

政府機關公開金鑰基礎建設 技術規範

(Technique Specification for the
Government Public Key Infrastructure)

第 1.1 版

主管機關：行政院研究發展考核委員會

執行機構：中華電信股份有限公司

中華民國九十二年二月十四日

目 錄

1 憑證政策及憑證實務作業基準	1
2 密碼模組.....	1
2.1 非對稱金鑰數位簽章演算法	1
2.1.1 PKCS#1 V2 所定義的 RSASSA-PKCS1-v1_5	1
2.1.2 PKCS#1 V2 所定義的 RSASSA-PSS.....	2
2.2 非對稱金鑰加解密演算法	2
2.3 非對稱金鑰長度	2
2.4 對稱金鑰加解密演算法	3
2.5 對稱金鑰長度	3
2.6 雜湊函數演算法	3
3 密碼語法及字碼.....	4
4 憑證及憑證廢止清冊	4
5 金鑰管理.....	5
6 憑證管理.....	5
7 應用服務.....	6
8 資訊安全管理.....	6
9 IC 卡與讀卡機	6
10 稽核與驗證.....	7
11 變更管理.....	7

政府機關公開金鑰基礎建設 (The Government Public Key Infrastructure , GPKI) 技術規範係依據最新國際標準來訂定，為建置我國電子化政府建置公開金鑰基礎建設的參考依據，相關標準說明如下：

1 憑證政策及憑證實務作業基準

符合 PKIX Certificate Policy and Certification Practices Framework(IETF RFC 2527 或更新版)。

2 密碼模組

2.1 非對稱金鑰數位簽章演算法

採用 RSA 金鑰對時，應採用以下簽章演算法之一：

2.1.1 PKCS#1 V2 所定義的 RSASSA-PKCS1-v1_5

簽章演算法 OID 依所搭配之雜湊函數不同，說明如下：

(1) 搭配 SHA-1 時，簽章演算法之 OID 為 sha1WithRSAEncryption (1.2.840.113549.1.1.5)。

(2) 搭配 SHA-256 時，簽章演算法之 OID 為 sha256WithRSAEncryption (1.2.840.113549.1.1.11)。

(3) 搭配 SHA-384 時，簽章演算法之 OID 為 sha384WithRSAEncryption (1.2.840.113549.1.1.12)。

(4) 搭配 SHA-512 時，簽章演算法之 OID 為

sha512WithRSAEncryption (1.2.840.113549.1.1.13)

2.1.2 PKCS#1 V2 所定義的 RSASSA-PSS

簽章演算法 OID 為 id-RSASSA-PSS (1.2.840.113549.1.1.10)

2.2 非對稱金鑰加解密演算法

採用 RSA 金鑰對時，應採用以下加解密演算法之一：

(1)PKCS#1 V2 所定義的 RSAES-PKCS1-v1_5，加解密演算法
OID 為 rsaEncryption (1.2.840.113549.1.1.1)

(2)PKCS#1 V2 所定義的 RSAES-OAEP，加解密演算法 OID
為 id-RSAES-OAEP (1.2.840.113549.1.1.7)

2.3 非對稱金鑰長度

(1)憑證總管理中心 (Root CA): RSA 4096 Bits (含) 以上，
或其他強度相等的金鑰。

(2)下層憑證管理中心 (Subordinate CA): RSA 2048 bits (含)
以上，或其他強度相等的金鑰。

(3)憑證註冊中心 (RA): RSA 1024 bits (含) 以上，或其他
強度相等的金鑰。

(4)終端個體 (EE): RSA 1024 bits (含) 以上，或其他強度相
等的金鑰。

2.4 對稱金鑰加解密演算法

應採用以下加解密演算法之一：

(1)ANSI X9.52-1998 所定義的 3-Key Triple-DES，加解密演算法 OID 為 des-EDE3-CBC (1.2.840.113549.3.7)。

(2)IETF RFC 2268 所定義的 RC-2，加解密演算法 OID 為 rc2-CBC (1.2.840.113549.3.2)。

(3)NIST FIPS PUBS 197 所定義的 AES(即 Rijndael 演算法)，AES 又因所採用的金鑰長度不同，分別以 AES-128、AES-192 及 AES-256 來表示，並必須依運算模式不同而採用由 NIST CSOR 所登記的不同 OID。

2.5 對稱金鑰長度

有效金鑰長度 128 bits (含) 以上。

2.6 雜湊函數演算法

應採用以下雜湊函數之一：

(1)NIST FIPS PUBS 180-1 所定義的 SHA-1，雜湊函數 OID 為 id-SHA1 (1.3.14.3.2.26)。

(2)NIST FIPS PUBS 180-2 所定義的 SHA-256，雜湊函數 OID 為 id-SHA256 (2.16.840.1.101.3.4.2.1)。

(3)NIST FIPS PUBS 180-2 所定義的 SHA-384，雜湊函數 OID 為 id-SHA384 (2.16.840.1.101.3.4.2.2)。

(4)NIST FIPS PUBS 180-2 所定義的 SHA-512 , 雜湊函數 OID 為 id-SHA384 (2.16.840.1.101.3.4.2.3)

3 密碼語法及字碼

(1)ASN.1 語法：符合 ITU-T X.680 (1997) X.681 (1997) X.682 (1997)(含) 以上。

(2)ASN.1 編碼：符合 ITU-T X.690(1997) X.691(1997)(含) 以上。

(3)中文字碼集(Character set)：CNS 11643 或 ISO 10646。

(4)中文字碼編碼：UTF-8 (IETF RFC 2279 或更新版)

(5)數位信封標準：語法符合 Cryptographic Message Syntax Standard (PKCS #7 V1.5 或更新版)或 Cryptographic Message Syntax (CMS) (IETF RFC 2630 或更新版)

4 憑證及憑證廢止清冊

(1)憑證格式：採用 X.509 V3 Certificate , 符合 ITU-T X.509:2000 | ISO/IEC 9594-8:2001(含)以上及 PKIX Certificate and CRL Profile (IETF RFC 3280 或更新版)和 PKIX Qualified Certificates Profile(IETF RFC 3039 或更新版)。

(2)憑證廢止清冊：採用 X.509 V2 CRL ,符合 ITU-T X.509:2000 | ISO/IEC 9594-8:2001(含)以上及 PKIX Certificate and CRL Profile (IETF RFC 3280 或更新版)。

(3)憑證及憑證廢止清冊格式剖繪：請參考「政府公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」。

5 金鑰管理

(1)金鑰管理：符合 ISO 11770。

(2)金鑰產生之亂數測試：符合 US FIPS 140-1 (含) 以上或 NIST SP800.22。

(3)金鑰產生之質數產生及測試：符合 ANSI X9.80 或 ANSI X9.31。

(4)私密金鑰語法及保護方式：符合 PKCS #12 V1.0 或使用 RSA IC 卡或使用硬體密碼模組。

6 憑證管理

(1)憑證管理訊息格式與協定：符合 Certificate Management Protocol (CMP) (IETF RFC 2510 或更新版) 或 Certificate Management Messages over CMS(CMC) (IETF RFC 2797 或更新版)。

(2)憑證簽發要求格式：符合 Certificate Request Message Format (CRMF)(IETF RFC 2511 或更新版)或 Certification Request Syntax Standard (PKCS #10 V1.7 或更新版)。

(3)線上憑證狀態詢問服務：符合 On-line Certificate Status Protocol (OCSP) (IETF RFC 2560 或更新版)。

(4)憑證申辦審核格式：符合 IETF PKIX 標準語法及通訊協定。

7 應用服務

(1)授權管理基礎建設 (Privilege Management Infrastructure, PMI): 符合 ITU-T X.509:2000 | ISO/IEC 9594-8:2001 (含) 以上。

(2)目錄服務：符合 IETF RFC 2559 PKI Operational Protocols - LDAPv2 及 IETF RFC 2587 PKI LDAPv2 Schema。

(3)時戳服務：符合 IETF PKIX RFC 3161 Time Stamp Protocol (含) 以上。

(4)安全插座層通訊協定：符合 Netscape Secure Sockets Layer V3.0 或 IETF RFC 2246 Transport Layer Security(TLS) Protocol V1.0。

8 資訊安全管理

(1) 行政院及所屬各機關資訊安全管理要點。

(2) 行政院及所屬各機關資訊安全管理規範。

(3) ISO 17799 Code of Practice For Information Security Management。

9 IC 卡與讀卡機

(1)IC 卡：ISO 7816，並具內部金鑰產生及內建的 RSA 運算功能，及提供 MS CAPI 及 PKCS #11 的應用界面。

(2)IC 卡讀卡機：PC/SC 1.0 以上。

10 稽核與驗證

(1)PKI 稽核評鑑：WebTrust AICPA/CICA WebTrust Program for Certification Authorities，或 ISO 15408 Certificate Issuing and Management Components Protection Profile (CIMC PP)。

(2)密碼模組安全等級驗證：FIPS 140-1(含)以上，或其他經行政機關電子憑證推行小組核可者。

11 變更管理

本技術規範可視需要進行變更，並在行政機關電子憑證推行小組核可後公佈施行。

