

BCSS及PSP系統安控 機制提升作業說明會

2026.8.7



臺灣集保結算所

簡報大綱

壹、緣由

貳、現行連線方式

參、安控作業項目

肆、年度工作基碼(Cross Domain Key)交換說明

伍、每日工作基碼(Working Key)交換說明

陸、交易電文驗證機制

柒、相關配合及注意事項

捌、整體時程

壹、緣由

- 一. 本公司BCSS系統及PSP系統，現行仍使用使用 MD5 雜湊函數演算法及Triple DES 演算法作為參加人交易驗證安控機制。依照美國國家標準暨技術研究院 (NIST) 公告，現行系統所使用之加密函數已不符合業界標準。
- 二. 配合金管會114年12月9日金管資字第1140197736號來函之會議紀錄，對稱式密碼雖較不受量子運算影響，但仍有安全風險。在後量子時代建議改用 AES-256加密演算法，另雜湊函數演算法也建議使用SHA-256演算法，以確保安全性與遷移規劃完整

貳、現行連線方式

一、瀏覽器工作站：

本公司現行瀏覽器工作站係使用PKI憑證進行安控驗證，如須進行調整，將依照各發證單位公告，配合辦理，本次提升無影響。

二、BDU傳檔工作站：

本公司現行使用之BDU傳檔工作站，亦使用PKI憑證進行安控驗證，故於本次提升無影響。

三、主機對主機(MQ)：

現行主機對主機連線方式，係使用MAC值進行交易驗證，既為本次提升項目之一。

參、安控作業項目

一、每年工作基碼(Cross Domain Key)交換：

每年12月份，由本公司進行年度基碼碼單印製及郵寄事宜，參加單位於接獲函文通知後，於指定日期進行人工基碼輸入及工作基碼交換確認作業。

二、每日工作基碼(Working Key)交換：

營業日早上06:00啟動，本公司OPC系統開始接受工作基碼交換請求。

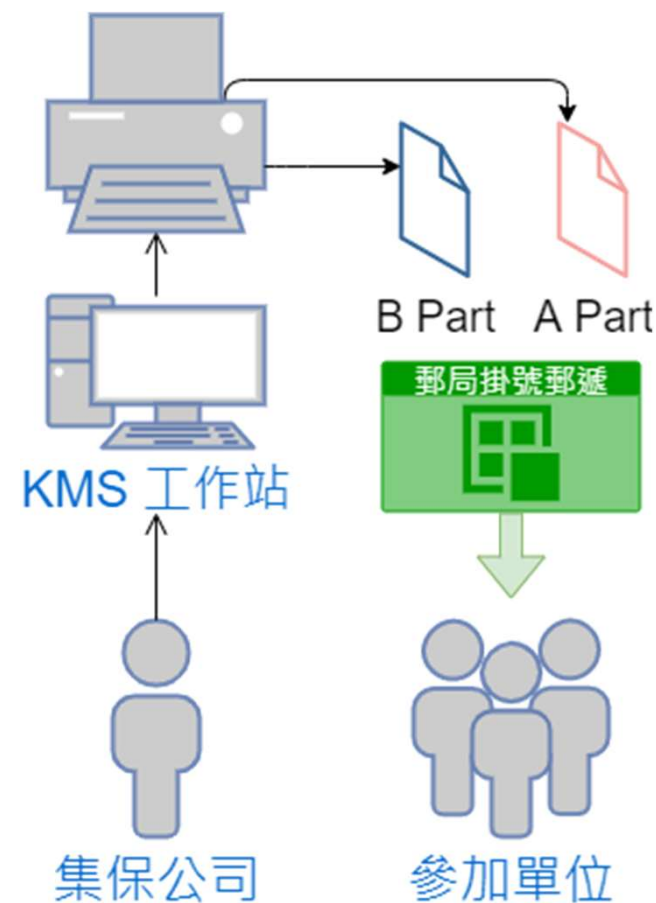
三、系統交易驗證：

交易電文使用每日交換之工作基碼進行交易電文MAC安控驗證，以確保電文傳輸之安全性。

肆、年度工作基碼(Cross Domain Key)交換

一、作業說明：

1. 每年由集保公司同仁操作KMS工作站(金鑰管理工作站)進行年度工作基碼交換作業。
2. KMS工作站列印複寫彌封之A、B碼單後，經由郵局掛號郵遞至各參加單位對應聯絡人。
3. 再由各參加單位操作人員，分持A、B碼單，進行年度工作基碼植入作業。



肆、年度工作基碼(Cross Domain Key)交換(續)

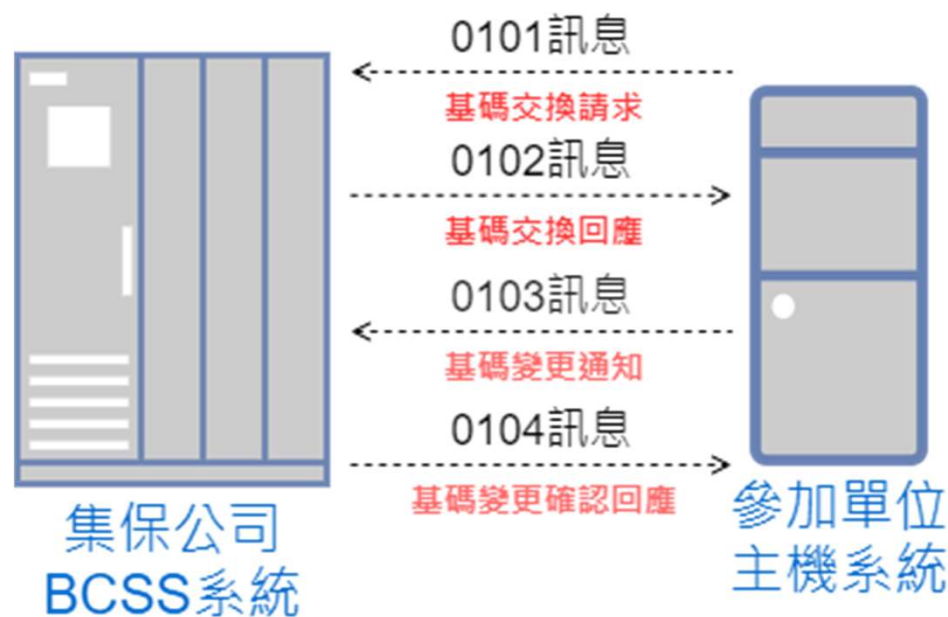
二、調整項目及計算公式：

1. 金鑰驗證碼演算法修改為AES-256，及金鑰長度增加為32位元組(bytes)。
2. 金鑰驗證碼(Check value)計算公式：
 - IV（初始向量）： $IV = 0x00 * 12$
 - Plaintext（明文資料）：待檢核之金鑰明文資料（CDK或A、B碼）
 - 金鑰驗證碼：CHK Value = Truncate-Right(AES-GCM-Encrypt (Key, IV, Key), 2)

伍、每日工作基碼(Working Key)交換

一、作業說明：

1. 每日工作機碼交換，由BCSS系統之OPC模組於接收0101訊息後，進行該參加單位之工作基碼產生，並以0102訊息回覆該參加單位。
2. 參加單位於收到0102訊息後，進行工作基碼解密，發送0103訊息以通知BCSS系統基碼已變更。
3. BCSS系統接收0103訊息後，回覆0104訊息確認基碼變更完成。



伍、每日工作基碼(Working Key)交換(續)

二、調整項目及計算公式：

1. 演算法修改為SHA256、AES-256，及金鑰長度增加為32位元組(bytes)。
2. 基碼交換計算公式 (GCM模式)：
 - **IV（初始向量）**： $IV = \text{Truncate-Left}(\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 12)$
 - **加密公式**： $\text{Ciphertext} = \text{AES-GCM-Encrypt}(\text{Key } IV, \text{Plaintext}), \text{NoPadding}$ 。
 - **解密公式**： $\text{Plaintext} = \text{AES-GCM-Decrypt}(\text{Key}, IV, \text{Ciphertext}), \text{NoPadding}$ 。
3. 基碼同步計算公式 (CTR模式)：
 - **IV（初始向量）**： $IV = \text{Truncate-Left}(\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 16)$
 - **加密公式**： $\text{Ciphertext} = \text{AES-CTR-Encrypt}(\text{Key}, IV, \text{Plaintext}), \text{NoPadding}$ 。

陸、交易電文驗證機制

修改項目及計算公式：

1. 修改使用SHA256雜湊函數演算法對XML電文進行雜湊值計算。
2. 修改使用AES256對稱式加密演算法，對前述之訊息雜湊值進行押碼，得出MAC值。
3. 計算公式：

IV (初始向量)： $IV = \text{Truncate-Left}(\text{SHA256}(\text{ORIGIN} || \text{yyyyMMdd}), 12)$

Plaintext (明文資料)：XML 訊息經 SHA-256 雜湊後所得之雜湊值，長度為 32 Bytes。

MAC值： $MAC = \text{Truncate-Left}(\text{AES-GCM-Encrypt}(\text{MACKey}, IV, \text{plaintext}), 8), \text{NoPadding}$

柒、相關配合及注意事項

一、系統修改：

1. 修改金鑰管理系統：增加AES金鑰手動輸入功能，供年度金鑰交換作業使用。
2. 修改每日工作基碼交換系統：修改雜湊函數演算法(SHA-256)及對稱式加密演算法(AES-256)。
3. 交易系統修改：修改交易系統程式，以符合本公司演算法驗證規範。

二、相關時程：

1. 預定於115年11月1日開放業務演練環境，各參加單位可依自訂時程與本公司進行測試。
2. 預定於115年12月21日營運環境正式啟用新舊演算法雙軌並行機制。
3. 116年度工作基碼交換作業，既可申請使用新版演算法工作基碼。
4. 預定於116年12月31日止，結束舊版(Triple-DES)系統服務。

三、注意事項：

1. 系統上線前，需於一個月前向本公司申請新版金鑰交換。
2. 上線前一日，於營業時段後，改用新版金鑰，並與本公司進行驗證測試。

捌、整體時程

工作項目	預計時程	備註
一、行政作業		
1、召開說明會及發函公告	115/8月	說明提升項目並公告介面規格文件
2、開放業務演練環境	115/11月	本公司業務演練系統開放供參加單位進行測試
3、本公司系統上線	115/12月	平行使用期間開始
二、雙軌並行期間		
1、協助參加單位進行轉換	115/11月~116/11月	協助參加單位或其廠商進行轉換
2、年度金鑰交換作業	115/12月	倘有參加單位已經完成測試，可申請使用AES演算法進行年度金鑰交換作業。
3、Tripel DES結束服務	116/12/31前	於115年公開說明會提前揭示日期，故117年之年度金鑰交換作業，將僅提供AES演算法金鑰供使用。



簡報結束 敬請指教

完善金融資產集保平台 引領金融服務數位創新 共推金融市場永續發展