林國恩教授於2002年10月11日
就智能式身份證電腦系統
因應對《人事登記條例》作出的修訂而採取的保安措施
所提出的意見

從保安及私隱角度而言，智能式身份證電腦系統須包括以下特點：

- 訂定取覽管制措施，以確保在網上傳送人事登記資料或將之儲存於資料庫時，不會在未獲授權的情況下披露有關資料。

- 在持證人獲發身份證後，不得在未獲授權的情況下取覽及修改儲存於身份證智能晶片內的人事登記資料。

- 套取以作身份核實用途的拇指指紋不得用作未獲《人事登記條例》認可的其他用途。

智能式身份證電腦系統結合了保安基礎設施、精密的智能卡運作系統及廣泛採用的防干擾讀卡設備，從而達到上述要求。此外，智能式身份證亦加入了額外的保安措施，以應付基本加密系統出現問題的突發情況。

保安基礎設施就透過智能式身份證電腦系統儲存、處理及傳送人事登記資料，對取覽該等資料實施及執行嚴格的管制。當局結合了保密權管理技術及端到端保安計劃，對該系統作出取覽管制及通訊保安。採用端到端保安措施，可確保透過政府電腦網絡傳送的人事登記資料，亦即由發送資料的辦事處傳送至入境處總部主伺服器的資料，可受到嚴密的加密措施保障，而不能在傳送過程中被截取資料。

當局採用MULTOS運作系統作為智能式身份證的操作平台。該系統設有內置保安機制，可將智能卡晶片所儲存的多種用途分開。該系統亦設有既定機制，以便在發卡後安全穩妥地在晶片載入及從晶片刪除某些用途。此等保安特點可確保智能式身份證能支援多種用途，而無須憂慮卡上用途之間會出現干擾(此類干擾所指的是一種卡上用途導致出現須取覽屬另一卡上用途的資料的情況)。此外，日後如須載入及刪除卡上用途，將只可由獲得智能式身份證電腦系統授權的有關方面進行。至於即場使用智能式身份證，亦即使用智能式身份證核實持證人身份時，有關方面會在實際安全的環境下進行各項敏感活動(如套取拇指指紋)，以便在有人試圖干擾設備以取覽敏感資料時，會導致設備內所載資料遭到刪除。

總括而言，智能式身份證電腦系統採用多種保安技術實施保安及風險管理措施，以達到人事登記資料的保安要求。採用智能卡技術可使日後簽發的身份證具有更高防偽能力，而採用MULTOS運作系統則容許以安全穩妥的方式在晶片內同時載入多種用途。採用防干擾技術可提供實際安全的環境，以供處理敏感資料，例如從持證人套取的拇指指紋模版。