政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪第 2.1 版修訂摘要

一、 因應微軟 Trusted Root Certificate Program 的最新要求：「2017 年 2 月 1 日起，所有用戶憑證皆須包含擴充欄位『增強金鑰使用方法(Extended Key Usage)』，用以說明該憑證之延伸用途」，修訂「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」第 1.2.3 節用戶公鑰憑證的欄位中有關 extKeyUsage 擴充欄位的標示說明，將該欄位修改為必要擴充欄位；同時，修訂 GCA、XCA、MOICA、MOEACA、HCA 以及伺服應用軟體之憑證格式，新增 extKeyUsage 欄位，以表示該憑證之延伸用途，修訂範圍包括下述 18 個憑證格式，修訂內容為新增下述 18 個憑證格式中有關 extKeyUsage 欄位的欄位說明(詳如附件 1)。

- 1.3.4 To-Be-Signed 政府機關憑證格式
- 1.3.5 To-Be-Signed 政府單位憑證格式
- 1.3.6 To-Be-Signed 公司憑證格式
- 1.3.7 To-Be-Signed 分公司憑證格式
- 1.3.8 To-Be-Signed 商號憑證格式
- 1.3.9 To-Be-Signed 有限合夥憑證格式
- 1.3.10 To-Be-Signed 有限合夥分支機構憑證格式
- 1.3.11 To-Be-Signed 社團法人憑證格式
- 1.3.12 To-Be-Signed 財團法人憑證格式
- 1.3.13 To-Be-Signed 學校憑證格式
- 1.3.14 To-Be-Signed 醫事機構憑證格式
- 1.3.15 To-Be-Signed 自由職業事務所憑證格式
- 1.3.16 To-Be-Signed 行政法人憑證格式
- 1.3.17 To-Be-Signed 其他組織或團體憑證格式
- 1.3.18 To-Be-Signed 自然人憑證格式
- 1.3.19 To-Be-Signed 外來人口自然人憑證格式
- 1.3.20 To-Be-Signed 醫事人員憑證格式
- 1.3.21.2 To-Be-Signed 專屬類伺服應用軟體憑證格式

二、 因應內政部憑證管理中心可提供行動自然人以及金門縣民卡之憑證簽發，修訂自然人憑證格式之 subjectDirectoryAttributes 欄位的 cardHolderRank 屬性，新增持卡人為正卡、附卡與行動載具時的相關說明。修訂內容如下：修訂「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.18 節 To-Be-Signed 自然人憑證格式中有關 subjectDirectoryAttributes 欄位屬性的相關說明(詳如附件 2)。

三、 因應公司同名但統編不同時亦可申請憑證之需求，修訂公司憑證格式與分公司憑證格式之 subject 欄位，新增 DN 項目 serialNumber，用於記錄憑證管理中心自動給定用戶之唯一序號。此外，亦修訂商號憑證格式之 subject 欄位，修改 DN 項目 serialNumber 為記錄憑證管理中心自動給定用戶之唯一序號。修訂內容如下：修訂「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.6 節 To-Be-Signed 公司憑證格式、第 1.3.7 節 To-Be-Signed 分公司憑證格式以及第 1.3.8 節 To-Be-Signed 商號憑證格式中有關 subject 欄位的相關說明(詳如附件 3)。

四、 依據 CA/Browser Forum Baseline Requirements 文件之規定，修訂 SSL 類伺服應用軟體憑證格式之 serialNumber 欄位，補充說明憑證序號需透過加密安全虛擬亂數產生器（Cryptographically Secure Pseudorandom Number Generator，CSPRNG）所產生之相關說明 。修訂內容如下：修訂「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.21.1 節 To-Be-Signed SSL 類伺服應用軟體憑證格式中有關 serialNumber 欄位的相關說明(詳如附件 4)。

五、 依據 CA/Browser Forum Baseline Requirements 文件之規定，修訂 SSL 類伺服應用軟體憑證格式之 subjectAltName 欄位，修改此欄位為必要欄位(Required)，以及修改此欄位可記錄的資訊內容為憑證簽發對象(Subject)之完全吻合網域名稱或網路位址。修訂內容如下：修訂「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.21.1 節 To-Be-Signed SSL 類伺服應用軟體憑證格式中有關 subjectAltName 欄位的相關說明(詳如附件 5)。

六、 因應憑證與憑證廢止清冊格式剖繪之規格所遵循的國際規範已提供新版標準，因此，將「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」中提及之標準「RFC 3280」修改為新版標準「RFC 5280」，同時，更新參考文獻來源說明。修訂範圍包括下述 4 個章節與 23 個憑證格式，修訂內容為修訂「政府機關公開金鑰 基礎建設憑證及憑證廢止清冊格式剖繪」中提及標準「RFC 3280」之相關說明，包括第 1.1.2 節 CA 公鑰憑證的設計原則、第 1.2.2 節用戶公鑰憑證的設計原則以及第 2.2 節憑證廢止清冊的設計原則等 3 個章節、下述 23 個憑證格式中有關 authorityInfoAccess 擴充欄位的 AccessDescription 之欄位說明、以及 SSL 類伺服應用軟體憑證格式、時戳伺服應用軟體憑證格式、OCSP 伺服器憑證格式等 3 個憑證格式之 extKeyUsage 欄位，同時，修訂第 3 章節參考文獻中有關標準「RFC 5280」之內容(詳如附件 6)。

- 1.1.2 CA 公鑰憑證的設計原則
- 1.2.2 用戶公鑰憑證的設計原則
- 1.3.2 To-Be-Signed 自發憑證格式
- 1.3.3 To-Be-Signed 交互憑證格式
- 1.3.4 To-Be-Signed 政府機關憑證格式

- 1.3.5 To-Be-Signed 政府單位憑證格式
- 1.3.6 To-Be-Signed 公司憑證格式
- 1.3.7 To-Be-Signed 分公司憑證格式
- 1.3.8 To-Be-Signed 商號憑證格式
- 1.3.9 To-Be-Signed 有限合夥憑證格式
- 1.3.10 To-Be-Signed 有限合夥分支機構憑證格式
- 1.3.11 To-Be-Signed 社團法人憑證格式
- 1.3.12 To-Be-Signed 財團法人憑證格式
- 1.3.13 To-Be-Signed 學校憑證格式
- 1.3.14 To-Be-Signed 醫事機構憑證格式
- 1.3.15 To-Be-Signed 自由職業事務所憑證格式
- 1.3.16 To-Be-Signed 行政法人憑證格式
- 1.3.17 To-Be-Signed 其他組織或團體憑證格式
- 1.3.18 To-Be-Signed 自然人憑證格式
- 1.3.19 To-Be-Signed 外來人口自然人憑證格式
- 1.3.20 To-Be-Signed 醫事人員憑證格式
- 1.3.21.1 To-Be-Signed SSL 類伺服應用軟體憑證格式
- 1.3.21.2 To-Be-Signed 專屬類伺服應用軟體憑證格式
- 1.3.21.3 To-Be-Signed 時戳伺服應用軟體憑證格式
- 1.3.22 To-Be-Signed OCSP 伺服器憑證格式
- 2.2 憑證廢止清冊的設計原則
- 3 參考文獻

七、 因文字遺漏，故修訂財團法人憑證格式之 signature 欄位，新增簽章演算法 sha256WithRSAEncryption 之 OID 資訊。修訂內容如下：修訂「政府機關公開金鑰 基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.12 節 To-Be-Signed 財團法人憑證格式中有關 signature 欄位的欄位說明(詳如附件 7)。

八、 因文字誤植，故修訂財團法人憑證格式之 subjectDirectoryAttrubutes 欄位，修改其 entityOID 屬性的說明，將原用詞為「社團法人」的文字修正為「財團法人」。修訂內容如下：修訂「政府機關公開金鑰 基礎建設憑證及憑證廢止清冊

格式剖繪」第 1.3.12 節 To-Be-Signed 財團法人憑證格式中有關 subjectDirectoryAttrubutes 欄位的相關文字(詳如附件 8)。

九、 因文字誤植，故修訂醫事機構憑證格式之 subjectDirectoryAttrubutes 欄位，修改其 cardHolderRank 屬性的說明，將原用詞為「副卡」的文字修正為「附卡」。修訂內容如下：修訂「政府機關公開金鑰 基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.14 節 To-Be-Signed 醫事機構憑證格式中有關 subjectDirectoryAttrubutes 欄位的相關文字(詳如附件 9)。

十、 因英文拼音有誤，故修訂 SSL 類伺服應用軟體憑證格式、時戳伺服應用軟體憑證格式以及 OCSP 伺服器憑證格式等 3 個憑證格式的 extKeyUsage 欄位，將該欄位中英文拼音為「Extneded」的文字修正為「Extended」。修訂內容如下：修訂「政府機關公開金鑰 基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.21.1 節 To-Be-Signed SSL 類伺服應用軟體憑證格式、第 1.3.21.3 節 To-Be-Signed 時戳伺服應用軟體憑證格式、以及第 1.3.22 節 To-Be-Signed OCSP 伺服器憑證格式等 3 個憑證格式之 extKeyUsage 欄位的欄位說明(詳如附件 10)。

十一、 因贅字造成語句不順，故修訂專屬類伺服應用軟體憑證格式與時戳伺服應用軟體憑證格式的 subjectAltName 欄位，刪除其說明資訊中的贅字「或」。修訂內容如下：修訂「政府機關公開金鑰 基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.21.2 節 To-Be-Signed 專屬類伺服應用軟體憑證格式以及第 1.3.21.3 節 To-Be-Signed 時戳伺服應用軟體憑證格式之 subjectAltName 欄位的欄位說明(詳如附件 11)。

十二、 因文字誤植，故修訂自發憑證格式之 certificatePolicies 欄位的說明，將原用詞為「Cross Certificate」的文字修正為「Self-Issued Certificate」。修訂內容如下：修訂「政府機關公開金鑰 基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.2 節 To-Be-Signed 自發憑證格式中有關 certificatePolicies 欄位的相關文字(詳如附件 12)。

十三、 依據微軟 Trusted Root Certificate Program 技術條款以及 CA/Browser Forum 之最新規範及其 Baseline Requirements 文件之規定，各類 SSL 憑證皆須依其憑證類別，於其擴充欄位 certificatePolicies 新增符合該憑證類別之 CA/Browser Forum 定義的 Certificate Policy OID，且簽發該 SSL 憑證之 CA 憑證與自發憑證亦須包含該新增之 Certificate Policy OID，故修訂自發憑證格式、交互憑證格式以及 SSL 類伺服應用軟體憑證格式的 certificatePolicies 欄位，新增有關該憑證類別使用 CA/Browser Forum 定義之 Certificate Policy OID 的相關說明。修訂內容如下：修訂「政府機關公開金鑰 基礎建設憑證及憑證廢止清冊格式剖繪」第 1.3.2 節 To-Be-Signed 自發憑證格式、第 1.3.3 節 To-Be-Signed 交互憑證格式以及第 1.3.21.1 節 To-Be-Signed SSL 類伺服應用軟體憑證格式之 certificatePolicies 欄位的欄位說明(詳如附件 13)。

附件 1

1.2.3 用戶公鑰憑證的欄位(P.12)

……

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

1.3.4 To-Be-Signed 政府機關憑證格式(P.42-43)

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	此欄位定義政府機關憑證的 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	在 GPKI 中，extKeyUsage 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	政府機關憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.5 To-Be-Signed 政府單位憑證格式(P.51-52)

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	此欄位定義政府單位憑證的 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	在 GPKI 中，extKeyUsage 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	政府單位憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.6 To-Be-Signed 公司憑證格式(P.61)

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	此欄位定義公司憑證的 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	在 GPKI 中，extKeyUsage 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	公司憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.7 To-Be-Signed 分公司憑證格式(P.70-71)

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	此欄位定義分公司憑證的 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	在 GPKI 中，extKeyUsage 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	分公司憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.8 To-Be-Signed 商號憑證格式(P.79-80)

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	此欄位定義商號憑證的 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	在 GPKI 中，extKeyUsage 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	商號憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.9 To-Be-Signed 有限合夥憑證格式(P.89)

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	此欄位定義有限合夥憑證的 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	在 GPKI 中，extKeyUsage 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	有限合夥憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.10 To-Be-Signed 有限合夥分支機構憑證格式(P.98-99)

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	此欄位定義有限合夥分支機構憑證的 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	在 GPKI 中，extKeyUsage 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	有限合夥分支機構憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.11 To-Be-Signed 社團法人憑證格式(P.108)

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	此欄位定義社團法人憑證的 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	在 GPKI 中，extKeyUsage 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	社團法人憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.12 To-Be-Signed 財團法人憑證格式(P.117-118)

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	此欄位定義財團法人憑證的 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	在 GPKI 中，extKeyUsage 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	財團法人憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.13 To-Be-Signed 學校憑證格式(P.126-127)

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	此欄位定義學校憑證的 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	在 GPKI 中，extKeyUsage 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	學校憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.14 To-Be-Signed 醫事機構憑證格式(P.136-137)

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	此欄位定義醫事機構憑證的 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	在 GPKI 中，extKeyUsage 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	醫事機構憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.15 To-Be-Signed 自由職業事務所憑證格式(P.145-146)

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	此欄位定義自由職業事務所憑證的 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	在 GPKI 中，extKeyUsage 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	自由職業事務所憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.16 To-Be-Signed 行政法人憑證格式(P.155)

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	此欄位定義行政法人憑證的 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	在 GPKI 中，extKeyUsage 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	行政法人憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.17 To-Be-Signed 其他組織或團體憑證格式(P.164-165)

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	此欄位定義其他組織或團體憑證的 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	在 GPKI 中，extKeyUsage 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	其他組織或團體憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.18 To-Be-Signed 自然人憑證格式(P.174)

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	此欄位定義自然人憑證的 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	在 GPKI 中，extKeyUsage 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	自然人憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.19 To-Be-Signed 外來人口自然人憑證格式(P.183-184)

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	此欄位定義外來人口自然人憑證的 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	在 GPKI 中，extKeyUsage 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	外來人口自然人憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.20 To-Be-Signed 醫事人員憑證格式(P.193)

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	此欄位定義醫事人員憑證的 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	在 GPKI 中，extKeyUsage 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	醫事人員憑證的 ExtKeyUsageSyntax 包含 1 至 2 個 KeyPurposeId
.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，亦為 Extended Key Usage 擴充欄位預設之 Key Purpose OID
.KeyPurposeId	KeyPurposeId 的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-kp-emailProtection (1.3.6.1.5.5.7.3.4)	id-kp-emailProtection 為 PKIX RFC 5280 所定義的 Key Purpose OID。此 Key Purpose OID 為 Optional，若 Subject Alternative Name 擴充欄位存在且記載 Subject 的 Email Address 時，則 Extended Key Usage 擴充欄位須包含此 Key Purpose OID

1.3.21.2 To-Be-Signed 專屬類伺服應用軟體憑證格式(P.213)

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	此欄位定義專屬類伺服應用軟體憑證的 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	在 GPKI 中，extKeyUsage 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	專屬類伺服應用軟體憑證的 ExtKeyUsageSyntax 包含 1 個 KeyPurposeId
.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

附件 2

1.3.18 To-Be-Signed 自然人憑證格式(P.173)

欄位	內容	說明
.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 (2.16.886.1.100.2.1)	此為代表 Subject Type 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

附件 3

1.3.6 To-Be-Signed 公司憑證格式(P.56)

欄位	內容	說明
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用戶之唯一序號* （依 PKIX 規定，所有 ASN.1 DirectoryString 文字編碼一律使用 UTF-8 編碼）

1.3.7 To-Be-Signed 分公司憑證格式(P.65)

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

1.3.8 To-Be-Signed 商號憑證格式(P.75)

欄位	內容	說明
subject	憑證簽發對象（Subject）之 X.500 Name	商號的 X.500 Name 格式如下： C=TW L=*縣市名稱* O=*商號的正式登記名稱*

		serialNumber=*憑證管理中心自動給定用戶之唯一序號(用以區分同名的商號，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）

附件 4

1.3.21.1 To-Be-Signed SSL 類伺服應用軟體憑證格式

(P.196-197)

欄位	內容	說明
serialNumber	憑證序號（Certificate Serial Number）	GPKI 的 SSL 類伺服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

附件 5

1.3.21.1 To-Be-Signed SSL 類伺服應用軟體憑證格式(P.202)

欄位	內容	說明
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI Server AP 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 只會包含 1 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 SSL/TLS Server 的 Fully Qualified Domain Name 或 IP address

附件 6

1.1.2 CA 公鑰憑證的設計原則(P.2)

除了遵循 X.509 標準[1]之外，GPKI 之 CA 公鑰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 3039)之憑證規格[3]。

……

- 盡量不要使用 X.509 v2 欄位（根據 RFC 5280 [2]之建議）。

1.2.2 用戶公鑰憑證的設計原則(P.10)

除了遵循 X.509 標準[1]之外，GPKI 用戶公鑰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 3039)之憑證規格[3]。

……

- 盡量不要使用 X.509 v2 欄位（根據 RFC 5280 [2]之建議）。

1.3.2 To-Be-Signed 自發憑證格式(P.26)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 Issuing CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交

	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	互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.3 To-Be-Signed 交互憑證格式(P.35)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 Issuing CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用

		AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.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，	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

	並在此欄中記載一個 OCSP 服務的 URL	

1.3.4 To-Be-Signed 政府機關憑證格式(P.45)

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

	(1.3.6.1.5.5.7.48.2)	
.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 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.5 To-Be-Signed 政府單位憑證格式(P.54)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省

	critical 的值必定是 FALSE	略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.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	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺

	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	服器能提供本憑證的狀態資訊

1.3.6 To-Be-Signed 公司憑證格式(P.63-64)

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

	態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	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 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.7 To-Be-Signed 分公司憑證格式(P.73)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension

.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod

.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.8 To-Be-Signed 商號憑證格式(P.82)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證

	accessMethod 與 accessLocation 二欄	及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.9 To-Be-Signed 有限合夥憑證格式(P.91-92)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP

.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
.AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod

	IDENTIFIER，此處填入 OID id-ad-ocsp (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 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.10 To-Be-Signed 有限合夥分支機構憑證格式(P.101)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp

		AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.11 To-Be-Signed 社團法人憑證格式(P.110)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其

		上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute

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

1.3.12 To-Be-Signed 財團法人憑證格式(P.120)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種

	SEQUENCE SIZE (1..MAX) OF AccessDescription	AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.13 To-Be-Signed 學校憑證格式(P.129)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此

	選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	URL 也可以是一個指向 LDAP 中 CA Entry 的 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 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.14 To-Be-Signed 醫事機構憑證格式(P.139)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET

		STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.15 To-Be-Signed 自由職業事務所憑證格式(P.148)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交

	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	互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.16 To-Be-Signed 行政法人憑證格式(P.157)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用

		AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.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，	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

	並在此欄中記載一個 OCSP 服務的 URL	

1.3.17 To-Be-Signed 其他組織或團體憑證格式(P.167)

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

	(1.3.6.1.5.5.7.48.2)	
.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 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.18 To-Be-Signed 自然人憑證格式(P.176)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省

	critical 的值必定是 FALSE	略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.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	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺

	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	服器能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(P.186)

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

	態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	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 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.20 To-Be-Signed 醫事人員憑證格式(P.195)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension

.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod

.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.21.1 To-Be-Signed SSL 類伺服應用軟體憑證格式

(P.203-P206)

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 SSL Server 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	SSL Server 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	id-kp-serverAuth 為 PKIX RFC 5280 所定義的 Key Purpose OID

	(1.3.6.1.5.5.7.3.1)	
.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

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

	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
.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 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.21.2 To-Be-Signed 專屬類伺服應用軟體憑證格式

(P.215)

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension

.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod

.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.21.3 To-Be-Signed 時戳伺服應用軟體憑證格式

(P.222, P224-225)

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	依據 RFC 3161 的規定 Timestamp Server 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	Timestamp Server 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 為 PKIX RFC 5280 及 RFC 3161 所定義的 Key Purpose OID

	id-kp-timeStamping (1.3.6.1.5.5.7.3.8)	

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址，並可視需要加上其他種類的存取資訊，例如：OCSP
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含 accessMethod 與 accessLocation 二欄	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料	此 URL 指向一個包含其他

	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	CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-ocsp (1.3.6.1.5.5.7.48.1)	id-ad-ocsp 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個 OCSP 服務的 URL	此 URL 指向一個線上憑證狀態查詢服務(OCSP)伺服器的 URL 網址，此 OCSP 伺服器能提供本憑證的狀態資訊

1.3.22 To-Be-Signed OCSP 伺服器憑證格式(P.230, P232)

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 OCSP Server 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	對於 extKeyUsage 這種

	OCTET STRING	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 Server 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

欄位	內容	說明
.authorityInfoAccess	Authority Info Access 擴充欄位	GPKI 使用此擴充欄位來記載 CA 公佈其本身憑證及其上層 CA 憑證的網址
.extnId	填入代表此擴充欄位的 OID id-pe-authorityInfoAccess (1.3.6.1.5.5.7.1.1)	authorityInfoAccess 是 PKIX 所定義的 Private Extension
.critical	在 GPKI 中，authorityInfoAccess 應為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 authorityInfoAccess 這種 Extension 而言，必須使用 AuthorityInfoAccessSyntax 的 DER 編碼做為此 OCTET STRING 的值
.AuthorityInfoAccessSyntax	AuthorityInfoAccessSyntax 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF AccessDescription	在 GPKI 憑證中，將至少含有 1 個 caIssuers 這種 AccessDescription，並可視需要加上其他種類的 AccessDescription，例如 ocsp AccessDescription
. AccessDescription	AccessDescription 為一 SEQUENCE，內含	此擴充欄位提供憑證應用軟體取得 Issuing CA 本身憑證

	accessMethod 與 accessLocation 二欄	及上層 CA 憑證的指引
.accessMethod	accessMethod 欄位的資料型態是 OBJECT IDENTIFIER，此處填入 OID id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	id-ad-caIssuers 為 PKIX RFC 5280 所定義的 accessMethod
.accessLocation	accessLocation 欄位的資料型態是 GeneralName，而 GeneralName 本身是一個 CHOICE 資料型態，GPKI 選用 CHOICE 中的 uniformResourceIdentifier，並在此欄中記載一個的 caIssuers 的 URL	此 URL 指向一個包含其他 CA 簽發給 Issuing CA 的交互憑證的檔案，該檔案的格式是 PKCS#7 憑證串列；此 URL 也可以是一個指向 LDAP 中 CA Entry 的 crossCertificatePair Attribute 的 URL 網址

2.2 憑證廢止清冊的設計原則(P.232)

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]。

……

3 參考文獻(P.257-258)

……

[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.

附件 7

1.3.12 To-Be-Signed 財團憑證格式(P.111)

欄位	內容	說明
signature	CA 簽發所用之簽章演算法之 AlgorithmIdentifier	此欄的值必須與外層 SIGNED 憑證之 algorithmIdentifier 欄的值相同
.algorithm	可為以下簽章演算法 OID 之一： sha1WithRSAEncryption (1.2.840.113549.1.1.5)、 sha256WithRSAEncryption (1.2.840.113549.1.1.11)	簽章演算法之 OID，GPKI 目前只使用以下簽章演算法： sha1WithRSAEncryption、 sha256WithRSAEncryption
.parameters	NULL	GPKI 使用的簽章演算法不需要 parameters，但其 parameters 必須填上 NULL，不可省略，NULL 之 DER 編碼為 0x0500

附件 8

1.3.12 To-Be-Signed 財團憑證格式(P.117)

欄位	內容	說明
.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

附件 9

1.3.14 To-Be-Signed 醫事機構憑證格式(P.135-136)

欄位	內容	說明
.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

附件 10

1.3.21.1 To-Be-Signed SSL 類伺服應用軟體憑證格式(P.203)

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 SSL Server 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	SSL Server 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

1.3.21.3 To-Be-Signed 時戳伺服應用軟體憑證格式(P.222)

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	依據 RFC 3161 的規定 Timestamp Server 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	Timestamp Server 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

1.3.22 To-Be-Signed OCSP 伺服器憑證格式(P.229)

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 OCSP Server 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	注意由於 TRUE 不是

	證的特殊用途，Extended Key Usage 設定是 critical extension，所以 critical 的值必定是 TRUE	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 Server 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

附件 11

1.3.21.2 To-Be-Signed 專屬類伺服應用軟體憑證格式(P.212)

欄位	內容	說明
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI Server AP 憑證中，此欄為只用於記錄 Subject 的 URL 位址	此欄位為 Optional，若 Server AP 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 Server AP 的 URL

1.3.21.3 To-Be-Signed 時戳伺服應用軟體憑證格式(P.221)

欄位	內容	說明
.subjectAltName	Subject Alternative Name 擴充欄位，在 GPKI Server AP	此欄位為 Optional，若 Server AP 沒有 URL，則本擴充欄

	憑證中，此欄為只用於記錄 Subject 的 URL 位址	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 Server AP 的 URL

附件 12

1.3.2 To-Be-Signed 自發憑證格式(P.21-22)

欄位	內容	說明
.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 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，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	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

	型態	Certificate Policy OID，或依循 CA/Browser Forum 最新規範之規定，填上符合其憑證類別之 CA/Browser Forum 定義的 Certificate Policy OID

附件 13

1.3.2 To-Be-Signed 自發憑證格式(P.22)

欄位	內容	說明
.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 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，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	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

	型態	Certificate Policy OID，或依循 CA/Browser Forum 最新規範之規定，填上符合其憑證類別之 CA/Browser Forum 定義的 Certificate Policy OID

1.3.3 To-Be-Signed 交互憑證格式(P.31)

欄位	內容	說明
.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	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 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，或依循 CA/Browser Forum 最新規範之規定，填上符合其憑證類別之 CA/Browser Forum 定義的 Certificate Policy OID

1.3.21.1 To-Be-Signed SSL 類伺服應用軟體憑證格式

(P.201-202)

欄位	內容	說明
.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 以及 CA/Browser Forum 定義之 Certificate Policy 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	在 GPKI 憑證中，SSL Server

	態是一個 SEQUENCE SIZE (1..MAX) OF PolicyInformation	憑證包含有 2 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
.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	依循 CA/Browser Forum 最新規範之規定，填上代表該憑證類別之 CA/Browser Forum 定義的 Certificate Policy OID