政府機關公開金鑰基礎建設技術規範第 1.2 版修正說明

一、修正密碼語法及字碼

修正規定	現行規定	修正說明
3. (1) ASN.1 語法：符合 CNS 13889-1（或 ITU-T X.680:2002 或其最新版）、CNS 13889-2（或 ITU-T X.681:2002 或其最新版）、CNS 13889-3（或 ITU-T X.682:2002 或其最新版）、CNS 13889-4（或 ITU-T X.683:2002 或其最新版。 (2) ASN.1 編碼：符合 CNS 13890-1（ITU-T X.690:2002 或其最新版）。 (3) 中文字碼集（Character set）：CNS 11643 或 CNS 14649 (或 ISO 10646 或其最新版)。	3. (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。	1.修訂 X.680~X.690 系列標準的版本為 2002 年版。 2.將 ITU-T X.680、X.681、X.682、X.683、X.690、ISO 10646 所對應的 CNS 國家標準列於國際標準之前。

二、修正密碼模組

修正規定	現行規定	修正說明
2.1.1(4) NIST FIPS PUB 180-2 所定義的 SHA-512，雜湊函數 OID 為 id-SHA512（2.16.840.1.101.3.4.2.3）。	2.1.1 (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）。	1.將 NIST FIPS PUBS 或 PUB 統一成 NIST FIPS PUB 這樣的寫法。 2.將 id-SHA384 之筆誤修正為 id-SHA512。
2.4.(1)ANSI X9.52-1998 所定義的 3-Key Triple-DES（有效金鑰長度 168 bits），加解密演算法 OID 為 des-EDE3-CBC（1.2.840.113549.3.7）。	2.1.4(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）。	明確註明 3-key triple-DES 其有效金鑰長度為 168 bits。

三、修正憑證及憑證廢止清冊

修正規定	現行規定	修正說明
4. (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 3739 或更新版)。	4. (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)。	PKIX Qualified Certificate Profile 更版為 RFC 3739。

四、修正金鑰管理

修正規定	現行規定	修正說明
5. (1) 金鑰管理：符合 CNS 14381 (或 ISO 11770 或其最新版)。	5. (1) 金鑰管理：符合 ISO 11770。	將 ISO 11770 所對應的 CNS14381 國家標準列於國際標準之前。

五、修正應用服務

修正規定	現行規定	修正說明
7. (2) 目錄服務：符合 IETF RFC 3377 Lightweight Directory Access Protocol (v3): Technical Specification 及 IETF RFC 2587 PKI LDAPv2 Schema。	7. (2) 目錄服務：符合 IETF RFC 2559 PKI Operational Protocols - LDAPv2 及 IETF RFC 2587 PKI LDAPv2 Schema。	RFC 2559 已經被 PKIX 作廢，故修正為 RFC 3377 LDAP v3。

六、修正資訊安全管理標準

修正規定	現行規定	修正說明
8. (3) CNS 17799 資訊技術－資訊安全管理之作業要點（或 ISO/IEC 17799:2005 Information Technology - Security Techniques - Code of Practice for Information Security Management 或其最新版）。	8. (3) ISO 17799 Code of Practice For Information Security Management。	1.配合 ISO 17799 於 2005 年 6 月更版。 2.將 ISO 17799 所對應的 CNS 國家標準列於國際標準之前。

六、修正稽核與驗證有關密碼模組安全等級驗證

修正規定	現行規定	修正說明
10. (2) NIST FIPS PUB 140，或其他經行政機關電子憑證推行小組核可者。	10. (2) 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。	配合 NIST FIPS PUB 140 系列更版。

七、修正 IC 卡與讀卡機

修正規定	現行規定	修正說明
9. (1) IC 卡：CNS 12971（或 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 的應用介面。	9. (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。	將 ISO 7816 相對應的 CNS12971 國家標準列於 ISO 國際標準之前。

八、修正變更管理

修正規定	現行規定	修正說明
11. 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。	11.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。	將「行政機關電子憑證推行小組」加上引號，以資區別。

九、其餘電子推行小組委員意見之回覆

委員意見	修正/現行規定	回覆
請統一 SHA-1、SHA-256 等演算法之表示法，並註明其出處。	修正規定: 2.1.1PKCS#1 V2 所定義的 RSASSA-PKCS1-v1_5	1 目前 GPKI 技術規範中所引用之 SHA-1、SHA-256 等雜湊函數演算法係由美國 NIST

	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)。	所定義，經查美國 NIST FIPS PUB 180-2 標準中對於這些雜湊函數演算法也是採用 SHA-1、SHA-256 這樣的寫法，故 GPKI 技術規範以沿用此標準寫法為宜。 2.目前 GPKI 技術規範已經明確標明這些雜湊函數演算法係出自於美國 NIST FIPS PUB 180-2 標準。
2.4 節部分： 1、請註明 3-Key 之 Key Length 為 112 bits 或 168 bits，並考量是否只接受 CBC Mode。 2、請考量是否採用比 RC-2 還新之 RC-4。	**修正規定:** 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（有效金鑰長度 168 bits），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 PUB 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 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。	1. 已經依要求明確註明 3-key triple-DES 其有效金鑰長度為 168 bits。 2.目前 GPKI 技術規範規定之數位信封應採用 IETF S/MIME 工作小組所制訂的 CMS 標準，而根據 S/MIME 的規範(請參考 RFC 3370)，對稱式加密演算法中對於 triple-DES 只支援 CBC Mode，故 GPKI 技術規範以沿用 S/MIME 規範為宜。 2.同樣根據 S/MIME 的規範，對稱式加密演算法中只支援 RC-2，並沒有支援 RC-4；而 S/MIME 規定所有數位信封加解密軟體至少都需支援 RC-2，此為 S/MIME 的最低需求，故 GPKI 技術規範以沿用 S/MIME 規範為宜。

格式化: 項目符號及編號

	現行規定: 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。	
(五)標準或規範部分，請將”（含）以上”修正為”或其最新版”。	(略)	已將”（含）以上”修正為”或其最新版”。