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 2.4 版

一、背景說明

(一) 因應經濟部工商憑證管理中心(Ministry of Economic Affairs Certification Authority, MOEACA)提供行動工商憑證以及內政部憑證管理中心(Ministry of the Interior Certification Authority, MOICA)提供外來人口申請行動自然人憑證，修訂相關憑證格式，新增憑證Subject之持有人使用行動載具或卡片持有人為行動載具持有人之說明。

(二) 因應量子計算對現行公開金鑰密碼技術(包含簽章與加密機制)之威脅，增訂支援後量子密碼(Post-Quantum Cryptography, PQC)憑證及憑證廢止清冊格式剖繪之相關規劃。

(三) 因應第一代政府憑證總管理中心(Government Root Certification Authority, GRCA)已停止使用sha1WithRSAEncryption簽章演算法簽發憑證廢止清冊(Certificate Revocation List, CRL)，修訂憑證廢止清冊格式使用之簽章演算法物件識別碼(Object Identifier, OID)。

(四) 修正文件中誤植、缺漏或過時資訊，並配合調整部分內容敘述、文句編排、對齊相關標準規範及更新引用之參考文獻。

二、修訂內容摘要

(一) 修訂公司憑證、分公司憑證、商業憑證及有限合夥憑證等憑證格式之subjectDirectoryAttributes擴充欄位，於其屬性cardHolderRank新增憑證Subject之持有人使用行動載具之相關說明。

(二) 修訂外來人口自然人憑證格式之subjectDirectoryAttributes擴充欄位，於其屬性cardHolderRank新增憑證Subject之卡片持有人為行動載具持有人之相關說明。

(三) 新增附錄A，說明支援 PQC 憑證及憑證廢止清冊格式剖繪之規劃，並載明相關格式及欄位設計須依附錄A所定規範辦理。

(四) 修訂CRL格式可使用之簽章演算法OID，移除與SHA-1雜湊函數演算法搭配使用之簽章演算法OID。

(五) 修訂自簽憑證、自發憑證及交互憑證等憑證格式之keyUsage擴充欄位，新增金鑰亦可用於簽發線上憑證狀態協定回應訊息時之金鑰用途相關說明。

(六) 修訂憑證及CRL設計原則之參考資料來源，並微調前述設計原則所引用之RFC標準與相容憑證/CRL格式的主體資訊。

(七) 修訂憑證及 CRL 格式之簽章演算法/金鑰描述，並統一修正用詞「SSL」或「SSL/TLS」為「TLS」。

(八) 修訂自發憑證、交互憑證及TLS類伺服器應用軟體憑證等憑證格式之certificatePolicies擴充欄位，刪除與憑證機構及瀏覽器論壇(CA/Browser Forum)定義之憑證政策(Certificate Policy, CP) OID相關之說明。

(九) 修訂公司憑證、分公司憑證、商業憑證、一站式專屬授權憑證及應用軟體客戶端專屬憑證等憑證格式之subject欄位，調整與MOEACA相關主體DN中serialNumber屬性欄位之敘述，明確其唯一序號所對應之主體。

(十) 修訂除自簽憑證格式外之所有憑證格式，調整其authorityInfoAccess擴充欄位之caIssuers存取資訊之敘述，明確納入單一DER編碼憑證之提供方式，以符合RFC 5280規範，並配合微調該擴充欄位相關文句。

三、修訂內容說明

(一) 修訂公司憑證、分公司憑證、商業憑證及有限合夥憑證等憑證格式之subjectDirectoryAttributes擴充欄位，於其屬性cardHolderRank新增憑證Subject之持有人使用行動載具之相關說明。

說明：因應MOEACA可提供行動工商憑證之簽發，故修訂公司憑證、分公司憑證、商業憑證及有限合夥憑證等憑證格式之

subjectDirectoryAttributes擴充欄位的屬性cardHolderRank，新增憑證Subject之持有人使用行動載具之相關說明。

(二) 修訂外來人口自然人憑證格式之subjectDirectoryAttributes擴充欄位，於其屬性cardHolderRank新增憑證Subject之卡片持有人為行動載具持有人之相關說明。

說明：因應MOICA可提供外來人口申請行動自然人憑證，故修訂外來人口自然人憑證格式之subjectDirectoryAttributes擴充欄位的屬性cardHolderRank，新增憑證Subject之卡片持有人為行動載具持有人之相關說明。

(三) 新增附錄A，說明支援 PQC 憑證及憑證廢止清冊格式剖繪之規劃，並載明相關格式及欄位設計須依附錄A所定規範辦理。

說明：因應量子計算對現行公開金鑰密碼技術(包含簽章與加密機制)之威脅，新增附錄A，說明支援PQC憑證及憑證廢止清冊格式剖繪之規劃，包含導入PQC演算法與相關技術標準時，既有憑證及憑證廢止清冊需配合調整之欄位與設計原則，並於第1.3節「憑證格式」與第2.4節「憑證廢止清冊格式」新增PQC憑證及憑證廢止清冊格式與演算法規劃之附錄參考說明，於第1.1.2節「CA憑證的設計原則」、第1.2.2節「用戶憑證的設計原則」及第2.2節「憑證廢止清冊的設計原則」

新增採用 PQC 演算法時應依附錄A規範辦理之說明。

(四) 修訂CRL格式可使用之簽章演算法OID，移除與SHA-1雜湊函數演算法搭配使用之簽章演算法OID。

說明：因應第一代GRCA已停止使用簽章演算法「sha1WithRSAEncryption」簽發CRL，故修訂CRL格式及其3種To-Be-Signed CRL所使用之簽章演算法OID，移除該簽章演算法相關資訊。

(五) 修訂自簽憑證、自發憑證及交互憑證等憑證格式之keyUsage擴充欄位，新增金鑰亦可用於簽發線上憑證狀態協定回應訊息時之金鑰用途相關說明。

說明：因自簽憑證、自發憑證及交互憑證等憑證格式之keyUsage擴充欄位遺漏金鑰亦可用於簽發線上憑證狀態協定回應訊息時之金鑰用途說明，故補充說明之。

(六) 修訂憑證及CRL設計原則之參考資料來源，並微調前述設計原則所引用之RFC標準與相容憑證/CRL格式的主體資訊。

說明：因憑證及CRL設計原則之參考資料已過時，故修訂相關參考文獻，並依更新後之參考文獻微調CA憑證、用戶憑證及CRL設計原則所引用之RFC標準與相容憑證/CRL格式的主體資訊。

(七) 修訂憑證及 CRL 格式之簽章演算法/金鑰描述，並統一修正用

詞「SSL」或「SSL/TLS」為「TLS」。

說明：修訂憑證及CRL格式(包含其To-Be-Signed憑證及CRL格式)之簽章演算法/金鑰描述，使其表達更為中性與準確。同時，考量SSL通訊協定已遭淘汰，故修訂用詞「SSL/TLS」，統一更改為「TLS」，以符合現行標準。

(八) 修訂自發憑證、交互憑證及TLS類伺服器應用軟體憑證等憑證格式之certificatePolicies擴充欄位，刪除與CA/Browser Forum定義之CP OID相關之說明。

說明：考量GPKI憑證政策以及GRCA與政府憑證管理中心(Government Certification Authority, GCA)之憑證實務作業基準已於先前版本移除遵循CA/Browser Forum所發布之Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates相關敘述，故配合修訂自發憑證、交互憑證及TLS類伺服器應用軟體憑證等憑證格式之certificatePolicies擴充欄位，刪除前述規範所對應之CP OID相關說明。

(九) 修訂公司憑證、分公司憑證、商業憑證、一站式專屬授權憑證及應用軟體客戶端專屬憑證等憑證格式之subject欄位，調整與MOEACA相關主體DN中serialNumber屬性欄位之敘述，明確其唯一序號所對應之主體。

說明：現行公司憑證、分公司憑證、商業憑證、一站式專屬授權憑證及應用軟體客戶端專屬憑證等憑證格式之subject欄位中serialNumber屬性欄位之敘述，對其唯一序號所對應之主體尚有釐清空間，為避免產生解讀歧異，故配合修訂相關敘述，明確其唯一序號之賦予對象，以提升欄位語意之一致性與辨識性。

(十) 修訂除自簽憑證格式外之所有憑證格式，調整其authorityInfoAccess擴充欄位之caIssuers存取資訊之敘述，明確納入單一DER編碼憑證之提供方式，以符合RFC 5280規範，並配合微調該擴充欄位相關文句。

說明：依RFC 5280規範，authorityInfoAccess擴充欄位之caIssuers存取位置得以單一DER編碼憑證或CMS(PKCS#7)憑證串列提供相關資訊，故修訂相關描述，明確納入單一DER編碼憑證之提供方式，並配合微調該擴充欄位相關文句；適用範圍為除自簽憑證格式外之所有憑證格式。