金融 XML 憑證共通性技術規範修正對照表

<table>
<tr><th>修 正 條 文 v1.2</th><th>現 行 條 文 v1.1</th><th>說 明</th></tr>
<tr><td>4.1.1 憑證欄位說明
<table><tr><th>欄 位</th><th>說 明</th></tr><tr><td>1. X.509v1 Field</td><td>憑證基本欄位</td></tr><tr><td>1.3. Signature Algorithm</td><td>簽章演算法，使用 SHA-1 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.5)或 SHA256 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.11) ，自 2017/1/1 起須使用 SHA256 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.11)</td></tr><tr><td>2. X.509v3 Extensions</td><td>X509 V3 Extensions</td></tr><tr><td>2.1.1. Key Identifier</td><td>憑證簽發者公開金鑰的 160-bits SHA-1 值或 256 bits SHA256 值，自 2017/1/1 起須使用 256 bits SHA256</td></tr><tr><td>2.2. Subject Key Identifier</td><td>憑證擁有者公開金鑰的 160-bits SHA-1 值或 256 bits SHA256 值，自 2017/1/1 起須使用 256 bits SHA256</td></tr></table></td><td>4.1.1 憑證欄位說明
<table><tr><th>欄 位</th><th>說 明</th></tr><tr><td>1. X.509v1 Field</td><td>憑證基本欄位</td></tr><tr><td>1.3. Signature Algorithm</td><td>簽章演算法，使用 SHA-1 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.5)</td></tr><tr><td>2. X.509v3 Extensions</td><td>X509 V3 Extensions</td></tr><tr><td>2.1.1. Key Identifier</td><td>憑證簽發者公開金鑰的 160-bits SHA-1 值</td></tr><tr><td>2.2. Subject Key Identifier</td><td>憑證擁有者公開金鑰的 160-bits SHA-1 值</td></tr></table></td><td>考量 SHA-1 演算法已不足夠，加強複雜度，提為 256</td></tr>
<tr><td>4.1.3 RCA 憑證
<table><tr><th>欄 位</th><th></th><th>內 容</th><th>說 明</th></tr><tr><td>1.3. Signature Algorithm</td><td>必</td><td>1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為</td><td>SHA-1 with RSA Encryption 或 SHA256 with RSA</td></tr></table></td><td>4.1.3 RCA 憑證
<table><tr><th>欄 位</th><th></th><th>內 容</th><th>說 明</th></tr><tr><td>1.3. Signature Algorithm</td><td>必</td><td>1.2.840.113549.1.1.5</td><td>SHA-1 with RSA Encryption</td></tr></table></td><td>考量演算法已不足夠，SHA 長度提為 256，RSA</td></tr>
</table>

		1.2.840.113549.1.1.11	Encryption，自2017/1/1起須使用SHA256 with RSA Encryption					長度提為4096
1.7. Subject Public Key Info	必		RCA公開金鑰，長度2048bits（含）以上，自2017/1/1起長度須為4096bits（含）以上	1.7. Subject Public Key Info	必		RCA公開金鑰，長度2048bits（含）以上	

4.1.4 PCA 憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自2017/1/1起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自2017/1/1起須使用SHA256 with RSA Encryption
1.7. Subject Public Key Info	必		PCA公開金鑰，長度2048bits（含）以上，自2017/1/1起長度須為4096bits（含）以上

4.1.4 PCA 憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5	SHA-1 with RSA Encryption
1.7. Subject Public Key Info	必		PCA公開金鑰，長度2048bits（含）以上

考量演算法已不足夠，SHA長度提為256，RSA長度提為4096

4.1.5 UCA 憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.7. Subject Public Key Info	必		UCA 公開金鑰，長度 2048bits (含)以上，自 2017/1/1 起長度須為 4096bits (含)以上

4.1.5 UCA 憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5	SHA-1 with RSA Encryption
1.7. Subject Public Key Info	必		UCA 公開金鑰，長度 2048bits (含)以上

考量演算法已不足夠，SHA 長度提為 256，RSA 長度提為 4096

4.1.6 RA 憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption

4.1.6 RA 憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5	SHA-1 with RSA Encryption

考量演算法已不足夠，SHA 長度提為 256，RSA 長度提為 2048

1.7. Subject Public Key Info	必		RA 公開金鑰，長度 1024bits (含)以上，自 2017/1/1 起長度須為 2048bits (含)以上

1.7. Subject Public Key Info	必		RA 公開金鑰，長度 1024bits

4.1.7.1 使用者簽章憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.7. Subject Public Key Info	必		使用者公開金鑰，長度 1024bits (含)以上，自 2017/1/1 起長度須為 2048bits (含)以上

4.1.7.1 使用者簽章憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5	SHA-1 with RSA Encryption
1.7. Subject Public Key Info	必		使用者公開金鑰，長度 1024bits

考量演算法已不足夠，SHA 長度提為 256，RSA 長度提為 2048

4.1.7.2 使用者加密憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自	SHA-1 with RSA Encryption 或

4.1.7.2 使用者加密憑證

欄　位		內　容	說　明
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5	SHA-1 with RSA Encryption

考量演算法已不足夠，SHA 長度提為

		2017/1/1 起須為 1.2.840.113549.1.1.11	SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption					256，RSA 長度提為 2048
1.7. Subject Public Key Info	必		使用者公開金鑰，長度 1024bits（含）以上，自 2017/1/1 起長度須為 2048bits（含）以上	1.7. Subject Public Key Info	必		使用者公開金鑰，長度 1024bits（含）以上	

4.3 憑證註銷清單說明

欄　位		內　容	說　明
1.2. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption

4.3 憑證註銷清單說明

欄　位		內　容	說　明
1.2. Signature Algorithm	必	1.2.840.113549.1.1.5	SHA-1 with RSA Encryption

考量 SHA-1 演算法已不足夠，加強複雜度，提為 256

4.4 使用者憑證申請訊息

欄　位		說　明
2. Signature Algorithm	必	簽章演算法，使用 SHA-1 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.5) 或 SHA256 with RSA

4.4 使用者憑證申請訊息

欄　位		說　明
2. Signature Algorithm	必	簽章演算法，使用 SHA-1 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.5)

考量 SHA-1 演算法已不足夠，加強複雜

	Encryption (PKCS#1-5) (1.2.840.113549.1.1.11)，自 2017/1/1 起須使用 SHA256 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.11)		度，提為256
6.2.5RCA 憑證有效性驗證 (7) RCA 憑證之拇指紋（FingerPrint），必須與 RCA 所公告的完全相符且是使用者所信任的。		6.2.5RCA 憑證有效性驗證 (7) RCA 憑證之 ~~SHA-1~~拇指紋（FingerPrint），必須與 RCA 所公告的完全相符且是使用者所信任的。	考量 SHA-1 演算法已不足夠，應於 6.2.6 節公告採用 SHA256
6.2.6RCA 憑證公告 (3) RCA 憑證拇指紋 FingerPrint(SHA1 或 SHA256 Hashing value，自 2017/1/1 起須使用 SHA256)。		6.2.6 RCA 憑證公告 (3) RCA 憑證拇指紋 FingerPrint(SHA-1 Hashing value)。	考量 SHA-1 演算法已不足夠，加強複雜度，提為256
8.2 金融機構所使用之憑證申請事項 金融機構在擔任註冊中心所需要的 RA 憑證，以及本身在處理客戶交易時所需使用之使用者憑證，應直接透過認證中心所提供之註冊中心機制向認證中心申請。受理客戶憑證註冊或資料異動時，其臨櫃作業應增加額外具「兩項(含)以上技術」之安全設計或經由另一位人員審核。		8.2 金融機構所使用之憑證申請事項 金融機構在擔任註冊中心所需要的 RA 憑證，以及本身在處理客戶交易時所需使用之使用者憑證，應直接透過認證中心所提供之註冊中心機制向認證中心申請。 金融機構向認證中心申請憑證的作業與 Server Base 使用者申請憑證的作業相同，請參考**錯誤! 找不到參照來源。**章節，其餘作業如憑	參考資安事件及憑證組織要求，憑證註冊作業應由具有 2FA 設備者執

金融機構向認證中心申請憑證的作業與 Server Base 使用者申請憑證的作業相同，請參考**錯誤! 找不到參照來源。**章節，其餘作業如憑證更新、註銷等亦相同。 上述「兩項(含)以上技術」之安全設計，係指應具有下列兩項(含)以上技術： ● 所知悉的資訊(如設備密碼、登入密碼等)。 ● 所持有的設備(如密碼產生器、密碼卡、晶片卡、電腦、手機、憑證載具等)。 ● 所擁有的生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈等)。	證更新、註銷等亦相同。	行或兩人以上授權放行
8.3 憑證（金鑰）儲存媒體保護機制 應用於高風險交易時，憑證金鑰應儲存於符合 Common Criteria EAL 4+(至少包含增項 AVA_VLA.4 或 AVA_VAN.5)或 ITSEC level E4 或 FIPS 140-1 Level 2 或其他相同安全強度之認證等晶片硬體內，以防止該私鑰被匯出或複製，且該晶片硬體不得常駐於產生交易指示之設備，確保交易安全。 為確保整體作業安全等級之一致性，設備代理行存取登記憑證時，需核對該憑證(金鑰)儲存媒體須使用經本會審核通過之中介軟體所支援的憑證載具。	8.3 憑證（金鑰）儲存媒體保護機制 為確保整體作業安全等級之一致性，設備代理行存取登記憑證時，需核對該憑證(金鑰)儲存媒體須使用經本會審核通過之中介軟體所支援的憑證載具。	參考各銀行使用狀況及國際認證，要求採用符合國際標準之硬體設備，以確保金鑰儲存安全
9.1 使用者端安控系統 接受他行憑證並應用於跨網使用時必須使用經本會審核通過之中介軟體所支援的憑證載具。	9.1 使用者端安控系統 <無>	跨網時須支援公會中介載具

9.2 金融機構端安控系統 為考量金融機構高安全度之需求，金融機構應使用 Hardware Secure Module(HSM)為金鑰儲存媒體，該設備應符合 Common Criteria EAL 4+(至少包含增項 AVA_VLA.4 或 AVA_VAN.5)或 ITSEC level E4 或 FIPS 140-1 Level 2 或其他相同安全強度之認證。	9.2 金融機構端安控系統 為考量金融機構高安全度之需求，建議金融機構使用 Hardware Secure Module(HSM)為金鑰儲存媒體，並建議 HSM 能通過 Federal Information Processing Standards Publications 140-1(FIPS PUB 140-1 或 FIPS 140-1) [FIPS 140-1]認證。 ~~建議 HSM 通過 FIPS 140-1 認證之理由：~~ ● ~~國際標準組織以 FIPS 140-1 為基礎訂定密碼方法評估準則(ISO 1996)。~~ ● ~~1997 年 7 月 1 日後，美國境內政府機關使用之相關密碼模組安全產品必須取得 FIPS 140-1 規格驗證。~~ ● ~~NIST 建議商業用途之相關密碼模組安全產品能遵循 FIPS 140-1 需求規格開發並通過 NIST 之驗證~~	參考各銀行使用狀況及國際認證，要求採用符合國際標準之硬體設備，以確保金鑰儲存安全