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 2.2 版(草案)修訂摘要

一、 因應經濟部工商憑證管理中心可提供公司、商業及有限合夥一站式線上申請作業網站授權使用者之專屬授權憑證的簽發，新增「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 1.2.1 節用戶公鑰憑證的種類中有關一站式專屬授權憑證之相關說明及第 1.3.23 節 To-Be-Signed 一站式專屬授權憑證格式。(詳如附件 1)。

二、 因分公司憑證主體 DN 排列順序有誤，故修訂分公司憑證格式之 subject 欄位，修改其欄位的 X.500 Name 格式說明，將項目 OU 與 serialNumber 的順序位置互相交換。修訂內容如下：修訂「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 1.3.7 節 To-Be-Signed 分公司憑證格式中有關 subject 欄位的相關說明(詳如附件 2)。

附件 1

1.2.1 用戶公鑰憑證的種類(P.7、P.10)

GPKI 之用戶公鑰憑證的種類目前包括政府機關(構)憑證、政府單位憑證、公司憑證、分公司憑證、商業憑證、有限合夥憑證、有限合夥分支機構憑證、社團法人憑證、財團法人憑證、學校憑證、醫事機構、自由職業事務所憑證、行政法人憑證、其他組織或團體憑證、自然人憑證、外來人口自然人憑證、醫事人員、伺服器應用軟體憑證、OCSP 伺服器憑證、公司與商業及有限合夥一站式線上申請作業網站之專屬授權憑證(以下簡稱一站式專屬授權憑證),各憑證的相關用戶為：

(1) 政府機關(構)憑證

簽發對象包含中央政府機關、地方政府機關、公營事業及公立機構。

(2) 政府單位憑證

簽發對象包含上述政府機關(構)之附屬單位，或附屬單位的附屬單位。

……

(19) OCSP 伺服器憑證

簽發對象為線上憑證狀態通訊協定(OCSP) 伺服器所使用的憑證。

(20) 一站式專屬授權憑證

簽發對象為公司、商業及有限合夥之一站式線上申請作業網站授權使用者。

1.3.23 To-Be-Signed 一站式專屬授權憑證格式(P.232-241)

欄位	內容	說明
version	v3(2)	GPKI 憑證格式使用 X.509 V3 憑證格式（注意 V3 的值是 2 而不是 3）
serialNumber	憑證序號（Certificate Serial Number）	GPKI 中所使用之憑證序號是一個長度為 16 Bytes 的正整數，根據 DER 編碼對正數所使用的 2's Compliment 規則，有些序號可能會在前面補上 0x00，而使的 16 Bytes 的正整數實際上佔用 17 Bytes 的空間
signature	CA 簽發所用之簽章演算法之 AlgorithmIdentifier	此欄的值必須與外層 SIGNED 憑證之 algorithmIdentifier 欄的值相同
.algorithm	可為以下簽章演算法 OID 之一： sha1WithRSAEncryption (1.2.840.113549.1.1.5)、 sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 目前只使用以下簽章演算法： sha1WithRSAEncryption、 sha256WithRSAEncryption
.parameters	NULL	GPKI 使用的簽章演算法不需要 parameters，但其 parameters 必須填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500
issuer	憑證簽發者（CA）之 X.500 Name	CA 本身的 DN(將由 CA 主管機關訂定之) （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
validity	憑證啟用時間與憑證失效時間	憑證效期長度視憑證政策而定

.notBefore	憑證啟用的格林威治時間（GMT），在此時間之前憑證無效	依 PKIX 規定在 2049/12/31 23:59:59（含）之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，在 2050/01/01 00:00:00（含）之後，使用 GeneralizedTime 資料型態，格式為 YYYYMMDDHHMMSSZ。以上兩種格式中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略
.notAfter	憑證失效的格林威治時間（GMT），在此時間之後憑證無效	依 PKIX 規定在 2049/12/31 23:59:59（含）之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，在 2050/01/01 00:00:00（含）之後，使用 GeneralizedTime 資料型態，格式為 YYYYMMDDHHMMSSZ。以上兩種格式中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略
subject	憑證簽發對象（Subject）之 X.500 Name	如果是公司申請之一站式專屬授權憑證，則其 X.509 Name 格式如下： C=TW O=*公司的正式登記名稱* serialNumber=*憑證管理中心自動給定用戶之唯一序號* CN=*公司、商業及有限合夥一站式線上申請作業網站授權使用者* 如果是商業申請之一站式專屬授權憑證，則其 X.509

		Name 格式如下： C=TW L=*縣市名稱* O=*商業的正式登記名稱* serialNumber=*憑證管理中心自動給定用戶之唯一序號* CN=*公司、商業及有限合夥一站式線上申請作業網站授權使用者* 如果是有限合夥申請之一站式專屬授權憑證，則其 X.509 Name 格式如下： C=TW O=*有限合夥的正式登記名稱* CN=*公司、商業及有限合夥一站式線上申請作業網站授權使用者* （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
subjectPublicKeyInfo	憑證主體的 Public Key Info	記載 Subject 的 Public Key 類別及 Public Key 的值
.algorithm	代表 subjectPublicKey 類別的 AlgorithmIdentifier	
.algorithm	OID rsaEncryption (1.2.840.113549.1.1.1)	Public Key 類別之 OID，GPKI 目前只使用 rsaEncryption 之 Public Key
.parameters	NULL	rsaEncryption 演算法雖然不需要 parameters，但其 parameters 必須填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500
.subjectPublicKey	BIT STRING，此 BIT STRING 內含 Subject Public	GPKI 目前只採用 RSA Public Key，所以此 BIT

	Key 的 DER 編碼值	STRING 的值將內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extrensions	SEQUENCE OF Extensions	內容為一串擴充欄位，包含以下的擴充欄位種類（實際在憑證中的順序可能不是照以下的順序）：
.authorityKeyIdentifier	Authority Key Identifier 擴充欄位，Key Identifier 的產生方式依照 PKIX 標準，取 Issuing CA 的 Public Key 的 SHA-1 Hash 值做為 Key Identifier	此擴充欄位的目的是標示 CA 用來簽發本憑證所使用的金鑰是哪一把，以便在 CA 更換金鑰及其本身憑證時判斷應該使用 CA 的哪一張 CA 憑證來檢驗此憑證
.extnId	填入代表此擴充欄位的 OID id-ce-authorityKeyIdentifier (2.5.29.35)	
.critical	在 GPKI 中，authorityKeyIdentifier 必定是 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityKeyIdentifier 這種 Extension 而言，必須使用 AuthorityKeyIdentifier 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityKeyIdentifier	AuthorityKeyIdentifier 的資料結構含有三個 Optional 的欄位，分別是 keyIdentifier、authorityCertIssuer 與 authorityCertSerialNumber 欄位	GPKI 憑證依據 PKIX，只採用 keyIdentifier 欄位，而不使用 authorityCertIssuer 與 authorityCertSerialNumber 欄位
.keyIdentifier	keyIdentifier 欄為的資料型	KeyIdentifier 的產生方式依

	態是 KeyIdentifier，而 KeyIDentifier 本身為一個 OCTET STRING 資料型態	照 PKIX 標準，取 Subject 的 Public Key 的 SHA-1 Hash 值做為 KeyIdentifier 的 OCTET STRING 值
.subjectKeyIdentifier	Subject Key Identifier 擴充欄位，Key Identifier 的產生方式依照 PKIX 標準，取 Subject 的 Public Key 的 SHA-1 Hash 值做為 Key Identifier	此擴充欄位的目的是標示 Subject 所使用的金鑰是哪一把
.extnId	填入代表此擴充欄位的 OID id-ce-subjectKeyIdentifier (2.5.29.14)	
.critical	在 GPKI 中，subjectKeyIdentifier 必定是 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 subjectKeyIdentifier 這種 Extension 而言，必須使用 KeyIdentifier 的 DER 編碼做為此 OCTET STRING 的值
.KeyIdentifier	KeyIDentifier 本身為一個 OCTET STRING 資料型態	KeyIdentifier 的產生方式依照 PKIX 標準，取 Subject 的 Public Key 的 SHA-1 Hash 值做為 KeyIdentifier 的 OCTET STRING 值
.keyUsage	Key Usage 擴充欄位，記載 Subject Public Key 相對應之 Private Key 的用途限制	一站式專屬授權憑證的金鑰限定為簽章用途，所以 Key Usage 將只包含 digitalSignature 用途
.extnId	填入代表此擴充欄位的 OID id-ce-keyUsage (2.5.29.15)	
.critical	在 GPKI 中，keyUsage 必定是 critical extension，所以 critical 的值必定是 TRUE	注意由於 TRUE 不是 DEFAULT VALUE，所以 DER 編碼中，此欄位不可被省略掉
.extnValue	extnValue 的資料型態是	對於 keyUsage 這種

	OCTET STRING	Extension 而言，必須使用 KeyUsage 的 DER 編碼做為此 OCTET STRING 的值
.KeyUsage	KeyUsage 本身為一個 Named BIT STRING 資料型態	一站式專屬授權憑證的金鑰限定為簽章用途，因此 Named BIT STRING 之 digitalSignature(0)這個 bit 將會被設為 1。
.certificatePolicies	Certificate Policies 擴充欄位，記載 CA 簽發此憑證所使用的憑證政策	填入 CA 簽發此憑證時所依據的 GPKI Certificate Policy 之 OID
.extnId	填入代表此擴充欄位的 OID id-ce-certificatePolicies (2.5.29.32)	
.critical	為了相容性起見，在 GPKI 中，certificatePolicies 被設定為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 certificatePolicies 這種 Extension 而言，必須使用 CertificatePolicies 的 DER 編碼做為此 OCTET STRING 的值
.CertificatePolicies	CertificatePolicies 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF PolicyInformation	在 GPKI 憑證中，EE Certificate 只能含有 1 個 PolicyInformation
.PolicyInformation	PolicyInformation 為一 SEQUENCE，內含 policyIdentifier 與 policyQualifiers 兩欄	GPKI 憑證只使用 policyIdentifier 欄位，而不使用 policyQualifiers 欄位
.policyIdentifier	policyIdentifier 欄為的資料型態是 CertPolicyId，而 CertPolicyId 本身為一個 OBJECT IDENTIFIER 資料	根據 CA 簽發此憑證時所採用的保證等級（Assurance Level），填上代表該保證等級之 GPKI Certificate Policy

	型態	OID
.subjectDirectoryAttributes	Subject Directory Attributes 擴充欄位，用來記錄 Subject 特有的屬性資料	不同憑證種類所使用的屬性欄位會有所不同
.extnId	填入代表此擴充欄位的 OID id-ce-subjectDirectoryAttributes (2.5.29.9)	
.critical	在 GPKI 中，subjectDirectoryAttributes 被設定為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 subjectDirectoryAttributes 這種 Extension 而言，必須使用 SubjectDirectoryAttributes 的 DER 編碼做為此 OCTET STRING 的值
.SubjectDirectoryAttributes	SubjectDirectoryAttributes 的資料型態是 SEQUENCE SIZE (1..MAX) OF Attribute	此欄可包含一串屬性，一站式專屬授權憑證會記錄下列屬性
.subjectType	Subject 類別屬性，其 type 與 values 如下：	此屬性用來區分此憑證 Subject 的類別
.type	OID id-chtpki-at-subjectType (2.16.886.1.100.2.1)	此為代表 Subject Type Attribute 之 OID
.values	OID id-chtpki-et-enterpriseUserForOnestopService (2.16.886.1.100.3.3.3)	此 OID 表示憑證 Subject 的類別為一站式線上申請作業網站授權使用者
.cardHolderRank	持卡人的正附卡等級，其 type 與 values 如下：	此屬性用來區分此憑證 Subject 之卡片持有人的是正卡或附卡持有人。由於一站式專屬授權憑證之憑證 Subject 之卡片持有人限定為附卡持有人，所以其 values

		將只能填入 printable 字串'secondary'
.type	OID id-chtpki-at-cardHolderRank (2.16.886.1.100.2.2)	此為代表 Card Holder Rank Attribute 之 OID
.values	填入 printable 字串'secondary'	secondary'表示卡片持有人是附卡持有人
.uniformOrganizationID	統一編號屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject（一站式線上申請作業網站授權使用者之公司、商業或有限合夥）的統一編號
.type	OID id-chtpki-at-uniformOrganizationID (2.16.886.1.100.2.101)	此為代表 Uniform Organization ID Attribute 之 OID
.values	填入該公司、商業或有限合夥的統一編號	國內所使用的統一編號有 8 個位數
.cRLDistributionPoints	CRL Distribution Points 擴充欄位，記載簽發此交互憑證之 CA 公佈此憑證相關之 CRL 的網址	此擴充欄位提供憑證應用軟體取得相關 CRL 的指引，目前 GPKI 所使用之 CRL Distribution Points 可包含 1 至 2 個 URL
.extnId	填入代表此擴充欄位的 OID id-ce-cRLDistributionPoints (2.5.29.31)	
.critical	在 GPKI 中，cRLDistributionPoints 被設定為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 cRLDistributionPoints 這種 Extension 而言，必須使用 CRLDistributionPoints 的 DER 編碼做為此 OCTET STRING 的值
.CRLDistributionPoints	CRLDistributionPoints 的資	在 GPKI 憑證格式中，欄位

	料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	CRLDistributionPoints 含有 1 至 2 個 DistributionPoint。如果含兩個 DistributionPoint 時，第 1 個為 Partitioned CRL 的 URL，第 2 個為 Complete CRL 的 URL；如果只含 1 個 DistributionPoint 時，則為 Complete CRL 的 URL
.DistributionPoint	DistributionPoint 為一 SEQUENCE，內含 distributionPoint、reasons 與 cRLIssuer 三欄	GPKI 憑證只使用 distributionPoint 欄位，而不使用 reasons 與 cRLIssuer 這兩個欄位
.distributionPoint	distributionPoint 欄位的資料型態是 DistributionPointName，而 DistributionPointName 本身為一個 CHOICE 資料型態，可選用 fullName 或 nameRelativeToCRLIssuer	GPKI 憑證的 CRL distributionPoint 是採用 fullName
.fullName	fullName 的資料型態是 GeneralNames 而 GeneralNames 的資料型態是 SEQUENCE SIZE (1..MAX) OF GeneralName	GPKI 憑證的 CRL distributionPoint 的 fullName 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載 CA 公佈 CRL 檔的 URL，且若該 CRL 為 Partitioned CRL 時，則此欄位所記載的 URL 必須與該 CRL 之 issuingDistributionPoint 擴充欄位中所記載的 URL 完全相同
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其

		上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個	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

	caIssuers 的 URL	的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

附件 2

1.3.7 To-Be-Signed 分公司憑證格式(P.65-66)

欄位	內容	說明
subject	憑證簽發對象（Subject）之 X.500 Name	分公司的 X.500 Name 格式如下： C=TW O=*公司的正式登記名稱* serialNumber=*憑證管理中心自動給定用戶之唯一序號* OU=*分公司的正式登記名稱* （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）