政府機關公開金鑰基礎建設(GPKI)

憑證及憑證廢止清冊格式剖繪第 2.3 版變更總說明

一、背景說明

本次修訂配合醫事憑證管理中心(HCA)不再提供SSL憑證之簽發、組織及團體憑證管理中心(XCA)提供應用系統專屬類憑證及經濟部工商憑證管理中心(MOEACA)提供新的客戶端專屬憑證等，並修正誤植文字。

二、修訂內容摘要

(一) 新增應用軟體客戶端專屬憑證格式之相關說明。

(二) 修訂SSL類伺服應用軟體憑證格式之說明。

(三) 修訂subjectAltName擴充欄位之說明。

(四) 將Server AP與SSL Server修改為「SSL/TLS Server」。

(五) 修訂專屬類伺服應用軟體憑證之說明。

(六) 修訂keyUsage擴充欄位內容，新增單金鑰對之金鑰用途為簽章用或加解密用時之相關說明。

(七) 修訂subject欄位之X.500 Name格式說明，將項目CN與serialNumber之順序位置互換。

(八) 修訂subject欄位之說明，將憑證主體識別名稱之格式名稱由「X.509 Name」修改為「X.500 Name」。

(九) 修訂Extensions擴充欄位名稱，將誤植之文字「Extrensions」或「extrensions」修正為「extensions 」。

三、修訂內容說明

(一) 新增應用軟體客戶端專屬憑證格式之相關說明：

說明：因應組織及團體憑證管理中心(XCA)可提供應用系統專屬類憑證以及經濟部工商憑證管理中心(MOEACA)可提供「公司與商業及有限合夥一站式線上申請作業網站」辦理新公司、新商業或新有限合夥設立登記用之預查憑證的簽發，故新增應用軟體客戶端專屬憑證格式，並更新用戶公鑰憑證種類之說明。

(二) 修訂SSL類伺服應用軟體憑證格式之說明：

說明：依據CA/Browser Forum Baseline Requirements對SSL憑證主體識別名稱之規定，並考量醫事憑證管理中心(HCA)不再提供SSL憑證之簽發，故修訂SSL類伺服應用軟體憑證格式之subject欄位，並更新伺服應用軟體憑證格式之相關說明。

(三) 修訂subjectAltName擴充欄位之說明：

說明：因SSL類伺服應用軟體憑證格式之subjectAltName擴充欄位有文字誤植，故修訂該擴充欄位內容之說明，將資料

型態GeneralNames可包含的GeneralName由1個改為1個或多個。

(四) 將Server AP與SSL Server修改為「SSL/TLS Server」：

說明：SSL類伺服應用軟體憑證格式中所述之Server AP、SSL Server及SSL/TLS Server等用詞之意義相同，為使其用詞一致，故統一修訂為「SSL/TLS Server」。

(五) 修訂專屬類伺服應用軟體憑證之說明：

說明：因專屬類伺服應用軟體憑證之簽發對象說明有誤，將簽發對象由「伺服應用軟體憑證」修改為「伺服應用軟體」，並微調該句標點符號之用法。

(六) 修訂keyUsage擴充欄位內容，新增單金鑰對之金鑰用途為簽章用或加解密用時之相關說明：

說明：因專屬類伺服應用軟體憑證格式之keyUsage擴充欄位遺漏單金鑰對用於簽章或加解密時之金鑰用途說明，故補充說明之。

(七) 修訂subject欄位之X.500 Name格式說明，將項目CN與serialNumber之順序位置互換：

說明：因調整一站式專屬授權憑證主體識別名稱之排列順序，故修訂該憑證格式之subject欄位，將X.500 Name格式中

之項目CN與serialNumber的順序位置相互交換。

(八) 修訂subject欄位之說明，將憑證主體識別名稱之格式名稱由「X.509 Name」修改為「X.500 Name」：

說明：因部分憑證格式之subject欄位用以描述憑證主體識別名稱之格式名稱有誤，故修訂該欄位內容之說明，將誤植該格式名稱「X.509 Name」修正為「X.500 Name」。

(九) 修訂Extensions擴充欄位名稱，將誤植之文字「Extrensions」或「extrensions」修正為「extensions 」：

說明：因憑證格式之Extensions欄位名稱有誤，故修訂該欄位名稱，將誤植之文字「Extrensions」或「extrensions」修正為「extensions 」。