二零零二年七月四日
討論文件

立法會保安事務委員會

香港特區身分證計劃
最新發展及第二次私隱影響評估報告

引言

本文件旨在向議員匯報香港特區身分證計劃的最新進展及第二次私隱影響評估報告的結果和建議。

背景

2. 在二零零二年四月九日的會議上，當局告知議員，把舊有的縮微膠卷身分證紀錄和一些舊式紙張索引卡轉換為電子影像的工作進展順利，而新智能式身分證電腦系統的系統分析和設計工作亦已展開。此外，兩項顧問研究(即第二次私隱影響評估和智能式身分證電腦系統保安檢討)也在進行中。我們並就第二期計劃的財政需求徵詢議員的意見。財務委員會已於二零零二年五月十日批准第二期的撥款。

最新發展

紀錄轉換工作

3. 紀錄轉換工作正按照計劃順利進行。截至二零零二年六月二十二日，約有 53%於一九八七年六月後簽發的身分證的紀錄，已由縮微膠卷轉換至數碼影像。我們有信心，紀錄轉換工作可如期完成，換言之，一九八七年七月一日開始簽發的身分證的紀錄，可於二零零三年五月新身分證面世前全部數碼化。

系統分析、設計和發展

4. 系統分析和設計工作如期於二零零二年四月底完成。承辦商隨即開始進行系統程式發展細節工作，包括原型開發及單元測試。我們期望系統發展工作會於二零零二年十月/十一月完

成，之後便會進行用戶驗收測試。我們同時亦正為購置預約系統和派籌系統的招標工作作最後籌備工作。另外，在政府產業署的協助下，我們正積極物色設立九間新身分證簽發辦事處的合適地點。

5. 智能式身分證電腦系統的承辦商與保安顧問和資料私隱顧問進行多次討論後，參照了兩位顧問的建議，修改了系統的設計。我們信納，最新的系統設計已能完全符合標書所訂的保安及資料私隱要求。

保安檢討

6. 保安顧問已就智能式身分證電腦系統的保安措施進行全面研究。研究範圍涵蓋系統各方面的情況，包括網絡及通訊、數據資料、應用程式、防止擅用系統措施、晶片及智能卡運作系統、智能卡讀卡設備、發卡後載入及取消卡上用途的安排、邏輯保安、實體保安、所採用的設計原則，以及保安及風險管理。承辦商已採納有關建議，而保安顧問亦已證實，以現今的技術水平來說，承辦商現制訂的智能式身分證電腦系統最新模式，穩妥安全。

第二次私隱影響評估

7. 第二次私隱影響評估報告包括智能式身分證電腦系統的概覽，以及評估技術設計如何回應首次私隱影響評估報告提出的主要資料私隱建議。報告確認智能式身分證電腦系統 中已加入一些主要管制措施，以減低第一次私隱影響評估報告所提出可能存在的私隱風險，詳情載於附件 I。對於因技術限制或業務因素而需要作出的主要設計改動(例如，礙於記憶體和處理速度的限制，卡內的處理器不能比較指紋模版，未能附合第一次私隱影響評估報告所建議的最理想設計)，報告也建議了適當的輔助管制措施，以減低資料私隱外洩的風險。評估報告並進一步提出一些可能引起私隱關注的系統設計問題和建議解決方法。最後，報告提議在人手程序加入數項保障資料措施。整體而言，資料私隱顧問認為，智能式身分證電腦系統的承辦商已能充分掌握私隱事宜，並已採取適當的保障資料措施，保障個人資料的私隱。

8. 第二次私隱影響評估報告的建議摘要載於附件 II，首次私隱影響評估報告所提建議的最新情況載於附件 III。我們已把第二次私隱影響評估報告和上述兩個附件送交個人資料私隱專員審議，並與專員討論了報告的建議摘要。私隱專員的意見和政府的回應已一併載列於附件 II。

保安局
二零零二年六月二十七日

智能式身分證電腦系統
如何處理首次私隱影響評估
提出的主要私隱風險

私隱外洩風險	減低私隱外洩風險的管制措施
智能式身分證可能會被用來儲存持證人不知情的資料	■ 身分證持有人會獲告知儲存於其智能式身分證內用作出入境事務用途的個人資料。持證人可使用自助資訊服務站，查看用作出入境事務用途所儲存的個人資料和與出入境事務無關的其他資料(目前只有電子證書)。 ■ 是否加入和使用與出入境事務無關的其他用途，完全由身分證持有人決定。如要在智能式身分證內加入與出入境事務無關的其他用途，必須得到持證人授權批准。 ■ 香港法例訂明身分證的內容。除非作出法例修訂，否則不得在身分證(晶片和卡面)載入額外資料。
智能式身分證可能會在持證人不知情的情況下，披露資料	■ 當局會明確界定和審慎管制披露儲存於智能式身分證內資料的方式。當局會採取措施，確保使用者知道儲存於身分證內用作出入境事務用途的資料。主要的管制措施包括： (a) 智能式身分證插入讀卡器後會與終端機相互認證； (b) 在披露已儲存和受保護的個人資料前，智能式身分證會向終端機作出授權； (c) 在發放已儲存的個人資料前，智能式身分證會通過智能卡終端機內置的安全存取模組，與終端設備相互認證；

智能式身分證電腦系統
如何處理首次私隱影響評估
提出的主要私隱風險

私隱外洩風險	減低私隱外洩風險的管制措施
	(d) 儲存於智能式身分證內的指紋模版會用來核對持證人的指紋，從而核實持證人身分。
智能式身分證可能會被用作執行持證人不知情的功能	■ 是否加入和使用與出入境事務無關的其他用途，完全由持證人決定。一切與出入境事務無關的其他用途，必須得到持證人授權才可加入和使用。 ■ 如有需要，入境處的服務站可為持證人更新智能式身分證上的逗留期限／逗留條件資料。持證人亦可使用服務站閱覽已更新的逗留期限／逗留條件資料。 ■ 智能式身分證使用者會獲告知其身分證所提供的功能。
私人密匙可能會受破壞	■ 入境處應用程式的加密匙會在受謹慎管制的環境下產生和安全地存入身分證內。 ■ 一經存入身分證內，敏感的加密匙便不會再離開該智能式身分證，因此受破壞的機會微乎其微。 ■ 每張智能式身分證的加密匙都是獨一無二的。加密匙如受到破壞，只會影響一張智能式身分證的加密匙。一個加密匙受損並不會使破壞者得以獲取智能式身分證電腦系統內的其他身分證加密匙。
私人密匙會被他人使用	■ 當私人密匙安全存入和儲存於智能式身分證的受保護記憶體後，任何人也不 ■ 可藉任何應用程式直接取覽私人密匙。相反，身分證內的應用程式只可以要求

智能式身分證電腦系統
如何處理首次私隱影響評估
提出的主要私隱風險

私隱外洩風險	減低私隱外洩風險的管制措施
	內置的加密裝置，使用私人密匙指標，執行加密功能。
傳送中的資料被截取	■ 智能式身分證和後端電腦系統傳送資料訊息期間，所有資料訊息都會被加密，並會透過獨有的編號和訊息認證碼，以保持其完整。 ■ 資料在網絡間傳送時，網絡加密措施會用以確保資料保密。
已記錄的生物特徵可能被他人存取	■ 智能式身分證與讀卡設備必須在讀取資料(包括生物特徵資料)前相互認證。 ■ 儲存在人事登記伺服器的生物特徵資料，在網絡和應用層面均受到取用管制和防火牆保護。 ■ 指紋影像會在儲存於影像管理系統前加密。通過智能式身分證和讀卡設備之間的相互認證，身分證內的指紋模版可受保護。 ■ 採用以公匙基建為本的機制，達至聯網協定安全的層次，來保護網絡。 ■ 智能式身分證只儲存根據數學方法所產生的指紋模版，而不是實質指紋影像。任何人不能單靠身分證內資料重新產生指紋影像。
已記錄的生物特徵被非法竊取，並被他人使用，冒充該人士	■ 在自助資訊服務站內，智能式身分證執行敏感功能前，必須把“真實”指紋與儲存在身分證內的指紋模版核對。服務站會核實手指的真偽。 ■ 服務站的設計可防干擾。服務站的記憶體會在下列情況下被刪除－(1)服務站

智能式身分證電腦系統
如何處理首次私隱影響評估
提出的主要私隱風險

私隱外洩風險	減低私隱外洩風險的管制措施
	外殼被打開；或(2)震盪感應器偵測到震盪(超過預設的強度)，從而減少未獲授權的指紋讀取器被安裝入內的機會。 ■ 已記錄的生物特徵將整套儲存於人事登記資料庫內。生物特徵資料會受取覽管制和加密保護。獨有的密匙會用作加密每個生物特徵影像。
冒充者獲得智能式身分證和所需資料，繼而使用不受監管的設備	■ 終端設備(自助資訊服務站和離線手提設備)只會在智能式身分證電腦系統中央場地的獲授權人員相互認證後，才可啟動。有關設備必須透過安全途徑，接收啟動指令。 ■ 智能式身分證在傳送儲存在證內的敏感資料前，會認證終端機。由於未獲授權的終端機不會獲得智能卡認證，因此不會披露敏感資料。
智能卡資料被未獲授權設備修改	■ 終端設備和智能式身分證，以及智能式身分證和後端電腦系統之間未經相互認證前，智能式身分證不會允許外界終端設備更改其內容。因此，必須透過端到端核准，才可更新身分證資料。 ■ 在每張智能式身分證內的“智能晶片”可防干擾。身分證設有多層主動防禦裝置，敏感資料(例如密匙資料)如受機械、光導、電力或電子干擾，便會被刪除。

第二次私隱影響評估
建議摘要

A. 有關智能式身分證電腦系統設計的關注事項

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
1.	有關智能式身分證電腦系統在用途和功能上的取覽管制和使用者概覽的編訂 (系統設計及控制)	當局應以“需要知道”為原則和根據使用者的職務和責任，決定是否給予取覽智能式身分證電腦系統資料的權力。 在編訂使用者概覽時，使用者取覽資料的級別對照表應確保會按使用者的職務適當劃分。取覽智能式身分證電腦系統資料的詳情亦應記錄在案。 職務劃分的範圍應廣泛涵蓋(但不限於)人事登記、智能卡個人化及發卡管理系統等功能。	--	會遵從。
2.	新服務站的設計應確保顯示屏難以讓不獲授權人士窺看個人資	如服務站顯示的個人資料只限身分證持有人取覽和個人資料在顯示屏顯示時，盡可能只可讓持證人閱覽，則可保障私隱。當局可藉多	--	會遵從。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
	料。 (系統設計及控制)	項措施達到此目的，例如裝設聚合物護罩以限制液晶體顯示屏的觀看角度(類似自動提款機的設計)，或考慮類似“投票間”的設計，避免公開顯示個人資料。 用以監察惡意破壞的監察攝像機不應裝設於可看到個人資料或鍵入的密碼／個人身分密碼的位置。		
3.	工作站(個人電腦)和使用者的配置控制。 (系統設計及控制)	智能式身分證電腦系統設計的一項重要要求，是能確保主要的人事登記資料絕對保密和不會不當地向第三者披露。為防止未獲授權披露資料，入境處應： ■ 取消“印出螢幕資料”的功能，防止不需要執行這功能的使用者使用；以及 ■ 取消“剪下及貼上”的功能，防止有人在工作站複製個人資料，作人事登記以外的用途。	--	會遵從。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
4.	其他政府部門查詢個人資料。 (系統設計及控制)	當局是根據法例或在獲得政務司司長書面批准的情況下，向一些政府部門披露人事登記資料。智能式身分證電腦系統實施後，有關程序必須符合有關法例，包括《個人資料(私隱)條例》所訂明的六項原則，唯獲有效豁免者除外。	--	會遵從。
5.	進行首次私隱影響評估後，擬儲存／顯示於新智能式身分證的個人資料的改動。 (系統設計及控制)	根據二零零零年六月十二日的智能式身分證可行性研究報告和智能式身分證電腦系統標書(標書編號：PT/0316/2001)，有關方面建議從智能式身分證上刪去以下資料欄(包括實體性及邏輯性的數據)： i. 已核實出生日期的標記 ii. 簽發辦事處的代號 iii. 遺失次數 iv. 擁有居留權的標記 v. 申領回港證的資格 特區政府曾深入討論加入擁有居留權的標記和申領回港證的資格	--	從市民的角度來看，他們認為身分證上的“三粒星”(***)標記非常重要和有用。舉例來說，入境處以身分證上的三粒星標記表示持證人擁有申領回港證的資格，持有此旅行證件的人士可進入澳門特別行政區。市民亦非常重視擁有居留權的指示標記，可作為他們在香港的居留身分的具體證明。取消這兩項資料會引起混亂和不明確情況。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		的問題，最後認為在身分證保留這些資料，對身分證持證人來說最為有利。特區政府的業務需要似乎較有關私隱問題的少數憂慮更為重要(現有身分證亦載有這些資料。)		
6.	服務站和手提設備的稽查程序記錄 (系統設計及控制)	服務站和手提設備均有稽查程序記錄功能。稽查程序記錄的現有設計可記錄持證人的身分證號碼、證件編號、事件日期時間和操作資料。這些稽查程序記錄會送往後端電腦系統儲存。儲存持證人的身分證號碼看來沒有需要，而且會侵犯私隱，因為持證人的身分證號碼和證件編號已分別儲存於人事登記資料庫內。為保障持證人身分證號碼的私隱，入境處考慮從記錄中刪去此項。 入境處也應嚴格管制取覽服務站和手提設備所保存的稽查程序記錄，以確保只有有需要的獲授權人士才可取覽稽查程序記錄。	支持顧問的建議。 額外儲存身分證號碼，可能會令處理查閱政府部門備存的個人記錄的要求時，產生運作問題。	原則上同意。會在系統實施前，研究建議的可行性和影響。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		第三次私隱影響評估應詳細檢討已執行的取覽管制措施。		
7.	入境處應要求智能式身分證電腦系統的承辦商承諾系統並無採用隱藏的“後門”程式編碼或“不能更改的使用者個人識別編碼”。 (系統設計及控制)	入境處應徹底復查編碼和確定設有適當程序，已確保製備高質素及安全的編碼。有關程序包括： ■ 由發展商進行第一層編碼復查 ■ 由計劃小組進行正式編碼復查 ■ 由發展商進行非正式的討論／同級編碼復查 ■ 由品質保證人員進行系統功能／用途／端到端復查 ■ 由使用者進行可用性測試 入境處也可考慮以抽樣形式查核編碼，確保沒有出現常見的保安弱點和編碼已妥為記錄，從而確保編碼安全穩妥。 智能式身分證電腦系統承辦商應	--	會遵從。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		在系統發展階段採取仔細的驗收程序。入境處或應考慮破壞性編碼的法律影響，如可能的話，更應確保承辦商的工作守則載有適當的說明或程序。		
8.	在人事登記資料庫使用監護人身分資料。 (系統設計及控制)	未成年人仕申領身分證時，其父母／監護人的身分證資料會暫時儲存於人事登記系統的“香港身分證”實體內的“監護人身分證前綴字母及號碼”欄。待申領程序辦妥後，有關資料便會清除。長期以這種可以電子方式讀取和搜尋的模式儲存這些資料，會自動和廣泛地把很多父母與其子女連繫起來。不適當使用這些資料會引致人與人之間的複雜關連。父母的身分證號碼原用於子女的身分證申請，以方便父母領取未成年子女的身分證，把有關資料作其他用途，會侵犯私隱和違反良好的私隱原則。	--	“監護人的身分證前綴字母及號碼”資料只會暫時儲存於人事登記資料庫內，以便確定監護人身分，從而登記和簽發未成年人身分證。發出未成年人身分證後，有關資料便會刪除。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		入境處應確保： ■ 這項監護人身分資料的儲存時限不應超越所需的時限，而儲存的方式，亦不應容易令大量未成年人自動與其父母連繫起來；以及 ■ 備有適當程序，可靠地從人事登記資料庫刪除這些監護人身分資料，或安排把這些資料儲存於不能搜尋和屬暫時性質的事項類別記錄內。		
9.	根據現行的設計，智能式身分證電腦系統能透過入境處服務站支援卡上與出入境事務無關的其他政府用途。 (系統設計及控制)	如能夠作出以下安排，有關私隱問題的憂慮可盡量減少： ■ 資訊科技基建設施(例如網絡和服務站)只作入境處智能式身分證有關用途使用；以及 ■ 就日後其他政府部門的用 ■ 途，另行設立非入境處的服務	公眾的觀感是一個難以處理的問題，需要小心正視。當局應進行宣傳，清楚解釋會把資料／用途分隔，並向市民保證只有獲授權 部門才可取覽他	在建議的系統設計下，與出入境事務有關和無關的資料會完全分隔儲存。此舉可防止入境處取覽與出入境事務無關的資料，反之亦然。我們同意顧問的意見，有關入境處資訊科技基建的應用所引起的私隱關注是一個觀感問題，但亦需要處

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		站。 但是，智能式身分證電腦系統實施後，由於與出入境事務無關的用途(包括香港郵政數碼證書(電子證書)和圖書證)不多，因此由入境處負責管理資訊科技運作和與基建設施相關的日常工作，實屬合理。 可是，如與出入境事務無關的用途日後有所增加，那由入境處同時肩負“智能卡發卡機構”和“智能卡應用提供機構”的角色便可能會出現運作問題及在觀感上會令人產生私隱關注。 特區政府可考慮就與出入境事務無關的用途在入境處之外設立一些設施，負責管理資訊科技運作和與基建設施有關的日常工作。如認為此安排恰當，當局也應實施適當的資料私隱和保安管制及措施。	們本身所備存的資料。 隨着與出入境事務無關的用途增加，當局宜提供獨立設施，以管理和控制這些用途。	理。 從顧客服務的角度來看，持證人若不能在入境處的服務站閱覽所有資料，而需要另外前往其他地方閱覽與出入境事務無關的資料，會對他們會造成很大不便。從成本效益的角度來看，若政府只為了讓市民取覽與出入境事務無關的有限資料(即電子證書)而需要在全港不同地區另設非入境處服務站，並不合乎經濟原則。 我們得悉報告的建議，並認同現時並無迫切需要就與出入境事務無關的用途設立額外設施，負責管理資訊科技運作和與基建設施有關的日常工作。不過，隨着日後與出入境事務無關的用途增加，政府會考慮這些建議。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
10.	為方便輸入資料，其他政府部門可通過電子方式，讀取智能式身分證卡面的某些個人資料。 (系統設計及控制)	如特區政府擬協助各獲授權人士讀取和取用智能式身分證「證面資料」，則儲存於「證面資料」應用程式的個人資料應盡量減少。 一個可行辦法，是把所示的資料限於身分證號碼和中英文姓名。如需要加入額外資料，例如出生日期和登記日期，則應說明需要加入這些資料的原因，以消除市民對私隱問題的疑慮。 持證人應可全權決定是否向某獲授權人士提供「證面資料」和經「證面資料」的應用程式以電子方式取用個人資料。經「證面資料」應用程式取用「證面資料」前，應先取得持證人的同意，例如透過鍵盤輸入／滑鼠按動／電子簽署等方式。	明白有需要推廣電子化政府服務，但在讀取或取用「證面資料」時，會在公用的公共服務電子化服務站留下電子記錄(例如稽查程序記錄)。為免中央控制機構可能追查資料，必須妥善管理稽查程序記錄，確保只可由適當人士取覽和保存。	政府認為有實際真正需要使用「證面資料」應用程式，以便提供電子化政府服務-現時只限於圖書證功能有這方面的需要。值得注意的是市民可自由選擇是否採用這項功能。另外，在讀取任何「證面資料」前，當局會先徵得市民同意。當局並會告知市民為何需要加入這些資料和應用詳情。 至於個人資料私隱專員對有關電子記錄的意見，事實上，只有公共圖書館的智能卡閱讀器（並非「公共服務電子化」的服務站）才可讀取「證面資料」。我們在落實圖書證的功能時會考慮有關意見。
11.	逗留期限的日期可能在申請身分證日期和簽發智能式身分證日	入境處在擬備操作程序手冊時，應採取步驟，確保逗留期限不會在發	--	會遵從。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
	期期間屆滿。 (程序)	卡期間屆滿。		
12.	把香港郵政數碼證書加入智能式身分證的選擇 (程序)	雖然香港郵政的數碼證書屬與出入境事務無關的用途，但市民或會以為簽發數碼證書是新香港特區身分證重新登記及簽發程序的一部分。持證人可能會對智能式身分證各用途／所儲存資料的性質，以及各有關方面的角色產生混淆。 入境處和其他有關部門／決策局應合力宣傳智能式身分證用途的性質和各有關方面的角色。這樣也可協助申請人明白為何其個人資料會分別提供予香港郵政和入境處，並分別由香港郵政和入境處確認。 當局就智能式身分證進行推廣和宣傳工作時，應讓香港市民得悉以下事項：	--	當局會在系統實施前，宣傳智能式身分證各用途的性質和各有關方面的角色。當局會透過不同途徑，告知市民加入香港郵政的數碼證書的選擇、好處、目的和用途。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		■ 他們可自行選擇是否在智能式身分證加入香港郵政的數碼證書； ■ 加入香港郵政數碼證書的好處、目的和用途；以及 ■ 選擇載入數碼證書後，他們的個人資料須提供予香港郵政。		
13.	收集個人資料的目的，以及收集可辨識個人身分的資料。 (披露／政策)	目前，人事登記－登記表格印載的“收集個人資料的目的”項下的“收集資料的目的”，當中有數個項目意思似乎不夠清晰，或需要作出修訂，包括： ■ *<u>第 1(c)項</u>* “提供必要的資料給選舉事務處從而修訂選民名冊”意思不清晰。 — 檢討所有申請表格時，應在新表格內反映那些個人資料，將會向選舉	“收集個人資料的目的”應純粹解釋收集有關資料的目的，以及會怎樣使用。	原則上同意。會徵詢律政司的意見，以便在人事登記－登記表格印載的“收集個人資料的目的”採用適當字眼。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		事務處提供。 ■ *第 1(e)項* "…為協助其他政府部門執行其他法例和規例所進行的入境管制任務"意思不清晰，因為資料使用者收集個人資料的目的，可能僅為執行一項職能或工作所需，或與執行該職能或工作有直接關係。 — 應更具體說明此項目。當局可考慮在人事登記一申請表格列舉可能使用市民提供的個人資料的政府部門，以及這些資料的用途。 ■ *第 1(h)項* 在"收集資料的目的"項下的"其他合法用途"可能流於空	--	

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		泛，未能符合讓資料當事人知悉有關資料的用途的規定。 — 應考慮訂明“合法用途”是指根據《人事登記條例》或香港法例批准的用途。 ■ *第 1(g)項* “作為統計及研究之用”意思不清晰。《個人資料(私隱)條例》第 62 條訂明，作為統計及研究之用的個人資料，可獲豁免而不受第 3 保障資料原則的條文(限制使用個人資料的原則)所規管，惟所得成果不會以識別任何資料當事人的身分的形式提供。 — 統計和研究通常採用總體數字，作每年報告之用，而不包括會識別個別人士身分的研究用	看來可採用“獲法例批准的其他用途”等字眼，惟須徵詢律政司的意見。 --	

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		途。有見及此，應進一步闡明這個項目，以涵蓋此情況。		
14.	在系統實施前，就系統控制及功能進行私隱檢討。 (未來工作)	除了按既定範疇，集中檢討已建立的程序的私隱問題外，第三次私隱影響評估應擴大範圍，包括檢討下列私隱事項： ■ 系統控制及操作 ■ 個人資料的保留期限(包括臨時資料檔案) ■ 系統設計的各項變更(包括變更控制機制) ■ 在系統實施前，須即時解決的系統控制及功能方面的主要不足之處 第三次私隱影響評估應就已加入智能式身分證電腦系統的所有主要加強私隱的系統控制和功能，進行全面評估。此檢討亦可在系統投產前，有助識別須加強私隱措施的	應擴大第三次私隱影響評估的範圍，以涵蓋與市民提出查閱資料要求的有關事宜。	第三次私隱影響評估約在二零零三年三月身分證應用程式的運作程序落實前進行。我們會考慮在第三次私隱影響評估中，加入建議的研究範疇。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見／建議	個人資料私隱 專員公署的意見	政府的回應／前瞻
		主要範疇。 第三次私隱影響評估集中檢討人手操作程序、系統控制和功能。是次檢討的主要結果撮要，應向公眾發表，從而加強他們對新智能式身分證系統私隱技術的信心。		
15.	將來使用者對智能式身分證電腦系統的更改要求 (未來工作)	在智能式身分證電腦系統實施後，應訂立有效的使用者更改要求程序，作為加強、提升和保養系統的重要一環。 隨着使用者對新系統日漸熟悉，他們很可能要求提升功能。在配合多項更改要求的同時，引入不在智能式身分證電腦系統原來設計之內的新功能，可能會產生新私隱問題。在批准提升系統的功能前，必須考慮私隱問題，特別是考慮《個人資料(私隱)條例》的保障資料原則，以及香港智能式身分證持有人可能關注的私隱問題。	--	會遵從。

B. 有關首次私隱影響評估建議的關注事項

項目	事項 (性質)	第二次私隱影響評估 顧問的意見	個人資料私隱 專員公署的意見	政府的回應／ 前瞻
1.	首次私隱影響評估和個人資料私隱專員公署均認為，最理想是卡內的處理器也可比較指紋模版，那麼，個人生物特徵資料便無須離開智能式身分證。 (首次私隱影響評估的設計改動)	明白目前的智能卡技術存在技術限制(記憶體和處理速度限制)，因此未能達至最理想的情況，在卡內比較指紋。有見及此，在智能式身分證電腦系統設計加設下列輔助管制措施，會盡量避免生物特徵資料離開智能卡後，在未獲授權的情況下被存取： ■ 智能卡應在傳送生物特徵資料作進一步分析前，認證讀卡設備。 ■ 智能卡應確保讀卡設備，已獲授權取用儲存在卡內的生物特徵資料。 ■ 從卡內讀取的生物特徵資料，除存入讀卡設備外，不應在其他地方顯露。 ■ 讀卡設備核實使用已儲存指紋模版的使用者身分後，應立即刪除讀	--	智能式身分證電腦系統已包括建議的所有輔助管制措施。一俟在卡內比較指紋的技術切實可行，我們會再作研究。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見	個人資料私隱 專員公署的意見	政府的回應／ 前瞻
		卡設備內的所有模版複本。 ■ 生物特徵鑑證設備應可防干擾，以防止在未獲授權的情況下，取用設備內的生物特徵資料。		
2.	若身分證能支援加密功能，則身分證必須安全地產生密匙，以及對數碼簽署和訊息加密匙對提供穩妥的儲存和使用方法。 (首次私隱影響評估的設計改動)	一般來說，若私人密匙在卡外產生後才載入卡內，則必須制定足夠控制措施，以確保密匙安全產生，避免密匙在載入智能卡時被披露。主要管制辦法的例子包括： ■ 密匙應為隨機產生，不可推斷。 ■ 應禁止在未獲授權的情況下，實體性及邏輯性接達產生密匙的系統。 ■ 產生加密匙對並把私人密匙載入卡內後，私人密匙的所有複本(在卡內的私人密匙除外)應採用無法復原的方法予以銷毀。 ■ 產生密匙的地點及把密匙載入卡內的傳送途徑必須安全。	--	入境處的智能式身分證電腦系統採用MULTOS 保安系統。MULTOS 的密匙管理中心，採用非對稱密匙把各項用途和數據穩妥儲存於智能卡內。 用以支援入境處各項應用功能的對稱密匙，在智能卡的個人化印製過程中，在密匙管理系統安全產生，然後載入卡內。 香港郵政電子證書應

項目	事項 (性質)	第二次私隱影響評估 顧問的意見	個人資料私隱 專員公署的意見	政府的回應／ 前瞻
		■ 應謹慎管理密匙產生設備。應用程式伺服器的配置及保養應按照獲批准的程序進行，包括電腦主機內資料的完整性、系統查核、系統內的排序，以及批准取覽檔案和目錄的設定，防止未獲授權的取覽。 智能卡初始化時，可安全產生入境處應用功能所採用的密匙，故入境處沒有太大需要在卡內產生密匙。		用程式的密匙由香港 郵政安全地產生後，再傳送到智能式身分證電腦系統，在身分證個人化印製過程中載入卡內。
3.	首次私隱影響評估建議在人事登記系統資料庫略去指紋影像，避免侵犯私隱。 (首次私隱影響評估設計改動)	入境處有真正業務和運作需要留存指紋影像，並把此影像與其他個人資料共同儲存在人事登記系統中央資料庫內。 從私隱角度來說，當局應制定下列主要管制措施，以防止不恰當地取覽及／或使用這些資料： ■ 人事登記系統的所有使用者必須經過身分核實。	--	智能式身分證電腦系統的設計已加入建議的技術管制措施。

項目	事項 (性質)	第二次私隱影響評估 顧問的意見	個人資料私隱 專員公署的意見	政府的回應／ 前瞻
		■ 人事登記系統應採取多層級別的取覽管制，讓具備不同權限及負責不同工作職能的入境處人員，只可取覽執行工作所需的資料。取覽私隱敏感資料，例如指紋影像，應限於必須知道有關資料的個別人士。 ■ 應保留詳細的稽查記錄，顯示誰人取覽資料、資料類別、取覽時間和目的。這些記錄應定期予以檢討，以查核使用者是否恰當取覽資料。 ■ 可被竊取的敏感資料，必須在網絡傳送時加密。 ■ 制定管制措施，以防止人事登記資料被存取作未獲授權的用途。 智能式身分證電腦系統已在設計內包括上述管制措施。		

首次私隱影響評估建議的最新情況

首次私隱影響評估關注事項的最新情況，以及香港特區政府的回應如下：

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
1	63 (立法)	人事登記／身分證系統的法例體制，應該加以檢討，以確保該體制能為整個新身分證系統提供一個全面的基礎。	將會檢討。	《2001 年人事登記(修訂)條例草案》已於二零零二年一月九日提交立法會。此條例草案就引進智能式身分證、在證內加入與出入境事務無關的用途的資料、推行全港性的身分證換領計劃，以及為更有效保障資料私隱所採取的額外措施，訂定條文。
2	64 (原則)	在最理想的情況下，持證人應有充分自主權，並可自願加入任何附加於新身分證內的附加應用或使用功能，而並非由政府純粹基於實際需要而加入有關功能。	除了駕駛執照或許不在可供自由選擇之列外，持證人可自由選擇是否把其他應用功能加入智能式身分證內。一直以來的諮詢結果都顯示社會已普遍接受了這種做法。政府會繼續與私隱專員商討，亦會在其他應用功能的可行性研究完成時，徵詢有關立法會事務委員會的意見。	所有將會在智能式身分證內加入的各項與出入境事務無關的用途（包括駕駛執照）均是自願的。

首次私隱影響評估建議的最新情況

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
3	65 (原則)	如果入境處將智能卡計劃的所有管理工作交由內部處理，並排除這項工作由其他政府機關或外判處理的可能性，將可減低對私隱問題的關注。	入境處肯定會負責登記及簽發身分證。政府會確保智能卡計劃的所有管理工作，包括其他增值功能的管理都安全穩妥，並能夠有效地保障每一個人的私隱。	人事登記處處長負責登記和簽發智能式身分證，以及管理與出入境事務相關的用途。電子證書(現唯一與出入境事務無關的用途但須在身分證內儲存的資料)，會由香港郵政負責。智能式身分證電腦系統的現有設計，確保資料會穩妥地分隔儲存，只有獲授權人士才可取覽。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
4	78 (原則)	如果智能式身分證內載有其他用途，以下情況都會引起對私隱問題的關注： ■ 智能卡計劃操作者是一個獨立的政府機構； ■ 外判智能卡的管理； ■ 智能卡計劃操作者是一家以外判或合資形式經營的商業營辦商；及 ■ 部分行政工作由另一間機構處理，而入境處保留掌管身分證登記及簽發的所有事宜。	有關智能卡的管理： ■ 已排除採用商業機構； ■ 有關身分證的事宜，入境處仍然會負責登記、簽發身分證及管理有關的登記記錄； ■ 有關身分證用途以外的事宜，一個由資訊科技及廣播局局長主持的高層跨部門督導委員會已成立，負責智能卡計劃的多功能部份。督導委員會會就加入在新智能式身分證內的各種用途提出建議。入境處是督導委員會的其中一名成員。 智能卡計劃操作者只是一組技術人員，他們只會在多用途功能方面提供技術上的意見及支援服務，例如提供求助台服務及為設備作證明等等。他們不會接觸到個別部門所備存的個人資料。	根據建議的《2001 年人事登記(修訂)條例草案》，行政長官會同行政會議是審批智能式身分證附加用途的機關，而人事登記處處長是管理智能式身分證加入或儲存這些附加用途的資料的機關。

首次私隱影響評估建議的最新情況

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
			我們正就實施各項附加功能進行多個可行性研究。根據可行性研究的結果及充份考慮私隱方面的關注後，我們將落實智能卡管理計劃的各方面設計。無論如何，我們沒有計劃將智能卡的管理外判。	

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
5	67 (技術性意見)	如果智能卡可以支援加密的功能，為確保最大的私隱保障，支援數碼簽署及訊息加密功能的私人密鑰應該只可以經由晶片產生。	將會在數碼證書的可行性研究中作出考慮。	入境處的應用功能採用 MULTOS 保安系統。MULTOS 的密匙管理中心，採用非對稱密匙把各項用途和數據穩妥儲存於智能卡內。透過安全存取模組，入境處的智能式身分證電腦系統採用對稱密匙，與終端機和人事登記後端系統安全地傳達訊息。 用以支援入境處各項應用功能的密匙，在初始化和個人化印製過程中安全地產生和存入卡內。由於對稱和不對稱密匙的產生環境安全，因此在卡內產生密匙的好處相應減少。 密匙(保密對話密匙)在卡內產生。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
6	71/72 (程序) 87/88 (技術性意見)	人事登記系統資料庫如果省略了拇指指紋，看來只會帶來有限的負面影響(對遺失或損毀身分證的人士有少許不便)，但可大大減低侵犯私隱的機會。 另一個可採用的方法，是人事登記系統的資料庫只儲存拇指指紋的模版數值。 入境處應： ■ 設計其他程序及步驟來處理以下情況：拇指指紋沒有儲存於人事登記系統的資料庫內或只以模版的形式儲存； ■ 在徵求標書文件內，要求投標者提供計劃書，該計劃書須就以下不同情況分別作出建議：人事登記系統的資	對人事登記系統資料庫不儲存拇指指紋的建議有極大保留。沒有了這最後的記錄和可作為獨特辨別身分的標籤的拇指指紋，入境處將無法快速和準確地確認聲稱持有已遺失或損壞的身分證人士的真正身分。更重要的是這建議將大大影響辨別在海外遺失身分證明文件及受危困的香港居民身分的進度。在一般情況下，大部份外國政府只會向入境處提供拇指指紋作身分核實。他們提供的拇指指紋圖像的質素通常僅足夠以目視與入境處的拇指指紋記錄互相核對。這些指紋圖像可能不足以產生模版作電腦核對之用。假如我們需要要求有關政府提供新一套拇指指紋圖像，將可能導致延誤。 相對以模版形式來儲存指紋，我們認為儲存已作加密處理的原指紋影像較為可取，因為前者會使以一對多個記錄的核對更加容易。使用專利的生物特徵模版	智能式身分證電腦系統的現有設計，會在人事登記系統資料庫儲存姆指指紋影像。由於市面上的模版演算法是專利產品，因此不宜在人事登記系統資料庫儲存姆指模版，以免入境處被鎖定於個別供應商獨有的特定技術。倘若需要更新或修訂演算法，供應商可能會收取高昂費用；假如供應商停止提供服務，情況更是不堪設想。 當局在技術設計層面採取額外私隱保障措施，並會考慮對現行法例作出改動。修訂現行《人事登記條例》，有助回應市民對資料私隱的關注。當局會訂定條文，懲處未經授權取用、使用、儲存和披露人事登記資料。至於禁止登記主任披露人事登記資料的條文(獲政務司司長的書面批准，則屬例外)，會由《人事登記規例》轉移至《人事登

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		料庫內儲存拇指指紋、只儲存拇指指紋的模版及兩者皆不儲存； ■ 進行試驗以證實這些步驟沒有大大減低計劃的完整性及沒有過度增加人事登記處辦事處或個別人士的人力及金錢上的負擔； ■ 若試驗的結果令人滿意，在推行新系統時，便不應將拇指指紋儲存於人事登記系統的資料庫內。	編寫技術亦容易被鎖定於供應商獨有的特定技術。一旦該供應商停止提供服務，我們便會面對要求全體市民再次向我們提供拇指指紋作新的編寫技術儲存的風險。這個風險應當儘量避免。 根據私隱專員公署的意見，我們會探討可否要求參與即將舉行的投標的銷售商，提供有建設性的提議，可同時處理這兩方面的問題。我們亦同意如果決定保留拇指指紋影像於人事登記記錄資料庫內，我們將制定適當法例／規則性和技術性的措施(例如拇指指紋的加密處理)，以限制取覽這些資料。並如較早前對市民作出的承諾，保證不會進行一個對多個的身分核對。	記條例》，從而提升此禁止條文的地位。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
7	82 (程序)	入境處需要確保有關收集個人資料的目的及只傳送個人資料與可接收的人士(資料保障原則第 1 原則(3)(b)(i)(B)款)，在現時及尤其在新制度下，與個人資料實際用途及披露相符合。	將會遵從。	入境處智能身分證計劃小組成立了智能身分證(總務)科，旨在檢討“收集個人資料的目的”和人事登記資料的使用。
8	82 (程序)	入境處應檢討該處表格上載有“有關收集個人資料的目的”是否足夠和正確，以符合資料保障原則第 1 原則(3)款所蘊含的目的。	將會遵從。	入境處智能身分證計劃小組成立了智能身分證(總務)科，旨在檢討人事登記處表格印載的“收集個人資料的目的”。
9	83 (程序)	入境處或須考慮是否在推行全民換證計劃時對有特別情況或需要的人士作出特別安排。這些人士可能包括： ■ 存在風險的人士(各類別已於評估報告第 79 頁的特別安排中提及)； ■ 進行正常的登記程序，可	建議中的特別安排，例如不套取拇指指紋或簽發額外身分證等，將會嚴重影響人事登記資料庫的完整性。 在公平的大前題下，我們應以同一標準服務全港市民，但如果有值得考慮的原因，我們會按個別情況考慮作出特別安排。	沒有進一步發展。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		能對他們本身或人事登記處職員造成困難的公眾知名人士；及 ■ 因宗教或道義理由或由於容顏破損而反對依循正常程序留存照片或拇指指紋的人士。		
10	83 (立法)	入境處須檢討是否需要更新《人事登記規例》第 4 條規定呈交的資料項目。	將會檢討。	現正進行內部檢討，以決定是否需要收集規例第 4 條訂明的所有資料。
11	84 (立法)	應考慮修改法例，給予個人法律保障，使其免除純粹基於技術錯誤而假定有罪(presumption of guilt)(例如：錯誤或損壞的身分證、讀卡機的失誤及失去聯絡連繫)。	香港法例建基於“假定無罪”的精神，根據已取得的法律意見，無須就這方面作出法例修訂。	沒有進一步發展。

首次私隱影響評估建議的最新情況

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
12	84 (程序)	入境處應檢討其記錄保存政策，並發展及實施一個處理所有儲存媒體內個人資料的程序時間表，以便當儲存資料的原有目的失效時，能符合資料保障原則第 2 原則(2)款及《個人資料(私隱)條例》第 26 條有關保留及刪除資料的要求。	目前，人事登記記錄在持證人死後仍會長時間保留，這是因為有關資料仍有可能需要作多項用途，例如用作審理居留權的申請或處理其後人就死者提出的登記事項證明書的申請。 儘管如此，政府仍會檢討記錄保存政策，以確保符合資料保障原則第 2 原則(2)款及條例第 26 條的規定。	入境處智能身分證計劃小組成立了智能身分證(總務)科，以檢討記錄保存政策。
13	84 (立法)	《人事登記條例》及規例和其他可能涉及的法律，將需要修改，以配合新身分證計劃。這些修改包括以下要素： 入境處以外其他部門讀取“不能看見的”身分證資料； 在各種情況下，持證人提供拇指指紋，用作與身分證內所記錄的數碼形式指紋比較。	將會就法例修改事宜尋求私隱專員的意見。	《2001 年人事登記(修訂)條例草案》已於二零零二年一月九日提交立法會，並加入相關的第 7(9)條(使用詳情的限制)和第 13 條(藉指紋核對以核實身分的權力)。

首次私隱影響評估建議的最新情況

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
14	85 (立法)	應修改《人事登記規例》第 24 條，明確訂明該條文涵蓋所有由入境處儲存並與人事登記功能有關的個人資料。	將會遵從。	《人事登記規例》第 4 條要求提供的詳情，已涵蓋入境處要求並與人事登記功能有關的所有個人資料。智能式身分證電腦系統所需的額外個人資料，已於《2001 年人事登記(修訂)條例草案》訂明。
15	85 (立法)	應考慮將禁止條文移進法例內或列作由立法會批准的修訂(即正面的不允許)(positive disallowance)，使禁止條文不會被其他已存在而又獲賦權索取資料的條文所凌駕。	將會遵從。	《2001 年人事登記(修訂)條例草案》已於二零零二年一月九日提交立法會，並加入相關的第 7(10)條(不得披露照片、指紋及詳情的責任)。
16	85 (立法)	以後所有按法律條款批准授權披露人事登記資料的事宜，也應通過立法會的正面審批程序(positive approval process)。	將會遵從。	《2001 年人事登記(修訂)條例草案》已於二零零二年一月九日提交立法會，並加入相關的第 7(10)條(不得披露照片、指紋及詳情的責任)。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
17	85 (立法)	人事登記條例應訂明，所有未獲授權使用(包括“純粹”瀏覽)及包括未獲授權披露有關資料，即屬違法，並將受到適當的懲處。	有需要與律政司共同就“純粹”瀏覽的問題作進一步研究，從而確立犯罪動機的定義。	《2001 年人事登記(修訂)條例草案》已於二零零二年一月九日提交立法會，並加入相關的第 7(10)條(不得披露照片、指紋及詳情的責任)和第 7(11)條(禁止未經授權處理詳情)。
18	85 (程序)	入境處應確保所有人事登記資料庫的資料及其他記錄(無論直接提供或從證上讀取資料)，應在《人事登記規例》第 24 條給予批准的情況下，才可以作出披露。	現在已經如是。 將來亦會繼續遵從。	沒有進一步發展。
19	85 (程序)	有關核對程序方面，入境處須確保在新系統中任何作進一步自動核對的要求，必須符合《個人資料(私隱)條例》所訂明的核對程序，並得到私隱專員的認可。	現在已經如是，將來亦會繼續遵從。	沒有進一步發展。
20	85 (原則)	假如入境處或政府能在以下方面作出承諾，有關香港特別行政區身分證所儲存的個人資料的使用或	原則上同意。 入境處傾向於採用接觸式智能卡。但	智能式身分證電腦系統採用接觸式智能卡技術。由於非接觸式智能卡技術發展日新月異，我們不排除

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		所提供的資料私隱方面的憂慮將大大減少： ■ 智能卡不會是非接觸式； ■ 卡面上所允許顯示的資料，將不會多於可行性研究報告所建議的； ■ 晶片內可能儲存的特定資料項目； ■ 獲准許直接從晶片上讀取資料的機構或機構類別，以及讀取資料的目的； ■ 獲准套取(或閱覽)拇指指紋並與卡內數碼化的指紋作比較的機構或機構類別，以及在什麼情況下批准這樣做；及 ■ 在什麼情況下會批准將單純影像化的資料(過往以微	對於完全排除使用非接觸式智能卡的可能性仍然有所保留，因為隨着科技的發展，非接觸式智能卡可能會與接觸式智能卡一樣安全可靠。	非接觸式智能卡日後可能會與接觸式智能卡一樣安全可靠。 會遵從可行性研究報告有關卡面資料和晶片資料內容的建議。智能式身分證的晶片可儲存的資料項目，已於《2001 年人事登記(修訂)條例草案》清楚訂明。此條例草案亦訂明在何種情況下，套取指紋與卡內模版作比較會獲批准。 持卡人的個人資料會按各項應用範圍分開處理，因此適用於個別用途的個人資料，只可在相應政府部門的終端機取覽。 不過，留存、取覽和比較指紋只限於在入境處指定終端機和服務站進行。 從縮微膠卷轉化成的電子影像會保留為靜態影像，僅供閱覽。當局不容許完全由機器讀取的格式，例如光學字元閱讀器或其他識別技

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		型膠卷攝影)轉變為可完全由機器讀取的格式。		術。
21	86 (原則)	人與人的連繫索引容易構成侵犯私隱的行為。入境處應確保在提供“聯繫人士”的資料(例如父母與子女、監護人與子女及配偶雙方等)予授權機構時，已取得適當的合法權力。換言之，根據《人事登記規例》第 24 條給予的批准必須明確訂明這些“有聯繫人士”的資料可作披露。	原則上同意。	《個人資料(私隱)條例》及《人事登記規例》第 24 條，已訂有足夠條文，規管“有聯繫人士”資料的披露。
22	86 (原則)	為人事登記／身分證用途而儲存於晶片內的資料應受可行性研究報告所提及的所有限制規管，特別是： ■ 只限於該報告現時所提出和闡述的資料項目； ■ 受到特定的技術保護；及	會遵從私隱專員的意見。	智能式身分證電腦系統的設計包括下列加強保障私隱的措施： ■ 市民可閱覽以電子方式儲存的資料 ■ 市民可下載／刪除應用功能 ■ 智能卡特有的保密下載功

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		■ 只可由指定和非常有限數目的儀器和機構，以及只為特定目的而取覽有關資料。		能 ■ 分隔儲存不同應用功能的具體資料 ■ 市民可啟動各項附加應用功能
23	86 (技術性意見)	新系統的規格說明應明確地包括資料、功能及用途的分隔和限制，身分證號碼應如目前一樣，只用來傳達有限的資料。	原則上同意，但須取決於現正為系統的多用途功能作研究的顧問的意見。	採用 MULTOS 晶片操作系統，把卡內資料、功能和用途穩妥地分隔儲存。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
24	87 (技術性意見)	徵求標書文件應明確要求計劃書清楚解釋如何保護資料及功能的完整性，並提供硬件、系統軟件及應用程式特徵的詳情。 智能卡應能作出查問及鑑別處理儀器和程序，並且只在結果滿意時才給以回應，以保障資料不會洩露予未經授權人士及不會由該等人士處理有關程序。 智能卡應能有效辨別出示智能卡人士的身分，以防冒充者行使持證人的特權。	將會遵從。	完成。 當局使用安全存取模組，相互認證智能卡和讀卡設備，從以保障資料不會洩露予未經授權人士及不會由該等人士處理有關程序。 持證人取用個人資料時，其身分會經核對指紋得到核實。
25	87 (技術性意見)	智能卡內儲存的生物特徵在任何情況下都不應離開晶片另作處理。徵求標書文件應鼓勵投標者妥善處理這事項。如果證實該技術是存在的話，便應視為“極為可取”的特徵，並在評估標書時佔相當重要的位置。	原則上同意，但須視乎技術性研究的結果而定，特別是處理程式的反應時間。政府將會要求投標者研究這事宜及提供解決方案。	原則上同意，但基於現有智能卡技術在記憶體和表現方面的限制，智能式身分證電腦系統未能做到這點。日後一俟技術許可，我們會再作研究。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
26	87 (技術性意見)	如果新身分證能夠支援加密功能，便應納入以下的附加規格說明: ■ 身分證必須能夠安全地產生密匙，及對數碼簽署和訊息加密匙對提供穩妥的儲存和使用方法； ■ 必須給予持證人選擇權，決定加密匙對和數碼證書的數目及使用； ■ 任何私人密匙的後備安排，均須由持證人全權決定，讓個別人士可真正自行選擇提供後備服務的機構，包括非政府服務的提供者； ■ 任何政府機構均不可進入及取覽這些後備設施；以及	密匙的產生和儲存的建議將會在未來數碼簽署的可行性研究中再作考慮。 政府將會對所提出的私人密匙後備安排作出考慮。	入境處的應用功能採用 MULTOS 保安系統。MULTOS 的密匙管理中心，採用非對稱密匙把各項用途和數據穩妥儲存於智能卡內。透過安全存取模組，入境處的智能式身分證電腦系統採用對稱密匙，與終端機和人事登記後端系統安全地傳達訊息。 用以支援入境處各項應用功能的密匙，在初始化和個人化印製過程中安全地產生和存入卡內。由於對稱和不對稱密匙的產生環境安全，因此在卡內產生密匙的好處相應減少。 密匙(保密對話密匙)在卡內產生。 目前只有由香港郵政簽發的電子證書於智能式身分證電腦系統實施後可予使用。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		■ 排除一切私人密匙的強迫性委託安排。		為確保絕對安全，當局不會提供後備私人密匙和託管服務，因為私人密匙不能抽離智能式身分證。
27	87 (原則)	假如入境處可確定數碼拇指指紋只會用作一對一比較，以核實個人所宣稱的身分，而不涉及其他目的，尤其是不會用作一個對多個比較，從而藉拇指指紋辨認某人的身分，將可減少私隱問題。	將會遵從。	智能式身分證電腦系統的設計僅容許對數碼拇指指紋進行一對一比較。
28	88/89 (技術上意見)	由合資格的獨立技術顧問進行技術性審核，並證明及確認在計劃的設計及推行時已全面及有效地處理以下風險： ■ 使用身分證儲存及披露不為持證人所知的資料，及執行不為持證人所知的功能； ■ 假如密匙將會支援加密功能，私人密匙被發現及被他	將會在進行下一輪私隱影響評估和保安審核時，跟進這些事項。	市民會獲告知其智能式身分證內儲存的個人資料。持證人可使用自助資訊服務站查看儲存在身分證內的個人資料。 只有持證人和獲授權人士才可取覽身分證儲存的資料。當局藉以下措施執行這項規定： ■ 使用內置安全存取模組認證讀卡設備

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		人使用的風險； ■ 與讀卡設備有關的以下風險：－ ■ 線路被截取，引致個人資料或連串資料被取覽； ■ 記錄的生物特徵為其他代理處、機構或個人截取； ■ 其他機構嘗試自行收錄生物特徵，作為較目視檢查身分證更有效的核實方式； ■ 記錄的生物特徵被人非法獲取及使用以偽裝他人身分； ■ 個人身分密碼(PIN)被截取； ■ 偽裝者在獲取身分證及任何所需資料後，冒認身分並		■ 使用儲存於智能卡的模版，核對持證人的指紋，從而核實其身分 全部程序會在持證人完全知情和協助下進行。 所簽發的智能式身分證經個人化後，一個私人密匙會留在卡內的受保護記憶空間內。技術上而言，該私人密匙只可經智能式身分證內的加密引擎使用，而不能由智能式身分證的應用功能或外界界面直接取用。 在傳送資料時，所有資料訊息都會加密，並會透過獨有的編號和訊息認證碼得以保持完整。 讀取資料(包括生物特徵資料)前，智能卡和讀卡設備必須經過相互認證。指紋影像儲存於資料庫前會

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		使用無人監察的讀卡設備；以及 ■ 未獲授權的讀卡設備修改身分證中的資料。		先加密。 終端機設備(包括自助資訊服務站和離線手提讀取器)僅在智能式身分證電腦系統中央服務站的獲授權人士，使用相互認證技術和透過安全的途徑發出所需的啓動指令後，才會啓動。 未經終端機設備和智能式身分證之間，以及終端機和後端電腦系統之間的相互認證，智能式身分證不會允許外界終端設備更改其內容。此舉確保更新身分證資料時必須得到端到端核准。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
29	89 (技術性意見)	新計劃應包括所有現有計劃的私隱保安特徵，包括其他入境處系統及外界系統如 ECACCS 的進入管制及界面管制。管制在任何時間均適用，包括流動登記等工作。	將會遵從。	除現有計劃的私隱保安特徵外，當局並會在智能式身分證電腦系統採用下列加強私隱措施： ■ 市民可閱覽以電子方式儲存的資料 ■ 市民可下載/刪除應用功能 ■ 智能卡特有的保密下載功能 ■ 分隔儲存不同應用功能的具體資料 ■ 市民可啟動各項附加應用功能
30	89 (技術性意見)	入境處應致力於結合電腦系統的進入管制及人力資源管理系統，包括在職員離職及休假期間，適時令用者身分編碼及密碼無效。	雖然有關建議涉及與另一個仍未發展或電腦化的系統結合，但政府同意應該朝着這個目標前進。	智能式身分證電腦系統備有以角色為本的取覽控制系統，可適時令用者身分編碼及密碼無效。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
31	89 (技術性意見)	應提高計劃中有關收集電腦記錄及稽查程序記錄的詳細規格，以確保能夠收集足夠的詳細資料。	將會遵從。	智能式身分證電腦系統的設計能提供詳盡的事項記錄和稽查程序記錄，從而顯示事項類別和所涉的人員。
32	89 (技術性意見)	應修改計劃的規格說明，有關系統的可靠性及適應性的標準應由可行性研究報告所建議的‘最少與現行系統相同’，修改為更高的標準。災難復原計劃應建基於更高要求，建議中的‘基本生存’(basic survival)模式並不足夠。	同意但必須視乎技術上是否可行和是否具備成本效益。	透過集合易供取用的電腦運作、後備電腦中心、超額網絡連結等的故障包容設計，智能式身分證電腦系統可達致高度的可靠性及適應性。
33	89 (原則)	入境處必須在相關的職員培訓計劃中，加入對身分證及使用身分證所涉及的私隱事項的認識及處理方法。	將會遵從。	入境處已在智能身分證計劃小組之下成立訓練分組，負責為人員提供這方面的培訓。
34	89 (立法)	將“要求未經授權披露人事登記資料(有或沒有提供報酬)”列為罪行。	將會遵從。	《2001 年人事登記(修訂)條例草案》已加入相關的第 7(11)條(禁止未經授權處理詳情)，並於二零零二年一月九日提交立法會。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
35	90 (立法)	對使用人事登記資料的人士或機構設定限制及／或條件(兩者均直接依據《人事登記規例》第 24 條及間接依據第 23 條)，並訂明違反上述限制或條件即屬違法。	將會遵從。	《2001 年人事登記(修訂)條例草案》已加入相關的第 7(11)條(禁止未經授權處理詳情)，並於二零零二年一月九日提交立法會。
36	90 (原則)	入境處應重申其承諾，會對任何違反保安及／或在法定權力以外使用有關個人資料的人員或僱員進行紀律處分。	將會遵從。	《2001 年人事登記(修訂)條例草案》已加入相關的第 7(11)條(禁止未經授權處理詳情)，並於二零零二年一月九日提交立法會。
37	90 (公眾諮詢)	政府公開向其他機構披露人事登記資料的整體數字，可充分證明政府堅守這個原則。	將會考慮。	當局會備存向其他政府部門披露人事登記資料的整體數字，唯一是有關用於“保障關於香港的保安、防衛或國際關係的目的”(《個人資料(私隱)條例》(第 486 章)第 57 條)的資料統計數字則除外。
38	90/91 (原則)	為了貫徹公開及高透明度的原則，私隱評估應盡量公開進行及廣泛搜集公眾意見。雖然公眾至今未有對這個私隱評估提出意見，但應	首次私隱影響評估報告的精要版本已分發給各立法會議員。政府亦會公開以後的評估報告。	我們在二零零二年四月九日的立法會保安事務委員會會議上向委員作出承諾，當局會匯報第二次私隱影響評估的結果。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		盡快向公眾公開私隱評估報告，以遵循《個人資料(私隱)條例》資料保障原則第 5 原則。 在最理想的情況下，應向大眾公開這份評估報告，以便立法會議員及其他人士考慮當中的建議。 該報告除了向大眾公開發表外，更應給予各主要的公眾代表。		
39	90 (公眾諮詢)	就香港特別行政區身分證計劃進行更廣泛諮詢，不但使公眾對計劃的信心增加，更有助入境處考慮其他有關身分證設計的關注事項。	首輪的公眾諮詢已於 2000 年 12 月完成。政府把與出入境事務無關的其他功能加入智能式身分證前，會先諮詢有關的立法會事務委員會。	在首次公眾諮詢活動諮詢了 18 個區議會的意見。第二輪宣傳諮詢工作已於二零零一年二月在本地八間大學及教育院校舉行。 在二零零一年二月底舉行的“香港資訊基建博覽 2001”，舉辦了為期三天的展覽。 當局由二零零零年十一月開始，在香港特區智能式身分證的網頁設有專用的電郵地址，以蒐集公眾的

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
				建議／意見。
40	91 (公眾諮詢)	為了加深有關人士對整個智能式身分證計劃的認識，入境處應準備技術性的簡報材料。	已於 2000 年 12 月初向各立法會議員送交新身分證系統可行性研究報告管理摘要的精要版本。	沒有進一步發展。
41	91 (公眾諮詢)	鑑於時間緊迫，入境處應考慮召開一個由各主要的公眾代表組成的諮詢小組，以提供一個有效渠道介紹建議的相關資料及收集回應，這項諮詢不需要於短期內完成，可與招標過程同時進行。	一個開放給市民及關注小組參加的立法會保安事務委員會特別會議，已於 2000 年 11 月 11 日舉行，並於 2000 年 12 月 6 日及 2001 年 1 月 6 日舉辦公開論壇，邀請公眾人士及關注小組參加。	當局已成立由代表智能卡及資訊科技工業人士參與的智能卡論壇，並在智能式身分證電腦系統標書截止投標前，在二零零一年八月三十一日和二零零一年九月二十一日舉行了兩次討論。 當局在智能式身分證電腦系統標書截止投標前，到訪本地大學的智能卡專業人員，徵詢他們的意見。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
42	92 (公眾諮詢)	在身分證換領計劃實施前，應當舉行大型公眾資訊及教育活動。活動內容應包括令市民知悉及明白如何使用建議中的自助資訊服務站，以查閱智能卡晶片上所儲存的資料。活動亦應闡釋各項私隱關注和已採取的處理方法。	正在安排中。	入境處智能身分證計劃小組在二零零二年五月成立了智能身分證(總務)科，與政府新聞處共同計劃主要宣傳和教育活動。
43	92 (公眾諮詢)	入境處應把私隱事項的資料包括在公眾資訊活動及推出新身分證計劃前後的有關宣傳活動中。	完成。各項具體保障私隱措施已詳列在宣傳單張內。	沒有進一步發展。
44	92 (程序)	入境處在應允查閱要求時，應採用現有的法定程序。 為有關申請而設計的大部分證書模版，是專為迎合這些特定需要而設的。 入境處應透過提供所有適用的個人資料及任何可能需要作出的解釋(例如代碼)，以確保這些要求的	已經遵從。	沒有進一步發展。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		回應已符合保障資料原則的第 6 原則及《個人資料(私隱)條例》第 19(1)條。		
45	92 (程序)	入境處應檢討保障資料原則的第 6 原則之下關於回應當事人查閱要求的過程，以確保個人可取覽所有有權取覽的人事登記資料。	已經遵從。	沒有進一步發展。
46	93 (專家意見)	徵求標書文件在分發予銷售商之前，應先由具有同類計劃經驗和私隱專業知識的人士正式檢討，以確保私隱影響評估報告中提出的額外私隱保障措施，已經詳細載入標書規格說明書內。	政府會將所有私隱影響評估所建議和政府所認同的私隱保障特點，以及額外私隱保障措施加入徵求標書文件內，並會在敲定徵求標書文件前諮詢私隱專員公署。	完成。我們在敲定智能式身分證電腦系統標書前，徵詢了個人資料私隱專員公署的意見。 智能式身分證電腦系統標書規格說明書第 VII 部，納入了第 13 條(資料私隱規定)。

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
47	93 (專家意見)	在落實合約之前，應先由具有同類計劃經驗和私隱專業知識的人士覆檢已揀選的標書，確保符合徵求標書文件的私隱設定要求。	政府會小心審核投標文件，確保符合徵求標書文件中的私隱設定要求，並會在落實合約前諮詢私隱專員公署。	標書的評審工作由一個跨部門的評審委員會(成員包括政府高級官員)根據中央投標委員會通過的指定甄選程序和準則進行。當局亦徵詢了個人資料私隱專員公署的意見，以決定所揀選的計劃書是否符合標書所訂明的私隱規定。根據個人資料私隱專員公署的意見，當局改良了計劃書，確保承辦商完全履行標書在私隱方面的規定。
48	95 (一般)	入境處須認清建議計劃中的重大私隱含意及由下列各項所引發實施綜合私隱策略的需要： ■ 合法授權及限制； ■ 最理想是直接向公眾進行諮詢，若然不可，至少也應諮詢主要代表； ■ 技術性的詳細規格說明書；	政府已就有關建議與私隱專員公署商討，並且同意私隱策略應包含下列範疇： 立法的事宜－確保所有必需的保障資料私隱措施已在法例中訂明，以防止濫用情況和建立公眾人士的信心； 行政的事宜－確保已制定程序上所需的保障措施和實務守則；	現正進行第二次私隱影響評估(二零零二年四月)。

首次私隱影響評估建議的最新情況

	頁碼 (性質)	顧問的意見／建議	政府的回應／前瞻 (首次私隱影響評估)	截至二零零二年四月三十日 的最新情況 (香港特區政府提供的資料)
		■ 組織的政策承諾； ■ 《個人資料(私隱)條例》的遵守；及 ■ 公眾意識、教育及培訓活動。 實施綜合私隱策略將涉及多個範疇，包括法例修改、政策承諾、以及在計劃的設計、招標、訂立合約和實施的各個階段的詳細規格設定。	技術性的事宜－確保系統中所需的加強保障私隱技術均在系統中完全建立； 宣傳的事宜－確保公眾完全了解身分證可以提供的功能和他們的資料私隱權利。 在計劃推行的不同階段，政府會再進行私隱影響評估。我們亦會與私隱專員公署共同訂立一套實務守則。	