所需的處理時間。自動記錄核查能協助登記主任進行自動而非人手的記錄核查，從而減少登記過程所需的時間。設有電子儲存櫃的自助領取證件服務站讓申請人能在安裝了自動證件分發器的領件站領取新的智能身份證，讓申請人可無須與登記辦事處預約，亦可自行領取新證。

[5] 可參考其他司法管轄區用於類似身份證的一些最新防偽特徵，包括透明窗口、全息圖效果、透鏡狀技術、彩色紫外線印刷等。

10. 建議的新「非接觸式」晶片介面將嚴格按照 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。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，防止晶片資料不會在「沒有持證人的同意下」或被「隔空」讀取，讀取晶片資料只可由持證人啟動。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。此外，整個通訊及資料傳送過程必須加密。

11. 跟現有的智能身份證晶片一樣，建議的新智能身份證晶片將不附設獨立電池，並且不能自行傳送任何訊號。如欲透過「非接觸式」晶片介面讀取晶片資料，必須由持證人啟動。持證人必須取出智能身份證，並將其放在獲授權的光學證件閱讀器上，以光學方法從卡面擷取「鑰匙文字串」(就跟拍照一樣，通常稱為基本存取控制 Basic Access Control)。有關認可閱讀器成功擷取「鑰匙文字串」後，閱讀器內置的特定運算程式將產生一條實時的一次性加密密匙。然後，加密密匙須由晶片認證，並要求晶片建立一對一的專用加密通訊通道。閱讀器須產生第二條不同的密匙，再經晶片進行相互認證後，方可讀取晶片所儲存的資料。

12. 由於使用認可的閱讀器以光學方法成功擷取印在卡面的「鑰匙文字串」是啟動晶片近距離無線傳送功能的「先決條件」，故此持證人可全權掌控是否把證件直接放在閱讀器上以啟動資料傳送功能。如持證人未有自行取出智能身份證，或經證書授權的特定閱讀器內沒有加密密匙，便不可能透過「非接觸式」晶片介面讀取晶片資料。

13. 有關建議採用的新「非接觸式」晶片介面的多重保障的詳細資料，
附件1 載於附件 1。

個人資料私隱保障

14. 除了上述設計上的多重保安特徵外，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資料有嚴格的規定，亦對使用或收集人事登記資料設有嚴格的規管。

15. 《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《人事登記規例》附表 1 指明的數據，則他即屬有合法權限而作出該項取覽，現時有關設施包括－

由入境處全權控制的入境事務設施

(a) e-道；

(b) 申請電子護照自助服務站；

(c) 澳門 e-道自助登記服務機；

(d) 智能身份證自助服務站；

在多用途智能身份證計劃下，須得到持證人同意的非入境事務設施[6]

(e) 公共圖書館服務；

(f) 康體通自助服務站；

(g) 醫健通系統；以及

(h) 公私營醫療合作－醫療病歷互聯試驗計劃。

16. 此外，《人事登記規例》第 12(1B)(b)條亦規定，如《人事登記規例》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》或香港任何其他法律的其他法律條文，均沒有賦予任何人同樣的合法權限取覽儲存於身份證內置晶片內的數據。

---

[6] 持證人如欲使用相關設施，必須把智能身份證插入讀卡機讀取晶片，按照《人事登記規例》第 12(1B)(a)條的授權閱讀晶片內的資料，並向相關設施提交這些資料，以使用各種公共服務。

17. 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(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。建議的新智能身份證的新晶片介面將受相同的法律條文規管。

18. 入境處將會委聘獨立的專家和顧問，確保在項目發展及將來推行的每個不同階段設有各種所需的保障，以符合有關個人資料保障及系統保安的法律規定。

19. 參考推行第一代智能身份證系統時的經驗，入境處會於推行新一代智能身份證系統的每一個關鍵階段(包括可行性研究、系統分析和設計、推行前及推行後等)，委託合資格的獨立顧問進行私隱影響評估，然後將每份私隱影響評估報告提交個人資料私隱專員公署(下稱「公署」)，讓公署就報告內容提供意見，以確保符合《個人資料(私隱)條例》(第 486 章)下的保障資料原則及其他規定。入境處會在下一個階段採納顧問和公署的建議(如有)，令推行新一代智能身份證系統的工作更為妥善。

20. 第一次私隱影響評估已在 2014 年 10 月完成。完成評估的顧問認為建議的存取保障措施及相互認證能有效防止智能身份證內儲存的個人資料透過非接觸式介面被非法讀取。顧問在第一次私隱影響評估中，就身份證介面、物料和卡身保安特徵等方面的技術評估和建議的摘要，載於附件 2。入境處已將第一份私隱影響評估報告提交公署，並會將公署的意見納入推行項目的下一個階段。

附件2

21. 除進行私隱影響評估外，入境處亦會委聘獨立的審計人員，在推行的不同階段，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智能身份證的保安措施能有效保護相關資料。

22. 入境處將會在項目推行期間，定期進行循規檢查，並預計在 2022 年全港市民換領身份證計劃完成後，委聘獨立顧問再進行私隱循規審核。

效益

23. 新一代智能身份證系統連同新智能身份證將有以下效益－

(a) **讓入境處在未來 10 年可維持現有的有效運作，避免可能出現的大規模系統故障**而嚴重擾亂人事登記程序，以及避免大量香港身份證出現故障；

(b) **利用最新科技作更快捷的資料檢索，並且減少晶片損壞**，從而**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 秒大幅減至 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%[7]。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)，故增加旅客流量對整體社會帶來莫大益處；

(c) **核實身份的程序更安全準確**，因新晶片的容量更大，能夠儲存解像度更高的相片影像(以支援容貌辨認技術，和提供平台作指紋核實 [8]以外的生物特徵認證之用)和最新的指紋模板，令核實身份的程序更安全準確；

(d) **加強智能身份證的防偽特徵**，以確保新智能身份證能在未來 10 年科技日新月異的情況下仍能**保持低偽證率**。新智能身份證將有更佳的外觀，卡面上的文字印刷質素更高，在正常使用情況下更耐用；以及

---

[7] 現時，每條 e-道平均每分鐘可處理 5 名身份證持有人(60 秒／12 秒)。引入新晶片介面的新智能身份證後，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%。

[8] 雖然指紋核實仍是非常有效的生物特徵認證技術，但一些身份證持有人卻因指紋細淺或模糊，而未能使用有關技術。同時，現有的智能身份證晶片所載的數碼相片因大小限制而未能支援容貌辨認技術。

(e) 透過提升老化的軟、硬件，以**提高系統的能力，應付可能出現的新公共服務需求**，包括推行各種新措施，例如網上填表服務、設有電子儲存櫃的自助領取證件服務站及自動記錄查核等，優化人事登記工作的程序。此外，政府資訊科技總監辦公室現正另行進行技術研究[9]，檢討智能身份證在多用途智能身份證計劃下的其他可行用途。

節省的成本及減免開支

24. 採用新一代智能身份證系統，入境處將能應付未來 10 年的服務需求，提升為市民提供的服務質素，更可節省成本和減免開支，細節如下－

(a) 由 2017-18 年度至 2022-23 年度累積減免 31 億 6,391 萬元的非經常開支，這是因無須支付升級現有系統以維持現有運作的費用及人手資源的開支而可減免的開支；

(b) 在 2018-19 年度及由 2019-20 年度起分別減免 1,279 萬元及 2,823 萬元的經常開支，這是因無須支付上文(a)項升級現有系統的額外經常保養開支而可減免的開支；

(c) 減免經常員工開支，減幅由 2017-18 年度的 82,000 元增至由 2026-27 年度起的 176 萬元，這是因無須支付預計因使用經升級的現有系統所產生的額外工作流程及其增加的工作量的員工費用而可減免的開支；

(d) 在 2017-18 年度、2018-19 年度及由 2019-20 年度起，分別可節省 814 萬元、3,910 萬元及 4,564 萬元的可變現經常開支，這是因無須支付每年採購現有智能身份證及保養現有系統的所需費用而可節省的開支；以及

---

[9] 政府資訊科技總監辦公室的技術研究將就多用途新智能身份證的結構和框架作出檢討和建議，包括找出應存入新智能身份證的新資料、探討新增值服務，以及就現有的智能身份證用途提出過渡安排和遷移策略。在推出任何新應用功能時，政府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，以及籌劃和實行保護數據及保障私隱的措施。

(e) 理論上在 2017-18 年度及由 2018-19 年度起，分別可節省 409,000 元及 163 萬元的經常開支，這是因推行新一代智能身份證系統中設有電子儲存櫃的自助領取證件服務站而理論上每年可節省的員工費用。

附件3 25. 有關推行新一代智能身份證系統的成本效益分析，載於附件 3。

對財政的影響

非經營開支

26. 我們估計新一代智能身份證系統在 2015-16 至 2022-23 8 個財政年度內涉及非經營開支合共 1,448,786,000 元。有關的分項數字如下－

(千元)

	項目	**2015-2016**	**2016-2017**	**2017-2018**	**2018-2019**	**2019-2020**	**2020-2021**	**2021-2022**	**2022-2023**	合計
(a)	硬件	-	11,844	22,761	192,999	18,760	20,465	20,465	3,411	290,705
(b)	軟件	-	5,103	8,779	73,905	7,839	8,552	8,552	1,426	114,156
(c)	通訊網絡	-	-	547	2,982	3,058	3,058	3,058	255	12,958
(d)	推行系統、合約員工及顧問服務	483	12,493	40,555	108,002	-	-	-	-	161,533
(e)	智能卡	-	-	33,405	112,200	112,200	112,200	112,200	-	482,205
(f)	場地準備及場地	-	-	63,103	66,384	26,000	26,000	26,000	12,760	220,247
(g)	宣傳	-	-	1,816	3,661	4,004	4,204	2,649	2,040	18,374
(h)	消耗品及雜項	-	-	-	3,872	4,224	4,224	4,224	353	16,897
(i)	應急費用	49	2,944	17,097	56,401	17,609	17,871	17,715	2,025	131,711
	合計	**532**	**32,384**	**188,063**	**620,406**	**193,694**	**196,574**	**194,863**	**22,270**	**1,448,786**

27. 關於上文第 26 段(a)項，2 億 9,071 萬元的預算開支是用以購置電腦硬件，例如伺服器、工作站、儲存裝置、網絡設備、身份證印製機，以及自助服務站等。

28. 關於上文第 26 段(b)項，1 億 1,416 萬元的預算開支是用以購置系統軟件、應用軟件及套裝。

29. 關於上文第 26 段(c)項，1,296 萬元的預算開支是用以支付換領身份證計劃的設置成本及通訊網絡的租用費。

30. 關於上文第 26 段(d)項，1 億 6,153 萬元的預算開支是用以僱用外間服務供應商和合約員工，以進行系統分析和設計、開發、測試、安裝及培訓等服務。有關開支亦包括僱用顧問，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，以及資訊科技保安風險評估及保安審計等顧問研究。

31. 關於上文第 26 段(e)項，4 億 8,221 萬元的預算開支是用以購買約 9 455 000 張特製的空白智能卡，其中 880 萬張卡會用於換領身份證計劃，55 000 張會用於系統測試，600 000 張則會用於應付人事登記辦事處在推行新智能身份證後首年的需要。

32. 關於上文第 26 段(f)項，2 億 2,025 萬元的預算開支是用以進行場地準備工程，包括 9 個身份證換證中心[10]、5 個現有的人事登記辦事處、1 個身份證印製中心[11]及電腦房設施，以及支付身份證換證中心的租金。

33. 關於上文第 26 段(g)項，1,837 萬元的預算開支是社區宣傳活動所需的宣傳費用，宣傳內容是向市民提供新智能身份證及換領身份證計劃的詳情。

34. 關於上文第 26 段(h)項，1,690 萬元的預算開支是用以購買換證中心的消耗品及雜項物品，以及人事登記辦事處初期使用的消耗品，包括打印機碳粉，以及支付政府一般服務的費用等。

---

[10] 考慮到現有的 5 個入境處人事登記辦事處在處理日常登記工作方面的最高服務量和工作量，入境處估計，需要在全港設立額外 9 個換證中心，方可應付一次性全港換領身份證計劃的工作。

[11] 身份證印製中心是為每位香港身份證持有人製造個人化身份證的場地。個人化的程序包括將數據載入晶片、印製，以及將個人肖像及其他資料刻蝕於卡面上等。

35. 關於上文第 26 段(i)項，1 億 3,171 萬元的預算開支是應急費用，款額相等於第 26 段(a)至(h)項開支的 10%。

經常開支

36. 我們估計有關項目在 2017-18 年度涉及的全年經常開支將為 175 萬元，到 2018-19 年度將增至 5,906 萬元，而由 2019-20 年度起將進一步增至 8,444 萬元，當中包括硬件及軟件的保養維修、智能卡、日常支援服務、通訊網絡費用、消耗品及服務費。這些開支會在相關年度的預算中反映，有關的分項數字如下－

		(千元)	
項目	**2017-18**	**2018-19**	**2019-20 和以後每個年度**
(a) 硬件保養維修	-	5,037	20,147
(b) 軟件保養維修	-	2,675	10,698
(c) 智能卡	-	30,600	30,600
(d) 日常支援服務	-	13,735	15,985
(e) 通訊網絡	1,253	5,009	5,009
(f) 消耗品	365	1,457	1,457
(g) 服務費	136	543	543
總計	**1,754**	**59,056**	**84,439**

37. 關於上文第 36 段(a)項，每年 2,015 萬元的預算開支是用於提供硬件保養維修，以維持系統的運作。

38. 關於上文第 36 段(b)項，每年 1,070 萬元的預算開支是用以支付軟件的保養維修和使用證費用，以維持系統的運作。

39. 關於上文第 36 段(c)項，每年 3,060 萬元的預算開支是用以購買 600 000 張新的空白智能卡，以應付人事登記辦事處現時的每年使用量。

40. 關於上文第 36 段(d)項，每年 1,599 萬元的預算開支是用於提供系統的日常支援服務。

41. 關於上文第 36 段(e)項，每年 501 萬元的預算開支是用以支付通訊網絡的租用費。

42. 關於上文第 36 段(f)項，每年 146 萬元的預算開支是用於購置打印機碳粉等消耗品。

43. 關於上文第 36 段(g)項，每年 543,000 元的預算開支是用以支付政府一般服務的費用。

一次性全港市民換領身份證計劃

44. 參考上一次換領身份證計劃，政府將會在 2018 年至 2022 年進行一次性全港市民換領身份證計劃，有序地分階段為所有香港身份證持有人更換現有的智能身份證[12]。這樣的安排，可盡量減輕一旦大量身份證發生故障，令公共服務受到延誤，及影響前線執法工作而造成的損害。倘擬議的換證計劃在 2018 年展開，入境處預計在為期 4 年的計劃中，將更換 880 萬張智能身份證。

45. 一支由內部人員和合約員工組成的專責隊伍將負責籌備和推行身份證換領計劃。根據我們最新的估算，這隊伍在 2016-17 至 2022-23 年度的預算員工開支約為 15 億元。一如上次身份證換領計劃的安排，入境處將檢討人手需求，並把上述預算開支納入相關年度的預算內。

推行計劃

46. 我們計劃按照下述時間表推行擬議的項目－

[12] 一如上次身份證換領計劃的做法，指定組別的香港身份證持有人(例如以出生年份劃分)將分批獲邀更換其智能身份證。

工作	預定完成日期
採購硬件、軟件和服務	2016 年第一季
開發及推行系統：	
系統分析及設計	2016 年第三季
系統開發	2017 年第二季
用戶驗收測試	2017 年第四季
場地準備工程	2018 年第二季
培訓	2018 年第二季
系統啟用	2018 年第一季

47. 新一代智能身份證系統推出後，換領身份證計劃將隨即在 2018 年第二季推行，為期 4 年。

公眾諮詢

48. 我們在 2015 年 1 月 6 日就上述建議諮詢立法會保安事務委員會。就委員的提問，我們提供了新智能身份證在保安及私隱保障方面的補充資料。委員會在 2015 年 2 月 3 日及 3 月 3 日的會議上作進一步討論，原則上支持將這項建議提交財務委員會。

背景

49. 根據《人事登記條例》及《人事登記規例》，在香港境內的人，除非獲豁免，或被排除於有關條文以外，否則必須領取身份證[13]。政府在 2003 年引入現行智能身份證系統，並在 2003 年至 2007 年推行全港

[13] 《人事登記條例》及《人事登記規例》規定，在香港境內的人，除非獲有關法例豁免或被排除於有關法例以外，例如短期逗留旅客、11 歲或以下的小童、年老人及體弱人士，否則必須領取身份證。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 16 個成員國(即所有簽發身份證成員國的 57%)備有特定的法定要求，讓獲授權人士可要求國民出示身份證。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。

市民換領身份證計劃，為所有身份證持有人換發(現時的)聚碳酸不碎膠智能身份證，以取代之前的電腦紙本身份證。現時大約有 900 萬張智能身份證正在使用。

50. 智能身份證系統是一個連線作業的電腦系統，用以支援智能身份證的登記及印製工作[14]，以及入境處的其他服務(例如核實香港特區護照申請人的身份等)。此外，系統亦可處理其他政策局或政府部門按法例提出核實個人資料以作指定用途的要求(例如警方用作核實身份及身份證是否有效，以及自動核實衞生署長者醫療券計劃申請人的登記及個人資料等)。

51. 現時的智能身份證以聚碳酸不碎膠製成，並置有接觸式晶片；持證人的個人資料以激光技術刻蝕於卡面，其指紋模板及面部影像則經加密技術保護後儲存於內置晶片內。透過指紋識別技術，入境處可核實持證人的身份，讓持證人以自助方式在各出入境管制站使用 e-道辦理出入境手續。此外，在政府資訊科技總監辦公室統籌的多用途智能身份證計劃下，持證人可將個人電子證書儲存於智能身份證晶片內，以便根據《電子交易條例》(第 553 章)進行商業或其他電子交易。持證人也可藉多用途智能身份證計劃使用其他政府服務，例如圖書證服務、預訂康樂設施、「醫健通」系統服務，以及醫療病歷互聯計劃。

52. 入境處於 2010 年 3 月委聘顧問為部門進行第三代資訊系統策略檢討。顧問公司在有關檢討完成後所提出的建議，包括推行新一代智能身份證系統，以解決現行系統軟、硬件過時的問題，以及應付新業務需要。第三代資訊系統策略檢討中提出了 8 個策略性資訊科技項目，這些項目會有系統地推行，新一代智能身份證系統屬當中的一部分。第三代資訊系統策略的 8 個項目如下－

(a) 新資訊科技基建設施[15]；

(b) 出入境管制系統[16]；

---

[14] 包括接受申請、核查記錄、審批個案、個人資料印製，以及簽發智能身份證。.

[15] 在 2011 年 12 月 9 日獲批准撥款 8 億 6,220 萬元，用以發展此項目(見 FCR(2011-12)56 號文件)。

[16] 在 2013 年 2 月 8 日獲批准撥款 9 億 1,222 萬元，用以發展此項目(見 FCR(2012-13)67 號文件)。

(c) 新一代智能身份證系統；

(d) 新一代電子護照系統；

(e) 簽證自動化系統；

(f) 個人證件個案決策支援系統；

(g) 調查個案處理系統；以及

(h) 人力資源管理系統。

53. 第三代資訊系統策略的 8 個項目互為關連，對入境處的關鍵業務運作亦屬不可或缺，因此全面推行所有項目極其重要，可取得協同效應，確保入境處服務的可持續性。推行第三代資訊系統策略亦會帶來契機，使整個部門提供的服務都得以改善。

保安局
2015 年 4 月

建議的新晶片介面的多重保障
補充資料

引言

建議的新晶片介面將會採用下文詳述的多重保安措施，以加強保護新智能身份證的資料。

保安特徵

依照為保密文件所訂的 ISO 標準設計的新晶片

2. 無線射頻識別（RFID）[1]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(例如追蹤貨物)、支援可達數百米範圍內的遠距離通訊，但通常對儲存資料只有很少甚或沒有任何保護的其他無線射頻識別標準和應用，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

3. 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，並須經過相互認證；以及

(c) 整個通訊及資料傳送過程必須加密。

---

[1] 無線射頻識別（RFID）廣泛涵蓋多種符合個別標準的無線通訊裝置。

4. 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[2](下稱「閱讀器」)，將身份證上印有「鑰匙文字串[3]」(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 1 條隨機加密密匙；

(II) 如認可閱讀器成功擷取「鑰匙文本串」(一如電腦掃描器擷取資料)，閱讀器就會根據所擷取的「鑰匙文本串」以及認可閱讀器的特定運算程式產生 1 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途徑後，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。

附錄 以上步驟的示意圖載於附錄。

5. 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。下文講述這些措施重點。

---

[2] 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。

[3] 「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。

(A) 無線通訊的存取控制

6. 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，若證件存放在錢包、銀包、衣物內，或是以其他方法隱藏起來，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)在距離認可閱讀器 2 厘米內，「鑰匙文字串」仍然無法被成功擷取，加密過程及隨後的無線通訊亦不會啟動(即停留在上文的**步驟 I**)。

7. 上述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)，亦已面世[4]。入境事務處(下稱「入境處」)將確保新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

8. 為提供額外保障，在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「鑰匙文字串」產生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

9. 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[5]，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

---

[4] 某些國家(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)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。

[5] 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 6 位數字號碼作為「鑰匙文字串」。

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

10. 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。

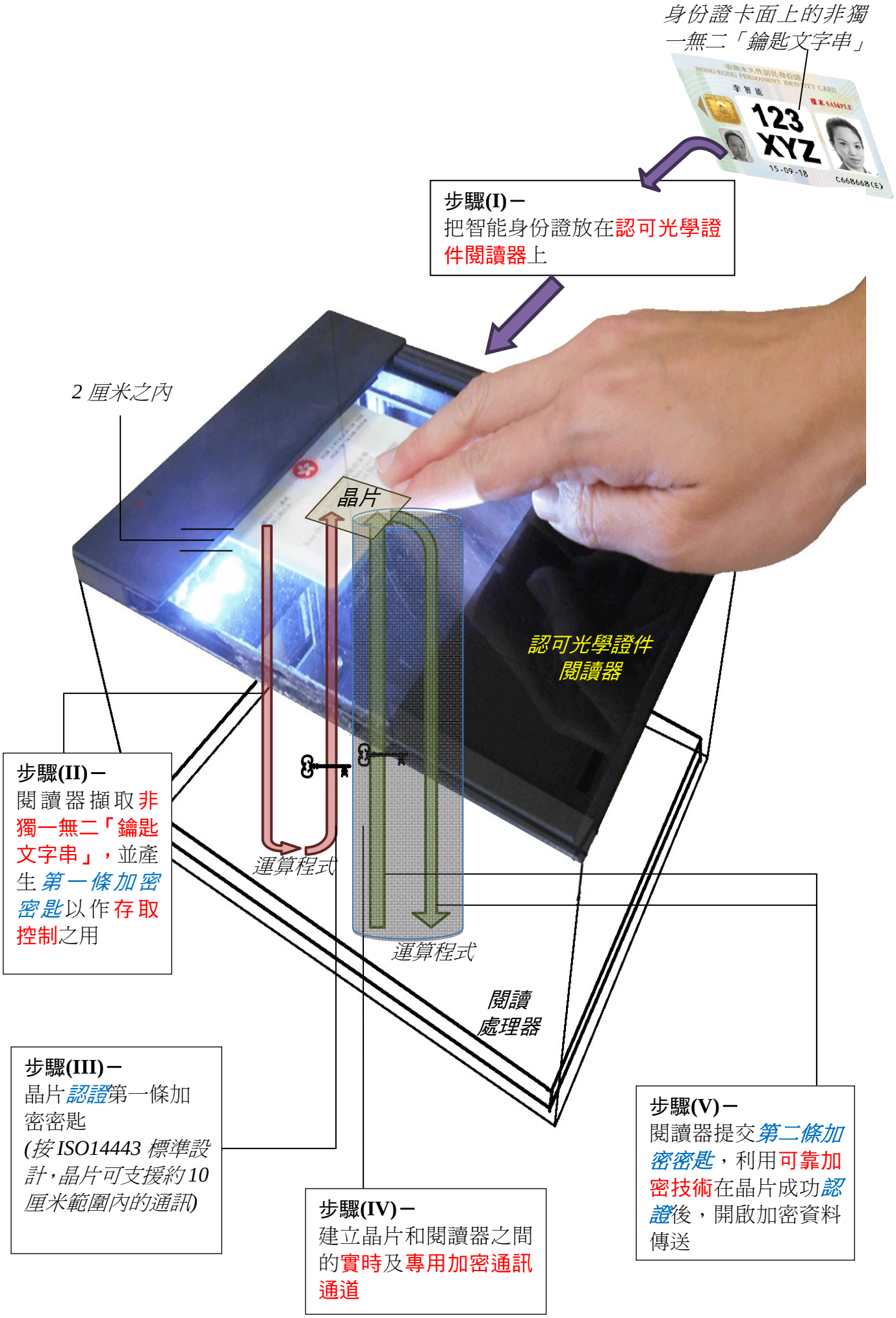
(E) 專用通訊通道

11. 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

12. 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，在多個司法管轄區已廣泛採用，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。

附錄


身份證卡面上的非獨一無二「鑰匙文字串」
123
XYZ
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
晶片
認可光學證件閱讀器
運算程式
運算程式
閱讀處理器
步驟(II)－
閱讀器擷取非獨一無二「鑰匙文字串」，並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)－
閱讀器提交第二條加密密匙，利用可靠加密技術在晶片成功認證後，開啟加密資料傳送

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。**

範疇	可能風險	評估結果／建議
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式介面外洩。	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在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

範疇	可能風險	評估結果／建議
		考慮用於新一代智能身份證系統的新防偽特徵－ 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。德國身份證在 2010 年 11 月推出，卡身內置無線射頻識別晶片。此外，在智能卡物料／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，而物料則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，以確保卡身恰當地具有所需的防偽特徵。 **並無察覺違反保障資料原則的情況。**

推行新一代智能身份證系統的成本效益分析

(千元)

	2015-16	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27	2027-28	總計
費用														
非經常														
非經營開支	532	32,384	188,063	620,406	193,694	196,574	194,863	22,270	-	-	-	-	-	1,448,786
員工開支	14,956	39,330	38,840	219,211	235,236	235,236	235,236	19,603	-	-	-	-	-	1,037,648
合約員工開支				110,088	120,096	120,096	120,096	10,008						480,384
小計	15,488	71,714	226,903	949,705	549,026	551,906	550,195	51,881	-	-	-	-	-	2,966,818
經常														
開支	-	-	1,754	59,056	84,439	84,439	84,439	84,439	84,439	84,439	84,439	84,439	84,439	820,761
員工開支	-	-	-	-	-	-	-	-	-	-	-	-	-	-
小計	-	-	1,754	59,056	84,439	84,439	84,439	84,439	84,439	84,439	84,439	84,439	84,439	820,761
費用總額	**15,488**	**71,714**	**228,657**	**1,008,761**	**633,465**	**636,345**	**634,634**	**136,320**	**84,439**	**84,439**	**84,439**	**84,439**	**84,439**	**3,787,579**
節省款額														
非經常														
減免的開支	-	-	242,961	938,191	641,124	641,324	639,769	60,542	-	-	-	-	-	3,163,911
小計	-	-	242,961	938,191	641,124	641,324	639,769	60,542	-	-	-	-	-	3,163,911
經常														
減免的開支	-	-	-	12,788	28,226	28,226	28,226	28,226	28,226	28,226	28,226	28,226	28,226	266,822
減免的員工開支	-	-	82	327	327	327	327	327	532	1,218	1,517	1,763	1,763	8,510
可變現的節省款額	-	-	8,141	39,100	45,637	45,637	45,637	45,637	45,637	45,637	45,637	45,637	45,637	457,974
理論上可節省的款額	-	-	409	1,634	1,634	1,634	1,634	1,634	1,634	1,634	1,634	1,634	1,634	16,749
小計	-	-	8,632	53,849	75,824	75,824	75,824	75,824	76,029	76,715	77,014	77,260	77,260	750,055
節省總額	-	-	**251,593**	**992,040**	**716,948**	**717,148**	**715,593**	**136,366**	**76,029**	**76,715**	**77,014**	**77,260**	**77,260**	**3,913,966**
節省淨額	**-15,488**	**-71,714**	**22,936**	**-16,721**	**83,483**	**80,803**	**80,959**	**46**	**-8,410**	**-7,724**	**-7,425**	**-7,179**	**-7,179**	**126,387**
累計節省淨額	**-15,488**	**-87,202**	**-64,266**	**-80,987**	**2,496**	**83,299**	**164,258**	**164,304**	**155,894**	**148,170**	**140,745**	**133,566**	**126,387**	**-**