

(香港大學計算機科學及資訊系統系  
資訊保安及密碼學研究中心用箋)

香港中區  
花園道3號  
萬國寶通銀行大廈3樓  
立法會秘書處  
《2001年人事登記(修訂)條例草案》委員會秘書

事由：《2001年人事登記(修訂)條例草案》

敬啟者：

因應閣下所發出有關“邀請各界就《2001年人事登記(修訂)條例草案》提出意見”的諮詢文件，本人謹代表香港大學資訊保安及密碼學研究中心就本港建議中的智能式身份證提出意見。由於本中心是一所保安技術研究中心，因此，所提意見將集中於推行具備多種用途功能的智能式身份證的技術事宜，而非該建議在法律方面的事宜。儘管如此，本中心希望從技術角度提出的意見，將有助公眾更深入瞭解新身份證所造成的影響。

- 有關新智能式身份證的普遍關注事項，是身份證晶片所儲存資料的保密及保障私隱問題。在保安設計方面的基本原則是，晶片內所儲存的資料應盡量減至最少。對於儲存於晶片內而未有印載於卡面的任何資料，均須訂定充分的取覽保障措施(例如加設密碼)，或採用最新加密技術予以加密。至於晶片內所儲存並同時印載於卡面的資料，最好仍以取覽保障措施或加密技術加以保護，以防止任何人利用電子方式複製有關資料。
- 任何以智能卡為基礎的系統均存在兩大保安問題。其一為智能卡的實體保安問題。為確保採用現時可接納的保安方法，政府當局應規定身份證的設計必須符合國際智能卡標準，例如ISO 7816系列的設計標準，使供應商可予以遵從。
- 另一關注事項是儲存於後端電腦伺服器的資料的保密及保障私隱問題，因智能卡將以之作為核實身份的工具。與上述智能卡實體保安問題相比之下，此問題更為重要，因為後端電腦伺服器所儲存的市民資料，料將遠較智能卡所儲存的資料為多。因此，所有有關的政府部門務須實施明確而足夠的保安措施，以確保後端電腦伺服器所儲存的資料得以保密，而資料的私隱亦獲得保障。

- 使用智能式身份證的優點之一，在於此種身份證實際上是一部微型電腦，以便可利用身份證及身份證閱讀器進行相互認證。倘能正確執行此種相互認證機制，將可防止系統遭到入侵，例如偽造身份證閱讀器以盜取身份證所儲存的資料。新的智能式身份證必須具備此特點。
- 本中心得悉智能式身份證將具備指紋認證功能。從保安角度而言，只在智能式身份證內儲存若干選定的指紋資料而非所有指紋資料，而且在技術上不可能重組取自身份證的指紋資料，實屬相當重要。倘有關係統設計得宜，即使只儲存選定的指紋資料，仍可進行具有成效及有效率的指紋認證工作。

以上所述是我們作為一羣資訊保安研究員所最為關注的事項。如有進一步的問題，請隨時與我們聯絡。

香港大學  
資訊保安及密碼學研究中心主任  
許志光博士

2002年9月19日