附件二、結合實體身分識別與網路身分識別功能於同一載具之印製規格

1□門禁差勤之身分識別晶片規格

(一)具備非接觸式感應介面，提供符合ISO14443A規格可用於實體安全控管機制。

(二)容量為1K 位元組 EEPROM。

(三)分為16個磁區，每個磁區為4塊，每塊16個位元組，以塊為存取單位。

(四)每個磁區有獨立的一組密碼及訪問控制。

(五)每張卡有唯一序列號，為32位元。

(六)無電源，自帶天線，內含加密控制邏輯和通訊邏輯電路。

(七)資料保存期為10年，可改寫10萬次，讀無限次。

(八)工作溫度：-25℃~70℃。

(九)工作頻率：13.56MHZ。

(十)通信速率：106K位元。

(十一)讀寫距離：10cm以內。

2□晶片規格（參照自然人憑證）

(一)8位元以上中央處理單元(CPU)。

(二)符合ISO 7816-1系列標準。

(三)工作環境，溫度： 0℃~50℃，相對溼度：20%~95%。

(四)通訊介面應符合ISO 7816-3之T=0或T=1通訊協定，回應重置訊號(Answer To Reset)應符合ISO 7816-3。

(五)加解密簽章運算

1、 提供下列對稱式加解密：

(1) DES，金鑰長度支援56 位元。

(2) 3DES，金鑰長度支援。

(3) RC2，金鑰長度支援。

(4) RC4，金鑰長度支援。

2、 提供非對稱式RSA加解密運算：

(1) 金鑰長度至少可支援1024位元以上。

(2) RSA運算必須支援PKCS#11以上Padding格式。

(3) RSA運算必須支援無Padding之raw data格式。

(六)卡片執行速度

1、 RSA私密金鑰1024/2048 位元的運算平均速度須少於200/950ms。

2、 RSA公開金鑰1024/2048 位元的運算平均速度須少於25/40ms。

3、 RSA 2048位元產生RSA金鑰對運算之平均時間小於30秒。

(七)提供32K以上EEPROM記憶體空間。

(八)安全規範通過FIPS 140-1 level 2以上或ITSEC E4 High以上安全等級之認證。

(九)介面軟體功能

1、 提供微軟CSP(Cryptographic Service Provider)與PKCS#11介面之Smart Card應用程式介面及其附屬函式庫(API and *.dll)。

2、 提供RSA 簽驗章、SHA1、SHA-2雜湊演算法、DES、3DES、RC2、RC4等演算法

3、 提供RSA PKCS#1及X.509 (raw)RSA簽驗章、SHA1、SHA-2雜湊演算法、DES、3DES 加解密等演算法

4、 配合CSP或PKCS#11可支援 IE 、Outlook系列、Mozilla Firefox操作本卡片。

3□相片規格

申請人提供之相片應參照內政部訂定之「國民身分證及戶口名簿製發相片影像檔建置管理辦法」附件三「國民身分證相片規格」；其提供數位化相片檔案者，影像解析度(Resolution)為300 DPI、影像大小為300*390 DPI、檔案型式為JEPG、檔案名稱由各機關自行統一格式。

4□實體身分識別面印刷規格

(一)請依據下列機關分級製作

1、 中央一級機關：無外框

2、 中央二級機關：單外框

3、 中央三級、四級機關：雙外框加三級機關全銜

4、 外框顏色原則為紅色

(二)至少需含下列防偽設計：

1、 微細字印刷

2、 UV隱形

3、 變色油墨（銀變紫）

（圖例如下）

5□ 網路身分識別面印刷規格：參照內政部憑證管理中心有關自然人憑證規定辦理。