

政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪
第 1.1 版修正說明

修正規定	現行規定	修正說明
<p>一、1.2.1 用戶公鑰憑證的種類</p> <p>GPKI 之用戶公鑰憑證的種類目前包括政府機關(構)公鑰憑證、政府單位公鑰憑證、公司憑證、分公司憑證、商號憑證、社團法人憑證、財團法人憑證、學校憑證、自然人憑證、伺服器應用軟體公鑰憑證，各憑證的相關用戶為：</p> <p>(6)社團法人憑證 簽發對象為依我國民法在我國登記的全國性或地方性社團法人。</p> <p>(7)財團法人憑證 簽發對象為依我國民法在我國登記的全國性或地方性財團法人。</p> <p>(8)學校憑證 簽發對象為依我國教育相關法規所設立的各級公私立學校。</p> <p>(9)自然人憑證 簽發對象為依我國戶籍法在我國設有戶籍的自然人。</p> <p>(10)伺服器應用軟體憑證 其對象為軟體程序，例如 Secure Web (SSL) Server、Time Stamp Server、OCSP Server 及專屬應用伺服器軟體等。</p>	<p>1.2.1 用戶公鑰憑證的種類</p> <p>GPKI 之用戶公鑰憑證的種類目前包括政府機關(構)公鑰憑證、政府單位公鑰憑證、公司憑證、分公司憑證、行號憑證、自然人憑證、伺服器應用軟體公鑰憑證，各憑證的相關用戶為：</p> <p>(6)自然人憑證 簽發對象為依我國戶籍法在我國設有戶籍的自然人。</p> <p>(7)伺服器應用軟體憑證 其對象為軟體程序，例如 Secure Web (SSL) Server、Time Stamp Server、OCSP Server 及專屬應用伺服器軟體等。</p>	<p>1. 新增社團法人、財團法人與學校三類憑證格式，以規範組織與團體憑證管理中心 (XCA) 簽發用戶憑證之格式。</p> <p>2. 依據商業登記法用詞將行號憑證改為商號憑證</p>
<p>二、新增 1.3.8 To-Be-Signed 社團法人憑證格式</p>	<p>無</p>	<p>規範 XCA 簽發社團法人憑證之格式。</p>
<p>三、新增 1.3.9 To-Be-Signed 財團法人憑證格式</p>	<p>無</p>	<p>規範 XCA 簽發財團法人憑證之格式。</p>
<p>四、新增 1.3.10 To-Be-Signed 學校憑證格式</p>	<p>無</p>	<p>規範 XCA 簽發學校憑證之格式。</p>

修正規定	現行規定	修正說明
<p>五、修改各章節憑證格式中之 accessLocation 欄位說明： 此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址</p>	<p>此 URL 指向一個包含 Issuing CA 本身憑證及其所有上層 CA 憑證（一直往上到 Root CA 憑證為止）的檔案，該檔案的格式是 PKCS#7 憑證串列</p>	<ol style="list-style-type: none"> 刪除「及其所有上層 CA 憑證（一直往上到 Root CA 憑證為止）」，因為根據測試，實務上的做法只需要在 PKCS#7 檔案中包含上一層 Issuing CA 的交互憑證即可。 容許 URL 指向一個 LDAP Entry 而不是只能指向一個 PKCS#7 檔案。 以下章節之憑證格式之 accessLocation 欄位說明皆做修正。 <ol style="list-style-type: none"> 1.3.2 To-Be-Signed 交互憑證格式。 1.3.3 To-Be-Signed 政府機關憑證格式。 1.3.4 To-Be-Signed 政府單位憑證。 1.3.5 To-Be-Signed 公司憑證格式。 1.3.6 To-Be-Signed 分公司憑證格式。 1.3.7 To-Be-Signed 行號憑證格式。 1.3.11 To-Be-Signed 自然人憑證格式。 1.3.12 To-Be-Signed Server AP 憑證格式。
<p>六、1.3.3 To-Be-Signed 政府機關憑證格式 subject 欄位政府機關的 X.500 Name 格式如下： C=TW L=縣市名稱(選擇性欄位，只適用於地方政府) L=鄉鎮市區名稱(選擇性欄位，只適用於地方政府) O=機關(構)的法定名稱 OU=附屬機關(構)的法定名稱(選擇性欄位，可以有多層)</p>	<p>1.3.3 To-Be-Signed 政府機關憑證格式 subject 欄位政府機關的 X.500 Name 格式如下： C=TW L=縣市名稱(選擇性欄位，只適用於地方政府) O=機關(構)的法定名稱 OU=附屬機關(構)的法定名稱(選擇性欄位，可以有多層)</p>	<p>修改命名規則，以便能命名至鄉鎮市區級的政府機關。</p>
<p>七、1.3.3 To-Be-Signed 政府機關憑證格式 entityOID 欄位內容：</p>	<p>1.3.3 To-Be-Signed 政府機關憑證格式 governmentOrganizationOID 欄</p>	<p>1. OID 代碼也適用於社團法人、財團法人與學校，所以把</p>

修正規定	現行規定	修正說明
<p>個體OID屬性,其 type 與 values 如下:</p> <p>說明: 此屬性用來記載此憑證 Subject 的 <u>OID</u></p>	<p>位</p> <p>內容: <u>政府機關/單位OID屬性</u>,其 type 與 values 如下:</p> <p>說明: 此屬性用來記載此憑證 Subject 的<u>政府機關代號</u></p>	<p>governmentOrganizationOID 這個 ASN.1 定義改為 entityOID,使其較為廣義。</p> <p>2. Value 之說明直接寫成記載 Subject 的OID,避免與人事行政局之「機關代碼」混淆。</p>
<p>八、1.3.3 To-Be-Signed 政府機關憑證格式 type 欄位</p> <p>內容: OID id-chtpki-at-<u>entityOID</u> (2.16.886.1.100.2.102)</p> <p>說明: 此為代表 <u>Entity</u> OID Attribute 之OID</p>	<p>1.3.3 To-Be-Signed 政府機關憑證格式 type 欄位</p> <p>內容: OID id-chtpki-at-<u>governmentOrganizationOID</u> (2.16.886.1.100.2.102)</p> <p>說明: 此為代表 <u>Government Organization</u> OID Attribute 之OID</p>	<p>OID 代碼也適用於社團法人、財團法人與學校,所以把 governmentOrganizationOID 這個 ASN.1 定義改為 entityOID,使其較為廣義。</p>
<p>九、1.3.4 To-Be-Signed 政府單位憑證格式 subject 欄位</p> <p>政府單位的 X.500 Name 格式如下: C=TW L=縣市名稱(選擇性欄位,只適用於地方政府) L=鄉鎮市區名稱(選擇性欄位,只適用於地方政府) O=機關(構)的法定名稱 OU=附屬機關(構)的法定名稱(選擇性欄位,可以有多層) OU=附屬單位的法定名稱</p>	<p>1.3.4 To-Be-Signed 政府單位憑證格式</p> <p>政府單位的 X.500 Name 格式如下: C=TW L=縣市名稱(選擇性欄位,只適用於地方政府) O=機關(構)的法定名稱 OU=附屬機關(構)或單位的法定名稱(選擇性欄位,可以有多層) OU=附屬單位的法定名稱</p>	<p>修改命名規則,以便能命名至鄉鎮市區級的政府單位。</p>
<p>十、1.3.4 To-Be-Signed 政府單位憑證格式 <u>entityOID</u> 欄位</p> <p>內容: 個體OID屬性,其 type 與 values 如下:</p> <p>說明: 此屬性用來記載此憑證 Subject 的 <u>OID</u></p>	<p>1.3.4 To-Be-Signed 政府單位憑證格式</p> <p><u>governmentOrganizationOID</u> 欄位</p> <p>內容: 政府機關/單位OID屬性,其 type 與 values 如下:</p> <p>說明 此屬性用來記載此憑證 Subject 的<u>政府單位代號</u></p>	<p>1. OID 代碼也適用於社團法人、財團法人與學校,所以把 governmentOrganizationOID 這個 ASN.1 定義改為 entityOID,使其較為廣義。</p> <p>2. Value 之說明直接寫成記載 Subject 的OID,避免與人事行政局之「單位代碼」混淆。</p>

修正規定	現行規定	修正說明
<p>十一、1.3.4 To-Be-Signed 政府單位憑證格式 type 欄位</p> <p>內容： OID id-cthpk-at-entityOID (2.16.886.1.100.2.102)</p> <p>說明： 此為代表 <u>Entity</u> OID Attribute 之 OID</p>	<p>1.3.4 To-Be-Signed 政府單位憑證格式 type 欄位</p> <p>內容： OID id-cthpk-at-governmentOrganizationOID (2.16.886.1.100.2.102)</p> <p>說明： 此為代表 <u>Government Organization</u> OID Attribute 之 OID</p>	<p>OID 代碼也適用於社團法人、財團法人與學校，所以把 governmentOrganizationOID 這個 ASN.1 定義改為 entityOID，使其較為廣義。</p>
<p>十二、1.3.12 To-Be-Signed Server AP 憑證格式 subject 欄位</p> <p>Server AP 的 X.509 Name 格式如下： C=TW L=縣市名稱(選擇性欄位，只適用於地方政府) L=鄉鎮市區名稱(選擇性欄位，只適用於地方政府) O=機關(構)的法定名稱 OU=附屬機關(構)或單位的法定名稱(選擇性欄位，可以有幾層) CN=伺服器應用軟體的名稱(可能是伺服器應用軟體之網域名稱、網路位址或其他文字名稱) serialNumber=伺服器應用軟體的識別代號(用以區分同一網域名稱或網路位址上不同的伺服器應用軟體)</p>	<p>1.3.12 To-Be-Signed Server AP 憑證格式 subject 欄位</p> <p>Server AP 的 X.509 Name 格式如下： C=TW L=縣市名稱(選擇性欄位，只適用於地方政府) O=機關(構)的法定名稱 OU=附屬機關(構)或單位的法定名稱(選擇性欄位，可以有幾層) CN=伺服器應用軟體的名稱(可能是伺服器應用軟體之網域名稱、網路位址或其他文字名稱) serialNumber=伺服器應用軟體的識別代號(用以區分同一網域名稱或網路位址上不同的伺服器應用軟體)</p>	<p>修改命名規則，以便能命名至鄉鎮市區級的政府機關單位之 Server AP。</p>
<p>十三、新增 3 參考文獻</p>		<p>參考文獻說明引述之標準</p>