行政院及所屬各機關公務人員電子識別證管理作業要點

 第九點第二款、附件一及附件二修正對照表

| 修　正　規　定 | 現　行　規　定 | 說明 |
| --- | --- | --- |
| 九、電子識別證之核發作業應依下列規定辦理：(二)前款步驟涉及申請資料填寫及彙整方式，得參考附件一；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，得參考附件二。 | 九、電子識別證之核發作業應依下列規定辦理：(二)前述步驟涉及申請資料填寫及彙整方式詳如附件一；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詳如附件二。 | 說明附件為參考性質，各機關可視需求自行調整申請書內容與卡片印製規格。 |
| 附件一、公務人員電子識別證申請資料填寫及彙整方式一、人事基本資料：由機關人事人員彙整電子試算表格，內有以下欄位(表例如下)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **編號** | **機關名稱** | **機關英文名稱** | **上級****機關名稱** | **上級機關英文縮寫** | **中文姓名** | **護照上英文姓名** | **國民身分證****統一編號** | **申請人****照片檔名** |
| **１** | **檔案管****理局** | **National Archives Administration** | **國家發展委員會** | **NDC** | **王大明** | **WANG,****DA-MING** | **A123456789** | **A123456789.jpg** |

 | 附件一、公務人員電子識別證申請資料填寫及彙整方式一、人事基本資料：由機關人事人員彙整電子試算表格，內有以下欄位(表例如下)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **編號** | **機關名稱** | **機關英文名稱** | **上級****機關名稱** | **上級機關英文縮寫** | **中文姓名** | **護照上英文姓名** | **國民身分證****統一編號** | **申請人****照片檔名** |
| **１** | **檔案管****理局** | **National Archives Administration** | **行政院研究發展考核委員會** | **RDEC** | **王大明** | **WANG,****DA-MING** | **A123456789** | **A123456789.jpg** |

 | 配合組織改造，修正機關名稱。 |
|  電子識別證申請資料表格各欄位格式說明:1. 機關名稱請至行政院人事行政

總處網站查詢：(<http://www.dgpa.gov.tw>)。1. 上級機關的英文縮寫，請詳細查明後正確填寫；無上級機關者免填。以檔案管理局為國家發展委員會（National Development Council）所屬機關為例，則於上級機關英文縮寫欄填具NDC。
 | 電子識別證申請資料表格各欄位格式說明:1. 機關名稱請至行政院人事行政局網站查詢：

 　　 (<http://www.cpa.gov.tw>)。1. 上級機關的英文縮寫，請詳細查明後正確填寫；無上級機關者免填。以檔案管理局為行政院研究發展考核委員會（Research, Development and Evaluation Commission, Executive Yuan）所屬機關為例，則於上級機關英文縮寫欄填具RDEC。
 | 配合組織改造，修正機關名稱及網址 |
| ３、姓名需使用Unicode碼；超出Unicode碼範圍以外的中文字，以國家標準交換碼（CNS11643）中文編碼#<PP-XXYY>的格式為之。 | 1. 姓名需使用標準BIG-5碼；超出BIG-5碼範圍以外的中文字，以國家標準交換碼（CNS11643）中文編碼#<PP-XXYY>的格式為之。
 | 修正編碼方式為Unicode碼 |
| 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(五)加解密簽章運算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。 (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。
 | 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(五)加解密簽章運算2、提供非對稱式RSA加解密運算： (1)金鑰長度至少可支援1024以上。 (六)卡片執行速度1. RSA私密金鑰1024 位元的

運算平均速度須少於 950ms。1. RSA公開金鑰1024 位元的運算平均速度須少於400ms。
2. RSA 1024 位元產生RSA金鑰對運算之平均時間小於15秒，最長小於60秒。
 | 修正演算法長度及卡片執行速度 |
| (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。
 | (九)介面軟體功能1. 支援Microsoft Cryptography Service Providers (CSP)與RSA PKCS#11介面。
2. 提供用戶可直接由IE、Outlook、Outlook Express、Netscape Browser及 Netscape Messenger中直接操作本卡片。
3. 提供Microsoft CSP與PKCS#11介面之Smart Card應用程式介面及其附屬函式庫(API and \*.dll)。
4. 提供詳細的Application Data Unit(APDU)指令範例文件，說明如何產生RSA金鑰對(Key Pair)和輸入憑證(Certificate)。
 | 配合演算法長度及功能，修正介面軟體功能 |
| （圖例如下）國發會識別證_最終版v2 | （圖例如下） | 配合組織改造，修正機關名稱及版面。 |