我國GPKI公鑰憑證簡介

中華電信股份有限公司
電信研究所
王文正 博士

GPKI階層式架構

政府憑證總管理中心
（GRCA）
政府憑證
管理中心
（GCA）
工商憑證
管理中心
（MOEACA）
內政部憑證
管理中心
（MOICA）
組織及團體
憑證管理中心
（XCA）
政府測試
憑證管理中心
（GTestCA）

GPKI公鑰憑証類別

- 政府機關（構）憑證
- 政府單位憑證
- 政府機關（構）單位伺服器應用軟體（Server AP）憑證
- 公司憑證
- 分公司憑證
- 商號憑證（原稱爲行號憑證）
- 社團法人憑證
- 財團法人憑證
- 學校憑證
- 自然人憑證
- 自由職業事務所憑證（尚未提供）
- 行政法人憑證（尚未提供）

X.509公鑰憑証格式

欄位名稱	說明
toBeSigned	憑證的To-Be-Signed部份（憑證的實際內容，見下表）
algorithmIdentifier	簽章演算法之AlgorithmIdentifier
signature	CA對憑證的簽章

End-Entity公鑰憑証格式

欄位名稱	說明
version	憑證格式的版本 v3(2)
serialNumber	憑證序號
signature	簽章演算法之AlgorithmIdentifier
issuer	憑證簽發者（ CA ）的名稱
validity	憑證的有效期限（起始和終止）
subject	憑證主體（發證對象）的名稱
subjectPublicKeyInfo	憑證主體的公鑰資訊
issuerUniqueIdentifier	此欄位依PKIX規定不使用
subjectUniqueIdentifier	此欄位依PKIX規定不使用
extensions	X.509 v3擴充欄位

End-Entity公鑰憑証擴充欄位格式

欄位名稱	是否critical	說明
authorityKeyIdentifier	FALSE	CA金鑰的Key Identifier（Public Key的Hash值）
subjectKeyIdentifier	FALSE	憑證主體（Subject）金鑰的Key Identifier（Public Key的Hash值）
keyUsage	TRUE	憑證主體（Subject）金鑰的用途（簽章或是加解密）
certificatePolicies	FALSE	此張憑證所符合的憑證政策（GPKI憑證政策保證等級第三級）
subjectAltName	FALSE	Optional欄位，用來記載憑證主體的Email（一般個體）或是URL（Server AP）
subjectDirectoryAttribute	FALSE	用來記載憑證主體之屬性資料（包括憑證類別及識別代碼等）
extKeyUsage	TRUE	記載憑證主體金鑰之特殊用途，此欄位只用於特殊的Server AP憑證
cRLDistributionPoints	FALSE	記載憑證CRL之網址
authorityInfoAccess	FALSE	記載CA憑證之網址

各類憑證主體的唯一識別代碼

- 政府機關（構）：OID
- 政府單位：OID
- 公司：統一編號
- 分公司：統一編號
- 商號：統一編號
- 社團法人：OID
- 財團法人：OID
- 學校：OID
- 自然人：身分證字號後四碼、憑證主體名稱序號（注意：不是憑證序號）

公司、分公司、商號及自然人之OID

- 公司之OID
  - 2.16.886.102.[公司統一編號]
- 分公司之OID
  - 2.16.886.102.[公司統一編號].[分公司統一編號]
- 商號之OID
  - 2.16.886.102.[縣市代碼].[商號統一編號]
- 自然人之OID
  - 2.16.886.100.[自然人憑證之主體名稱序號]

Useful Resources

- GPKI憑證及憑證廢止清冊格式剖繪1.1版 (http://grca.nat.gov.tw/download/GPKI%20Cert%20and%20CRL%20Profiles1.1.pdf)
- 政府OID查詢網站（http://oid.nat.gov.tw）
- XDS OID查詢網頁(http://oid.nat.gov.tw/xds/)
- 公鑰憑証處理安全檢查表 (http://gca.nat.gov.tw/download/AP_CHECKLIST.pdf)
- GPKI憑證政策 （ http://grca.nat.gov.tw/download/gpki_cp_v1.1.pdf ）
- 中華電信安全保密產品簡介 http://epki.com.tw/api/index.htm