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
(Certificate and CRL Profiles for the Government Public Key Infrastructure)
第 2.4 版

主管機關：數位發展部

執行機構：中華電信股份有限公司

中華民國 115 年 06 月 01 日

目　　錄

1 憑證格式剖繪

1.1 CA 憑證

1.1.1 CA 憑證的種類

依據 ITU-T X.509 | ISO/IEC 9594-8 公開金鑰憑證的標準[1]，CA 憑證（CA Certificate）可分為三類：

(1) 自簽憑證（Self-Signed Certificate）：

Self-Signed Certificate 是一種 CA Certificate，通常是階層式架構中 Root CA 自行簽發的 CA Certificate，是階層式 PKI 中的憑證信任起點；但有時在網狀 PKI 架構中，一般 CA 也可能簽發 Self-signed CA Certificate，以便做為所有直接信任該 CA 之用戶的憑證信任起點。

(2) 自發憑證（Self-Issued Certificate）：

Self-Issued Certificate 是一種 CA Certificate，是 GRCA 系統用在其舊金鑰到期，需更換新 CA 金鑰的時候，由 GRCA 系統舊 CA 金鑰與新 CA 金鑰互相簽署的憑證，以因應這段新舊金鑰交替過渡時期，作為由兩新舊金鑰所簽發之下屬 CA 憑證及用戶憑證之間相互信任的橋樑。

(3) 交互憑證（Cross Certificate）：

Cross Certificate 也是一種 CA Certificate，但 Cross Certificate 的簽發對象不是該 CA 本身，而是其他 CA，也就是某 CA 簽發給另一個 CA 的憑證，做為兩 CA 用戶之間憑證信任的橋樑；階層式 PKI 中上層 CA 簽發憑證予其下層 CA（Subordinate CA）之憑證屬此類憑證，而當 CA 與其他 PKI 之 CA 進行交互認證時，一個 CA 簽發給另一 CA 的憑證亦屬於此類憑證。

1.1.2 CA 憑證的設計原則

除了遵循 X.509 標準[1]之外，GPKI 之 CA 憑證欄位的設計並遵循以下原則：

- 符合 IETF PKIX Certificate and CRL Profile (RFC 5280)之憑證規格[2]。
- 符合 IETF PKIX Qualified Certificates Profile (RFC 3739)之憑證規格[3]。
- 與 Asia PKI Consortium 之憑證規格[4]相容。
- 與 FPKI 之憑證規格[5]相容。
- 與歐盟之憑證規格[6]相容。
- 與 Web Browser 相容。
- 盡量不要使用 X.509 v2 欄位（根據 RFC 5280 [2]之建議）。

當主管機關公告採用 PQC 演算法及其因應之憑證格式時，相關 CA 憑證欄位之設計與值之選用，應依本文件附錄 A 所列規範辦理。

1.1.3 CA 憑證的欄位

下表是根據以上所列原則而訂定的三種CA憑證所使用欄位。其中標註「✓」記號者，為該類憑證的必要欄位(Required Field)；標註「✗」記號者，則表示該類 CA 憑證中不使用此欄位：

欄位名稱(Field Name)	CA 憑證(CA Certificate)		
	Self-Signed Certificate	Self-Issued Certificate	Cross Certificate
version	✓	✓	✓
serialNumber	✓	✓	✓
signature	✓	✓	✓
issuer	✓	✓	✓
validity	✓	✓	✓
subject	✓	✓	✓
subjectPublicKeyInfo	✓	✓	✓
issuerUniqueIdentifier	×	×	×
subjectUniqueIdentifier	×	×	×
extensions	✓	✓	✓

以下三表是三種 CA 憑證所使用的擴充欄位，其中標註「✓」記號者，為該類憑證的必要擴充欄位(Required Extension Field)；標註「○」記號者，為該類憑證的選擇性擴充欄位(Optional Extension Field)；標有「×」記號者，則表示該類憑證中不使用此擴充欄位。下表並對標示各種擴充欄位是否標示為 critical，其中「TRUE」表示若使用此擴充欄位，則須必標示為 critical；「FLASE」表示此擴充欄位若使用則必標示為 non-critical；「N/A」（Not Applicable）表示在 GPKI 將不於 CA 憑證中使用該擴充欄位，因此無所謂 critical 或 non-critical 的情況。

Self-Signed Certificate：

擴充欄位 (EXTNESION FIELD)	Self-Signed Certificate	Critical

authorityKeyIdentifier	×	N/A
subjectKeyIdentifier	✓	FALSE
keyUsage	✓	TRUE
privateKeyUsagePeriod	×	N/A
certificatePolicies	×	N/A
policyMappings	×	N/A
subjectAltName	×	N/A
issuerAltName	×	N/A
subjectDirectoryAttribute	×	N/A
basicConstraints	✓	TRUE
nameConstraints	×	N/A
policyConstraints	×	N/A
extKeyUsage	×	N/A
cRLDistributionPoints	×	N/A
inhibitAnyPolicy	×	N/A
freshestCRL	×	N/A
authorityInfoAccess	×	N/A
subjectInfoAccess	×	N/A
hashedRootKey	× (101 年 9 月後不再包含此欄位)	N/A

Self-Issued Certificate：

擴充欄位 (EXTNESION FIELD)	**Self-Issued Certificate**	**Critical**

authorityKeyIdentifier	✓	FALSE
subjectKeyIdentifier	✓	FALSE
keyUsage	✓	TRUE
privateKeyUsagePeriod	×	N/A
certificatePolicies	✓	FALSE
policyMappings	✓	FALSE
subjectAltName	×	N/A
issuerAltName	×	N/A
subjectDirectoryAttribute	×	N/A
basicConstraints	✓	TRUE
nameConstraints	×	N/A
policyConstraints	○	TRUE
extKeyUsage	×	N/A
cRLDistributionPoints	✓	FALSE
inhibitAnyPolicy	○	TRUE
freshestCRL	×	N/A
authorityInfoAccess	✓	FALSE
subjectInfoAccess	×	N/A
hashedRootKey	×	N/A

Cross Certificate：

擴充欄位 (EXTNESION FIELD)	**Cross Certificate**	**Critical**

authorityKeyIdentifier	✓	FALSE
subjectKeyIdentifier	✓	FALSE
keyUsage	✓	TRUE
privateKeyUsagePeriod	×	N/A
certificatePolicies	✓	FALSE
policyMappings	✓	FALSE
subjectAltName	×	N/A
issuerAltName	×	N/A
subjectDirectoryAttribute	×	N/A
basicConstraints	✓	TRUE
nameConstraints	×	N/A
policyConstraints	○	TRUE
extKeyUsage	×	N/A
cRLDistributionPoints	✓	FALSE
inhibitAnyPolicy	○	TRUE
freshestCRL	×	N/A
authorityInfoAccess	✓	FALSE
subjectInfoAccess	×	N/A
hashedRootKey	×	N/A

1.2 用戶憑證

1.2.1 用戶憑證的種類

GPKI 之用戶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)及應用軟體客戶端專屬憑證，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。

(3) 公司憑證

簽發對象為依我國公司法在我國登記設立的本國公司。

(4) 分公司憑證

簽發對象為依我國公司法在我國登記設立的分公司。

(5) 商業憑證

簽發對象為依我國商業登記法在我國登記設立的商業。

(6) 有限合夥憑證

簽發對象為依我國有限合夥法在我國登記設立的有限合夥。

(7) 有限合夥分支機構憑證

簽發對象為依我國有限合夥法在我國登記設立有限合夥之分支機構。

(8) 社團法人憑證

簽發對象為依我國民法在我國登記設立的全國性或地方性社團法人。

(9) 財團法人憑證

簽發對象為依我國民法在我國登記設立的全國性或地方性財團法人。

(10) 學校憑證

簽發對象為依我國教育相關法規在我國登記設立的各級公私立學校。

(11) 醫事機構憑證

簽發對象包含依據我國醫事相關法規立案登記之公立、私立、法人醫事機構。

(12) 自由職業事務所憑證

簽發對象為依我國各種專業證照相關法規在我國登記設立的自由職業事務所。

(13) 行政法人憑證

簽發對象為除國家及地方自治團體外，由中央目的事業主管機關，為執行特定公共任務，依法律設立具人事及財務自主性之公法人。

(14) 其他組織或團體憑證

簽發對象為在我國登記設立之上述範圍以外的其他組織或團體。

(15) 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。

(16) 外來人口自然人憑證

簽發對象為依我國移民署相關法規及外國人停留居留及永久居留辦法在我國申請停留並經許可的外來人口自然人。

(17) 醫事人員憑證

簽發對象包含依據我國醫事相關法規取得醫事服務資格之醫事人員。

(18) 伺服器應用軟體憑證

簽發對象為政府機關（構）及政府單位的伺服器應用軟體，或是由醫事機構建置而用於醫療、健保或公共衛生等相關醫事服務用途的伺服器應

用軟體，包括 TLS 類伺服器應用軟體、專屬類伺服器應用軟體或時戳伺服器應用軟體等。

以上所謂時戳伺服器應用軟體係指提供 RFC3161 Time-Stamp Protocol（TSP）服務的伺服器；而伺服器應用軟體的用途是否合於所謂「用於醫事服務用途」由衛生福利部認定之。

(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。

(21)應用軟體客戶端專屬憑證

簽發對象為組織及團體建置的服務軟體之應用與「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之應用。

1.2.2 用戶憑證的設計原則

除了遵循 X.509 標準[1]之外，GPKI 用戶憑證欄位的設計並遵循以下原則：

- 符合 IETF PKIX Certificate and CRL Profile (RFC 5280)之憑證規格[2]。
- 符合 IETF PKIX Qualified Certificates Profile (RFC 3739)之憑證規格[3]。
- 與 Asia PKI Consortium 之憑證規格[4]相容。

- 與 FPKI 之憑證規格[5]相容。
- 與歐盟之憑證規格[6]相容。
- 與 Web Browser 相容。
- 與 TLS(含 HTTPS)等通訊協定[7,8]所使用之憑證規格相容。
- 與 Internet IP Security(IPsec)之憑證規格[9]相容。
- 盡量不要使用 X.509 v2 欄位（根據 RFC 5280 [2]之建議）。

當主管機關公告採用 PQC 演算法及其因應之憑證格式時，相關用戶憑證欄位之設計與值之選用，應依本文件附錄 A 所列規範辦理。

1.2.3 用戶憑證的欄位

下表係依據上列原則訂定的用戶憑證欄位，其中標註「✓」記號的欄位者，為該類憑證的必要欄位(Required Field)，標註「×」記號者，則為該類憑證不需使用的欄位：

欄位名稱(Field Name)	**終端個體憑證 (EE Certificate)**
version	✓
serialNumber	✓
signature	✓
issuer	✓
validity	✓
subject	✓
subjectPublicKeyInfo	✓

issuerUniqueIdentifier	×
subjectUniqueIdentifier	×
extensions	✓

下表係各類憑證所使用的擴充欄位，其中標註「✓」記號者，為該類憑證的必要擴充欄位(Required Extension Field)；標註「○」記號者，為該類憑證的選擇性擴充欄位(Optional Extension Field)；標註「×」記號者，則表示該類憑證中不需使用的擴充欄位。下表標註各種擴充欄位是否為 critical，其中「TRUE」表示若使用此擴充欄位，則必須標示為 critical；「FALSE」表示此擴充欄位若使用則必標示為 non-critical；而「N/A」則表示在 CA 憑證中不使用該擴充欄位，因此並無 critical 或 non-critical 的情況：

擴充欄位 (EXTNESION FIELD)	**終端個體憑證** **(EE Certificate)**	**critical**
authorityKeyIdentifier	✓	FALSE
subjectKeyIdentifier	✓	FALSE
keyUsage	✓	TRUE
privateKeyUsagePeriod	×	N/A
certificatePolicies	✓	FALSE
policyMappings	×	N/A
subjectAltName	○	FALSE
issuerAltName	×	N/A
subjectDirectoryAttribute	○	FALSE
basicConstraints	×	N/A
nameConstraints	×	N/A

policyConstraints	×	N/A
extKeyUsage	×	N/A
cRLDistributionPoints	✓	FALSE
inhibitAnyPolicy	×	N/A
freshestCRL	×	N/A
authorityInfoAccess	✓	FALSE
subjectInfoAccess	×	N/A
hashedRootKey	×	N/A

1.3 憑證格式

GPKI 所採用的憑證為 X.509 公開金鑰憑證[1]。X.509 公開金鑰憑證是一種 SIGNED 資料，其格式如下：

欄位	內容	說明
toBeSigned	To-Be-Signed 憑證（尚未簽章的憑證）	To-Be-Signed 憑證的格式都是遵循 X.509 標準，但內容隨憑證種類的不同而有所差異，GPKI 相關的各類 To-Be-Signed 憑證內容詳見後面的說明
algorithmIdentifier	CA 對此憑證簽章所用之簽章演算法之 AlgorithmIdentifier	此欄的值必須與 toBeSigned 憑證內的 signature 欄的值相同
.algorithm	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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
signature	CA 對憑證的簽章	此簽章是 CA 對 toBeSigned 欄位中的 To-Be-Signed 憑證所做的簽章

以上憑證格式對於各類憑證都是相同的，但是各類憑證內部的 To-Be-

Signed 憑證部分會因各類別的主體名稱（Subject Name）與所需填入的屬性資料不同而有不同的內容。各種憑證之 To-Be-Signed 憑證格式分別說明如後。

為因應後量子密碼（Post-Quantum Cryptography, PQC）技術的發展，GPKI 已規劃支援相關憑證格式與演算法，相關說明請參閱附錄 A。

1.3.1 To-Be-Signed 自簽憑證格式

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 對此憑證簽章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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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）的名稱	CA 本身的 X.500 DN(CA 之 DN 將由主管機關訂定之)（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	依 PKIX 規定在 2049/12/31

	（GMT），在此時間之前憑證無效	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	憑證主體（Subject）的名稱	CA 本身的 X.500 DN，此 DN 必須與 issuer 欄位中的 DN 相同(CA 之 DN 將由主管機關訂定之) （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE {

		modulus INTEGER, publicExponent INTEGER }
extensions	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）:
.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	自簽憑證之 Key Usage 將至少包含 keyCertSign 與 cRLSign 兩種用途；若其相對應之私密金鑰可用於簽發線上憑證狀態協定回應訊息時，則 Key Usage 將再包含 digitalSignature
.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 OCTET STRING	對於 keyUsage 這種 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	自簽憑證的私密金鑰僅用於簽發憑證與 CRL 時，則此

		Named BIT STRING 之 keyCertSign(5)與 cRLSign(6) 這兩個 Bit 將會被設為 1；若該私密金鑰亦可用於簽發線上憑證狀態協定回應訊息時，則此 Named BIT STRING 之 digitalSignature(0)、keyCertSign(5)及 cRLSign(6) 這三個 Bit 將會被設為 1
.basicConstraints	Basic Constraints 擴充欄位	此擴充欄位的目的是標示此憑證為 CA 憑證
.extnId	填入代表此擴充欄位的 OID id-ce-basicConstraints (2.5.29.19)	
.critical	在 GPKI 中，basicConstraints 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 OCTET STRING	對於 basicConstraints 這種 Extension 而言，必須使用 BasicConstraints 的 DER 編碼做為此 OCTET STRING 的值
.BasicConstraints	BasicConstraints ::= SEQUENCE { cA BOOLEAN DEFAULT FALSE, pathLenConstraint INTEGER (0..MAX) OPTIONAL }	在 GPKI 中，自簽憑證只會使用 cA 子欄位，而不會使用 pathLenConstraint 子欄位
.Ca	填入 TRUE，標示此憑證為 CA 憑證	注意由於 TRUE 不是 DEFAULT VALUE，所以 DER 編碼中，此欄位不可被省略掉
.hashedRootKey	Hashed Root Key 擴充欄位，記載 CA 預定使用的下一把公開金鑰的 Hash 值	此擴充欄位為 SET 標準所定義的 Private Extension，在 SET 定義中此欄位必須是 critical 的擴充欄位，但是基於相容性的考量，GPKI 將此欄位設為 non-critical 的選擇性擴充欄位。GPKI 自 101 年 9 月以後簽發的自簽憑證將不再包含 hashedRootKey 欄位。
.extnId	填入代表此擴充欄位的 OID id-set-hashedRootKey (2.23.42.7 0)	
.critical	在 GPKI 中，hashedRootKey 必定是 non-critical extension，所以	注意由於 FALSE 是 DEFAULT VALUE，所以

	critical 的值必定是 FALSE	DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 hashedRootKey 這種 Extension 而言，必須使用 SET 所定義的 RootKeyThumb 的 DER 編碼做為此 OCTET STRING 的值
.RootKeyThumb	RootKeyThumb::= SEQUENCE { rootKeyThumbprint DigestedData }	RootKeyThumb 是一個 SEQUENCE，裡面只含有一個 PKCS#7 DigestedData 子欄位
.rootKeyThumbprint	rootKeyThumbprint 的資料型態是一個 PKCS#7 DigestedData，其定義如下： DigestedData ::= SEQUENCE { version INTEGER, algorithm AlgorithmIdentifier, contentInfo ContentInfo digest OCTET STRING }	
.version	version 的值為 0	參照 SET 中所定義的版本值 ddVer0(0)
.algorithm	標示用來取 Next Root Public Key Thumb 之雜湊函數的 AlgorithmIdentifier	
.algorithm	OID id-SHA1 (1.3.14.3.2.26)	參照 SET 之定義，使用 SHA-1 雜湊函數
.parameters	NULL	SHA-1 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
.contentInfo	contentInfo 的資料型態為 ContentInfo，其定義如下： ContentInfo ::= SEQUENCE { contentType ContentType, content Content OPTIONAL}	參照 SET 之定義，只使用 contentType 子欄位，而省略定 content 子欄位
.contentType	OID id-set-rootKeyThumb (2.23.42.3.0.0)	參照 SET 之定義，標示此 DigestedData 內含 Next Root Public Key Thumb 資料
.digest	OCTET STRING，此 OCTET STRING 內含下一把預計使用之 Root Public Key 的 PublicKeyInfo 的 SHA-1 雜湊值	注意依據 SET 之定義，Next Root Public Key Thumb 是針對整個 SubjectPublicKeyInfo 取雜湊值，而非只取 SubjectPublicKey 的雜湊值，此與 PKIX 所定義的 KeyIdentifier 取法不同

1.3.2 To-Be-Signed 自發憑證格式

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	Issuing CA 對此憑證簽章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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	此交互憑證之 Issuing CA 的 DN(將由各 CA 之主管機關訂定之) （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	憑證主體（Subject）之 X.500 Name	此自發憑證之 Subject CA 的 DN(將由各 CA 之主管機關訂定之) （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
subjectPublicKeyInfo	憑證主體的 Public Key Info	記載 Subject CA 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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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	此擴充欄位的目的是標示 Issuing CA 用來簽發本憑證

	方式依照 PKIX 標準，取 Issuing CA 的 Public Key 的 SHA-1 Hash 值做為 Key Identifier	所使用的金鑰是哪一把，以便在 Issuing CA 更換金鑰及其本身憑證時判斷應該使用 Issuing 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 ::= SEQUENCE { keyIdentifier [0] KeyIdentifier OPTIONAL, authorityCertIssuer [1] GeneralNames OPTIONAL, authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }	GPKI 憑證依據 PKIX，只採用 keyIdentifier 欄位，而不使用 authorityCertIssuer 與 authorityCertSerialNumber 欄位
.keyIdentifier	keyIdentifier 欄為的資料型態是 KeyIdentifier，而 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
.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 CA 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	自發憑證之 Key Usage 將至少包含 keyCertSign 與 cRLSign 兩種用途；若其相對應之私密金鑰可用於簽發線上憑證狀態協定回應訊息時，則 Key Usage 將再包含 digitalSignature
.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 OCTET STRING	對於 keyUsage 這種 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	自發憑證的私密金鑰僅用於簽發憑證與 CRL 時，則此 Named BIT STRING 之 keyCertSign(5)與 cRLSign(6) 這兩個 Bit 將會被設為 1；若該私密金鑰亦可用於簽發線上憑證狀態協定回應訊息時，則此 Named BIT STRING 之 digitalSignature(0)、keyCertSign(5)及 cRLSign(6) 這三個 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	注意：對於 Self-Issued Certificate 而言，此擴充欄位是用來標示 Subject CA 所被允許採用的各種 Certificate Policies，而不是標示 Issuing CA 簽發此憑證時所遵循的 Certificate Polcies
.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	注意由於 FALSE 是

	中，certificatePolicies 被設定為 non-critical extension，所以 critical 的值必定是 FALSE	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，Self-Issued Certificate 可能含有 1 個或多個 PolicyInformation，每個 PolicyInformation 的內容如下：
*.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 資料型態	根據 Subject CA 被 Issuing CA 認證通過的保證等級（Assurance Level），填上代表該保證等級之 GPKI Certificate Policy OID
.policyMappings	(Optional)Policy Mappings 擴充欄位，用來記載各 GPKI Certificate Policy 如何與 Subject CA domain 的各 Certificate Policy 對等	此欄位為 Optional，唯有當 Subject CA 所屬 domain 的 Certificate Policy 並非 GPKI Certificate Policy 時，才需要使用此欄位
.extnId	填入代表此擴充欄位的 OID id-ce-policyMappings (2.5.29.33)	
.critical	遵循 PKIX，在 GPKI 中，policyMappings 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，此欄位將被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 policyMappings 這種 Extension 而言，必須使用 PolicyMappings 的 DER 編碼做為此 OCTET STRING 的值
.PolicyMappings	PolicyMappings 的資料型態是一個 SEQUENCE，可包含 n（n >= 1）對的 Policy Pairs	每一個 Policy Pair 的內容將包含一對有對等關係的 Certificate Policy 的 OID，分別為 GPKI Certificate Policy 的 OID 與 Subject CA 所遵循

		之 Certificate Policy 的 OID
.basicConstraints	Basic Constraints 擴充欄位	此擴充欄位的目的是標示此憑證為 CA 憑證，並可選擇性地用來限制由此憑證以後的 Certification Path 長度
.extnId	填入代表此擴充欄位的 OID id-ce-basicConstraints (2.5.29.19)	
.critical	在 GPKI 中， basicConstraints 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 OCTET STRING	對於 basicConstraints 這種 Extension 而言，必須使用 BasicConstraints 的 DER 編碼做為此 OCTET STRING 的值
.BasicConstraints	BasicConstraints ::= SEQUENCE { cA BOOLEAN DEFAULT FALSE, pathLenConstraint INTEGER (0..MAX) OPTIONAL }	在 GPKI 中，交互憑證必會使用 cA 子欄位；而 pathLenConstraint 子欄位是有需要限制 Certification Path 長度時，才選擇性地使用
.cA	填入 TRUE，標示此憑證為 CA 憑證	注意由於 TRUE 不是 DEFAULT VALUE，所以 DER 編碼中，此欄位不可被省略掉
.pathLenConstraint	(Optional)必要時可填入 Certification Path 長度限制的值	若省略此欄，代表不設 Certification Path 長度限制； 0 代表 Subject CA 只能簽發 EE 憑證，不能簽發與其他 CA 進行 Cross Certification； 1 代表 Subject CA 除了能簽發 EE 憑證外，只能再與外面 1 層 CA 進行 Cross Certification； 2 代表 Subject CA 除了能簽發 EE 憑證，能再與外面 1 層 CA 進行 Cross Certification，而該外層 CA 又能再與更外面 1 層 CA 進行 Cross Certification； 餘此類推。
.policyConstraints	(Optional)Policy Constraints 擴充欄位，用來限制 Certification Path 中的憑證	此欄位為 Optional，唯有當 Issuing CA 需要對 Subject CA 簽發憑證時是否需要明確包

	必須含有明確且可接受的 Certificate Policy 擴充欄位，或是用來禁止在 Certification Path 中使用 Policy Mapping 機制	含 Certificate Policy 擴充欄位時，或是要禁止 Subject CA 簽發憑證時使用 PolicyMapping 時，才需要使用此欄位
.extnId	填入代表此擴充欄位的 OID id-ce-policyConstraints (2.5.29.36)	
.critical	在 GPKI 中，policyConstraints 被設定是 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 OCTET STRING	對於 policyConstraints 這種 Extension 而言，必須使用 PolicyConstraints 的 DER 編碼做為此 OCTET STRING 的值
.PolicyConstraints	PolicyConstraints ::= SEQUENCE { requireExplicitPolicy [0] SkipCerts OPTIONAL, inhibitPolicyMapping [1] SkipCerts OPTIONAL } SkipCerts ::= INTEGER (0..MAX)	requireExplicitPolicy 子欄位與 inhibitPolicyMapping 子欄位雖然都是 Optional 的，但是兩者至少其中之一必須有值才行，不能兩者都省略掉
.requireExplicitPolicy	必須是整數值，整數 0 是指此張憑證本身	此整數值表示在 Certification Path 中，由此張憑證算起之第幾張憑證必須開始含有 Certificate Policies 擴充欄位，且該 Certificate Policies 擴充欄位中必須含有可接受的 Policy OID
.inhibitPolicyMapping	必須是整數值，整數 0 是指此張憑證本身	此整數值表示在 Certification Path 中，由此張憑證算起之第幾張憑證開始不許使用 Policy Mapping 機制
.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/CARL 的網址	此擴充欄位提供憑證應用軟體取得相關 CRL/CARL 的指引，目前 GPKI 所使用之 CRL Distribution Points 為一個 URL 網址
.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，	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省

	所以 critical 的值必定是 FALSE	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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證中，將只含有 1 個 DistributionPoint
.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
.inhibitAnyPolicy	(Optional)Inhibit Any-Policy 擴充欄位，用來限制在 Certification Path 中使用 anyPolicy 這個特殊的 Certificate Policy OID（OID 值為 2.5.29.32.0）	此欄位為 Optional，唯有當 Issuing CA 需要禁止 Subject CA 或其下屬 CA 簽發憑證時使用 anyPolicy 這個特殊的 Certificate Policy OID 時，才需要使用此欄位
.extnId	填入代表此擴充欄位的 OID id-ce-inhibitAnyPolicy (2.5.29.54)	
.critical	在 GPKI 中，inhibitAnyPolicy 被設定是 critical extension，所以	注意由於 TRUE 不是 DEFAULT VALUE，所以 DER 編碼中，此欄位不可被

	critical 的值必定是 TRUE	省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 policyConstraints 這種 Extension 而言，必須使用 PolicyConstraints 的 DER 編碼做為此 OCTET STRING 的值
.InhibitAnyPolicy	必須是整數值，整數 0 是指此張憑證本身	此整數值表示在 Certification Path 中，由此張憑證算起之第幾張憑證開始不許使用 anyPolicy 這個特殊的 Certificate Policy OID
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，

	CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.3 To-Be-Signed 交互憑證格式

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	Issuing CA 對此憑證簽章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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	此交互憑證之 Issuing CA 的 DN(將由各 CA 之主管機關訂定之) （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	憑證主體（Subject）之 X.500 Name	此交互憑證之 Subject CA 的 DN(將由各 CA 之主管機關訂定之) （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
subjectPublicKeyInfo	憑證主體的 Public Key Info	記載 Subject CA 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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 Issuing CA 用來簽發本憑證所使用的金鑰是哪一把，以便在 Issuing CA 更換金鑰及其本身憑證時判斷應該使用 Issuing 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 ::= SEQUENCE { keyIdentifier [0] KeyIdentifier OPTIONAL, authorityCertIssuer [1] GeneralNames OPTIONAL, authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }	GPKI 憑證依據 PKIX，只採用 keyIdentifier 欄位，而不使用 authorityCertIssuer 與 authorityCertSerialNumber 欄位
.keyIdentifier	keyIdentifier 欄為的資料型態是 KeyIdentifier，而	KeyIdentifier 的產生方式依照 PKIX 標準，取 Subject 的

	KeyIDentifier 本身為一個 OCTET STRING 資料型態	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 CA 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	交互憑證之 Key Usage 將至少包含 keyCertSign 與 cRLSign 兩種用途；若其相對應之私密金鑰可用於簽發線上憑證狀態協定回應訊息時，則 Key Usage 將再包含 digitalSignature
.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 OCTET STRING	對於 keyUsage 這種 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	交互憑證的私密金鑰僅用於簽發憑證與 CRL 時，則此 Named BIT STRING 之

		keyCertSign(5)與 cRLSign(6)這兩個 Bit 將會被設為 1；若該私密金鑰亦可用於簽發線上憑證狀態協定回應訊息時，則此 Named BIT STRING 之 digitalSignature(0)、keyCertSign(5)及 cRLSign(6)這三個 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	注意：對於 Cross Certificate 而言，此擴充欄位是用來標示 Subject CA 所被允許採用的各種 Certificate Policies，而不是標示 Issuing CA 簽發此憑證時所遵循的 Certificate Polcies
.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，Cross Certificate 可能含有 1 個或多個 PolicyInformation，每個 PolicyInformation 的內容如下：
*.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 資料型態	根據 Subject CA 被 Issuing CA 認證通過的保證等級（Assurance Level），填上代表該保證等級之 GPKI Certificate Policy OID
.policyMappings	(Optional)Policy Mappings 擴	此欄位為 Optional，唯有當

	充欄位，用來記載各 GPKI Certificate Policy 如何與 Subject CA domain 的各 Certificate Policy 對等	Subject CA 所屬 domain 的 Certificate Policy 並非 GPKI Certificate Policy 時，才需要使用此欄位
.extnId	填入代表此擴充欄位的 OID id-ce-policyMappings (2.5.29.33)	
.critical	遵循 PKIX，在 GPKI 中，policyMappings 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，此欄位將被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 policyMappings 這種 Extension 而言，必須使用 PolicyMappings 的 DER 編碼做為此 OCTET STRING 的值
.PolicyMappings	PolicyMappings 的資料型態是一個 SEQUENCE，可包含 n（n >= 1）對的 Policy Pairs	每一個 Policy Pair 的內容將包含一對有對等關係的 Certificate Policy 的 OID，分別為 GPKI Certificate Policy 的 OID 與 Subject CA 所遵循之 Certificate Policy 的 OID
.basicConstraints	Basic Constraints 擴充欄位	此擴充欄位的目的是標示此憑證為 CA 憑證，並可選擇性地用來限制由此憑證以後的 Certification Path 長度
.extnId	填入代表此擴充欄位的 OID id-ce-basicConstraints (2.5.29.19)	
.critical	在 GPKI 中，basicConstraints 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 OCTET STRING	對於 basicConstraints 這種 Extension 而言，必須使用 BasicConstraints 的 DER 編碼做為此 OCTET STRING 的值
.BasicConstraints	BasicConstraints ::= SEQUENCE { cA BOOLEAN DEFAULT FALSE, pathLenConstraint INTEGER (0..MAX) OPTIONAL }	在 GPKI 中，交互憑證必會使用 cA 子欄位；而 pathLenConstraint 子欄位是有需要限制 Certification Path 長度時，才選擇性地使用
.cA	填入 TRUE，標示此憑證為 CA 憑證	注意由於 TRUE 不是 DEFAULT VALUE，所以 DER 編碼中，此欄位不可被

		省略掉
.pathLenConstraint	(Optional)必要時可填入 Certification Path 長度限制的值	若省略此欄，代表不設 Certification Path 長度限制； 0 代表 Subject CA 只能簽發 EE 憑證，不能簽發與其他 CA 進行 Cross Certification； 1 代表 Subject CA 除了能簽發 EE 憑證外，只能再與外面 1 層 CA 進行 Cross Certification； 2 代表 Subject CA 除了能簽發 EE 憑證，能再與外面 1 層 CA 進行 Cross Certification，而該外層 CA 又能再與更外面 1 層 CA 進行 Cross Certification； 餘此類推。
.policyConstraints	(Optional)Policy Constraints 擴充欄位，用來限制 Certification Path 中的憑證必須含有明確且可接受的 Certificate Policy 擴充欄位，或是用來禁止在 Certification Path 中使用 Policy Mapping 機制	此欄位為 Optional，唯有當 Issuing CA 需要對 Subject CA 簽發憑證時是否需要明確包含 Certificate Policy 擴充欄位時，或是要禁止 Subject CA 簽發憑證時使用 PolicyMapping 時，才需要使用此欄位
.extnId	填入代表此擴充欄位的 OID id-ce-policyConstraints (2.5.29.36)	
.critical	在 GPKI 中，policyConstraints 被設定是 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 OCTET STRING	對於 policyConstraints 這種 Extension 而言，必須使用 PolicyConstraints 的 DER 編碼做為此 OCTET STRING 的值
.PolicyConstraints	PolicyConstraints ::= SEQUENCE { requireExplicitPolicy [0] SkipCerts OPTIONAL, inhibitPolicyMapping [1] SkipCerts OPTIONAL } SkipCerts ::= INTEGER (0..MAX)	requireExplicitPolicy 子欄位與 inhibitPolicyMapping 子欄位雖然都是 Optional 的，但是兩者至少其中之一必須有值才行，不能兩者都省略掉
.requireExplicitPolicy	必須是整數值，整數 0 是指此張憑證本身	此整數值表示在 Certification Path 中，由此張憑證算起之

		第幾張憑證必須開始含有 Certificate Policies 擴充欄位，且該 Certificate Policies 擴充欄位中必須含有可接受的 Policy OID
.inhibitPolicyMapping	必須是整數值，整數 0 是指此張憑證本身	此整數值表示在 Certification Path 中，由此張憑證算起之第幾張憑證開始不許使用 Policy Mapping 機制
.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/CARL 的網址	此擴充欄位提供憑證應用軟體取得相關 CRL/CARL 的指引，目前 GPKI 所使用之 CRL Distribution Points 為一個 URL 網址
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證中，將只含有 1 個 DistributionPoint
.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	GPKI 憑證的 CRL distributionPoint 的 fullName

	GeneralNames 的資料型態是 SEQUENCE SIZE (1..MAX) OF GeneralName	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
.inhibitAnyPolicy	(Optional)Inhibit Any-Policy 擴充欄位，用來限制在 Certification Path 中使用 anyPolicy 這個特殊的 Certificate Policy OID（OID 值為 2.5.29.32.0）	此欄位為 Optional，唯有當 Issuing CA 需要禁止 Subject CA 或其下屬 CA 簽發憑證時使用 anyPolicy 這個特殊的 Certificate Policy OID 時，才需要使用此欄位
.extnId	填入代表此擴充欄位的 OID id-ce-inhibitAnyPolicy (2.5.29.54)	
.critical	在 GPKI 中，inhibitAnyPolicy 被設定是 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 OCTET STRING	對於 policyConstraints 這種 Extension 而言，必須使用 PolicyConstraints 的 DER 編碼做為此 OCTET STRING 的值
.InhibitAnyPolicy	必須是整數值，整數 0 是指此張憑證本身	此整數值表示在 Certification Path 中，由此張憑證算起之第幾張憑證開始不許使用 anyPolicy 這個特殊的 Certificate Policy OID
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.4 To-Be-Signed 政府機關憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	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)* （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 目前可使用 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	GPKI 目前可採用 RSA

	STRING 內含 Subject Public Key 的 DER 編碼值	Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	此擴充欄位的目的是標示 Subject 所使用的金鑰是哪一把

	Identifier	
.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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與

		dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 政府機關憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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	對於 subjectAltName 這種

	OCTET STRING	Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，政府機關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-GovernmentAgency (2.16.886.1.100.3.2.1.1)	此 OID 表示憑證 Subject 的類別為政府機關
.cardHolderRank	持卡人的正附卡等級，其	此屬性用來區分此憑證

	type 與 values 如下：	Subject 之卡片持有人的是正卡或附卡持有人
.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’primary’ 或’ secondary’	‘primary’ 表示卡片持有人是正卡持有人，’secondary’ 表示卡片持有人是附卡持有人
.entityOID	個體 OID 屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的 OID
.type	OID id-chtpki-at-entityOID (2.16.886.1.100.2.102)	此為代表 Entity OID Attribute 之 OID
.values	填入政府機關之 OID	由 GPKI Naming Authority 統一編配之政府機關 OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 憑證只使用 distributionPoint 欄位，而不

	distributionPoint、reasons 與 cRLIssuer 三欄	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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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	在 GPKI 憑證規格中，此擴充欄位至少包含 1 個

	SEQUENCE SIZE (1..MAX) OF AccessDescription	caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.5 To-Be-Signed 政府單位憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	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)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* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }

extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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，	注意由於 FALSE 是

	subjectKeyIdentifier 必定是 non-critical extension，所以 critical 的值必定是 FALSE	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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 政府單位憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 的資料型態	GPKI 憑證的

	是 GeneralNames 而 GeneralNames 的資料型態是 SEQUENCE SIZE (1..MAX) OF GeneralName	SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，政府單位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-governmentUnit (2.16.886.1.100.3.2.1.2)	此 OID 表示憑證 Subject 的類別為政府單位
.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
.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’	‘primary’ 表示卡片持有人

	primary’ 或’ secondary’	是正卡持有人，’ secondary’ 表示卡片持有人是附卡持有人
.entityOID	個體 OID 屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的 OID
.type	OID id-chtpki-at-entityOID (2.16.886.1.100.2.102)	此為代表 Entity OID Attribute 之 OID
.values	填入政府單位 OID	由 GPKI Naming Authority 統一編配之政府單位 OID
.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 網址
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 憑證的 CRL distributionPoint 是採用 fullName

	DistributionPointName 本身為一個 CHOICE 資料型態，可選用 fullName 或 nameRelativeToCRLIssuer	
.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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 AccessDescription
. AccessDescription	AccessDescription 為一	此擴充欄位提供憑證應用軟

	SEQUENCE，內含 accessMethod 與 accessLocation 二欄	體取得與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.6 To-Be-Signed 公司憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	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公司之唯一序號* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個公司 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 公司憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.subjectDirectoryAttributes	Subject Directory Attributes 擴充欄位，用來記錄	不同憑證種類所使用的屬性欄位會有所不同

	Subject 特有的屬性資料	
.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，公司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-company (2.16.886.1.100.3.2.2.1.1)	此 OID 表示憑證 Subject 的類別為公司
.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
.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’primary’、’secondary’或’mobile’	‘primary’表示卡片持有人是正卡持有人，’secondary’表示卡片持有人是附卡持有人，’mobile’表示持有人使用行動載具，行動載具視為附卡的一種
.uniformOrganizationID	統一編號屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject（公司）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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 憑證的 CRL distributionPoint 的 fullName 只會包含 1 個 GeneralName

	SIZE (1..MAX) OF 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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	此 URL 指向與簽發本憑證

	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 caIssuers 的 URL	之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.7 To-Be-Signed 分公司憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption	簽章演算法之 OID，GPKI 可使用簽章演算法

	(1.2.840.113549.1.1.11)	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	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公司之唯一序號* 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）
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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個分公司 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含

		digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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	GPKI 憑證只使用

	SEQUENCE，內含 policyIdentifier 與 policyQualifiers 兩欄	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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 分公司憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被

	extension，所以 critical 的值必定是 FALSE	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，分公司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-companyBranch (2.16.886.1.100.3.2.3.3.1)	此 OID 表示憑證 Subject 的類別為分公司
.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
.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’ primary’ 、’ secondary’ 或’ mobile’	‘primary’ 表示卡片持有人是正卡持有人，’ secondary’ 表示卡片持有人是附卡持有人，’ mobile’ 表示持有人使用行動載具，行動載具視為附卡的一種
.uniformOrganizationID	統一編號屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject（分公司）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	填入該分公司的統一編號	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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之

	caIssuers 的 URL	cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.8 To-Be-Signed 商業憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	商業的 X.500 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商業之唯一序號(用以區分同名的商業，從民國 99 年 12 月 25 日起簽發的憑證皆包含*

		serialNumber 欄位) （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個商業 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與

		dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 商業憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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	對於

	OCTET STRING	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，商業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-proprietorship (2.16.886.1.100.3.2.3.1)	此 OID 表示憑證 Subject 的類別為商業
.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
.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’ primary’ 、’ secondary’ 或’ mobile’	‘primary’ 表示卡片持有人是正卡持有人，’ secondary’ 表示卡片持有人是附卡持有人，’ mobile’ 表示持有人使用行動載具，行動載具視為附卡的一種
.uniformOrganizationID	統一編號屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject（商業）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	填入該商業的統一編號	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，	注意由於 FALSE 是

	cRLDistributionPoints 被設定為 non-critical extension，所以 critical 的值必定是 FALSE	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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型	id-ad-ocsp 為 PKIX RFC

	態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.9 To-Be-Signed 有限合夥憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	有限合夥的 X.500 Name 格式如下： C=TW O=*有限合夥的正式登記名稱* （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
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	Public Key 類別之 OID，

	(1.2.840.113549.1.1.1)	GPKI 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而	KeyIdentifier 的產生方式依照 PKIX 標準，取 Subject

	KeyIDentifier 本身為一個 OCTET STRING 資料型態	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	GPKI 每個有限合夥 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 有限合夥憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證

		中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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)	此欄可包含一串屬性，有限合夥憑證會記錄下列屬性

	OF Attribute	
.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-limitedPartnership (2.16.886.1.100.3.2.2.1.3)	此 OID 表示憑證 Subject 的類別為有限合夥
.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
.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’ primary’ 、’ secondary’ 或’ mobile’	‘primary’ 表示卡片持有人是正卡持有人，’ secondary’ 表示卡片持有人是附卡持有人，’ mobile’ 表示持有人使用行動載具，行動載具視為附卡的一種
.uniformOrganizationID	統一編號屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject（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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess	authorityInfoAccess 是 PKIX 所定義的 Private Extension

	(1.3.6.1.5.5.7.1.1)	
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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	此 URL 指向 OCSP 伺服器，可提供本憑證的狀態資訊

	選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	

1.3.10 To-Be-Signed 有限合夥分支機構憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	有限合夥分支機構的 X.500 Name 格式如下： C=TW O=*有限合夥的正式登記名稱* OU=*有限合夥分支機構的正式登記名稱* （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.subjectKeyIdentifier	Subject Key Identifier 擴充欄位，Key Identifier 的產生方式依照 PKIX 標準，取	此擴充欄位的目的是標示 Subject 所使用的金鑰是哪一把

	Subject 的 Public Key 的 SHA-1 Hash 值做為 Key Identifier	
.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	GPKI 每個有限合夥分支機構 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為

		加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 有限合夥分支機構憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 被設定為	注意由於 FALSE 是 DEFAULT VALUE，所以

	non-critical extension，所以 critical 的值必定是 FALSE	DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，有限合夥分支機構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-	此 OID 表示憑證 Subject 的

	limitedPartnershipBranch (2.16.886.1.100.3.2.3.3.2)	類別為有限合夥分支機構
.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
.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’primary’ 或’secondary’	‘primary’ 表示卡片持有人是正卡持有人，’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（有限合夥分支機構）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	填入該有限合夥分支機構的統一編號	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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.11 To-Be-Signed 社團法人憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	社團法人的 X.500 Name 格式如下： C=TW L=*縣市名稱(選擇性欄位，只適用於地方性社團法人)* L=*鄉鎮市區名稱(選擇性欄位，只適用於地方性社團法人)* O=*社團法人的正式登記名稱* （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
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 目前可使用 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 目前可採用 RSA Public Key，其 BIT

	Key 的 DER 編碼值	STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個

		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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 政府機關憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用

		SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，社團法人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-nonprofitSocietyBasedCorporation (2.16.886.1.100.3.2.2.2.1)	此 OID 表示憑證 Subject 的類別為社團法人
.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
.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’primary’ 或’secondary’	‘primary’表示卡片持有人是正卡持有人，’secondary’表示卡片持有人是附卡持有人
.entityOID	個體 OID 屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的 OID
.type	OID id-chtpki-at-entityOID (2.16.886.1.100.2.102)	此為代表 Entity OID Attribute 之 OID
.values	填入社團法人之 OID	由 GPKI Naming Authority 統一編配之社團法人 OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 憑證只使用 distributionPoint 欄位，而不使用 reasons 與 cRLIssuer 這

	cRLIssuer 三欄	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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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	在 GPKI 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種

	SIZE (1..MAX) OF AccessDescription	AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.12 To-Be-Signed 財團法人憑證格式

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	GPKI 中所使用之憑證序號

	Number）	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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	財團法人的 X.500 Name 格式如下： C=TW L=*縣市名稱(選擇性欄位，只適用於地方性財團法人)* L=*鄉鎮市區名稱(選擇性欄位，只適用於地方性財團法人)* O=*財團法人的正式登記名稱* （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 政府機關憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 的資料型態是 GeneralNames 而 GeneralNames 的資料型態是	GPKI 憑證的 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName

	SEQUENCE SIZE (1..MAX) OF GeneralName	
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，財團法人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-nonprofitFoundationBasedCorporation (2.16.886.1.100.3.2.2.2.2)	此 OID 表示憑證 Subject 的類別為財團法人
.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
.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’primary’ 或’secondary’	‘primary’ 表示卡片持有人是正卡持有人，’secondary’ 表示卡片持有人

		是附卡持有人
.entityOID	個體 OID 屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的 OID
.type	OID id-chtpki-at-entityOID (2.16.886.1.100.2.102)	此為代表 Entity OID Attribute 之 OID
.values	填入財團法人之 OID	由 GPKI Naming Authority 統一編配之財團法人 OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 憑證的 CRL distributionPoint 是採用 fullName

	態，可選用 fullName 或 nameRelativeToCRLIssuer	
.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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與	此擴充欄位提供憑證應用軟體取得與本憑證驗證相關之指引資訊

	accessLocation 二欄	
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.13 To-Be-Signed 學校憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	學校的 X.500 Name 格式如下： C=TW L=*縣市名稱(選擇性欄位，只適用於地區性學校)* L=*鄉鎮市區名稱(選擇性欄位，只適用於地區性學校)* O=*學校的正式登記名稱* *OU=附屬學校的名稱(選擇性欄位，只適用於附屬學校)* 如為學校財團法人所設私立學校時，其 X.500 Name 格式亦可為如下： C=TW O=*學校財團法人的正式登記名稱* OU=*學校的正式登記名稱* OU=*附屬學校的名稱(選擇性欄位，只適用於附屬學校)* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE {

		modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 Bit 將會被設為 1
.certificatePolicies	Certificate Policies 擴充欄位，記載 CA 簽發此憑證所	填入 CA 簽發此憑證時所依據的 GPKI Certificate Policy

	使用的憑證政策	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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 政府機關憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值

.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，學校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-school (2.16.886.1.100.3.2.11)	此 OID 表示憑證 Subject 的類別為學校
.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
.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’primary’ 或’ secondary’	‘primary’ 表示卡片持有人是正卡持有人，’secondary’ 表示卡片持有人是附卡持有人
.entityOID	個體 OID 屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的 OID
.type	OID id-chtpki-at-entityOID (2.16.886.1.100.2.102)	此為代表 Entity OID Attribute 之 OID
.values	填入學校之 OID	由 GPKI Naming Authority 統一編配之學校 OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 憑證的 CRL distributionPoint 是採用

	DistributionPointName，而 DistributionPointName 本身為一個 CHOICE 資料型態，可選用 fullName 或 nameRelativeToCRLIssuer	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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.14 To-Be-Signed 醫事機構憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	醫事機構的 X.500 Name，由衛生福利部醫事管理系統提供。 （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個醫事機構 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 醫事機構憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，醫事機構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-medicalOrganization (2.16.886.1.100.3.2.21)	此 OID 表示憑證 Subject 的類別為醫事機構
.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 (註：正卡的私密金鑰載體一定是 IC 卡，而附卡的私密金鑰載體則可能是 IC 卡，也可能是非 IC 卡類的 Token，例如軟體密碼模組、硬體密碼模組或是其他型態的 Token；凡是使用非 IC 卡的 Token，則其憑證格式將與 IC 卡類的憑證格式相同，唯其 cardHolderRank 一定註記為附卡，以便與正卡有所區別)
.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’primary’ 或’ secondary’	‘primary’ 表示卡片持有人是正卡持有人，’secondary’ 表示卡片持有人是附卡持有人
.medicalOrganizationID	醫事機構代碼屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject（醫事機購）的醫事機構代碼
.type	OID id-chtpki-at-medicalOrganizationID (2.16.886.1.100.2.111)	此為代表 Medical Organization ID Attribute 之 OID
.values	填入該醫事機構的醫事機構代碼	此欄位值為一個 ASN.1 UTF8String 格式的字串
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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	在 GPKI 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視

	AccessDescription	需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.15 To-Be-Signed 自由職業事務所憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	自由職業事務所的 X.500 Name 格式如下： C=TW L=*縣市名稱(選擇性欄位，只適用於地區性自由職業事務所)* O=*自由職業事務所的正式登記名稱* serialNumber=*自由職業事務所的 OID 識別碼（用以區分同名的自由職業事務所，此為 option 值）* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被

	critical 的值必定是 FALSE	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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 政府機關憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 的資料型態是 GeneralNames 而 GeneralNames 的資料型態	GPKI 憑證的 SubjectAltName 的 GeneralNames 只會包含 1 個

	是 SEQUENCE SIZE (1..MAX) OF GeneralName	GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，自由職業事務所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-professionalFirm (2.16.886.1.100.3.2.3.4)	此 OID 表示憑證 Subject 的類別為自由職業事務所
.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
.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’primary’ 或’secondary’	‘primary’表示卡片持有人是正卡持有人，’secondary’表示卡片持有人

		是附卡持有人
.entityOID	個體 OID 屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的 OID
.type	OID id-chtpki-at-entityOID (2.16.886.1.100.2.102)	此為代表 Entity OID Attribute 之 OID
.values	填入自由職業事務所之 OID	由 GPKI Naming Authority 統一編配之自由職業事務所 OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 憑證的 CRL distributionPoint 是採用 fullName

	為一個 CHOICE 資料型態，可選用 fullName 或 nameRelativeToCRLIssuer	
.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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含	此擴充欄位提供憑證應用軟體取得與本憑證驗證相關之

	accessMethod 與 accessLocation 二欄	指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.16 To-Be-Signed 行政法人憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	行政法人的 X.500 Name 格式如下： C=TW L=*縣市名稱(選擇性欄位，只適用於地區性行政法人)* O=*行政法人的正式登記名稱* （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）
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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個 Subject 建議使用

	Subject Public Key 相對應之 Private Key 的用途限制	的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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	在 GPKI 憑證中，EE Certificate 只能含有 1 個

	SEQUENCE SIZE (1..MAX) OF PolicyInformation	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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 政府機關憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，行政法人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-publicCorporation (2.16.886.1.100.3.2.2.3)	此 OID 表示憑證 Subject 的類別為行政法人
.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
.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’primary’ 或’secondary’	‘primary’ 表示卡片持有人是正卡持有人，’secondary’ 表示卡片持有人是附卡持有人
.entityOID	個體 OID 屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的 OID
.type	OID id-chtpki-at-entityOID (2.16.886.1.100.2.102)	此為代表 Entity OID Attribute 之 OID
.values	填入行政法人之 OID	由 GPKI Naming Authority 統一編配之行政法人 OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型	id-ad-ocsp 為 PKIX RFC

	態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.17 To-Be-Signed 其他組織或團體憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	其他組織或團體的 X.500 Name 格式如下： C=TW L=*縣市名稱(選擇性欄位，只適用於地區性組織或團體)* L=*鄉鎮市名稱(選擇性欄位，只適用於地區性組織或團體)* O=*組織或團體的正式登記名稱* serialNumber=其他*組織或團體的 OID 識別碼(用以區分同名的組織或團體，此為 option 值)*（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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途

.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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	根據 CA 簽發此憑證時所採

	型態是 CertPolicyId，而 CertPolicyId 本身為一個 OBJECT IDENTIFIER 資料型態	用的保證等級（Assurance Level），填上代表該保證等級之 GPKI Certificate Policy OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 政府機關憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，其他組織或團體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-otherOrganization(2.16.886.1.100.3.2.49)	此 OID 表示憑證 Subject 的類別為其他組織或團體
.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
.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’primary’ 或’ secondary’	‘primary’ 表示卡片持有人是正卡持有人，’secondary’ 表示卡片持有人是附卡持有人
.entityOID	個體 OID 屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的 OID
.type	OID id-chtpki-at-entityOID (2.16.886.1.100.2.102)	此為代表 Entity OID Attribute 之 OID
.values	填入組織或團體之 OID	由 GPKI Naming Authority 統一編配之組織或團體 OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊

		存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列 (certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.18 To-Be-Signed 自然人憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	自然人的 X.500 Name 格式如下： C=TW CN=*戶籍登記之中文姓名* serialNumber=*個人序號(流水號用以區分同名的人)* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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

.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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之

	態	digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 自然人憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	

.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，自然人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	此為代表 Subject Type

	(2.16.886.1.100.2.1)	Attribute 之 OID
.values	OID id-chtpki-et-citizen (2.16.886.1.100.3.1.1)	此 OID 表示憑證 Subject 的類別為國民
.cardHolderRank	持卡人的載具等級，其 type 與 values 如下：	此屬性為 Optional，若憑證不含此屬性時，則視為正卡憑證；若憑證含此屬性時，則此憑證 Subject 之卡片持有人只可為附卡或行動載具持有人。
.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’ 或’mobile’	‘secondary’表示卡片持有人是附卡持有人，’mobile’表示卡片持有人是行動載具持有人
.tailOfPersonalID	身分識別證號尾碼屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的身分識別證號尾碼 (自然人的身分識別證為中華民國國民身分證，因此，取其末 4 碼作為身分識別證號尾碼) (註：由於國民身分證字號為個人隱私資料，故不於憑證中公佈其全部的號碼，只取末幾碼)
.type	OID id-chtpki-at-tailOfPersonalID (2.16.886.1.100.2.51)	此為代表 Tail of Personal ID Attribute 之 OID
.values	填入 Subject 的中華民國國民身分證字號末 4 碼	例如身分證字號為 A123456789 則此欄填入 6789
.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	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉

	FALSE	
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 使用此擴充欄位記載

	位	簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列 (certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod

	(1.3.6.1.5.5.7.48.1)	
.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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.19 To-Be-Signed 外來人口自然人憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	憑證效期長度視憑證政策而

	間	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	外來人口自然人的 X.500 Name 格式如下： C=TW CN=*內政部移民署登記之中文/英文姓名* serialNumber=*個人序號(流水號用以區分同名的人)* （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 目前可使用

		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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 KeyIDentifier 本身為一個	KeyIdentifier 的產生方式依照 PKIX 標準，取 Subject 的 Public Key 的 SHA-1

	OCTET STRING 資料型態	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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 外來人口自然人憑證中此欄位只用於記載 Subject 的 Email Address	此欄位為 Optional，若憑證的 Subject 沒有 Email Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID	

	id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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，外來人口自然人憑證會記錄下列屬性
.subjectType	Subject 類別屬性，其 type	此屬性用來區分此憑證

	與 values 如下：	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-alienResident (2.16.886.1.100.3.1.9)	此 OID 表示憑證 Subject 的類別為外來人口自然人
.cardHolderRank	持卡人的載具等級，其 type 與 values 如下：	此屬性為 Optional，若憑證不含此屬性時，則視為正卡憑證；若憑證含此屬性時，則此憑證 Subject 之卡片持有人為正卡、附卡或行動載具持有人。
.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’ primary’ 、’ secondary’ 或’ mobile’	‘primary’ 表示卡片持有人是正卡持有人，’ secondary’ 表示卡片持有人是附卡持有人，’ mobile’ 表示卡片持有人是行動載具持有人
.tailOfPersonalID	身分識別證號尾碼屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的身分識別證號尾碼(外來人口自然人的身分識別證為居留證，因此，取其末 4 碼作為身分識別證號尾碼) (註：由於居留證號為個人隱私資料，故不於憑證中公佈其全部的號碼，只取末幾碼)
.type	OID id-chtpki-at-tailOfPersonalID (2.16.886.1.100.2.51)	此為代表 Tail of Personal ID Attribute 之 OID
.values	填入 Subject 的居留證號末 4 碼	例如居留證號為 AA12345678，則此欄填入 5678
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.20 To-Be-Signed 醫事人員憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	醫事人員的 X.500 Name 格式如下： C=TW CN=*醫事人員之中文姓名(以衛生福利部醫事管理系統所登記的姓名為準)* serialNumber=*個人序號(流水號用以區分同名的人)* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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	GPKI 憑證依據 PKIX，只採用 keyIdentifier 欄位，而不使用 authorityCertIssuer 與 authorityCertSerialNumber 欄位

	authorityCertSerialNumber 欄位	
.keyIdentifier	keyIdentifier 欄為的資料型態是 KeyIdentifier，而 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
.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	GPKI 每個 Subject 建議使用的私密金鑰為雙金鑰對（Dual Key Pairs）系統，分為簽章及加解密兩對，其中驗簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 醫事人員	此欄位為 Optional，若憑證的 Subject 沒有 Email

	憑證中此欄位只用於記載 Subject 的 Email Address	Address，或是不希望將 Email Address 公佈在憑證中，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 rfc822Name，並在此欄中記載 Subject 的 Email Address
.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	此欄可包含一串屬性，醫事人員憑證會記錄下列屬性

	SEQUENCE SIZE (1..MAX) OF Attribute	
.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-medicalPerson (2.16.886.1.100.3.1.7)	此 OID 表示憑證 Subject 的類別為醫事人員
.medicalPersonID	醫事人員身分識別代號屬性，其 type 與 values 如下：	此屬性用來記載此憑證 Subject 的國民身分證字號頭碼尾碼，其格式為 *XX-YYYY*，其中 *XX* 為國民身分證字號的頭 2 碼，*YYYY* 為國民身分證字號的末 4 碼 (註：由於國民身分證字號為個人隱私資料，故不於憑證中公佈其全部的號碼)
.type	OID id-chtpki-at-medicalPersonID (2.16.886.1.100.2.57)	此為代表 Medical Person ID Attribute 之 OID
.values	此欄位值為一個 ASN.1 UTF8String 格式的字串，其字串格式為 *XX-YYYY*，其中 *XX* 為國民身分證字號的頭 2 碼，*YYYY* 為國民身分證字號的末 4 碼	例如身分證字號為 A123456789 則此欄填入 A1-6789
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess	authorityInfoAccess 是 PKIX 所定義的 Private Extension

	(1.3.6.1.5.5.7.1.1)	
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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	此 URL 指向 OCSP 伺服器，可提供本憑證的狀態資訊

	選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	

1.3.21 To-Be-Signed 伺服器應用軟體憑證格式

簽發對象為政府機關（構）及政府單位的伺服器應用軟體，或是由醫事機構建置而用於醫療、健保或公共衛生等相關醫事服務用途的伺服器應用軟體，又細分為以下幾類：

(1) TLS 類伺服器應用軟體憑證：

簽發對象為政府機關（構）、政府單位所建置的 TLS 伺服器。

(2) 專屬類伺服器應用軟體憑證：

簽發對象為政府機關（構）、政府單位、或醫事機構所建置的特殊用途之伺服器應用軟體（例如用來提供身分識別服務的伺服器等）。

(3) 時戳伺服器應用軟體：

簽發對象為為政府機關（構）、政府單位、或醫事機構所建置的時戳伺服器(Timestamp Server)。

1.3.21.1 To-Be-Signed TLS 類伺服器應用軟體憑證格式

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 的 TLS 類伺服器應用軟體憑證所使用之憑證序號是一個透過加密安全虛擬亂數產生器（Cryptographically Secure Pseudorandom Number

		Generator，CSPRNG）所產生之長度為 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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	政府機關（構）或政府單位建置 TLS 伺服器，其 X.500 Name 格式如下： C=TW L=*主體所在管轄區域(例如地方政府使用縣市名稱，中央機關使用台灣等方式表示之)* L=*主體所在管轄區域(選擇性欄位，例如地方政府使用鄉鎮區名稱)* 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)* CN=*伺服器的網域名稱（Domain Name）或網路位址（IP Address）* 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)* （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 目前可使用 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	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內

	Public Key 的 DER 編碼值	含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	此擴充欄位的目的是標示 Subject 所使用的金鑰是哪一把

	Identifier	
.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	TLS 憑證的金鑰可以作為數位簽章、金鑰加密用途，所以 Key Usage 將包含 Digital Signature、keyEncipherment 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 OCTET STRING	對於 keyUsage 這種 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	TLS 憑證的金鑰可作為數位簽章、金鑰加密用途，因此 Named BIT STRING 之 digitalSignature (0)及 keyEncipherment(2)這兩個 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，TLS 憑證只能含有 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 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI TLS 憑證中，此欄位用於記錄 Subject 的完全吻合網域名稱(Fully Qualified Domain Name)或網路位址(IP Address)	此欄位為 Required
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼

		做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 可包含 1 個或多個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態，可選用 dNSName 或 iPAddress 類型	GPKI 選用 CHOICE 中的 dNSName 或 iPAddress 類型，並依據所選類型在此欄中記載該 TLS 伺服器的 Fully Qualified Domain Name 或 IP address
.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，TLS 類伺服器應用軟體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-applicationProcess (2.16.886.1.100.3.3.1)	此 OID 表示憑證 Subject 的類別為伺服器應用軟體
.extKeyUsage	Extended Key Usage 擴充	此欄位定義 TLS 憑證的

	欄位，記載 Subject Public Key 相對應之 Private Key 的特殊用途	Private Key 的延伸用途
.extnId	填入代表此擴充欄位的 OID id-ce-extKeyUsage (2.5.29.37)	
.critical	為了強制應用系統識別此憑證的特殊用途，Extended Key Usage 設定是 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 OCTET STRING	對於 extKeyUsage 這種 Extension 而言，必須使用 ExtKeyUsageSyntax 的 DER 編碼做為此 OCTET STRING 的值
.ExtKeyUsageSyntax	ExtKeyUsageSyntax 的資料型態是 SEQUENCE SIZE (1..MAX) OF KeyPurposeId	TLS 憑證的 ExtKeyUsageSyntax 會包含 2 個 KeyPurposeId
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-serverAuth (1.3.6.1.5.5.7.3.1)	id-kp-serverAuth 為 PKIX RFC 5280 所定義的 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	id-kp-clientAuth 為 PKIX RFC 5280 所定義的 Key Purpose OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊

.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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	此 URL 指向 OCSP 伺服器，

	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	可提供本憑證的狀態資訊

1.3.21.2 To-Be-Signed 專屬類伺服器應用軟體憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	依 PKIX 規定在 2049/12/31 23:59:59（含）之前使用

	憑證無效	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	如果是政府機關（構）或政府單位建置之伺服器應用軟體，則其 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)或單位的法定名稱(選擇性欄位，可以有多層)* CN=*伺服器應用軟體的名稱(可能是伺服器應用軟體之中文名稱)* 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)* 如果是醫事機構建置之伺服器應用軟體，則其 X.500 Name 格式如下：

		醫事機構的 X.500 Name (格式同醫事機構憑證的 Subject Name) CN=*伺服器應用軟體的名稱(可能是伺服器應用軟體之中文名稱)* 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)* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	可依伺服器應用軟體之需求採用單金鑰對(Single Key Pair)或雙金鑰對（Dual Key Pairs）系統，若為單金鑰對，則當該 Subject 所使用的金鑰對為簽章用金鑰對時，其 KeyUsage 將包含 digitalSignature，若為加解密用金鑰對時，則其 KeyUsage 將包含 keyEncipherment 與 dataEncipherment 兩種用途，若簽章及解密共用一對，則其 Key Usage 將包含 digitalSignature、keyEncipherment 與 dataEncipherment 三種用途；若為雙金鑰對，則該 Subject 建議的金鑰對將分為簽章及加解密兩對，其中簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若伺服器應用軟體採用單金鑰對(Single Key Pair)，且此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT

		STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 Bit 將會被設為 1，若此憑證為驗簽章與加解密用憑證，則此 Named BIT STRING 之 digitalSignature (0)、keyEncipherment(2)與 dataEncipherment (3)這三個 Bit 都將會被設為 1。 若伺服器應用軟體採用雙金鑰對(Dual Key Pair)，而此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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	GPKI 憑證只使用 policyIdentifier 欄位，而不使

	policyIdentifier 與 policyQualifiers 兩欄	用 policyQualifiers 欄位
.policyIdentifier	policyIdentifier 欄為的資料型態是 CertPolicyId，而 CertPolicyId 本身為一個 OBJECT IDENTIFIER 資料型態	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 OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 伺服器應用軟體憑證中，此欄為只用於記錄 Subject 的 URL 位址	此欄位為 Optional，若伺服器應用軟體沒有 URL，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載該伺服器應用軟體的 URL
.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	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省

	extension，所以 critical 的值必定是 FALSE	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，專屬類伺服器應用軟體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-applicationProcess (2.16.886.1.100.3.3.1)	此 OID 表示憑證 Subject 的類別為伺服器應用軟體
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉

	FALSE	
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.21.3 To-Be-Signed 時戳伺服器應用軟體憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	如果是政府機關（構）或政府單位建置之伺服器應用軟體，則其 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)或單位的法定名稱(選擇性欄位，可以有多層)* 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)* 如果是醫事機構建置之伺服器應用軟體，則其 X.500 Name 格式如下： *醫事機構的 X.500 Name (格式同醫事機構憑證的 Subject Name)* 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) （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	時戳伺服器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 OCTET STRING	對於 keyUsage 這種 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	時戳伺服器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 資料型態	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 OID

.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 伺服器應用軟體憑證中，此欄為只用於記錄 Subject 的 URL 位址	此欄位為 Optional，若伺服器應用軟體沒有 URL，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載該伺服器應用軟體的 URL
.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，時戳伺服器應用軟體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-applicationProcess (2.16.886.1.100.3.3.1)	此 OID 表示憑證 Subject 的類別為伺服器應用軟體
.extKeyUsage	Extended Key Usage 擴充欄位，記載 Subject Public Key 相對應之 Private Key 的特殊用途	依據 RFC 3161 的規定時戳伺服器的憑證必須含有此擴充欄位
.extnId	填入代表此擴充欄位的 OID id-ce-extKeyUsage (2.5.29.37)	
.critical	為了強制應用系統識別此憑證的特殊用途，Extended Key Usage 設定是 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 OCTET STRING	對於 extKeyUsage 這種 Extension 而言，必須使用 ExtKeyUsageSyntax 的 DER 編碼做為此 OCTET STRING 的值
.ExtKeyUsageSyntax	ExtKeyUsageSyntax 的資料型態是 SEQUENCE SIZE (1..MAX) OF KeyPurposeId	時戳伺服器憑證的 ExtKeyUsageSyntax 只會包含 1 個 KeyPurposeId
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-timeStamping (1.3.6.1.5.5.7.3.8)	id-kp-timeStamping 為 PKIX RFC 5280 及 RFC 3161 所定義的 Key Purpose OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之

	caIssuers 的 URL	cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

1.3.22 To-Be-Signed OCSP 伺服器憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	如果是政府機關（構）或政府單位建置之伺服器應用軟體，則其 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)或單位的法定名稱(選擇性欄位，可以有多層)* CN=*伺服器應用軟體的名稱(可能是伺服器應用軟體之中*

		文名稱) 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)* 如果是醫事機構建置之伺服器應用軟體，則其 X.500 Name 格式如下： *醫事機構的 X.500 Name (格式同醫事機構憑證的 Subject Name)* CN=*伺服器應用軟體的名稱(可能是伺服器應用軟體之中文名稱)* 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)* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省

	以 critical 的值必定是 FALSE	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	OCSP 伺服器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 OCTET STRING	對於 keyUsage 這種 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	OCSP 伺服器憑證的金鑰可作為數位簽章用途，因此 Named BIT STRING 之 digitalSignature (0)這一個 bit 將會被設為 1。
.extKeyUsage	Extended Key Usage 擴充欄位，記載 Subject Public Key 相對應之 Private Key 的特殊用途	此欄位定義 OCSP 伺服器憑證的 Private Key 的延伸用途
.extnId	填入代表此擴充欄位的 OID id-ce-extKeyUsage (2.5.29.37)	
.critical	為了強制應用系統識別此憑證的特殊用途，Extended Key Usage 設定是 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 OCTET STRING	對於 extKeyUsage 這種

		Extension 而言，必須使用 ExtKeyUsageSyntax 的 DER 編碼做為此 OCTET STRING 的值
.ExtKeyUsageSyntax	ExtKeyUsageSyntax 的資料型態是 SEQUENCE SIZE (1..MAX) OF KeyPurposeId	OCSP 伺服器憑證的 ExtKeyUsageSyntax 會包含 1 個 KeyPurposeId
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9)	id-kp-OCSPSigning 為 PKIX RFC 5280 所定義的 Key Purpose OID
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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	GPKI 憑證只使用 distributionPoint 欄位，而不使用 reasons 與 cRLIssuer 這

	與 cRLIssuer 三欄	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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置
.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	在 GPKI 憑證規格中，此擴充欄位將包含 1 個 caIssuers 這種 AccessDescription

	SIZE (1..MAX) OF 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與本憑證驗證相關之指引資訊
.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的 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 的 URL 網址

1.3.23 To-Be-Signed 一站式專屬授權憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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.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公司之唯一序號* 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.500 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商業之唯一序號* 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.500 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 目前可使用 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	GPKI 目前可採用 RSA

	STRING 內含 Subject Public Key 的 DER 編碼值	Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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 欄為的資料型態是 KeyIdentifier，而 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
.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	此擴充欄位的目的是標示 Subject 所使用的金鑰是哪一把

	Identifier	
.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 OCTET STRING	對於 keyUsage 這種 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	注意由於 FALSE 是 DEFAULT VALUE，所以

	定為 non-critical extension，所以 critical 的值必定是 FALSE	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 資料型態	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 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	對於 cRLDistributionPoints

	OCTET STRING	這種 Extension 而言，必須使用 CRLDistributionPoints 的 DER 編碼做為此 OCTET STRING 的值
.CRLDistributionPoints	CRLDistributionPoints 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供

		OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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	此 URL 指向 OCSP 伺服

	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	器，可提供本憑證的狀態資訊

1.3.24 To-Be-Signed 應用軟體客戶端專屬憑證格式

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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	依 PKIX 規定在 2049/12/31 23:59:59（含）之前使用

	憑證無效	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	如果是組織及團體建置的服務軟體之應用，則其 X.500 Name 格式如下： C=TW L=*縣市名稱(選擇性欄位，只適用於地區性組織或團體)* L=*鄉鎮市名稱(選擇性欄位，只適用於地區性組織或團體)* O=*組織或團體的正式登記名稱* serialNumber=*此組織或團體的 OID 識別碼* CN=*某應用軟體的名稱* 如果為「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之應用，則其 X.500 Name 格式如下： C=TW L=*縣市名稱(選擇性欄位，只適用於辦理新商業設立登記之應用)* O=*名稱預查核准之公司、商*

		業或有限合夥的名稱 CN=*準公司、準商業及準有限合夥設立一站式線上申請專屬使用者* serialNumber=*憑證管理中心自動給定準公司、準商業或準有限合夥之唯一序號* （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 目前可使用 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 Key 的 DER 編碼值	GPKI 目前可採用 RSA Public Key，其 BIT STRING 的值內含以下資料型態的 DER 編碼： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER }
extensions	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	注意由於 FALSE 是 DEFAULT VALUE，所以

	是 non-critical extension，所以 critical 的值必定是 FALSE	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 欄為的資料型態是 KeyIdentifier，而 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
.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	可依伺服器應用軟體之需求

	載 Subject Public Key 相對應之 Private Key 的用途限制	採用單金鑰對(Single Key Pair)或雙金鑰對（Dual Key Pairs）系統，若為單金鑰對，則該 Subject 所使用的私密金鑰對為簽章用金鑰對時，則其 KeyUsage 將包含 digitalSignature，若為加解密用金鑰對時，則其 KeyUsage 將包含 keyEncipherment 與 dataEncipherment 兩種用途，若簽章及解密共用一對，則其 Key Usage 將包含 digitalSignature、keyEncipherment 與 dataEncipherment 三種用途；若為雙金鑰對，則該 Subject 建議的金鑰對將分為簽章及加解密兩對，其中簽章用憑證之 Key Usage 將包含 digitalSignature，而加解密憑證之 Key Usage 將包含 keyEncipherment 與 dataEncipherment 兩種用途
.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 OCTET STRING	對於 keyUsage 這種 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	若伺服器應用軟體採用單金鑰對(Single Key Pair)，且此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個

		Bit 將會被設為 1，若此憑證為驗簽章與加解密用憑證，則此 Named BIT STRING 之 digitalSignature (0)、keyEncipherment(2)與 dataEncipherment (3)這三個 Bit 都將會被設為 1。 若伺服器應用軟體採用雙金鑰對(Dual Key Pair)，而此憑證為驗簽章用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 Bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 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	根據 CA 簽發此憑證時所採

	型態是 CertPolicyId，而 CertPolicyId 本身為一個 OBJECT IDENTIFIER 資料型態	用的保證等級（Assurance Level），填上代表該保證等級之 GPKI Certificate Policy OID
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI 伺服器應用軟體憑證中，此欄為只用於記錄 Subject 的 URL 位址	此欄位為 Optional，若伺服器應用軟體沒有 URL，則本擴充欄位可省略
.extnId	填入代表此擴充欄位的 OID id-ce-subjectAltName (2.5.29.17)	
.critical	在 GPKI 中，subjectAltName 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 subjectAltName 這種 Extension 而言，必須使用 SubjectAltName 的 DER 編碼做為此 OCTET STRING 的值
.SubjectAltName	SubjectAltName 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 SubjectAltName 的 GeneralNames 只會包含 1 個 GeneralName
.GeneralName	GeneralName 是一個 CHOICE 資料型態	GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載該伺服器應用軟體的 URL
.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	對於

	OCTET STRING	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，專屬類伺服器應用軟體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-applicationProcess (2.16.886.1.100.3.3.1)	此 OID 表示憑證 Subject 的類別為伺服器應用軟體
.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 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 憑證格式中，欄位 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 使用此擴充欄位記載簽發本憑證之 CA 憑證資訊存取位置，並可視需要提供 OCSP 的存取資訊
.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 憑證規格中，此擴充欄位至少包含 1 個 caIssuers 這種 AccessDescription，並可視需要加上 ocsp 的 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與本憑證驗證相關之指引資訊
.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 caIssuers 的 URL	此 URL 指向與簽發本憑證之 CA 相關之憑證資訊。該資訊得以單一 DER 編碼之憑證，或 BER/DER 編碼之 CMS (PKCS#7)憑證串列(certs-only)提供；亦可為指向 LDAP 中 CA Entry 之 cACertificate 或 crossCertificatePair Attribute 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 OCSP 伺服器，可提供本憑證的狀態資訊

2 憑證廢止清冊格式剖繪

2.1 憑證廢止清冊種類

憑證廢止清冊共分為三類：完整憑證廢止清冊(Complete CRL)、動憑證廢止清冊(Delta CRL)以及部分憑證廢止清冊(Partitioned CRL)。

2.2 憑證廢止清冊的設計原則

除了遵循 X.509 標準[1]之外，GPKI 之憑證廢止清冊欄位的設計並遵循以下原則：

- 符合 IETF PKIX Certificate and CRL Profile (RFC 5280)之 CRL 規格[2]。
- 與 Asia PKI Consortium 之 CRL 規格[4]相容。
- 與 FPKI 之 CRL 規格[5]相容。
- 與歐盟之 CRL 規格[6]相容。
- 與 Web Browser 相容。

當主管機關公告採用 PQC 演算法及其因應之憑證廢止清冊格式時，相關憑證廢止清冊欄位之設計與值之選用，應依本文件附錄 A 所列規範辦理。

2.3 憑證廢止清冊欄位

下表是根據以上所列原則而訂定的三種憑證廢止清冊所使用欄位。其中標註「✓」記號者，為該類憑證廢止清冊的必要欄位(Required Field)；若標註「✗」記號者，則表示該類憑證廢止清冊中不使用此欄位：

欄位名稱(Field Name)	憑證廢止清冊(CRL)		
	Complete CRL	Delta CRL	Partitioned CRL
version	✓	✓	✓
signature	✓	✓	✓
issuer	✓	✓	✓
thisUpdate	✓	✓	✓
nextUpdate	✓	✓	✓
revokedCertificates	✓	✓	✓
crlExtensions	✓	✓	✓

下表是三種憑證廢止清冊中 revokedCertificate 欄位中每一個 Entry 所使用的 CRL Entry 擴充欄位(CRL Entry Extensions)，其中標註「✓」記號者，為該類憑證廢止清冊 Entry 的必要擴充欄位(Required Extension Field)；標註「〇」記號者，為該類憑證廢止清冊 Entry 的選擇性擴充欄位(Optional Extension Field)；標有「×」記號者，則表示該類憑證廢止清冊 Entry 中不使用此擴充欄位。下表並對標示各種擴充欄位是否標示為 critical，其中「TRUE」表示若使用此擴充欄位，則須必標示為 critical；「FLASE」表示此擴充欄位若使用則必標示為 non-critical；「N/A」（Not Applicable）表示在 GPKI 將不於憑證廢止清冊中使用該 CRL Entry 擴充欄位，因此無所謂 critical 或 non-critical 的情況：

CRL Entry 擴充欄位 (CRL ENTRY EXTNESION FIELD)	憑證廢止清冊(CRL)			Critical
	Complete CRL	Delta CRL	Partitioned CRL	
reasonCode	✓	✓	✓	FALSE
holdInstructionCode	×	×	×	N/A
invalidityDate	×	×	×	N/A

certificateIssuer	×	×	×	N/A

下表是三種憑證廢止清冊所使用的 CRL 擴充欄位(CRL Extensions)，其中標註「✓」記號者，為該類憑證廢止清冊的必要擴充欄位(Required Extension Field)；標註「○」記號者，為該類憑證廢止清冊的選擇性擴充欄位(Optional Extension Field)；標有「×」記號者，則表示該類憑證廢止清冊中不使用此擴充欄位。下表並對標示各種擴充欄位是否標示為 critical，其中「TRUE」表示若使用此擴充欄位，則須必標示為 critical；「FLASE」表示此擴充欄位若使用則必標示為 non-critical；「N/A」（Not Applicable）表示在 GPKI 將不於憑證廢止清冊中使用該 CRL 擴充欄位，因此無所謂 critical 或 non-critical 的情況：

CRL 擴充欄位 (CRL EXTNESION FIELD)	**憑證廢止清冊(CRL)**			**Critical**
	Complete CRL	Delta CRL	Partitioned CRL	
authorityKeyIdentifier	✓	✓	✓	FALSE
issuerAltName	×	×	×	N/A
cRLNumber	✓	✓	✓	FALSE
deltaCRLIndicator	×	✓	×	TRUE
issuingDistributionPoint	×	×	✓	TRUE
freshestCRL	○	×	×	FALSE

2.4 憑證廢止清冊格式

GPKI 所採用的憑證廢止清冊為 X.509 CRL [1]。X.509 CRL 是一種 SIGNED 資料，其格式如下：

欄位	內容	說明

toBeSigned	To-Be-Signed CRL（尚未簽章的 CRL）	To-Be-Signed CRL 的格式都是遵循 X.509 標準，但內容隨 CRL 為 Complete CRL 或 Delta CRL 的不同而有所差異，此兩類 To-Be-Signed CRL 內容詳見後面的說明
algorithmIdentifier	CA 對此 CRL 簽章所用之簽章演算法之 AlgorithmIdentifier	此欄的值必須與 toBeSigned CRL 內的 signature 欄的值相同
.algorithm	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 sha256WithRSAEncryption
.parameters	NULL	簽章演算法雖然不需要 parameters，但其 parameters 必須填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500
signature	CA 對 CRL 的簽章	此簽章是 CA 對 toBeSigned 欄位中的 To-Be-Signed CRL 所做的簽章

以上格式對於 Complete CRL、 Delta CRL 與 Partition CRL 都是相同的，但是三類 CRL 內部的 To-Be-Signed 部分會稍有差異。此三類 To-Be-Signed CRL 格式分別說明如後。

為因應後量子密碼技術的發展，GPKI 已規劃支援相關憑證廢止清冊格式與演算法，相關說明請參閱附錄 A。

2.4.1 To-Be-Signed 完整憑證廢止清冊(Complete CRL)的內容

欄位	內容	說明
version	v2(1)	CRL 的版本，GPKI 使用 v2 之 CRL 格式（注意 V2 的值是 1 而不是 2）
signature		簽 CRL 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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	CA 的 DN	此 DN 必須要與 CA cRLSign Certificate 之 issuer 欄位之 DN 相同 （註：在 GPKI 中 keyCertSign Certificate 與 cRLSign Certificate 是同一張）
thisUpdate	本次 CRL 更新的格林威治時間（GMT）	1. 依 PKIX 規定在 2049/12/31 23:59:59 之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略。 2. CA 保證在 thisUpdate 之前的發生的所有憑證廢止（Revocation）與暫停使用（Suspension）事件都會紀錄在此 Complete CRL 中。 3. 當 CA 在產生 Complete CRL 時，如果有憑證原本被暫停使用，但在 thisUpdate 之前被恢復使用（Resumption），則此憑證的暫停使用紀錄就會被移除，而不紀錄在此 Complete CRL 中或後續的 CRL 中，除非此憑證又再次地被廢止或暫停使用。 4. 當 CA 在產生 Complete CRL 時，如果有憑證原本被廢止或暫停使用，但在 thisUpdate 之前憑證過期（Expiration，即

		thisUpdate 時間已超過憑證的 notAfter 時間），則該憑證的廢止或暫停使用紀錄就會被移除，而不紀錄在此 Complete CRL 中。
nextUpdate	預計下次 CRL 更新的格林威治時間（GMT）	1. 依 PKIX 規定在 2049/12/31 23:59:59 之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略。 2. 如果沒有意外，此 nextUpdate 時間將會變成下次產生之 Complete CRL 的 thisUpdate 時間。
revokedCertificates	RevokedCertificate ::= SEQUENCE OF RevokedCertificate	在 thisUpdate 之前的發生的所有有效（Effective）的憑證廢止（Revocation）與暫停使用（Suspension）事件都會紀錄在 revokedCertificates 中（註：所謂有效（Effective）是只該憑證尚未過期，或暫停使用的憑證沒有被恢復使用）
*.RevokedCertificate	填入一連串的 RevokedCertificate 紀錄，每一個 RevokedCertificate 紀錄的內容如下：	
.userCertificate	填入被廢止憑證之憑證序號 CertificateSerialNumber	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，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
.revocationDate	憑證被廢止或暫停使用的格林威治時間（GMT）	1. 依 PKIX 規定在 2049/12/31 23:59:59 之前使用 UTCTime 資料型

		態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略。 2. 此 revocationDate 時間是 CA 收到廢止或暫停使用申告的時間，請勿與 invalidityDate 這個 CRLEntryExtension 混淆（註：基於安全理由 GPKI 並不使用 invalidityDate 這個 CRLEntryExtension）。 3. 此 revocationDate 時間是憑證第一次進入 CRL 紀錄的時間，如果有一張憑證原本被暫停使用，但在沒恢復使用前即因其他理由（例如確定私密金鑰失竊）被改為廢止，則憑證的 CRLReason 將會被改變，但是此憑證的 revocationDate 時間應該沿用原來憑證暫停使用所紀錄的 revocationDate 時間。
.crlEntryExtensions	SEQUENCE OF CRLEntryExtension（註：CRLEntryExtension 資料型態的格式與 Public-Key Certificate 的 Extension 資料型態的格式完全相同）	可填入一連串 CRLEntryExtension，但 GPKI 只使用 reasonCode 這個 CRLEntryExtension
.reasonCode	GPKI 只使用 reasonCode 這個 CRLEntryExtension，其內容如下：	
.extnId	填入 id-ce-reasonCode (也就是 2.5.29.21)這個 OID	
.critical	reasonCode 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 reasonCode 這種 Extension 而言，必須使用以下 CRLReason 的 DER 編碼之一做為此 OCTET STRING 的值，CRLReason 本身為一個 ENUMERATED	在 GPKI 中規定有些 CRLReason 不得使用於 Complete CRL 中 （註：以下所指的憑證，如無特別聲明，則包含 Public-Key Certificate 與 Attribute Certificate 兩種）
	unused(0)	遵照 PKIX 的規定，在 GPKI 中不得使用此 CRLReason
	keyCompromise(1)	當 EE 的私密金鑰遺失或懷疑被竊取或破解，而欲廢止憑證，則使用此 CRLReason
	caCompromise(2)	當懷疑或確定 CA keyCertSign 或 cRLSign 私密金鑰遭竊或被破解時使用此 CRLReason，但此 CRLReason 不得使用於廢止 EE Certificate，只能用於廢止 CA Certificate （註：當懷疑或確定 CA keyCertSign 私密金鑰遭竊或被破解而必須廢止已經簽發的所有 EE 憑證，重新產製 CA 金鑰對，並重新簽發所有 EE 憑證時，則 EE 憑證廢止的 CRLReason 應該使用 superseded）
	affiliationChanged(3)	當 EE 與憑證內容相關之身分資料改變（例如改名、遷移戶籍、換工作）時必須廢止憑證，則使用此 CRLReason
	superseded(4)	當 EE 因某種需要（例如更換新卡、CA Hand-Over 而重發所有憑證、CA 為了更新憑證格式而重發所有憑證、或因密碼破解方法的突破而必須改用更安全的金鑰種類或長度）而更新憑證，必須廢止原來之憑證時，使用此 CRLReason
	cessationOfOperation(5)	當 EE 憑證並沒有任何特殊理由，而純粹不想再繼續使用

		（例如「剪卡」）或不得不作廢時，使用此 CRLReason
	certificateHold(6)	當 EE 憑證暫停使用（Suspension）時使用此 CRLReason（例如「掛失」）
	removeFromCRL(8)	此 CRLReason 只能出現在 Delta CRL 中，不得使用於 Complete CRL
	privilegeWithdrawn(9) （註：X.509 4th Edition）	1. 當 EE 的 privilege 被取消（例如遭撤銷登記或褫奪公權）時，使用此 CRLReason 2. 此 CRLReason 通常不是由 EE 主動發起，而通常是在 CA/RA 或 AA「逕行廢止」EE 憑證時才會使用 3. 此 CRLReason 通常用於廢止 Attribute Certificate，但也可能用於廢止 Public-Key Certificate
	aACompromise(10) （註：X.509 4th Edition）	當懷疑 AA 簽發 Attribute Certificate 用之私密金鑰此 CRLReason 遭竊或被破解時使用此 CRLReason，但此 CRLReason 不得使用於廢止 Public-Key Certificate，只能用於廢止 AA 本身之 Public-Key Certificate 與 EE 之 Attribute Certificate
crlExtensions	SEQUENCE OF CRLExtensions （註：CRLExtension 資料型態的格式與 Public-Key Certificate 的 Extension 資料型態的格式完全相同）	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 CRL 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	在 GPKI 中，CRL 依據 PKIX，只採用 keyIdentifier 欄位，而不使用 authorityCertIssuer 與 authorityCertSerialNumber 欄位
.keyIdentifier	keyIdentifier 欄為的資料型態是 KeyIdentifier，而 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
.cRLNumber	cRLNumber CRLExtension 的內容如下：	cRLNumber 擴充欄位的內容是用來記錄此 CRL 的序號
.extnId	填入 id-ce-cRLNumber (也就是 2.5.29.20)這個 OID	
.critical	cRLNumber 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 cRLNumber 這種 Extension 而言，必須使用 CRLNumber 的 DER 編碼做為此 OCTET STRING 的值，而 CRLNumber 本身為一個 INEGER (0..MAX) 正整數資料型態	根據 X.509 標準，CRL Number 必須是一個 monotonically increasing sequence number。在 GPKI 中，憑證廢止清冊的 CRLNumber 值應為一個長度小於或等於 7 bytes 的正整數。
.freshestCRL	freshestCRL CRLExtension，其內容如下：	freshestCRL 擴充欄位為 Optional，當 CA 有提供 Delta CRL 時才需要在 Complete

		CRL 中使用此擴充欄位，此擴充欄位是用來提供憑證應用軟體取得 Delta CRL 的指引，目前 GPKI 所使用之 Delta CRL Distribution Points 為一個 URL 網址
.extnId	填入 id-ce-freshestCRL (也就是 2.5.29.46)這個 OID	
.critical	freshestCRL 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 freshestCRL 這種 Extension 而言，必須使用 CRLDistributionPoints 的 DER 編碼做為此 OCTET STRING 的值
.CRLDistributionPoints	CRLDistributionPoints 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF DistributionPoint	在 GPKI 中，freshestCRL 擴充欄位中，將只含有 1 個 DistributionPoint
.DistributionPoint	DistributionPoint 為一 SEQUENCE，內含 distributionPoint、reasons 與 cRLIssuer 三欄	在 GPKI 中，freshestCRL 擴充欄位只使用 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	在 GPKI 中，Delta 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	在 GPKI 中，Delta 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 Delta CRL 檔的 URL

2.4.2 To-Be-Signed 異動憑證廢止清冊(Delta CRL)的內容

欄位	內容	說明
version	v2(1)	CRL 的版本，GPKI 使用 v2 之 CRL 格式（注意 V2 的值是 1 而不是 2）
signature		簽 CRL 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	簽章演算法的 OID sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 可使用簽章演算法 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	CA 的 DN	此 DN 必須要與 CA cRLSign Certificate 之 issuer 欄位之 DN 相同 （註：在 GPKI 中 keyCertSign Certificate 與 cRLSign Certificate 是同一張）
thisUpdate	本次 CRL 更新的格林威治時間（GMT）	1. 依 PKIX 規定在 2049/12/31 23:59:59 之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略 2. CA 保證在 Base CRL 的 thisUpdate 到此 Delta CRL 的 thisUpdate 之間的發生的所有憑證廢止（Revocation）、暫停使用（Suspension）與恢復

		使用（Resumption）事件都會紀錄在此 Delta CRL 中 3. CA 保證如果在此 Delta CRL 的 thisUpdate 之前，如有憑證原本被廢止或暫停使用，但在 Base CRL 的 thisUpdate 到此 Delta CRL 的 thisUpdate 之間此憑證發生過期（Expiration，即已經過了憑證的 notAfter 時間）的事件，則此事件將會被紀錄在此 Delta CRL 中
nextUpdate	預計下次 CRL 更新的格林威治時間（GMT）	1. 依 PKIX 規定在 2049/12/31 23:59:59 之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略 2. 如果沒有意外，此 nextUpdate 時間將會變成下次產生之 Delta CRL 的 thisUpdate 時間
revokedCertificates	RevokedCertificate ::= SEQUENCE OF RevokedCertificate	1. 在 Base CRL 的 thisUpdate 到此 Delta CRL 的 thisUpdate 之間的發生的所有憑證廢止（Revocation）、暫停使用（Suspension）與恢復使用（Resumption）事件都會紀錄在此 Delta CRL 中 2. 在此 Delta CRL 的 thisUpdate 之前，如有憑證原本被廢止或暫停使用，但在 Base CRL 的 thisUpdate 到此 Delta CRL 的 thisUpdate 之間此憑證發生過期

		（Expiration，即已經過了憑證的 notAfter 時間）的事件，則此事件將會被紀錄在此 Delta CRL 中
*.RevokedCertificate	填入一連串的 RevokedCertificate 紀錄，每一個 RevokedCertificate 紀錄的內容如下：	
.userCertificate	填入被廢止憑證之憑證序號 CertificateSerialNumber	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，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
.revocationDate	憑證被廢止或暫停使用的格林威治時間（GMT）	1. 依 PKIX 規定在 2049/12/31 23:59:59 之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略 2. 此 revocationDate 時間是 CA 收到廢止或暫停使用申告的時間，請勿與 invalidityDate 這個 CRLEntryExtension 混淆（註：基於安全理由 GPKI 並不使用 invalidityDate 這個 CRLEntryExtension） 3. 此 revocationDate 時間是憑證第一次進入 CRL 紀錄的時間，如果有一張憑證原本被暫停使用，但在沒恢復使用前即因其他理由（例如確定私密金鑰失竊）被改為廢止，則憑證的 CRLReason 將會被改變，但是此憑證的

		revocationDate 時間應該沿用原來憑證暫停使用所紀錄的 revocationDate 時間
.crlEntryExtensions	SEQUENCE OF CRLEntryExtension（註：CRLEntryExtension 資料型態的格式與 Public-Key Certificate 的 Extension 資料型態的格式完全相同）	可填入一連串 CRLEntryExtension，但 GPKI 只使用 reasonCode 這個 CRLEntryExtension
.reasonCode	GPKI 只使用 reasonCode 這個 CRLEntryExtension，其內容如下：	
.extnId	填入 id-ce-reasonCode (也就是 2.5.29.21)這個 OID	
.critical	reasonCode 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 reasonCode 這種 Extension 而言，必須使用以下 CRLReason 的 DER 編碼之一做為此 OCTET STRING 的值，CRLReason 本身為一個 ENUMERATED	在 GPKI 中規定有些 CRLReason 不得使用於 Delta CRL 中 （註：以下所指的憑證，如無特別聲明，則包含 Public-Key Certificate 與 Attribute Certificate 兩種）
	unused(0)	遵照 PKIX 的規定，在 GPKI 中不得使用此 CRLReason
	keyCompromise(1)	當 EE 的私密金鑰遺失或懷疑被竊取或破解，而欲廢止憑證，則使用此 CRLReason
	caCompromise(2)	當懷疑或確定 CA keyCertSign 或 cRLSign 私密金鑰遭竊或被破解時使用此 CRLReason，但此 CRLReason 不得使用於廢止 EE Certificate，只能用於廢止 CA Certificate （註：當懷疑或確定 CA keyCertSign 私密金鑰遭竊或被破解而必須廢止已經簽發的所有 EE 憑證，重新產製

		CA 金鑰對，並重新簽發所有 EE 憑證時，則 EE 憑證廢止的 CRLReason 應該使用 superseded）
	affiliationChanged(3)	當 EE 與憑證內容相關之身分資料改變（例如改名、遷移戶籍、換工作）時必須廢止憑證，則使用此 CRLReason
	superseded(4)	當 EE 因某種需要（例如更換新卡、CA Hand-Over 而重發所有憑證、CA 為了更新憑證格式而重發所有憑證、或因密碼破解方法的突破而必須改用更安全的金鑰種類或長度）而更新憑證，必須廢止原來之憑證時，使用此 CRLReason
	cessationOfOperation(5)	當 EE 憑證並沒有任何特殊理由，而純粹不想再繼續使用（例如「剪卡」）或不得不作廢時，使用此 CRLReason
	certificateHold(6)	當 EE 憑證暫停使用（Suspension）時使用此 CRLReason（例如「掛失」）
	removeFromCRL(8)	1. 如果有一張憑證原本在此 Delta CRL 的 Base CRL 中被紀錄為暫停使用的狀態，但在 Base CRL 的 thisUpdate 到此 Delta CRL 的 thisUpdate 之間憑證被恢復使用（Resumption），則在 Delta CRL 中加入一筆 CRLReason 為 removeFromCRL 的 RevokedCertificate 紀錄，而該 RevokedCertificate 紀錄的 revocationDate 則表示該憑證被恢復使用的時間 2. 如果有一張憑證原本在此 Delta CRL 的 Base CRL 中被紀錄為廢止或

		暫停使用，但是憑證在 Base CRL 的 thisUpdate 到此 Delta CRL 的 thisUpdate 之間過期（Expiration，即在 Delta CRL 的 thisUpdate 時間之前已經過了憑證的 notAfter 時間），則 CA 會主動在此 Delta CRL 中加入一筆 RevokedCertificate 紀錄，其 CRLReason 為 removeFromCRL，其 revocationDate 時間則為該憑證的 notAfter 時間 3. 此 CRLReason 只能出現在 Delta CRL 中，不得使用於 Complete CRL
	privilegeWithdrawn(9) （註：X.509 4th Edition）	1. 當 EE 的 privilege 被取消（例如遭撤銷登記或褫奪公權）時，使用此 CRLReason 2. 此 CRLReason 通常不是由 EE 主動發起，而通常是在 CA/RA 或 AA「逕行廢止」EE 憑證時才會使用 3. 此 CRLReason 通常用於廢止 Attribute Certificate，但也可能用於廢止 Public-Key Certificate
	aACompromise(10) （註：X.509 4th Edition）	當懷疑 AA 簽發 Attribute Certificate 用之私密金鑰此 CRLReason 遭竊或被破解時使用此 CRLReason，但此 CRLReason 不得使用於廢止 EE Public-Key Certificate，只能用於廢止 AA 本身之 Public-Key Certificate 與 EE 之 Attribute Certificate
crlExtensions	SEQUENCE OF CRLExtensions （註：CRLExtension 資料	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

	型態的格式與 Public-Key Certificate 的 Extension 資料型態的格式完全相同）	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 CRL 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	在 GPKI 中，CRL 依據 PKIX，只採用 keyIdentifier 欄位，而不使用 authorityCertIssuer 與 authorityCertSerialNumber 欄位
.keyIdentifier	keyIdentifier 欄為的資料型態是 KeyIdentifier，而 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
.cRLNumber	cRLNumber CRLExtension 的內容如下：	
.extnId	填入 id-ce-cRLNumber (也就是 2.5.29.20)這個 OID	
.critical	cRLNumber 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	根據 X.509 標準，CRL Number 必須是一個

	cRLNumber 這種 Extension 而言，必須使用 CRLNumber 的 DER 編碼做為此 OCTET STRING 的值，而 CRLNumber 本身為一個 INEGER (0..MAX) 正整數資料型態	monotonically increasing sequence number。在 GPKI 中，憑證廢止清冊的 CRLNumber 值應為一個長度小於或等於 7 bytes 的正整數。
.deltaCRLIndicator	deltaCRLIndicator CRLExtension 的內容如下：	
.extnId	填入 id-ce-deltaCRLIndicator (也就是 2.5.29.27)這個 OID	
.critical	deltaCRLIndicator 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，此欄位不可省略，而在 DER 編碼中 TRUE 的 DER Value 必須編為 0xFF
.extnValue	extnValue 的資料型態是 OCTET STRING，對於 deltaCRLIndicator 這種 Extension 而言，必須使用 BaseCRLNumber 的 DER 編碼做為此 OCTET STRING 的值（也就是 Base CRL 的 CRLNumber 值），而 CRLNumber 本身為一個 INEGER (0..MAX) 正整數資料型態	BaseCRLNumber 是用來指明此 Delta CRL 是以哪一個 Complete CRL 做為 Base CRL（BaseCRLNumber = CRLNumber of the Complete CRL used as the Base CRL for this Delta CRL）

2.4.3 To-Be-Signed 部分憑證廢止清冊(Partitioned CRL)的內容

欄位	內容	說明
version	v2(1)	CRL 的版本，GPKI 使用 v2 之 CRL 格式（注意 V2 的值是 1 而不是 2）
signature		簽 CRL 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	簽章演算法的 OID	簽章演算法之 OID，GPKI 可

	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	使用簽章演算法 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	CA 的 DN	此 DN 必須要與 CA cRLSign Certificate 之 issuer 欄位之 DN 相同 （註：在 GPKI 中 keyCertSign Certificate 與 cRLSign Certificate 是同一張）
thisUpdate	本次 CRL 更新的格林威治時間（GMT）	5. 依 PKIX 規定在 2049/12/31 23:59:59 之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略。 6. CA 保證在 thisUpdate 之前的發生的所有憑證廢止（Revocation）與暫停使用（Suspension）事件都會紀錄在此 Partitioned CRL 中。 7. 當 CA 在產生 Partitioned CRL 時，如果有憑證原本被暫停使用，但在 thisUpdate 之前被恢復使用（Resumption），則此憑證的暫停使用紀錄就會被移除，而不紀錄在此 Partitioned CRL 中或後續的 CRL 中，除非此憑證又再次地被廢止或暫停使用。 8. 當 CA 在產生 Partitioned CRL 時，如果有憑證原本被廢止或暫停使用，但在 thisUpdate 之前憑證

		過期（Expiration，即 thisUpdate 時間已超過憑證的 notAfter 時間），則該憑證的廢止或暫停使用紀錄就會被移除，而不紀錄在此 Partitioned CRL 中。
nextUpdate	預計下次 CRL 更新的格林威治時間（GMT）	3. 依 PKIX 規定在 2049/12/31 23:59:59 之前使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略。 4. 如果沒有意外，此 nextUpdate 時間將會變成下次產生之 Partitioned CRL 的 thisUpdate 時間。
revokedCertificates	RevokedCertificate ::= SEQUENCE OF RevokedCertificate	在 thisUpdate 之前的發生的所有有效（Effective）的憑證廢止（Revocation）與暫停使用（Suspension）事件都會紀錄在 revokedCertificates 中（註：所謂有效（Effective）是只該憑證尚未過期，或暫停使用的憑證沒有被恢復使用）
*.RevokedCertificate	填入一連串的 RevokedCertificate 紀錄，每一個 RevokedCertificate 紀錄的內容如下：	
.userCertificate	填入被廢止憑證之憑證序號 CertificateSerialNumber	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，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
.revocationDate	憑證被廢止或暫停使用的格林威治時間（GMT）	4. 依 PKIX 規定在 2049/12/31 23:59:59 之前

		使用 UTCTime 資料型態，格式為 YYMMDDHHMMSSZ，其中即使秒數 SS 為 00 也不可省略，而最後的 Z 表示 GMT 時間也不可省略。 5. 此 revocationDate 時間是 CA 收到廢止或暫停使用申告的時間，請勿與 invalidityDate 這個 CRLEntryExtension 混淆（註：基於安全理由 GPKI 並不使用 invalidityDate 這個 CRLEntryExtension）。 6. 此 revocationDate 時間是憑證第一次進入 CRL 紀錄的時間，如果有一張憑證原本被暫停使用，但在沒恢復使用前即因其他理由（例如確定私密金鑰失竊）被改為廢止，則憑證的 CRLReason 將會被改變，但是此憑證的 revocationDate 時間應該沿用原來憑證暫停使用所紀錄的 revocationDate 時間。
.crlEntryExtensions	SEQUENCE OF CRLEntryExtension（註：CRLEntryExtension 資料型態的格式與 Public-Key Certificate 的 Extension 資料型態的格式完全相同）	可填入一連串 CRLEntryExtension，但 GPKI 只使用 reasonCode 這個 CRLEntryExtension
.reasonCode	GPKI 只使用 reasonCode 這個 CRLEntryExtension，其內容如下：	
.extnId	填入 id-ce-reasonCode (也就是 2.5.29.21)這個 OID	
.critical	reasonCode 必定是 non-critical extension，所以	注意由於 FALSE 是 DEFAULT VALUE，所以

	critical 的值必定是 FALSE	DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING，對於 reasonCode 這種 Extension 而言，必須使用以下 CRLReason 的 DER 編碼之一做為此 OCTET STRING 的值，CRLReason 本身為一個 ENUMERATED	在 GPKI 中規定有些 CRLReason 不得使用於 Complete CRL 中（註：以下所指的憑證，如無特別聲明，則包含 Public-Key Certificate 與 Attribute Certificate 兩種）
	unused(0)	遵照 PKIX 的規定，在 GPKI 中不得使用此 CRLReason
	keyCompromise(1)	當 EE 的私密金鑰遺失或懷疑被竊取或破解，而欲廢止憑證，則使用此 CRLReason
	caCompromise(2)	當懷疑或確定 CA keyCertSign 或 cRLSign 私密金鑰遭竊或被破解時使用此 CRLReason，但此 CRLReason 不得使用於廢止 EE Certificate，只能用於廢止 CA Certificate（註：當懷疑或確定 CA keyCertSign 私密金鑰遭竊或被破解而必須廢止已經簽發的所有 EE 憑證，重新產製 CA 金鑰對，並重新簽發所有 EE 憑證時，則 EE 憑證廢止的 CRLReason 應該使用 superseded）
	affiliationChanged(3)	當 EE 與憑證內容相關之身分資料改變（例如改名、遷移戶籍、換工作）時必須廢止憑證，則使用此 CRLReason
	superseded(4)	當 EE 因某種需要（例如更換新卡、CA Hand-Over 而重發所有憑證、CA 為了更新憑證格式而重發所有憑證、或因密碼破解方法的突破而必須改用更安全的金鑰種類或長度）而更新憑證，必須廢止原來之憑證時，使用此 CRLReason
	cessationOfOperation(5)	當 EE 憑證並沒有任何特殊理

		由，而純粹不想再繼續使用（例如「剪卡」）或不得不作廢時，使用此 CRLReason
	certificateHold(6)	當 EE 憑證暫停使用（Suspension）時使用此 CRLReason（例如「掛失」）
	removeFromCRL(8)	此 CRLReason 只能出現在 Delta CRL 中，不得使用於 Complete CRL
	privilegeWithdrawn(9) （註：X.509 4th Edition）	4. 當 EE 的 privilege 被取消（例如遭撤銷登記或褫奪公權）時，使用此 CRLReason 5. 此 CRLReason 通常不是由 EE 主動發起，而通常是在 CA/RA 或 AA「逕行廢止」EE 憑證時才會使用 6. 此 CRLReason 通常用於廢止 Attribute Certificate，但也可能用於廢止 Public-Key Certificate
	aACompromise(10) （註：X.509 4th Edition）	當懷疑 AA 簽發 Attribute Certificate 用之私密金鑰此 CRLReason 遭竊或被破解時使用此 CRLReason，但此 CRLReason 不得使用於廢止 Public-Key Certificate，只能用於廢止 AA 本身之 Public-Key Certificate 與 EE 之 Attribute Certificate
crlExtensions	SEQUENCE OF CRLExtensions （註：CRLExtension 資料型態的格式與 Public-Key Certificate 的 Extension 資料型態的格式完全相同）	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 CRL 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	在 GPKI 中，CRL 依據 PKIX，只採用 keyIdentifier 欄位，而不使用 authorityCertIssuer 與 authorityCertSerialNumber 欄位
.keyIdentifier	keyIdentifier 欄為的資料型態是 KeyIdentifier，而 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
.cRLNumber	cRLNumber CRLExtension 的內容如下：	cRLNumber 擴充欄位的內容是用來記錄此 CRL 的序號
.extnId	填入 id-ce-cRLNumber (也就是 2.5.29.20)這個 OID	
.critical	cRLNumber 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 cRLNumber 這種 Extension 而言，必須使用 CRLNumber 的 DER 編碼做為此 OCTET STRING 的值，而 CRLNumber 本身為一個 INEGER (0..MAX) 正整數資料型態	根據 X.509 標準，CRL Number 必須是一個 monotonically increasing sequence number。在 GPKI 中，憑證廢止清冊的 CRLNumber 值應為一個長度小於或等於 7 bytes 的正整數。
.issuingDistributionPoint	issuingDistributionPoint CRLExtension，其內容如	issuingDistributionPoint 擴充欄位是用來提供憑證應用軟

	下：	體比對此 CRL 是否與要驗證的憑證的 CRL 位址相符合，目前 Partitioned CRL 所使用之 Issuing Distribution Point 為一個 URL 網址，即是此 CRL 的發佈點位址
.extnId	填入 id-ce-issuingDistributionPoint (也就是 2.5.29.28)這個 OID	
.critical	在 Partitioned CRL 中，issuingDistributionPoint 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 OCTET STRING	對於 issuingDistributionPoint 這種 Extension 而言，必須使用 IssuingDistributionPoint 資料型態的 DER 編碼做為此 OCTET STRING 的值
.IssuingDistributionPoint	IssuingDistributionPoint 為一 SEQUENCE，內含 distributionPoint、onlyContainsUserCerts、onlyContainsCACerts、onlySomeReasons 與 indirectCRL 五欄	在 Partitioned CRL 中，issuingDistributionPoint 擴充欄位只使用 distributionPoint 欄位，而不使用其他四種欄位
.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	在 GPKI 中，Partitioned CRL 的 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	在 GPKI 中，Partitioned CRL 的 distributionPoint 欄位之 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，並在此欄中記載本 CRL 的發佈點 URL。若使用此 Partitioned CRL 驗證憑證有效

		性時，則被驗憑證 cRLDistributionPoints 欄位所記載的各個 URL 必須至少有一個與此欄所記載的 URL 完全相同。

3 參考文獻

[1] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks”.

[2] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. and Polk, W., “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, IETF RFC 5280, May 2008.

[3] Santesson, S., Nystrom, M., Polk, T., “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”, IETF RFC 3739, March 2004.

[4] Japan PKI Forum, Korea PKI Forum, PKI Forum Singapore, Chinese Taipei PKI Forum, “Achieving PKI Interoperability 2003 – Results of the JKST-IWG Interoperability project”, July 2003.

[5] Federal Public Key Infrastructure Policy Authority (FPKIPA), “Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profile”, October 2022.

[6] ETSI EN 319 412-2, “Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons”, June 2025.

[7] Dierks, T., Rescorla, E., “The Transport Layer Security (TLS) Protocol Version 1.2”, IETF RFC 5246, August 2008.

[8] Rescorla, E., “The Transport Layer Security (TLS) Protocol Version 1.3”, IETF

RFC 8446, August 2018.

[9] Korver, B., “The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX”, IETF RFC 4945, August 2007.

附錄 A：PQC 憑證及憑證廢止清冊格式剖繪

本附錄屬規範性(Normative)，旨在說明 GPKI 導入 PQC 演算法及相關技術標準時，既有 X.509 公開金鑰憑證與憑證廢止清冊格式剖繪規劃所需配合調整之欄位與設計原則。其中，傳統 RSA 演算法相關資訊應依演算法汰換時程逐步移除。

A.1. PQC 憑證格式剖繪

A.1.1. PQC 憑證格式的設計原則

除遵循 X.509 標準[1]及 RFC 5280[2]之憑證規格外，並參考以下原則：

- 符合 IETF PKIX ML-DSA 演算法識別碼 (RFC 9881)之規範[A-1]。
- 符合 IETF PKIX ML-KEM 演算法識別碼 (RFC 9935)之規範[A-2]。
- 適用於 X.509 PKI 架構之 Composite ML-DSA 之使用規範[A-3]。
- 適用於 X.509 PKI 架構之 Composite ML-KEM 之使用規範[A-4]。

A.1.2. PQC 憑證格式的欄位調整

A.1.2.1. 憑證格式

導入 PQC 演算法及其金鑰機制後的憑證仍為 X.509 公開金鑰憑證[1]，屬於一種 SIGNED 資料，其憑證格式欄位調整如下。

欄位	內容	說明

toBeSigned	To-Be-Signed 憑證（尚未簽章的憑證）	To-Be-Signed 憑證的格式遵循 X.509 標準，但內容隨憑證種類的不同而有所差異，GPKI 相關的各類 To-Be-Signed 憑證內容詳見後面的說明
algorithmIdentifier	CA 對此 To-Be-Signed 憑證進行簽章時所使用之 AlgorithmIdentifier	此欄的值必須與 toBeSigned 憑證內的 signature 欄的值相同
.algorithm	可為以下簽章演算法 OID 之一： sha256WithRSAEncryption (1.2.840.113549.1.1.11) id-ml-dsa-65 (2.16.840.1.101.3.4.3.18) id-ml-dsa-87 (2.16.840.1.101.3.4.3.19) id-MLDSA65-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.41) id-MLDSA65-RSA3072-PKCS15-SHA512 (1.3.6.1.5.5.7.6.42) id-MLDSA65-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.43) id-MLDSA65-RSA4096-PKCS15-SHA512 (1.3.6.1.5.5.7.6.44) id-MLDSA87-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.52) id-MLDSA87-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.53)	簽章演算法之 OID，GPKI 可使用以下簽章演算法 OID： 1. 傳統簽章演算法： ● sha256WithRSAEncryption 2. PQC 簽章演算法（ML-DSA）： ● id-ml-dsa-65 ● id-ml-dsa-87 3. 混合 PQC 簽章演算法（ML-DSA 搭配 RSA）： ● id-MLDSA65-RSA3072-PSS-SHA512 ● id-MLDSA65-RSA3072-PKCS15-SHA512 ● id-MLDSA65-RSA4096-PSS-SHA512 ● id-MLDSA65-RSA4096-PKCS15-SHA512 ● id-MLDSA87-RSA3072-PSS-SHA512 ● id-MLDSA87-RSA4096-PSS-SHA512
.parameters	簽章演算法 OID 為 sha256WithRSAEncryption 時，必須包含 parameters，且其值為 NULL；其餘簽章演算法 OID 不得包含 parameters	GPKI 使用傳統簽章演算法時，須包含 parameters 並填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500；使用 PQC 簽章演算法或混合 PQC 簽章演算法時，不得包含 parameters，應予省略
signature	CA 對 To-Be-Signed 憑證的簽章	此簽章是 CA 對 toBeSigned 欄位中的 To-Be-Signed 憑證所做的簽章

A.1.2.2. To-Be-Signed 憑證格式

在導入 PQC 演算法及其金鑰機制後，憑證格式中的 To-Be-Signed 憑證有部分欄位與擴充欄位須配合調整，分別說明如下：

(1)「signature」欄位

欄位	內容	說明
signature	CA 對此 To-Be-Signed 憑證進行簽章時所使用之 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： sha256WithRSAEncryption (1.2.840.113549.1.1.11) id-ml-dsa-65 (2.16.840.1.101.3.4.3.18) id-ml-dsa-87 (2.16.840.1.101.3.4.3.19) id-MLDSA65-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.41) id-MLDSA65-RSA3072-PKCS15-SHA512 (1.3.6.1.5.5.7.6.42) id-MLDSA65-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.43) id-MLDSA65-RSA4096-PKCS15-SHA512 (1.3.6.1.5.5.7.6.44) id-MLDSA87-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.52) id-MLDSA87-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.53)	簽章演算法之 OID，GPKI 可使用以下簽章演算法 OID： 1. 傳統簽章演算法： ● sha256WithRSAEncryption 2. PQC 簽章演算法（ML-DSA）： ● id-ml-dsa-65 ● id-ml-dsa-87 3. 混合 PQC 簽章演算法（ML-DSA 搭配 RSA）： ● id-MLDSA65-RSA3072-PSS-SHA512 ● id-MLDSA65-RSA3072-PKCS15-SHA512 ● id-MLDSA65-RSA4096-PSS-SHA512 ● id-MLDSA65-RSA4096-PKCS15-SHA512 ● id-MLDSA87-RSA3072-PSS-SHA512 ● id-MLDSA87-RSA4096-PSS-SHA512
.parameters	簽章演算法 OID 為 sha256WithRSAEncryption 時，必須包含 parameters，且其值為 NULL；其餘簽章演算法 OID 不得包含 parameters	GPKI 使用之簽章演算法 OID 為傳統簽章演算法時，須包含 parameters 並填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500；使用 PQC 簽章演算法或混合 PQC 簽章演算法時，不得包含

		parameters，應予省略

(2)「SubjectPublicKeyInfo」欄位

由於 PQC 演算法及其混合模式不支援「雙重用途（Dual Usage）」，因此，「SubjectPublicKeyInfo」欄位依憑證種類與金鑰用途而有所差異，主要可分為四種，第一種為僅供簽發憑證與 CRL 及驗簽章用的 CA 憑證，第二種為僅供驗簽章用的用戶憑證，第三種為提供驗簽章與金鑰加密用的 TLS 類伺服器應用軟體憑證及採用單金鑰對或雙金鑰對系統提供驗簽章與加密用的用戶憑證，第四種為採用雙金鑰對提供驗簽章與加密用的用戶憑證。其欄位說明分述如下：

- 僅供簽發憑證與 CRL 及驗簽章用的 CA 憑證

此處所指的 CA 憑證包含自簽憑證、自發憑證及交互憑證。

欄位	內容	說明
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	可為以下 Public Key 類別 OID 之一： rsaEncryption (1.2.840.113549.1.1.1) id-ml-dsa-65 (2.16.840.1.101.3.4.3.18) id-ml-dsa-87 (2.16.840.1.101.3.4.3.19) id-MLDSA65-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.41) id-MLDSA65-RSA3072-PKCS15-SHA512 (1.3.6.1.5.5.7.6.42) id-MLDSA65-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.43) id-MLDSA65-RSA4096-PKCS15-SHA512	GPKI 可使用之 Public Key 類別 OID 為： 1. 傳統演算法： ● rsaEncryption 2. PQC 演算法（ML-DSA）： ● id-ml-dsa-65 ● id-ml-dsa-87 3. 混合 PQC 演算法（ML-DSA 搭配 RSA）： ● id-MLDSA65-RSA3072-PSS-SHA512 ● id-MLDSA65-RSA3072-PKCS15-SHA512 ● id-MLDSA65-RSA4096-PSS-SHA512 ● id-MLDSA65-RSA4096-PKCS15-

	(1.3.6.1.5.5.7.6.44) id-MLDSA87-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.52) id-MLDSA87-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.53)	SHA512 ● id-MLDSA87-RSA3072-PSS-SHA512 ● id-MLDSA87-RSA4096-PSS-SHA512
.parameters	Public Key 類別 OID 為 rsaEncryption 時，必須包含 parameters，且其值為 NULL；其餘 Public Key 類別 OID 不得包含 parameters	GPKI 使用之 Public Key 類別 OID 為傳統演算法時，須包含 parameters 並填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500；使用 PQC 演算法或混合 PQC 演算法時，不得包含 parameters，應予省略
.subjectPublicKey	BIT STRING，用以包含 Subject Public Key 之位元組資料，其內容依各演算法規定，可能為 DER 編碼值或未經 ASN.1 封裝之原始位元組	GPKI 採用 RSA Public Key 時，此 BIT STRING 內容為以下資料型態的 DER 編碼值： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER } GPKI 採用 ML-DSA Public Key 時，此 BIT STRING 內容為對應 Public Key 的原始位元組資料，且不進行任何 ASN.1 結構封裝 GPKI 採用 Composite ML-DSA Public Key 時，此 BIT STRING 的內容為未經 ASN.1 封裝之 Public Key 原始位元組串接值，其串接順序依規定依序為 ML-DSA Public Key 在前、RSA Public Key 在後

➢ 僅供驗簽章用的用戶憑證

此處所指的用戶憑證則為時戳伺服器應用軟體憑證、OCSP 伺服器憑證以及一站式專屬授權憑證。

欄位	內容	說明
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	可為以下 Public Key 類別 OID 之一： rsaEncryption (1.2.840.113549.1.1.1) id-ml-dsa-44 (2.16.840.1.101.3.4.3.17) id-ml-dsa-65 (2.16.840.1.101.3.4.3.18) id-ml-dsa-87 (2.16.840.1.101.3.4.3.19) id-MLDSA44-RSA2048-PSS-SHA256 (1.3.6.1.5.5.7.6.37) id-MLDSA44-RSA2048-PKCS15-SHA256 (1.3.6.1.5.5.7.6.38) id-MLDSA65-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.41) id-MLDSA65-RSA3072-PKCS15-SHA512 (1.3.6.1.5.5.7.6.42) id-MLDSA65-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.43) id-MLDSA65-RSA4096-PKCS15-SHA512 (1.3.6.1.5.5.7.6.44) id-MLDSA87-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.52) id-MLDSA87-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.53)	GPKI 可使用之 Public Key 類別 OID 為： 1. 傳統演算法： ● rsaEncryption 2. PQC 演算法（ML-DSA）： ● id-ml-dsa-44 ● id-ml-dsa-65 ● id-ml-dsa-87 3. 混合 PQC 演算法（ML-DSA 搭配 RSA）： ● id-MLDSA44-RSA2048-PSS-SHA256 ● id-MLDSA44-RSA2048-PKCS15-SHA256 ● id-MLDSA65-RSA3072-PSS-SHA512 ● id-MLDSA65-RSA3072-PKCS15-SHA512 ● id-MLDSA65-RSA4096-PSS-SHA512 ● id-MLDSA65-RSA4096-PKCS15-SHA512 ● id-MLDSA87-RSA3072-PSS-SHA512 ● id-MLDSA87-RSA4096-PSS-SHA512
.parameters	Public Key 類別 OID 為 rsaEncryption 時，必須包含 parameters，且其值為 NULL；其餘 Public Key 類別 OID 不得包含 parameters	GPKI 使用之 Public Key 類別 OID 為傳統演算法時，須包含 parameters 並填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500；使用 PQC 演算法或混合 PQC 演算法時，不得包含 parameters，應予省略
.subjectPublicKey	BIT STRING，用以包含 Subject Public Key 之位元組資料，其內容依各演算法規定，可能為 DER 編碼值或未經 ASN.1 封裝	GPKI 採用 RSA Public Key 時，此 BIT STRING 內容為以下資料型態的 DER 編碼值：

	之原始位元組	RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER } GPKI 採用 ML-DSA Public Key 時，此 BIT STRING 內容為對應 Public Key 的原始位元組資料，且不進行任何 ASN.1 結構封裝 GPKI 採用 Composite ML-DSA Public Key 時，此 BIT STRING 的內容為未經 ASN.1 封裝之 Public Key 原始位元組串接值，其串接順序依規定依序為 ML-DSA Public Key 在前、RSA Public Key 在後

- 提供驗簽章與金鑰加密用的 TLS 類伺服器應用軟體憑證及採用單金鑰對或雙金鑰對系統提供驗簽章與加密用的用戶憑證

此處所指的用戶憑證包含專屬類伺服器應用軟體憑證與應用軟體客戶端專屬憑證。

欄位	內容	說明
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	可為以下 Public Key 類別 OID 之一： rsaEncryption (1.2.840.113549.1.1.1) id-ml-dsa-44 (2.16.840.1.101.3.4.3.17) id-ml-dsa-65 (2.16.840.1.101.3.4.3.18) id-ml-dsa-87 (2.16.840.1.101.3.4.3.19) id-MLDSA44-RSA2048-PSS-SHA256 (1.3.6.1.5.5.7.6.37) id-MLDSA44-RSA2048-PKCS15-SHA256	依憑證用途，GPKI 可使用之 Public Key 類別 OID 分別為： 1. 驗證簽章： ● 傳統演算法：rsaEncryption ● PQC 演算法（ML-DSA）：id-ml-dsa-44、id-ml-dsa-65、id-ml-dsa-87 ● 混合 PQC 演算法（ML-DSA 搭配 RSA）：id-MLDSA44-RSA2048-PSS-

	(1.3.6.1.5.5.7.6.38) id-MLDSA65-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.41) id-MLDSA65-RSA3072-PKCS15-SHA512 (1.3.6.1.5.5.7.6.42) id-MLDSA65-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.43) id-MLDSA65-RSA4096-PKCS15-SHA512 (1.3.6.1.5.5.7.6.44) id-MLDSA87-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.52) id-MLDSA87-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.53) id-alg-ml-kem-512 (2.16.840.1.101.3.4.4.1) id-alg-ml-kem-768 (2.16.840.1.101.3.4.4.2) id-alg-ml-kem-1024 (2.16.840.1.101.3.4.4.3) id-MLKEM768-RSA2048-SHA3-256 (1.3.6.1.5.5.7.6.55) id-MLKEM768-RSA3072-SHA3-256 (1.3.6.1.5.5.7.6.56) id-MLKEM768-RSA4096-SHA3-256 (1.3.6.1.5.5.7.6.57) id-MLKEM1024-RSA3072-SHA3-256 (1.3.6.1.5.5.7.6.62)	SHA256、id-MLDSA44-RSA2048-PKCS15-SHA256、id-MLDSA65-RSA3072-PSS-SHA512、id-MLDSA65-RSA3072-PKCS15-SHA512、id-MLDSA65-RSA4096-PSS-SHA512、id-MLDSA65-RSA4096-PKCS15-SHA512、id-MLDSA87-RSA3072-PSS-SHA512、id-MLDSA87-RSA4096-PSS-SHA512 2. 加密： ● 傳統演算法：rsaEncryption ● PQC 演算法（ML-KEM）：id-alg-ml-kem-512、id-alg-ml-kem-768、id-alg-ml-kem-1024 ● 混合 PQC 演算法（ML-KEM 搭配 RSA）：id-MLKEM768-RSA2048-SHA3-256、id-MLKEM768-RSA3072-SHA3-256、id-MLKEM768-RSA4096-SHA3-256、id-MLKEM1024-RSA3072-SHA3-256 3. 驗證簽章與加密： ● 傳統演算法：rsaEncryption
.parameters	Public Key 類別 OID 為 rsaEncryption 時，必須包含 parameters，且其值為 NULL；其餘 Public Key 類別 OID 不得包含 parameters	GPKI 使用之 Public Key 類別 OID 為傳統演算法時，須包含 parameters 並填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500；使用 PQC 演算法或混合 PQC 演算法時，不得包含 parameters，應予省略
.subjectPublicKey	BIT STRING，用以包含 Subject	GPKI 採用 RSA Public Key

	Public Key 之位元組資料，其內容依各演算法規定，可能為 DER 編碼值或未經 ASN.1 封裝之原始位元組	時，此 BIT STRING 內容為以下資料型態的 DER 編碼值： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER } GPKI 採用 ML-DSA 或 ML-KEM Public Key 時，此 BIT STRING 內容為對應 Public Key 的原始位元組資料，且不進行 任何 ASN.1 結構封裝 GPKI 採用 Composite ML-DSA 或 Composite ML-KEM Public Key 時，此 BIT STRING 的內容為未經 ASN.1 封裝之 Public Key 原始位元組串接值，其串接順序依規定依序為 ML-DSA/ML-KEM Public Key 在前、RSA Public Key 在後

➢ 採用雙金鑰對提供驗簽章與加密用的用戶憑證

除上述所列之用戶憑證類型外，其餘所有用戶憑證均歸屬於此項。

欄位	內容	說明
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	可為以下 Public Key 類別 OID 之一： rsaEncryption (1.2.840.113549.1.1.1) id-ml-dsa-44 (2.16.840.1.101.3.4.3.17) id-ml-dsa-65 (2.16.840.1.101.3.4.3.18) id-ml-dsa-87 (2.16.840.1.101.3.4.3.19) id-MLDSA44-RSA2048-PSS-SHA256 (1.3.6.1.5.5.7.6.37)	依憑證用途，GPKI 可使用之 Public Key 類別 OID 分別為： 1. 驗證簽章： ● 傳統演算法：rsaEncryption ● PQC 演算法（ML-DSA）：id-ml-dsa-44、id-ml-dsa-65、id-ml-dsa-87 ● 混合 PQC 演算法（ML-DSA 搭配

	id-MLDSA44-RSA2048-PKCS15-SHA256 (1.3.6.1.5.5.7.6.38) id-MLDSA65-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.41) id-MLDSA65-RSA3072-PKCS15-SHA512 (1.3.6.1.5.5.7.6.42) id-MLDSA65-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.43) id-MLDSA65-RSA4096-PKCS15-SHA512 (1.3.6.1.5.5.7.6.44) id-MLDSA87-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.52) id-MLDSA87-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.53) id-alg-ml-kem-512 (2.16.840.1.101.3.4.4.1) id-alg-ml-kem-768 (2.16.840.1.101.3.4.4.2) id-alg-ml-kem-1024 (2.16.840.1.101.3.4.4.3) id-MLKEM768-RSA2048-SHA3-256 (1.3.6.1.5.5.7.6.55) id-MLKEM768-RSA3072-SHA3-256 (1.3.6.1.5.5.7.6.56) id-MLKEM768-RSA4096-SHA3-256 (1.3.6.1.5.5.7.6.57) id-MLKEM1024-RSA3072-SHA3-256 (1.3.6.1.5.5.7.6.62)	RSA）：id-MLDSA44-RSA2048-PSS-SHA256、id-MLDSA44-RSA2048-PKCS15-SHA256、id-MLDSA65-RSA3072-PSS-SHA512、id-MLDSA65-RSA3072-PKCS15-SHA512、id-MLDSA65-RSA4096-PSS-SHA512、id-MLDSA65-RSA4096-PKCS15-SHA512、id-MLDSA87-RSA3072-PSS-SHA512、id-MLDSA87-RSA4096-PSS-SHA512 2. 加密： ● 傳統演算法：rsaEncryption ● PQC 演算法（ML-KEM）：id-alg-ml-kem-512、id-alg-ml-kem-768、id-alg-ml-kem-1024 ● 混合 PQC 演算法（ML-KEM 搭配 RSA）：id-MLKEM768-RSA2048-SHA3-256、id-MLKEM768-RSA3072-SHA3-256、id-MLKEM768-RSA4096-SHA3-256、id-MLKEM1024-RSA3072-SHA3-256
.parameters	Public Key 類別 OID 為 rsaEncryption 時，必須包含 parameters，且其值為 NULL；其餘 Public Key 類別 OID 不得包含 parameters	GPKI 使用之 Public Key 類別 OID 為傳統演算法時，須包含 parameters 並填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500；使用 PQC 演算法或混合 PQC 演算法時，不得包含 parameters，應予省略
.subjectPublicKey	BIT STRING，用以包含 Subject	GPKI 採用 RSA Public Key

	Public Key 之位元組資料，其內容依各演算法規定，可能為 DER 編碼值或未經 ASN.1 封裝之原始位元組	時，此 BIT STRING 內容為以下資料型態的 DER 編碼值： RSAPublicKey ::= SEQUENCE { modulus INTEGER, publicExponent INTEGER } GPKI 採用 ML-DSA 或 ML-KEM Public Key 時，此 BIT STRING 內容為對應 Public Key 的原始位元組資料，且不進行任何 ASN.1 結構封裝 GPKI 採用 Composite ML-DSA 或 Composite ML-KEM Public Key 時，此 BIT STRING 的內容為未經 ASN.1 封裝之 Public Key 原始位元組串接值，其串接順序依規定依序為 ML-DSA/ML-KEM Public Key 在前、RSA Public Key 在後

(3)「keyUsage」擴充欄位

此擴充欄位會依金鑰用途而有所差異，主要可分為五種，第一種為僅供簽發憑證與 CRL 及驗簽章用的 CA 憑證，第二種為僅供驗簽章用的用戶憑證，第三種為提供驗簽章與金鑰加密用的 TLS 類伺服器應用軟體憑證，第四種為採用單金鑰對或雙金鑰對系統提供驗簽章與加密用的用戶憑證，第五種為採用雙金鑰對提供驗簽章與加密用的用戶憑證。

其中，第一種與第二種憑證之「keyUsage」擴充欄位內容已符合 PQC 演算法要求，無須調整。另外三種憑證的「keyUsage」擴充欄位分述如下：

- 提供驗簽章與金鑰加密用的 TLS 類伺服器應用軟體憑證

欄位	內容	說明
.keyUsage	Key Usage 擴充欄位，記載 Subject Public Key 相對	TLS 憑證的 Key Usage 應依金鑰演算法設定用途。若金

	應之 Private Key 的用途限制	鑰對採用傳統演算法產製，則可用於簽章與金鑰加密，憑證的 Key Usage 應包含 digitalSignature 與 keyEncipherment；若金鑰對採用 PQC 演算法（ML-DSA）或混合 PQC 演算法（ML-DSA 搭配 RSA）產製，僅可用於簽章，憑證的 Key Usage 應包含 digitalSignature；若金鑰對採用 PQC 演算法（ML-KEM）或混合 PQC 演算法（ML-KEM 搭配 RSA）產製，僅可用於金鑰加密，憑證的 Key Usage 僅可設定為 keyEncipherment
.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 OCTET STRING	對於 keyUsage 這種 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	Key Usage 應依金鑰演算法設定用途。若金鑰對採用傳統演算法產製，憑證可用於驗證簽章與金鑰加密，Named BIT STRING 之 digitalSignature(0)與 keyEncipherment(2)這兩個 Bit 應設為 1；若金鑰對採用 PQC 演算法（ML-DSA）或混合 PQC 演算法（ML-DSA 搭配 RSA）產製，憑證僅可用於驗證簽章，Named BIT STRING 之 digitalSignature(0)這個 Bit 應設為 1；若金鑰對採用 PQC 演算法（ML-KEM）或混合 PQC 演算法

		（ML-KEM 搭配 RSA）產製，憑證僅可用於金鑰加密，Named BIT STRING 之 keyEncipherment(2)這個 Bit 須為唯一設為 1 的 Bit

➢ 採用單金鑰對或雙金鑰對系統提供驗簽章與加密用的用戶憑證

欄位	內容	說明
.keyUsage	Key Usage 擴充欄位，記載 Subject Public Key 相對應之 Private Key 的用途限制	可依需求採用單金鑰對（Single Key Pair）或雙金鑰對（Dual Key Pairs）系統。若採用單金鑰對，並用於簽章，驗簽章用憑證的 Key Usage 應包含 digitalSignature；若用於加解密，憑證須依金鑰演算法設定用途，採用傳統演算法產製金鑰對時，Key Usage 應包含 keyEncipherment 與 dataEncipherment，採用 PQC 演算法（ML-KEM）或混合 PQC 演算法（ML-KEM 搭配 RSA）產製時，則僅可設定為 keyEncipherment；若同時用於簽章與加解密，Key Usage 應包含 digitalSignature、keyEncipherment 及 dataEncipherment。若採用雙金鑰對，則建議分別用於簽章與加解密用途；其中，驗簽章用憑證的 Key Usage 應包含 digitalSignature，加密用憑證則須依金鑰演算法設定用途，採用傳統演算法時，Key Usage 應包含 keyEncipherment 與 dataEncipherment，若採用 PQC 演算法（ML-KEM） 或混合 PQC 演算法（ML-KEM 搭配 RSA）時，則僅可設定為 keyEncipherment
.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 OCTET STRING	對於 keyUsage 這種 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	若採用單金鑰對，當憑證用於驗證簽章，Named BIT STRING 之 digitalSignature(0)這個 Bit 應設為 1；憑證用於加密且金鑰對採用傳統演算法產製，Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment(3)這兩個 Bit 應設為 1；若金鑰對採用 PQC 演算法（ML-KEM） 或混合 PQC 演算法（ML-KEM 搭配 RSA）產製，則 Named BIT STRING 之 keyEncipherment(2)這個 Bit 須為唯一設為 1 的 Bit；當憑證同時用於驗證簽章與加密，此 Named BIT STRING 之 digitalSignature (0)、keyEncipherment(2)與 dataEncipherment (3)這三個 Bit 應設為 1。若採用雙金鑰對，當憑證用於驗證簽章，此 Named BIT STRING 之 digitalSignature(0)這個 Bit 應設為 1；若憑證用於加密，且金鑰對採用傳統演算法產製，則 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment(3)這兩個 Bit 應設為 1；若金鑰對採用 PQC 演算法（ML-KEM） 或混合 PQC 演算法（ML-KEM 搭配 RSA）產製，則 Named BIT STRING 之

		keyEncipherment(2)這個 Bit 須為唯一設為 1 的 Bit

- 採用雙金鑰對提供驗簽章與加密用的用戶憑證

欄位	內容	說明
.keyUsage	Key Usage 擴充欄位，記載 Subject Public Key 相對應之 Private Key 的用途限制	GPKI 建議每個 Subject 採用雙金鑰對（Dual Key Pairs）系統，分別用於簽章與加解密用途。其中，驗簽章用憑證的 Key Usage 應包含 digitalSignature；加密用憑證則須依金鑰演算法設定用途。若該金鑰對採用傳統演算法產製，則加密用憑證的 Key Usage 應包含 keyEncipherment 與 dataEncipherment；若採用 PQC 演算法（ML-KEM）或混合 PQC 演算法（ML-KEM 搭配 RSA）產製，則僅可設定為 keyEncipherment
.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 OCTET STRING	對於 keyUsage 這種 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	若憑證用於驗證簽章，則此 Named BIT STRING 之 digitalSignature(0)這個 Bit 應設為 1；若憑證用於加密，且金鑰對採用傳統演算法產製，則 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment(3)這兩個 Bit 應設為 1；若金鑰對採用 PQC 演算法（ML-

		KEM）或混合 PQC 演算法（ML-KEM 搭配 RSA）產製，則 Named BIT STRING 之 keyEncipherment(2)這個 Bit 須為唯一設為 1 的 Bit

(4)「extKeyUsage」擴充欄位

TLS 類伺服器應用軟體憑證之「extKeyUsage」擴充欄位會依其「keyUsage」擴充欄位的內容進行設定，其欄位說明如下：

欄位	內容	說明
.extKeyUsage	Extended Key Usage 擴充欄位，記載 Subject Public Key 相對應之 Private Key 的特殊用途	此欄位定義 TLS 憑證的 Private Key 的延伸用途
.extnId	填入代表此擴充欄位的 OID id-ce-extKeyUsage (2.5.29.37)	
.critical	為了強制應用系統識別此憑證的特殊用途，Extended Key Usage 設定是 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 OCTET STRING	對於 extKeyUsage 這種 Extension 而言，必須使用 ExtKeyUsageSyntax 的 DER 編碼做為此 OCTET STRING 的值
.ExtKeyUsageSyntax	ExtKeyUsageSyntax 的資料型態是 SEQUENCE SIZE (1..MAX) OF KeyPurposeId	TLS 憑證的 ExtKeyUsageSyntax 至少包含 1 個 KeyPurposeId
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-serverAuth (1.3.6.1.5.5.7.3.1)	此欄位為 Required，id-kp-serverAuth 為 PKIX RFC 5280 所定義的 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	此欄位為 Optional，id-kp-clientAuth 為 PKIX RFC 5280 所定義的 Key Purpose OID，當 Key Usage 僅設定 Named BIT STRING 之 keyEncipherment(2)為 1 時，

		此欄位應省略

A.2. PQC 憑證廢止清冊格式剖繪

A.2.1. PQC 憑證廢止清冊格式的設計原則

除遵循 X.509 標準[1]及 RFC 5280[2]之 CRL 規格外，並參考以下原則：

- 符合 IETF PKIX ML-DSA 演算法識別碼 (RFC 9881)之規範[A-1]。
- 適用於 X.509 PKI 架構之 Composite ML-DSA 之使用規範[A-3]。

A.2.2. PQC 憑證廢止清冊格式的欄位調整

A.2.2.1. 憑證廢止清冊格式

導入 PQC 演算法及其金鑰機制後的憑證廢止清冊仍為 X.509 CRL[1]，屬於一種 SIGNED 資料，其憑證廢止清冊格式欄位調整如下。

欄位	內容	說明
toBeSigned	To-Be-Signed CRL（尚未簽章的 CRL）	To-Be-Signed CRL 的格式遵循 X.509 標準，但內容隨 CRL 種類的不同而有所差異，此各類 To-Be-Signed CRL 內容詳見後面的說明
algorithmIdentifier	CA 對此 To-Be-Signed CRL 進行簽章時所使用之 AlgorithmIdentifier	此欄的值必須與 toBeSigned CRL 內的 signature 欄的值相同

.algorithm	可為以下簽章演算法 OID 之一： sha256WithRSAEncryption (1.2.840.113549.1.1.11) id-ml-dsa-65 (2.16.840.1.101.3.4.3.18) id-ml-dsa-87 (2.16.840.1.101.3.4.3.19) id-MLDSA65-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.41) id-MLDSA65-RSA3072-PKCS15-SHA512 (1.3.6.1.5.5.7.6.42) id-MLDSA65-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.43) id-MLDSA65-RSA4096-PKCS15-SHA512 (1.3.6.1.5.5.7.6.44) id-MLDSA87-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.52) id-MLDSA87-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.53)	簽章演算法之 OID，GPKI 可使用以下簽章演算法 OID： 1. 傳統簽章演算法： ● sha256WithRSAEncryption 2. PQC 簽章演算法（ML-DSA）： ● id-ml-dsa-65 ● id-ml-dsa-87 3. 混合 PQC 簽章演算法（ML-DSA 搭配 RSA）： ● id-MLDSA65-RSA3072-PSS-SHA512 ● id-MLDSA65-RSA3072-PKCS15-SHA512 ● id-MLDSA65-RSA4096-PSS-SHA512 ● id-MLDSA65-RSA4096-PKCS15-SHA512 ● id-MLDSA87-RSA3072-PSS-SHA512 ● id-MLDSA87-RSA4096-PSS-SHA512
.parameters	簽章演算法 OID 為 sha256WithRSAEncryption 時，必須包含 parameters，且其值為 NULL；其餘簽章演算法 OID 不得包含 parameters	GPKI 使用傳統簽章演算法時，須包含 parameters 並填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500；使用 PQC 簽章演算法或混合 PQC 簽章演算法時，不得包含 parameters，應予省略
signature	CA 對 To-Be-Signed CRL 的簽章	此簽章是 CA 對 toBeSigned 欄位中的 To-Be-Signed CRL 所做的簽章

A.2.2.2. To-Be-Signed 憑證廢止清冊格式

導入 PQC 演算法及其金鑰機制後，憑證廢止清冊格式中 To-Be-Signed CRL 的「signature」欄位需進行相應調整，說明如下：

欄位	內容	說明
signature	CA 對此 To-Be-Signed CRL 進行簽章時所使用之 AlgorithmIdentifier	此欄的值必須與外層 SIGNED CRL 之 algorithmIdentifier 欄的值相同

.algorithm	可為以下簽章演算法 OID 之 一： sha256WithRSAEncryption (1.2.840.113549.1.1.11) id-ml-dsa-65 (2.16.840.1.101.3.4.3.18) id-ml-dsa-87 (2.16.840.1.101.3.4.3.19) id-MLDSA65-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.41) id-MLDSA65-RSA3072-PKCS15-SHA512 (1.3.6.1.5.5.7.6.42) id-MLDSA65-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.43) id-MLDSA65-RSA4096-PKCS15-SHA512 (1.3.6.1.5.5.7.6.44) id-MLDSA87-RSA3072-PSS-SHA512 (1.3.6.1.5.5.7.6.52) id-MLDSA87-RSA4096-PSS-SHA512 (1.3.6.1.5.5.7.6.53)	簽章演算法之 OID，GPKI 可使用以下簽章演算法 OID： 1. 傳統簽章演算法： ● sha256WithRSAEncryption 2. PQC 簽章演算法（ML-DSA）： ● id-ml-dsa-65 ● id-ml-dsa-87 3. 混合 PQC 簽章演算法（ML-DSA 搭配 RSA）： ● id-MLDSA65-RSA3072-PSS-SHA512 ● id-MLDSA65-RSA3072-PKCS15-SHA512 ● id-MLDSA65-RSA4096-PSS-SHA512 ● id-MLDSA65-RSA4096-PKCS15-SHA512 ● id-MLDSA87-RSA3072-PSS-SHA512 ● id-MLDSA87-RSA4096-PSS-SHA512
.parameters	簽章演算法 OID 為 sha256WithRSAEncryption 時，必須包含 parameters，且其值為 NULL；其餘簽章演算法 OID 不得包含 parameters	GPKI 使用之簽章演算法 OID 為傳統簽章演算法時，須包含 parameters 並填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500；使用 PQC 簽章演算法或混合 PQC 簽章演算法時，不得包含 parameters，應予省略

A.3. PQC 技術相關參考文獻

[A-1] Massimo, J., Kampanakis, P., Turner, S., Westerbaan, B. E., "Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", IETF RFC 9881, October 2025.

[A-2] Turner, S., Kampanakis, P., Massimo, J., Westerbaan, B. E., "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based

Key-Encapsulation Mechanism (ML-KEM)", IETF RFC 9935, March 2026.

[A-3] Ounsworth, M., Gray, J., Pala, M., Klaussner, J., Fluhrer, S., "Composite Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for use in X.509 Public Key Infrastructure", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-sigs-19, April 21, 2026.

[A-4] Ounsworth, M., Gray, J., Pala, M., Klaussner, J., Fluhrer, S., "Composite ML-KEM for use in X.509 Public Key Infrastructure", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-kem-14, March 27, 2026.