

## 【4】 安控作業

### 【4.1】 OPC 作業

適合對象：以主機對主機方式連線至本系統之款項收付銀行。

押碼原則：訊息皆須押碼。

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：本系統與款項收付銀行間有一組 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款項收付銀行基碼保管人員。款項收付銀行以人工方式分別鍵入 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：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。

#### 【4.1.1】 OPC 作業處理

##### 【4.1.1.1】 交換 MAC 工作基碼 — ECB 模組

1. 此作業為本系統每天啟動時之第一個動作，未完成交換 MAC 工作基碼將不允許任何交易的進行。
2. 作業程序說明：

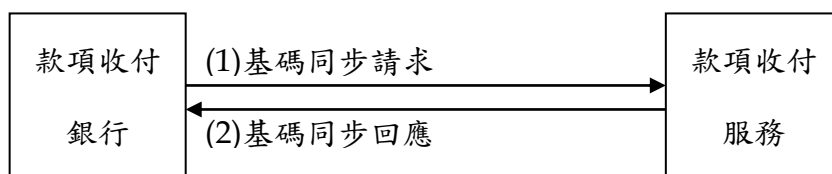


#### OPC 作業流程說明

1. 原則上由款項收付銀行啟動交換 MAC 工作基碼，依(1)，(2)，(3)，(4)程序進行。當異常狀況回復時，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。
2. 款項收付銀行將〈換 KEY 請求〉置於 OPC queue 內。
3. 本系統將 MAC 工作基碼以〈換 KEY〉訊息回應置於款項收付銀行的 queue 內(此 queue 與本系統交易所使用的 queue 相同)。
4. 款項收付銀行產生 N+1 以〈換 KEY 回應〉訊息回應(置於 OPC queue 內)。
5. 本系統產生 N+2 以〈換 KEY 確認〉訊息回應(置於款項收付銀行的 queue 內)。
6. 款項收付銀行確認〈換 KEY 確認〉訊息無誤後則此 MAC 工作基碼即生效啟用。
7. 每一個款項收付銀行與本系統間交換的訊息均設有 Time-out，目前暫時設定為二分鐘。

#### 【4.1.1.2】基碼同步 — CBC 模組

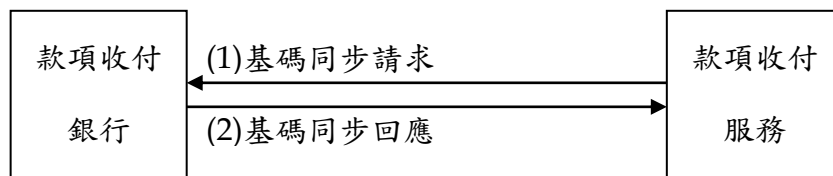
1. 此作業主要供款項收付銀行與本系統確認 MAC 工作基碼是否同步之用，此作業可由款項收付銀行或本系統啟動。
2. 由款項收付銀行啟動作業程序說明：



款項收付銀行啟動之基碼同步作業流程說明圖

1. 款項收付銀行將〈基碼同步請求〉置於 OPC queue 內。
2. 本系統產生〈基碼同步回應〉置於款項收付銀行 queue 內(此 queue 與本系統交易所使用的 queue 相同)。
3. 每一個款項收付銀行與本系統間交換的訊息均設有 Time-out，目前暫時設定為二分鐘。

由本系統啟動作業程序說明：



#### 本系統啟動之基碼同步作業流程說明圖

1. 本系統產生〈基碼同步請求〉置於款項收付銀行 queue 內(此 queue 與本系統交易所使用的 queue 相同)。
2. 款項收付銀行將〈基碼同步回應〉置於 OPC queue 內。
3. 每一個款項收付銀行與本系統間交換的訊息均設有 Time-out，目前暫時設定為二分鐘。

## OPC 訊息格式

### 1. 要求變更基碼通知交易請求

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

### 2. 要求變更基碼通知交易回應

| 欄位名稱                 | DTD      | 欄位說明 | 格式 | 長度 | 屬性 |
|----------------------|----------|------|----|----|----|
| Message Type<br>訊息代號 | MSG_TYPE | 0100 | N  | 4  | M  |
| Process Code<br>作業代號 | PRC_CODE | 0102 | N  | 4  | M  |

|                          |           |                                                                                                                    |   |    |   |
|--------------------------|-----------|--------------------------------------------------------------------------------------------------------------------|---|----|---|
| Audit No<br>流水編號         | AUDIT_NO  | <p>◆若基碼交換為使用單位所啟動，則同“要求變更基碼通知交易請求”訊息之流水編號。</p> <p>◆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’</p> | N | 7  | M |
| Participant ID<br>使用單位代號 | ORIGIN    | 使用單位代號                                                                                                             | C | 8  | M |
| Time Stamp<br>時間戳記       | TS        | YYYYMMDDHHMMSS                                                                                                     | N | 14 | M |
| Response Code<br>回應代號    | RSP_CODE  | <p>0001：成功</p> <p>0304：AR 錯誤</p> <p>0106：XML 錯誤</p>                                                                | N | 4  | M |
| Key ID<br>基碼代號           | KEY_ID    | 02                                                                                                                 | N | 2  | M |
| New Key<br>新工作基碼         | NEW_KEY   | <p>此新工作基碼係由 Kcd 及 NK 經過 3DES 加密產生之 16 進位字串。</p> <p>NEW_KEY = 3DES (Kcd , NK)。</p>                                  | C | 32 | M |
| Random Number<br>隨機亂數    | RANDOM_NO | <p>此隨機亂數係由 NK 及 RN 經過 3DES 加密產生之 16 進位字串。</p> <p>RANDOM_NO = 3DES (NK , RN)。</p>                                   | C | 16 | M |

3DES：Triple DES 之簡寫。

NK：未加密過之工作基碼。

Kcd : Cross Domain Key 之簡寫。

Kcd = A 碼 xor B 碼 (A、B 碼 由臺灣集中保管結算所股份有限公司提供，每 6 ~ 12 個月更換一次)。

RN: 未加密前之 Random Number 之簡寫。

### 3. 變更基碼通知交易回應

| 欄位名稱                     | DTD       | 欄位說明                                                                       | 格式 | 長度 | 屬性 |
|--------------------------|-----------|----------------------------------------------------------------------------|----|----|----|
| Message Type<br>訊息代號     | MSG_TYPE  | 0100                                                                       | N  | 4  | M  |
| Process Code<br>作業代號     | PRC_CODE  | 0103                                                                       | N  | 4  | M  |
| Audit No<br>流水編號         | AUDIT_NO  | 同換“要求變更基碼通知交易請求”訊息之流水編號                                                    | N  | 7  | M  |
| Participant ID<br>使用單位代號 | ORIGIN    | 使用單位代號                                                                     | C  | 8  | M  |
| Time Stamp<br>時間戳記       | TS        | YYYYMMDDHHMMSS                                                             | N  | 14 | M  |
| Response Code<br>回應代號    | RSP_CODE  | 預設值—“0001”                                                                 | N  | 4  | M  |
| Random Number<br>隨機亂數    | RANDOM_NO | 此隨機亂數係由 NK 及 RN1 經過 3DES 加密產生之 16 進位字串。<br><br>RANDOM_NO = 3DES (NK, RN1)。 | C  | 16 | M  |

NK = UN3DES (Kcd, NEW\_KEY)。

$RN1 = RN + 1$  (16 進位加法)。

$RN = UN3DES(NK, 3DES(NK, RN))$ 。

#### 4. 變更基碼通知交易確認

| 欄位名稱                     | DTD       | 欄位說明                                                                             | 格式 | 長度 | 屬性 |
|--------------------------|-----------|----------------------------------------------------------------------------------|----|----|----|
| Message Type<br>訊息代號     | MSG_TYPE  | 0100                                                                             | N  | 4  | M  |
| Process Code<br>作業代號     | PRC_CODE  | 0104                                                                             | N  | 4  | M  |
| Audit No<br>流水編號         | AUDIT_NO  | 同換“要求變更基碼通知交易請求”訊息之流水編號                                                          | N  | 7  | M  |
| Participant ID<br>使用單位代號 | ORIGIN    | 使用單位代號                                                                           | C  | 8  | M  |
| Time Stamp<br>時間戳記       | TS        | YYYYMMDDHHMMSS                                                                   | N  | 14 | M  |
| Response Code<br>回應代號    | RSP_CODE  | 0001：成功<br>0103：Timeout<br>0104：其他錯誤<br>0106：XML 錯誤<br>0302：MAC 錯誤<br>0304：AR 錯誤 | N  | 4  | M  |
| Random Number<br>隨機亂數    | RANDOM_NO | 此隨機亂數係由 NK 及 RN2 經過 3DES 加密產生之 16 進位字串。<br>RANDOM_NO = 3DES                      | C  | 16 | M  |

|  |  |            |  |  |  |
|--|--|------------|--|--|--|
|  |  | (NK, RN2)。 |  |  |  |
|--|--|------------|--|--|--|

NK = UN3DES (Kcd, NEW\_KEY)。

RN2 = RN1 + 1 (16 進位加法)。

RN2 = UN3DES (NK, 3DES (NK, RN1+1))。

## 5.基碼同步請求

| 欄位名稱                     | DTD      | 欄位說明                                                                                                                       | 格式 | 長度 | 屬性 |
|--------------------------|----------|----------------------------------------------------------------------------------------------------------------------------|----|----|----|
| Message Type<br>訊息代號     | MSG_TYPE | 0200                                                                                                                       | N  | 4  | M  |
| Process Code<br>作業代號     | PRC_CODE | 0211                                                                                                                       | N  | 4  | M  |
| Audit No<br>流水編號         | AUDIT_NO | <p>◆若基碼同步請求為使用單位所啟動，則由使用單位自行編訂之流水號且不可重複。</p> <p>◆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。</p> <p>如：'9123456'</p> | N  | 7  | M  |
| Participant ID<br>使用單位代號 | ORIGIN   |                                                                                                                            | C  | 8  | M  |
| Time Stamp<br>時間戳記       | TS       | YYYYMMDDHHMMSS                                                                                                             | N  | 14 | M  |
| Response Code<br>回應代號    | RSP_CODE | 預設值—"0001"                                                                                                                 | N  | 4  | M  |

|                         |               |                                                                                            |   |   |   |
|-------------------------|---------------|--------------------------------------------------------------------------------------------|---|---|---|
| Key Sync Data<br>基碼同步資料 | KEY_SYNC_DATA | 以當日之日期，格式為<br>YYYYMMDD，Pack 為 4 個字<br>元，再候補 4 個字元 x'00'後，<br>以 MAC 工作基碼押碼<br>所得之值的前 4 個字元。 | C | 8 | M |
|-------------------------|---------------|--------------------------------------------------------------------------------------------|---|---|---|

說明：

1. 若基碼同步請求由本系統發動時，KEY\_SYNC\_DATA 內之英文字母皆為小寫，  
若基碼同步請求由使用單位發動時，KEY\_SYNC\_DATA 內之英文字母大小寫皆可  
(本系統會自動轉換成小寫)。
2. 例如：日期為 20011101，  
MAC(NK, "2001110100000000") = "3f23ae0156a3...."，  
KEY\_SYNC\_DATA = "3f23ae01"。

## 6. 基碼同步回應

| 欄位名稱                     | DTD      | 欄位說明                        | 格式 | 長度 | 屬性 |
|--------------------------|----------|-----------------------------|----|----|----|
| Message Type<br>訊息代號     | MSG_TYPE | 0200                        | N  | 4  | M  |
| Process Code<br>作業代號     | PRC_CODE | 0222                        | N  | 4  | M  |
| Audit No<br>流水編號         | AUDIT_NO | 同基碼同步請求之流水編號                | N  | 7  | M  |
| Participant ID<br>使用單位代號 | ORIGIN   |                             | C  | 8  | M  |
| Time Stamp<br>時間戳記       | TS       | YYYYMMDDHHMMSS              | N  | 14 | M  |
| Response Code<br>回應代號    | RSP_CODE | 0001：成功<br><br>0103：Timeout | N  | 4  | M  |

本文件著作權屬臺灣集中保管結算所股份有限公司所有，未經本公司許可不得引伸或翻印

|  |  |             |  |  |  |
|--|--|-------------|--|--|--|
|  |  | 0104：其他錯誤   |  |  |  |
|  |  | 0106：XML 錯誤 |  |  |  |
|  |  | 0302：MAC 錯誤 |  |  |  |
|  |  | 0304：AR 錯誤  |  |  |  |

## 【4.1.2】 OPC XML DTD 檔案

說明: OPC XML 訊息格式的為

```
<?xml version="1.0" encoding="CNS11643?"><!DOCTYPE OPCMESSAGE
SYSTEM "OPC_PSP.dtd"><OPCMESSAGE ...></OPCMESSAGE>
```

以下為 OPC\_PSP.DTD

```
<!--
```

```
    OPC_PSP.dtd
```

```
-->
```

```
<!ELEMENT OPCMESSAGE
```

```
(CHG_KEY_REQ|CHG_KEY|CHG_KEY_RSP|CHG_KEY_CFRM|KEY_SYNC|KEY_SYNC_RSP)>
```

```
<!ATTLIST OPCMESSAGE
```

```
    ORIGIN CDATA #REQUIRED
```

```
    MSG_TYPE(0100|0200) #REQUIRED
```

```
    PRC_CODE(0100|0102|0103|0104|0211|0222) #REQUIRED
```

```
    AUDIT_NO CDATA #REQUIRED
```

```
    TS CDATA #REQUIRED
```

```
    RSP_CODE(0000|0001) #REQUIRED
```

```
>
```

```
<!ELEMENT CHG_KEY_REQ EMPTY>
```

```
<!ELEMENT CHG_KEY EMPTY>
```

```
<!ATTLIST CHG_KEY
```

```
KEY_ID CDATA #REQUIRED
NEW_KEY CDATA #REQUIRED
RANDOM_NO CDATA #REQUIRED
>

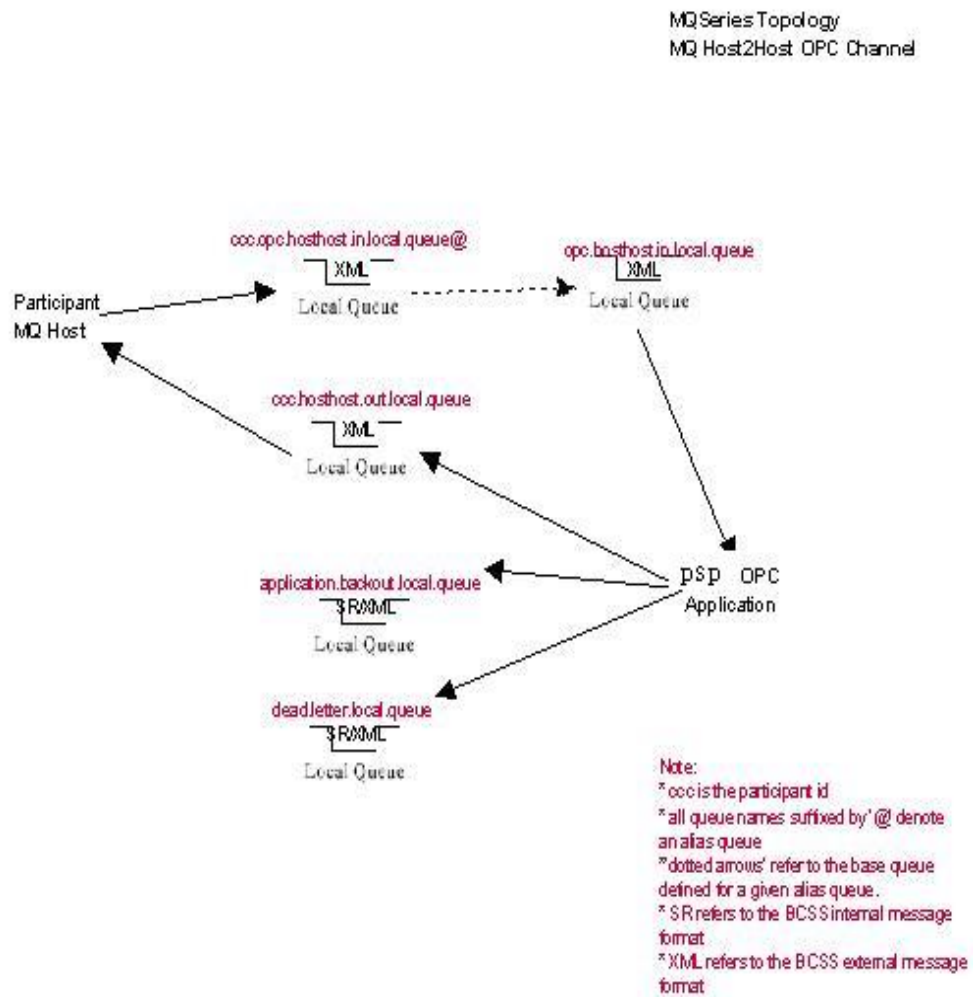
<!ELEMENT CHG_KEY_RSP EMPTY>
<!ATTLIST CHG_KEY_RSP
    RANDOM_NO CDATA #REQUIRED
>

<!ELEMENT CHG_KEY_CFRM EMPTY>
<!ATTLIST CHG_KEY_CFRM
    RANDOM_NO CDATA #REQUIRED
>

<!ELEMENT KEY_SYNC EMPTY>
<!ATTLIST CHG_KEY_RSP
    KEY_SYNC_DATA CDATA #REQUIRED
>

<!ELEMENT KEY_SYNC_RSP EMPTY>
```

## MQ 架構



## OPC 作業 MQ 架構圖

## 【4.2】 訊息押碼處理說明

### 【4.2.1】 作業方式類別

| 使用單位連線方式                | 基碼儲存/<br>交換 | 適用範圍       | 是否需要參<br>加單位開發 |
|-------------------------|-------------|------------|----------------|
| MQ Server, Host to Host | OPC         | 所上下傳的訊息    | Y              |
| MQ Client UP/ download  | IC 卡        | 所有上傳至系統的訊息 | N(Y)*          |
| Browser                 | IC 卡        | 非查詢的交易請求   | N              |

\*本介面規格主要在說明 MQ Server, Host to Host (OPC MAC 作業)以及 MQ Client UP/ download (IC 卡 MAC 作業)連線方式之 MAC 作業。使用單位必須依其連線方式採用適當的 MAC 作業。若使用單位採用 Browser 或系統所提供之 MQ Client UP/ download 連線方式，則無需自行開發 MAC 介面。

### 【4.2.2】 OPC MAC 作業說明

#### 1. 訊息格式及長度

| 〈XML 格式訊息〉 | 使用單位代號  | MAC     |
|------------|---------|---------|
| (變動長度)     | 8 bytes | 8 bytes |

#### 2. MAC 產生方式

2.1 訊息傳送端(款項收付銀行或臺灣集中保管結算所股份有限公司)以 SHA-1 方式對〈XML 格式訊息〉做 hash 後(160 bits)，再附加 32 bits x'00'(共計 192 bits，24 bytes)。

message hash = SHA1(〈XML 格式訊息〉) + "00000000"。

2.2 將該 24 bytes 以 MAC 工作基碼產生 MAC，取左邊 4 個位元組(4 bytes)作為 MAC 值，MAC 值於傳送時須先轉為 16 進位表示後，再轉為 8 bytes 之字串。

MAC 值 = 取 MAC(工作基碼, message hash) 左邊 4 個位元組。

### 3. MAC 驗證方式

訊息接收端(款項收付銀行或臺灣集中保管結算所股份有限公司)使用相同之 MAC 產生方式產生 MAC 值並驗證 MAC 值是否正確。

### 4. 押碼方式

押碼不押 Header，只押 Body 內容，由<SvcMsg>起始至</SvcMsg>，範例如下灰底框：

```
<?xml version="1.0" encoding="CNS11643"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header>
    <scoi:SvcCor      xmlns:scoi="http://wsgw.icp.ibm.com/svccor/interface/"
env:actor="http://schemas.xmlsoap.org/soap/actor/next"
env:mustUnderstand="1">
      <scoi:Service>
        <scoi:SvcMd>ASYN</scoi:SvcMd>
        <scoi:SvcId>IS940PICRQ</scoi:SvcId>
        <scoi:SsnId>0108032411191</scoi:SsnId>
        <scoi:MsgId>I940PICQ-GTWY-PSPF-0324-940000011191</scoi:MsgId>
        <scoi:MsgTs>2008-03-24 09:00:00</scoi:MsgTs>
      </scoi:Service>
      <scoi:Address>
        <scoi:From>

<scoi:Node>http://psp.tdcc.com.tw/node/pid/S0000001/</scoi:Node>
        </scoi:From>
        <scoi:To>

<scoi:Node>http://psp.tdcc.com.tw/node/pid/S0110000/</scoi:Node>
        </scoi:To>
      </scoi:Address>
      <scoi:Process>
        <scoi:PcsId>1417QYM7X0</scoi:PcsId>
      </scoi:Process>
      <scoi:MAC>
        <scoi:MACValue>89F4F0B0</scoi:MACValue>
```

```
</scoi:MAC>
</scoi:SvcCor>
</env:Header>
<env:Body>
  <SvcMsg xmlns="http://wsgw.icp.ibm.com/interface/">
    <PmtInConfirmSvc>
      <PmtInConfirm resend="N">
        <BusDt>2008-03-24</BusDt>
        <InfoType>040</InfoType>
        <Bank>0110000</Bank>
        <BankNm>上海商業儲蓄銀行</BankNm>
        <AcctId>05108000055111</AcctId>
        <CshAmt>100000</CshAmt>
        <CshCcy>AUD</CshCcy>
      </PmtInConfirm>
    </PmtInConfirmSvc>
  </SvcMsg>
</env:Body>
</env:Envelope>
```

### 【4.3】押碼錯誤處理原則

#### 【4.3.1】使用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。
  - 2.1 若工作基碼無誤，該 MAC error 可能屬個別訊息問題，使用單位只要啟動“[PS802RSDRQ 重送訊息指令](#)”要求重送該筆訊息即可。
  - 2.2 若“工作基碼錯誤時，使用單位須重新啟動“要求變更基碼通知交易請求”。  
“要求變更基碼通知交易請求”未完成前，本系統不接受使用單位傳送任何之交割訊息或指令。基碼變更完成前，使用單位所接收之訊息可能有用前一把 key(old key)押 MAC 之訊息，使用單位須捨去這些訊息，同時再啟動“[PS802RSDRQ 重送訊息指令](#)”要求本系統重送遺漏之訊息。

#### 【4.3.2】使用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”
  - 1.1 若工作基碼無誤，使用單位只須重押 Mac 並重送該筆訊息即可。
  - 1.2 若工作基碼錯誤時，使用單位須重新啟動“要求變更基碼通知交易請求”。“要求變更基碼通知交易請求”未完成前，本系統不接受使用單位傳送任何之交割訊息或指令。基碼變更完成前，使用單位所接收之訊息可能有用前一把 key(old key)押 MAC 之訊息，使用單位須捨去這些訊息，同時再啟動“[PS802RSDRQ 重送訊息指令](#)”要求本系統重送遺漏之訊息。

## 【4.4】 Triple-DES 之說明

所謂 Triple-DES 顧名思義便是將一個明文資料做了三次的 DES 運算，而如何將明文做三次 DES 運算可能就使用的基碼之不同或加解密順序之不同而有不同之模式。本系統採目前最廣泛被使用之 EDE2 模式，其基碼長度為 112 bits，是傳統 DES 基碼長度（56 bits）的二倍，以下將做更詳細的說明：

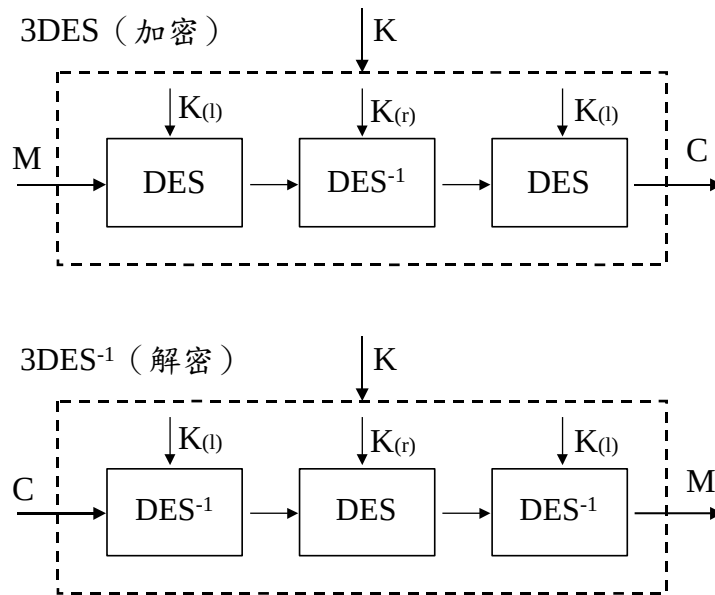
DES-EDE2: 使用 2 個不同的基碼，依序做 DES 加密、DES 解密及 DES 加密，其中第 1 及第 3 個運算將使用第 1 個基碼，而第二個運算則使用第 2 個基碼。

本文件將以 3DES 表示以上所指的 DES-EDE2，其與 DES 的關係如下：

$$3DES(K, M) = DES(k_l, DES^{-1}(K_r, DES(K_l, M))) = C$$

$$3DES^{-1}(K, C) = DES^{-1}(K_l, DES(K_r, DES^{-1}(K_l, C))) = M$$

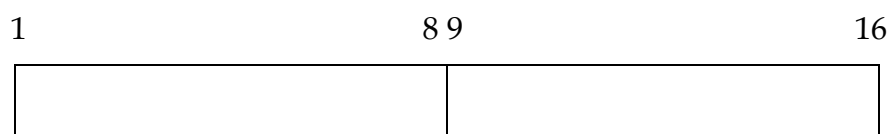
其中 K 為 Triple DES 的基碼，M 為明文資料，C 為密文資料。



Triple DES (EDE2 mode)

由上可知 3DES 是以 DES 的運算為基礎，而其基碼長度為 16 bytes (16 bits 為 Parity Check)，因此，其表達式如  $K = K_{(l)} + K_{(r)}$ ，也就是  $K_{(l)}$  為 K 的 1 到 8 個 BYTE，而  $K_{(r)}$  為 K 的 9 到 16 個 BYTE，其結構如下：

Byte



輸入驗證碼與建立驗證碼之運算方式相同，其表達式如下所示：

$$C_1 = 3DES(K, K_{left})$$

$$Checksum = \text{the Last 2 bytes of } 3DES(K, C_1 \oplus K_{right})$$

當 K 表基碼之 A 碼或 B 碼，則所計算出之 CheckSum 值為輸入驗證碼，若 K 表

所欲建立之 Triple-DES 基碼，則所計算出之 CheckSum 值為建立驗證碼。