

臺灣集中保管結算所股份有限公司

安控作業說明及介面規格書

金融資訊部
中華民國 115 年 8 月

【1】基本說明	4
【1.1】作業處理說明	4
【2】演算法規格與公式	5
【2.1】演算法規格	5
【2.2】演算法公式說明	8
【3】作業處理說明	12
【3.1】交換工作基碼 — AES/GCM 模組	12
【3.2】工作基碼同步 — AES/CTR 模組	15
【4】訊息格式列表	17
【4.1】變更基碼請求訊息	17
【4.2】變更基碼回應訊息	18
【4.3】變更基碼通知訊息	19
【4.4】變更基碼確認訊息	20
【4.5】基碼同步請求訊息	21
【4.6】基碼同步回應訊息	22
【5】其他說明	23
【5.1】訊息 MAC 押碼處理說明	23
【5.2】押碼錯誤處理原則	25
【5.3】KMS 金鑰管理系統	26

文件修訂歷程

版次	修訂日期	變更說明	備註
2.0	2026/08/21	● 新增 AES 演算法規格及公式說明 ● 修改 OPC 訊息流程說明 ● 修改各訊息中文名稱 「要求變更基碼通知交易請求訊息」修改為「變更基碼請求訊息」 「要求變更基碼通知交易回應訊息」修改為「變更基碼回應訊息」 「變更基碼通知交易回應訊息」修改為「變更基碼通知訊息」 「變更基碼通知交易確認訊息」修改為「變更基碼確認訊息」 ● 新增「訊息 MAC 押碼處理說明」 ● 新增「KMS 金鑰管理系統說明」	2026 安控機制提升作業案

【1】基本說明

【1.1】作業處理說明

適合對象：參加單位以主機對主機方式連線至本公司之票券保管結算交割系統(BCSS)或款項收付服務平台(PSP)系統。

押碼原則：除交割狀態通知訊息(訊息代號 002、012、032 及 040)不需押碼外，其餘訊息均須押碼。

連線方式：訊息以 XML 格式，透過 TCP/IP、MQ 及 OPC 進行訊息交換。

基碼：

1. Cross Domain 基碼（即 Cross Domain Key、年度基碼、CDK）：

本系統與參加單位間有一組 Cross Domain 基碼，臺灣集中保管結算所股份有限公司會將 Cross Domain 基碼 A，B 碼單以郵寄方式送交參加單位基碼保管人員。參加單位以人工方式分別輸入 A，B 碼以建置 Cross Domain 基碼。原則上此基碼每年更換。

2. MAC 工作基碼（即 MAC Key）：

本系統需要一組 MAC 工作基碼。此基碼以 OPC 方式，線上交換，每日更新。

【2】演算法規格與公式

【2.1】演算法規格

OPC 基碼交換及基碼同步作業，分別使用兩種模式。基碼交換作業使用 AES-256-GCM 進行，基碼同步作業使用 AES-256-CTR 進行。以下為規格列表及名詞定義：

一、演算法規格列表：

OPC 基碼交換及基碼同步作業，使用 AES-256 加解密演算法。工作基碼交換使用 AES256/GCM 操作模式；基碼同步使用 AES256/CTR 操作模式。

項目	GCM 規格內容	CTR 規格內容
演算法 (Algorithm)	AES-256 (FIPS PUB 197)	AES-256 (FIPS PUB 197)
操作模式 (Mode)	GCM (NIST SP 800-38D)	CTR (NIST SP 800-38A)
填充模式 (Padding)	NoPadding	NoPadding
初始化向量 (IV)	12 位元組(Bytes)	16 位元組(Bytes)
認證標籤 (Tag)	16 位元組(Bytes)	N/A (不具備完整性校驗)

二、演算法名詞說明表

本規格文件，後續演算法公式說明，皆以此說明表為準。

參數	定義	說明
AES256 GCM	演算模式名稱	AES 演算法，採用 32 Bytes (256 bits)金鑰，GCM 模式。
AES256 CTR	演算模式名稱	AES 演算法，採用 32 Bytes (256 bits)金鑰，CTR 模式。
Padding	填充模式	GCM 及 CTR 模式皆使用 NoPadding 模式
Plaintext	未加密明文	於演算中，被加密之資料視為未加密明文
Ciphertext	已加密密文	● GCM 模式： 輸出為 Ciphertext (Length = Plaintext Length + Tag Length) ● CTR 模式： 輸出為 Ciphertext (Length = Plaintext Length)
T	認證標籤 (Authentication Tag)	● GCM 模式： 必須保留 16 Bytes 長度之認證標籤，用於解密時的完整性驗證 ● CTR 模式： 無須保留認證標籤
IV	初始化向量 (Initialization Vector)	● GCM 模式： 以參加單位代號串接營業日期(yyyyMMdd)進行 SHA256 雜湊演算後，<u>取前 12 個位元組</u> ● CTR 模式： 以參加單位代號串接營業日期(yyyyMMdd)進行 SHA256 雜湊演算後，<u>取前 16 個位元組</u>

E_K	運算金鑰	加解密運算中，所使用金鑰，以代號 E_K 表示
RN	隨機亂數	長度 8 Bytes 隨機亂數資料
RN^E $(RN+1)^E$ $(RN+2)^E$	加密後隨機亂數	RN^E ：加密後之隨機亂數 $(RN+1)^E$ ：加密後之隨機亂數+1 $(RN+2)^E$ ：加密後之隨機亂數+2
$SYNC$	基碼同步值	加密演算後之同步值，長度為 8 位元組

【2.2】演算法公式說明

【2.2.1】演算法公式說明 – AES/GCM 模式：

一、AES/GCM/Nopadding 加密演算：

1. 加密演算公式：

$$Ciphertext = AES-GCM-Encrypt (E_K, IV, Plaintext), NoPadding$$

2. 輸入資料：

輸入 *Plaintext* (明文)，其長度依輸入之明文內容而定，例如：

- 工作基碼：32 位元組 (Bytes)
- 隨機亂數 (Nonce)：8 位元組 (Bytes)

3. 輸出資料：

$$Ciphertext = C \parallel T \text{ (即加密後密文與認證標籤之串接結果)}。$$

4. 說明：

用於工作基碼交換時，使用工作基碼對輸入之隨機亂數 (Nonce) 或工作基碼進行加密運算。輸出資料格式為 $C \parallel T$ ，其中 C 為密文 (*Ciphertext*)， T 為認證標籤 (Authentication Tag)。輸出資料總長度為明文長度加上認證標籤長度 (16 位元組 (Bytes))。例如，當輸入之 *Plaintext* 長度為 32 位元組 (Bytes) 時，輸出資料長度為 $32 + 16 = 48$ 位元組 (Bytes)；當輸入之 *Plaintext* 長度為 8 位元組 (Bytes) 時，輸出資料長度為 $8 + 16 = 24$ 位元組 (Bytes)。

二、AES/GCM/Nopadding 解密演算：

1. 解密演算公式：

$$Plaintext = \text{AES-GCM-Decrypt}(E_K, IV, Ciphertext), NoPadding$$

2. 輸入資料：

輸入資料為 Ciphertext (密文) 資料 (C || T)，其中 C 為密文 (Ciphertext)，T 為認證標籤 (Authentication Tag)。

3. 輸出資料：

輸出為 Plaintext (解密後明文)，其長度依輸入之密文內容而定，例如：

- 工作基碼：32 位元組 (Bytes)
- 隨機亂數 (Nonce)：8 位元組 (Bytes)

4. 說明：

用於工作基碼交換時，對加密後之工作基碼或隨機亂數密文 (C || T) 執行 AES-GCM 解密運算。解密成功後，可還原原始明文，其中工作基碼長度為 32 位元組 (Bytes)，隨機亂數 (Nonce) 長度為 8 位元組 (Bytes)。

【2.2.2】演算法公式說明 – AES/CTR 模式：

一、AES/CTR/Nopadding 加密演算：

1. 加密演算公式：

$$Ciphertext = \text{AES-CTR-Encrypt} (E_K, IV, Plaintext), NoPadding$$

2. 輸入資料：

輸入 *Plaintext* (明文) 為當日日期字串 (格式：yyyyMMdd，共 8 個字元)，將其轉換為十六進位表示轉為 4 位元組 (Bytes) 之二進位資料，並於後續補 4 位元組 (Bytes) 0x00，形成固定長度 8 位元組 (Bytes) 之明文。

3. 輸出資料：

Ciphertext (加密後密文)，長度固定為 8 位元組 (Bytes)。

4. 說明：

用於工作基碼同步時之同步值計算，以工作金鑰 (E_K) 及初始向量 (IV) 執行 AES-CTR 加密。由於 CTR 模式不需進行填充 (*NoPadding*)，加密後密文長度與輸入明文長度相同，因此當輸入之 *Plaintext* 為 8 位元組 (Bytes) 時，輸出之 *Ciphertext* 亦為 8 位元組 (Bytes)。

【2.2.3】演算法公式說明 – GCM 模式導出初始向量 (IV)：

1. 計算使用公式：

$$IV = \text{Truncate-Left}(\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 12)$$

其中，Truncate-Left(X, 12) 表示取雜湊結果最左側 12 位元組 (Bytes) 作為初始向量 (IV)。

2. 說明：

使用 AES-GCM 模式進行加解密時，初始向量 (IV) 由參加單位代號 (ORIGIN) 與當日營業日期 (格式：yyyyMMdd) 串接後作為輸入資料，執行 SHA-256 雜湊運算，再取雜湊結果最左側 12 位元組 (Bytes) 作為 IV。

【2.2.4】CTR 模式導出初始向量 (IV) 公式：

1. 計算使用公式：

$$IV = \text{Truncate-Left}(\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 16)$$

其中，Truncate-Left(X, 16) 表示取 SHA-256 雜湊結果最左側 16 位元組 (Bytes) 作為 IV。

2. 說明：

使用 AES-CTR 模式進行加密時，初始向量 (IV) 由參加單位代號 (ORIGIN) 與當日營業日期 (格式：yyyyMMdd) 串接後作為輸入資料，執行 SHA-256 雜湊運算，再取雜湊結果最左側 16 位元組 (Bytes) 作為 IV。

【3】作業處理說明

【3.1】交換工作基碼 — AES/GCM模組

1. 本作業為本系統每日啟動時之第一項作業。系統須完成 MAC 工作基碼交換後，方可受理後續交易。

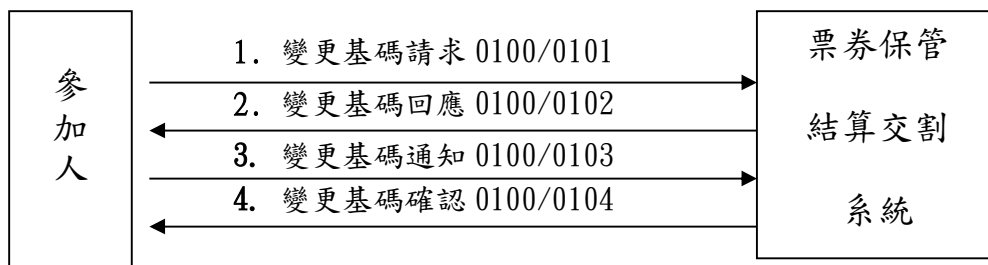


圖 1-1 OPC 作業流程說明

2. 作業程序說明：

原則上由參加單位啟動交換 MAC 工作基碼，依(1)、(2)、(3)、(4)程序進行。當異常狀況恢復時，此程序亦可能由系統主動依(2)、(3)、(4)程序進行交換 MAC 工作基碼。

- a. 參加單位將【變更基碼請求 (0100/0101)】訊息置於 **OPC Queue**，發送至本系統，以發起變更基碼通知交易。
- b. 本系統接收【變更基碼請求 (0100/0101)】訊息後，產生【變更基碼回應 (0100/0102)】訊息，將加密後之 **MAC 工作基碼**置於訊息中，並將該訊息置於參加單位之 **Queue**，發送至參加單位系統（使用與本系統交易相同之 **Queue**）。
- c. 參加單位接收到本系統回訊之【變更基碼回應 (0100/0102)】訊息後，

應使用以下公式進行解密：

導出 IV (初始向量)：

$$IV = \text{Truncate-Left} (\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 12)$$

解密工作基碼明文 (MACKey)：

$$\text{MACKey} = \text{AES-GCM-Decrypt} (\text{CDK}, IV, \text{MACKey}^E), \text{NoPadding}$$

解密隨機亂數 (RN)：

$$RN = \text{AES-GCM-Decrypt} (\text{MACKey}, IV, \text{RN}^E), \text{NoPadding}$$

RN 為系統隨機產生之 8 位元組 (Bytes) 亂數 (Nonce)。

- d. 參加單位完成前述作業後，應使用 MAC 工作基碼明文對隨機亂數加 1 ($RN+1$) 之結果進行加密，並產生【變更基碼通知(0100/0103)】訊息，將該訊息置於 OPC Queue，以完成變更基碼通知交易回應。

導出 IV (初始向量)：

$$IV = \text{Truncate-Left} (\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 12)$$

加密隨機亂數加 1：

$$(\text{RN}+1)^E = \text{AES-GCM-Encrypt} (\text{MACKey}, IV, (\text{RN}+1)), \text{NoPadding}$$

$RN+1$ 為將前述亂數視為 64 位元無號整數，其十六進位值以 Big-Endian 方式進行 +1 運算。

- e. 本系統接收【變更基碼通知(0100/0103)】訊息後，解密取得隨機亂數加 1 ($RN+1$) 之結果，並與預期值進行比對。若比對結果正確，則計算隨機亂數加 2 ($RN+2$)，並以【變更基碼確認(0100/0104)】訊息回應，並將該訊息置於參加單位之 Queue。其加密方式如下：

導出 IV (初始向量)：

$IV = \text{Truncate-Left} (\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 12)$

加密隨機亂數加 2：

$(RN+2)^E = \text{AES-GCM-Encrypt} (\text{MACKey}, IV, RN+2), \text{NoPadding}$

$RN+2$ 為將前述亂數視為 64 位元無號整數，其十六進位值加 2

(Nonce + 2) 之結果。

- f. 參加單位確認【變更基碼確認(0100/0104)】訊息內容無誤後，該 MAC 工作基碼即正式生效並啟用。
- g. 本系統與各參加單位間交換之每筆訊息均設有逾時 (Time-out) 機制，目前逾時時間設定為 2 分鐘。

【3.2】工作基碼同步 — AES/CTR模組

1. 本作業主要用於確認參加單位與本系統間之 MAC 工作基碼是否已完成同步。本作業可由參加單位或本系統任一方發起。
2. 由參加單位啟動作業程序說明：

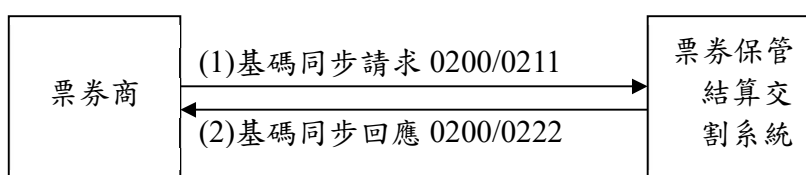


圖 1-2 票券商啟動之基碼同步作業流程說明圖

- a. 參加單位將【基碼同步請求 (0200/0211)】訊息置於 OPC Queue，發起基碼同步作業。該訊息之 SYNC 值依下列公式計算：

導出 IV (初始向量)：

$$IV = \text{Truncate-Left} (\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 16)$$

Plaintext (明文資料)：

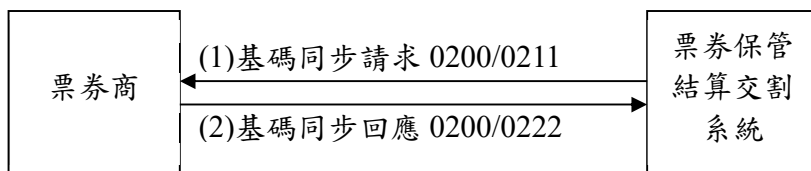
$$\text{yyyyMMdd} + (0x00 * 4)$$

Ciphertext (加密密文)：

$$\text{SYNC}^E = \text{AES-CTR-Encrypt} (\text{MACKey}, IV, \text{plaintext}, \text{NoPadding})$$

- b. 本系統接收【基碼同步請求 (0200/0211)】訊息後，進行 SYNC 值比對。若比對結果正確，則產生【基碼同步回應 (0200/0222)】訊息，並將該訊息置於參加單位之 Queue，發送至參加單位系統（使用與本系統交易相同之 Queue）。
- c. 本系統與各參加單位間交換之每筆訊息均設有逾時 (Time-out) 機制，目前逾時時間設定為 2 分鐘。

3. 由本系統啟動作業程序說明：



- a. 本系統產生【基碼同步請求 (0200/0211)】訊息，並將該訊息置於參加單位之 Queue，發送至參加單位系統（使用與本系統交易相同之 Queue）。訊息中之 SYNC 欄位值依前述公式計算。
- b. 參加單位接收基碼同步請求 (0200/0211) 訊息後，進行 SYNC 值比對。若比對結果正確，則產生基碼同步回應 (0200/0222) 訊息，並將該訊息置於 OPC Queue，發送至本系統。
- c. 本系統與各參加單位間交換之每筆訊息均設有逾時 (Time-out) 機制，目前逾時時間設定為 **2 分鐘**。

【4】訊息格式列表

【4.1】變更基碼請求訊息

欄位名稱	DTD	欄位說明	格式	長度	屬性
Message Type 訊息代號	MSG_TYPE	0100	N	4	M
Process Code 作業代號	PRC_CODE	0101	N	4	M
Audit No 流水編號	AUDIT_NO	由參加單位自行編訂之流水號且不可重複	N	7	M
Participant ID 參加單位代號	ORIGIN	參加單位代號	C	8	M
Time Stamp 時間戳記	TS	YYYYMMDDHHMMSS	N	14	M
Response Code 回應代號	RSP_CODE	預設值—“0001”	N	4	M

【4.2】變更基碼回應訊息

欄位名稱	DTD	欄位說明	格式	長度	屬性
Message Type 訊息代號	MSG_TYPE	0100	N	4	M
Process Code 作業代號	PRC_CODE	0102	N	4	M
Audit No 流水編號	AUDIT_NO	◆若基碼交換為參加單位所啟動，則同“變更基碼請求”訊息之流水編號。 ◆若基碼交換為臺灣集中保管結算所股份有限公司所啟動，則為系統編訂之以‘9’為首之不重複之流水編號。如：‘9123456’	N	7	M
Participant ID 參加單位代號	ORIGIN	參加單位代號	C	8	M
Time Stamp 時間戳記	TS	YYYYMMDDHHMMSS	N	14	M
Response Code 回應代號	RSP_CODE	0001：成功 0304：加解密錯誤 0106：XML 錯誤 0107：參加單位代號錯誤	N	4	M
Key ID 基碼代號	KEY_ID	02	N	2	M
New Key 新工作基碼	NEW_KEY	此新工作基碼係由 Kcd 及 NK 經過 AES 加密產生之 16 進位字串 (HEX)。	C	96	M
Random Number 隨機亂數	RANDOM_NO	此隨機亂數係由 NK 及 RN 經過 AES 加密產生之 16 進位字串 (HEX)。	C	48	M

【4.3】變更基碼通知訊息

欄位名稱	DTD	欄位說明	格式	長度	屬性
Message Type 訊息代號	MSG_TYPE	0100	N	4	M
Process Code 作業代號	PRC_CODE	0103	N	4	M
Audit No 流水編號	AUDIT_NO	同「變更基碼請求」訊息之流水編號	N	7	M
Participant ID 參加單位代號	ORIGIN	參加單位代號	C	8	M
Time Stamp 時間戳記	TS	YYYYMMDDHHMMSS	N	14	M
Response Code 回應代號	RSP_CODE	預設值—“0001”	N	4	M
Random Number 隨機亂數	RANDOM_NO	此隨機亂數係由 NK 及 RN+1 經過 AES 加密產生之 16 進位字串。	C	48	M

【4.4】變更基碼確認訊息

欄位名稱	DTD	欄位說明	格式	長度	屬性
Message Type 訊息代號	MSG_TYPE	0100	N	4	M
Process Code 作業代號	PRC_CODE	0104	N	4	M
Audit No 流水編號	AUDIT_NO	同「變更基碼請求」訊息之流水編號	N	7	M
Participant ID 參加單位代號	ORIGIN	參加單位代號	C	8	M
Time Stamp 時間戳記	TS	YYYYMMDDHHMMSS	N	14	M
Response Code 回應代號	RSP_CODE	0001：成功 0103：Timeout 0104：其他錯誤 0106：XML 錯誤 0302：MAC 錯誤 0304：加解密錯誤	N	4	M
Random Number 隨機亂數	RANDOM_NO	此隨機亂數係由 NK 及 RN+2 經過 AES 加密產生之 16 進位字串。	C	48	M

【4.5】基碼同步請求訊息

欄位名稱	DTD	欄位說明	格式	長度	屬性
Message Type 訊息代號	MSG_TYPE	0200	N	4	M
Process Code 作業代號	PRC_CODE	0211	N	4	M
Audit No 流水編號	AUDIT_NO	◆若基碼同步請求為參加單位所啟動，則由參加單位自行編訂之流水號且不可重複。 ◆若基碼同步請求為臺灣集中保管結算所股份有限公司所啟動，則為系統編訂之以'9'為首之不重複之流水編號。如：'9123456'	N	7	M
Participant ID 參加單位代號	ORIGIN		C	8	M
Time Stamp 時間戳記	TS	YYYYMMDDHHMMSS	N	14	M
Response Code 回應代號	RSP_CODE	預設值—"0001"	N	4	M
Key Sync Data 基碼同步資料	KEY_SYNC_DATA	以當日之日期，格式為YYYYMMDD，Pack為4個位元組，再後補4個x'00'位元組後，以MAC工作基碼押碼，所得之值。	C	16	M

【4.6】基礎同步回應訊息

欄位名稱	DTD	欄位說明	格式	長度	屬性
Message Type 訊息代號	MSG_TYPE	0200	N	4	M
Process Code 作業代號	PRC_CODE	0222	N	4	M
Audit No 流水編號	AUDIT_NO	同基礎同步請求之流水編號	N	7	M
Participant ID 參加單位代號	ORIGIN		C	8	M
Time Stamp 時間戳記	TS	YYYYMMDDHHMMSS	N	14	M
Response Code 回應代號	RSP_CODE	0001：成功 0103：Timeout 0104：其他錯誤 0106：XML 錯誤 0302：SYNC 值驗證錯誤 0304：加解密錯誤	N	4	M

【5】其他說明

【5.1】訊息MAC押碼處理說明

一、作業方式類別

參加單位連線方式	工作基碼交換	適用範圍	是否需要參加單位開發
MQ Server 主機對主機	OPC	上下傳的訊息	Y

二、MAC 押碼作業說明

1. 訊息格式及長度

產生之 MAC 以串接方式與 XML 訊息及參加單位代號串接合併後進行傳送，整體訊息格式如下：

[XML] || [PRTY_ID] || [MAC value]，各別資料長度如下表：

資料類型	XML 訊息	參加單位代號	MAC
資料長度	變動長度	8 字元、8 位元組 (Bytes)	16 字元(HEX)、8 位元組 (Bytes)

範例如下：

```
<?xml version="1.0" encoding="CNS11643"?><!DOCTYPE BCSSMESSAGE
SYSTEM "FiscBCSS.dtd"><BCSSMESSAGE ORIGIN="BCSS" TS="2026-07-
22T14:30:00" BCSS_BUS_DT="2026-07-22" MSG_TYPE="516"
SNDR_REF="0000000000001" ACTION="FN" RESEND="N"><FL_TRANS
F_DIR="d" F_ID="STFIS07" F_NM="STFIS07.20260722.txt" IP_ADDR="localhost"
REF="PDFPJSRPLZCIE"/></BCSSMESSAGE>B9990004D49FC5BE3DDE09D
```

2. MAC 產生方式

- a. 訊息傳送端（參加人或臺灣集中保管結算所股份有限公司）對 XML 訊息字串執行 SHA-256 雜湊運算，產生 32 位元組(Bytes) 之雜湊值。
- b. 若 XML 訊息內容包含中文字元，應先將 XML 訊息編碼轉換為 CNS11643 編碼，再執行 SHA-256 雜湊運算。
- c. 使用 MAC 工作基碼 (MAC Key) 作為 AES-256-GCM 加密金鑰，對上述 SHA-256 雜湊值執行加密運算，並取加密結果最左側 8 位元組 (Bytes) 作為 MAC 值。MAC 值於傳送時須轉換為十六進位格式傳送（共 16 個字元）。

其計算公式如下：

IV (初始向量)：

$$IV = \text{Truncate-Left}(\text{SHA256}(\text{ORIGIN} \parallel \text{yyyyMMdd}), 12)$$

Plaintext (明文資料)：

XML 訊息經 SHA-256 雜湊後所得之雜湊值，長度為 32 位元組 (Bytes)。

MAC 計算公式：

$$\text{Truncate-Left}(\text{AES-GCM-Encrypt}(\text{MACKey}, IV, \text{Plaintext}), 8)$$

3. MAC 驗證方式

訊息接收端(參加人或臺灣集中保管結算所股份有限公司)使用相同之 MAC 產生方式，重新計算 MAC 值並驗證 MAC 值是否正確。

【5.2】押碼錯誤處理原則

一、參加單位收到來自本系統之訊息押碼錯誤處理方式

1. 捨去該筆訊息。
2. 啟動“OPC 基碼同步請求”交易。
 - a. 若工作基碼無誤，該 MAC error 可能屬個別訊息問題，參加單位只要啟動“004 重送訊息指令”要求重送該筆訊息即可。
 - b. 若工作基碼錯誤時，參加單位須重新啟動“變更基碼請求”作業。
 - c. 變更基碼請求作業未完成前，本系統不接受參加單位傳送任何之交割訊息或指令。
 - d. 基碼變更完成前，參加單位所接收之訊息可能有用前一把 key(old key)押碼之訊息，參加單位須捨去使用舊工作基碼所押碼之訊息，再啟動“004 重送訊息指令”要求本系統重送遺漏之訊息。

二、參加單位所傳送之訊息押碼錯誤處理方式

1. 啟動“OPC 基碼同步請求交易”
 - a. 若工作基碼無誤，參加單位只須重新押碼並重送該筆訊息即可。
 - b. 若工作基碼錯誤，參加單位須重新啟動“變更基碼請求”作業。
 - c. 變更基碼請求作業未完成前，本系統不接受參加單位傳送任何之交割訊息或指令。基碼變更完成前，參加單位所接收之訊息可能有用前一把 key(old key)押碼之訊息，參加單位須捨去使用舊工作基碼所押碼之訊息，再啟動“004 重送訊息指令”要求本系統重送遺漏之訊息。

【5.3】KMS金鑰管理系統

KMS 為金鑰管理系統 (Key Management System) 之簡稱，各參加單位使用名稱可能有所不同。

KMS 系統主要用於年度基碼 (CDK) 交換作業。於輸入 CDK 之 A 碼、B 碼時，需一併輸入 A 碼、B 碼及 CDK 之檢核碼 (CHK Value)。檢核碼計算方式如下：

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)。

CHK Value：

$$CHK = \text{Truncate-Right}(\text{AES-GCM-Encrypt}(Key, IV, Key), 2)$$

其中 Plaintext 為待檢核之金鑰或 A、B 碼。使用相同金鑰或 A、B 碼執行 AES-GCM 加密。完成加密運算後，得出加密結果之密文，並取該密文最右側 2 位元組 (Bytes) 作為對應金鑰或 A、B 碼之檢核碼 (CHK Value)。

輸入完成 A 碼及 B 碼之後，KMS 將 A 碼與 B 碼進行 XOR，即得出該參加單位之年度基碼 (即 CDK)。

年度基碼 (CDK)：

$$CDK = (A \text{ part}) \text{ XOR } (B \text{ part})$$