文書及檔案管理
電腦化作業規範

（九十三年修正版）

行政院研究發展考核委員會

中華民國九十三年六月

文件修訂履歷

發行/修訂版次	發行/修訂生效日期	發行與變更說明	修訂/審核人員	備註
1.00	93.06.29	初版發行。	修訂：邵敏毅__	
1.01	93.08.03	修正 93_交換用標籤.ent 第 15 行<!ELEMENT 受文者 <!ELEMENT 受文者 (((姓名,職稱?,機關代碼,單位代碼?)|(全銜,機關代碼)|(單位名,機關代碼,單位代碼)),含附件?,內含本文與附件之可攜式文件檔名?)|交換表)>	修訂：邵敏毅	
1.02	93.11.30	刪除有受文者的令及公告	修訂：邵敏毅	
1.03	94.01.06	修正機密等級變換改為機密等級變更	修訂：邵敏毅	
1.04	94.03.16	增加文件修訂履歷		

文書及檔案管理
電腦化作業規範

（九十三年修正版）

行政院秘書處

行政院研究發展考核委員會

交通部

行政院主計處

彙編

文書及檔案管理電腦化作業規範

目錄

文書及檔案管理電腦化作業規範
（九十三年修正版）

壹、前言

「文書及檔案管理電腦化作業規範」分二大部分，分別為作業規範及技術規範。作業規範是提供文書、檔案及資訊人員使用，技術規範是提供資訊人員開發公文電腦化作業系統使用。

貳、作業規範

一、作業目標

(一)訂定各機關之文書處理、檔案管理標準作業流程及共同性規範。

(二)以電腦輔助文書製作，提高品質，減少重覆繕打之時間、人力及可能造成之錯誤。

(三)藉電腦輔助文書流程管理，確實掌握文書處理流程及時效，並予以稽催管制。

(四)經由網路傳遞交換，大幅提***升***文書交換效率。

(五)以電腦輔助檔案管理，促進檔案目錄彙整公布，便於查詢調卷，提***升***決策***品質***效果與便利民眾申請應用。

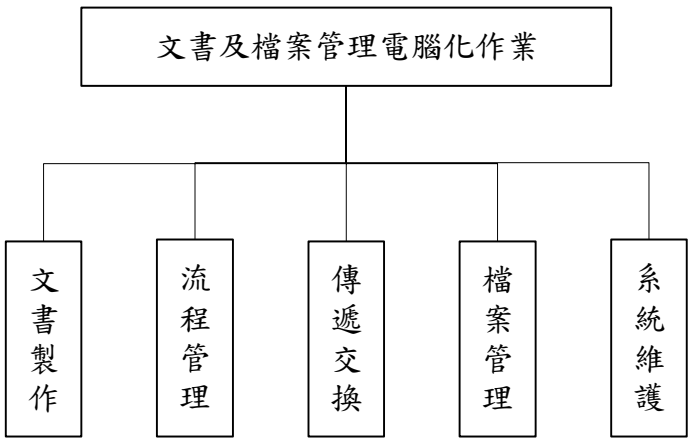
(六)***為提升發文收文處理效率，郵寄信封得以開窗式信封處理，便於郵寄文件自動化處理。***

二、作業範圍

本作業規範涵蓋文書製作、流程管理、傳遞交換、檔案管理，並涵蓋一般公文、訴願、陳情、人民申請、專案管制、民意代表質詢案件等之文書及檔案管理作業(但不含訴願、陳情、人民申請、專案管制等之實質處理)。

三、作業功能

文書處理及檔案管理電腦化作業包括從電腦輔助承辦人製作公文之文書製作、文書處理過程之流程管理、檔管介面、透過通信網路進行公文傳遞交換，另提供電腦化作業之檔案備份、檔案重整、作業權限設定等系統維護功能(如圖一)。



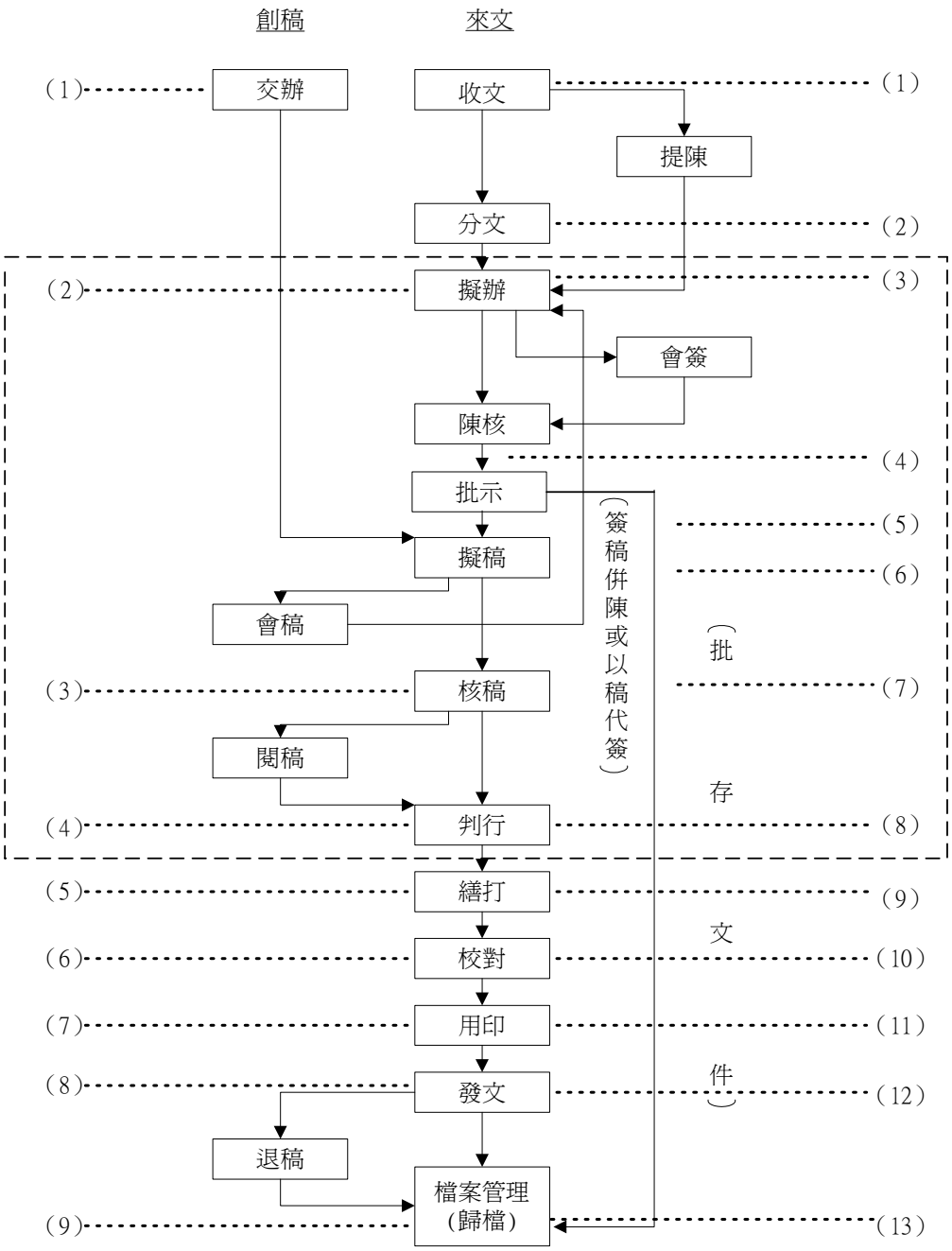
圖一　電腦化作業功能

以上五大作業項目之細部功能，如收發文時自動擷取相關公文字號、及印製各式文書及統計報表等，得視各機關實際需要自行訂定。

四、作業流程

現行文書處理流程如圖二所示。電腦化後，作業流程中若干決策點仍由人工作業判定，詳如圖三至圖六。

現行文書處理流程



圖二　現行文書處理流程

電腦化作業流程

(一)文書製作(詳圖三)

1、公文文書電子檔包括公文本文檔及附件檔。

2、已訂有標準格式之公文類型為：

- 令
- 函(書函、交辦(議)案件通知單、催辦案件通知單、移文單、機密文書機密等級變更或註銷建議單、機密文書機密等級變更或註銷通知單格式亦同)

  函稿格式同函，為函製作過程中所用，部分欄位資料如受文者、發文日期、發文字號等於發文時加列
- 公告
- 開會通知單
- 簽
- 簽稿會核單
- 會銜公文會辦單
- 公文時效統計
- *其他定型化表單*

  前述公文紙格式及組成欄位請參見「文書處理手冊」相關說明，製作範例亦請參見該手冊，惟公文時效統計請參見「文書流程管理手冊」。

3、公文附件類型分為文字檔、靜態圖形檔、工程圖檔、動畫檔、聲音檔、動態影像檔、紙本文件及無法電子化之實物等，其處理原則如下：

- 附件用紙尺寸除法令另有規定者外，以採用國家標準總號五號用紙尺度 A4 為原則。

- 已電子化之附件按「參之二、附件採用格式」傳送。
- 大量附件如：研究報告、書籍等，以於本文中敘明檔案儲存位置，如：網址，由收方按存取控制機制自行下載為原則；第一類公文電子交換之附件大小，以不超過 500K 為原則，超過者應改置於共用附件下載區供收文方下載使用。
- 紙本文件適合轉換成電子附件者，請參酌檔案管理局「機關檔案管理*資訊化作業*要點」辦理。
- 錄音帶、錄影帶等適合轉換成電子附件者，轉換後按「參之二、附件採用格式」傳送。
- 無法電子化之實體附件，連同公文本文仍以傳統方式傳送。

其他類型之附件或採用之格式在「參之二、附件採用格式」所列之外者，若要進行交換，以收文端能解讀該附件為原則，故發文端必須確定收文端已有或能從適當管道獲得呈現該附件檔之軟體工具。

4、文書製作時，公文及附件應編列頁碼。

5、為提升文書發文收文作業效率，公文呈現列印時，郵遞區號、地址、受文者、發文日期、發文字號應列於左上角左邊留白 23 公厘、上方留白 50 公厘區域，以上四欄資訊區域以橫座標 100 公厘、縱座標 45 公厘為顯示區域，且每欄資訊以一行為原則。

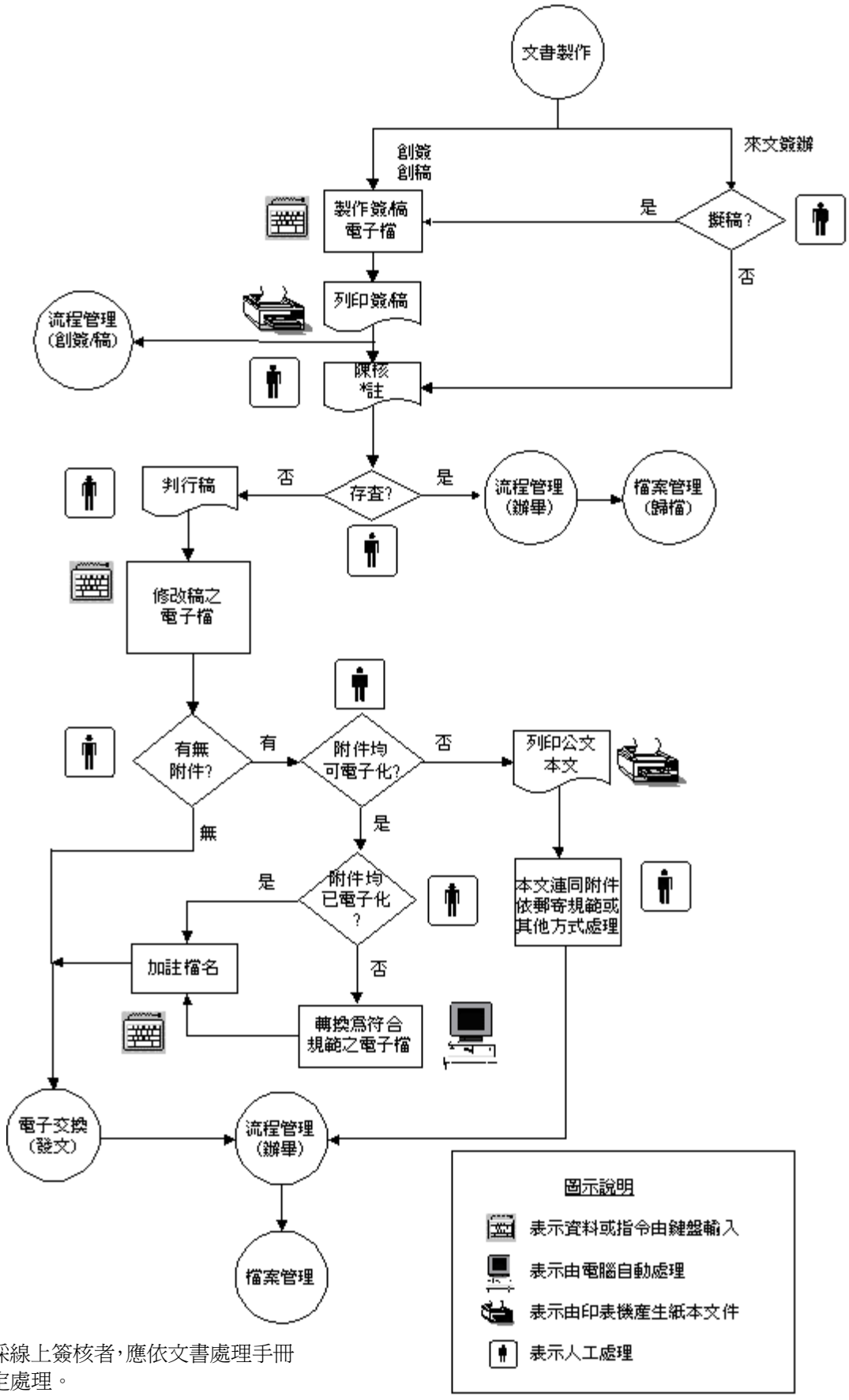
(二)流程管理(詳圖四)

1、收文部分經總收發／單位收發登錄即進入管制。創簽(稿)於開始陳核前登錄相關管理欄位後進入管制。

2、公文流程管理查詢，可劃分為承辦公文查詢(不論結案或未結案，均可用總收文號、單位收文號、創簽(稿)號、收文日期、來文機關、承辦人等條件做綜合查詢)、公文流程狀態查詢(如以公文字號)、及逾時未結公文查詢。

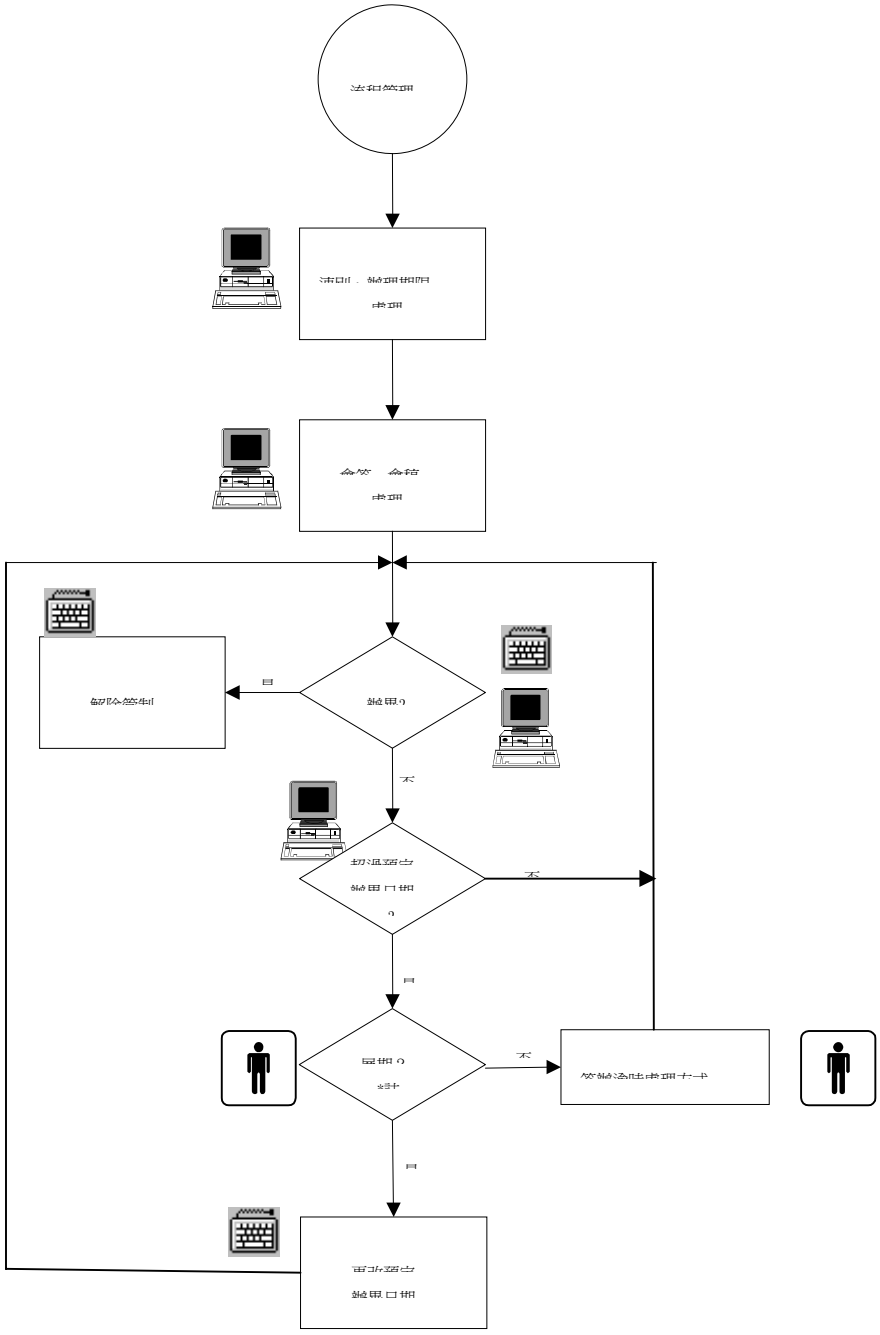
3、稽催管制應依分層管制原則，由各機關於期限內按規定格式，自動計算彙整機關上個月公文時效統計資料，以電子公務訊息郵遞等指定方式傳送主管機關。

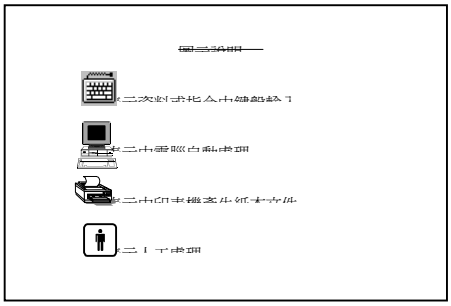
4、不同類別公文於流程管制時，應依文書流程管理手冊之規定，作為稽催之準據。



*註:陳核採線上簽核者,應依文書處理手冊等規定處理。

圖三：文書製作示意圖





*註：屆期係指事後屆期部分，催辦應依文書處理手冊規定辦理

圖四　文書流程管理流程示意圖

(三)傳遞交換(詳圖五及圖六)

1、執行機關公文電子交換作業，需產生符合共同傳輸檔案格式定義之電子公文檔案，進行後續處理，不需採原貌重現方式。共同傳輸檔案格式參見「參之一」。

2、機關公文傳遞交換處理機制分為三類：屬用第三者集中處理服務者(即公文電子交換中心)為第一類；屬點對點直接電子交換者為第二類；屬發文方登載電子公布欄者為第三類。三類機制之選用由各機關於進行傳遞交換作業時，自行考量、決定。

3、選用第一、二類處理機制者，須先產生含括執行電子交換機關資料之交換表。

4、基於機關公文電子交換應以電子認證方式辦理，第一、二類處理機制應含括：加解簽章、正副本分送、收方自動回復訊息等必備基本要項。其他如通信紀錄儲存、電子信封加密、機關群組管理、怠慢處理、存證等屬加值服務，由各機關視各公文性質或需求加列於執行電子交換之功能中。

5、各機關應設置電子公布欄，對於須發文通報週知之傳閱性公文，以登載電子公布欄，且於網際網路上可閱讀者為原則，並得輔以電子郵遞告之，或請有需用機關轉載應用，不另以書面通報。

6、單位收(發)文比照總收(發)文辦理。

7、文書單位於傳遞交換(發文)作業之前，增補總發文檔(或單位發文檔)相關欄位：總發文號、發文字號、發文日期、發文機關、公文本文檔名、附件說明、附件檔名。

8、文書單位於傳遞交換(收文)作業時，則可由電腦自動設定或擷取總收文檔(或單位收文檔)相關欄位：總收文號、來文字號、來文日期、來文機關、公文本文檔名、附件說明、附件檔名。公文及附件應由系統

自動加印頁碼及騎縫標識，***騎縫標識的位置應由系統隨機產生，不得為同一位置。***

9、會銜公文由主辦機關辦理傳送作業，惟在確實發文前之會稿或會銜作業仍依「文書處理手冊」相關規定辦理。

10、為以電子認證方式安全傳遞交換公文，並運用中文碼對照服務，進行傳遞交換處理時，有關傳遞交換作業規範、中文碼處理原則、與電子認證相關之政府憑證管理中心規範及智慧卡設備規範，參見「參之三」至「參之六」各節。

(四)檔案管理(詳圖七)

1、檔案管理作業應依據檔案法及相關法令規定辦理，其程序包括：點收、立案、編目、保管、檢調、清理、安全維護等事項。

2、檔案管理資訊化作業應與文書處理結合，避免相關欄位重覆建檔，並依「機關檔案管理資訊化作業要點」辦理。

3、各機關辦畢案件應於五日內歸檔，並依「檔案分類編案規範」及「檔案編目規範」之規定，完成案由（名）項、發（來）文者項、文件形式項、相關編號項、日期項、媒體型式項、檔案外觀項、關聯項、主題項及附註項之立案編目作業，並依規定將機關檔案電子目錄按季送交檔案中央主管機關彙整公布。

4、檔案保管作業包括檔案之整理、裝訂、分置及存放事項，並宜視需要進行微縮、掃描等檔案複製儲存作業。完成電子儲存之檔案全文應與檔案目錄連結，以利應用。

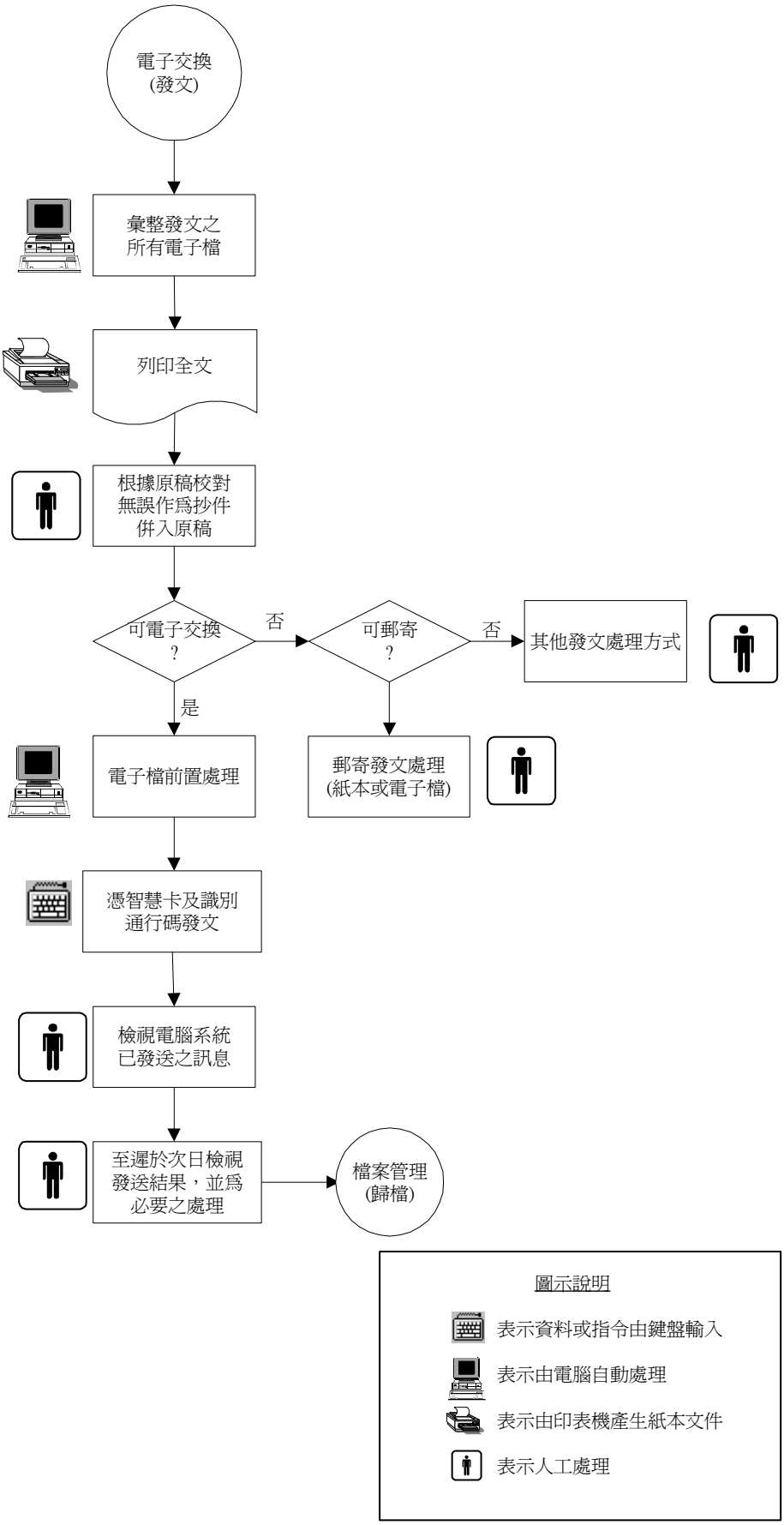
5、屆滿保存年限或屆臨移轉年限之檔案，應依「機關檔案保存年限及銷毀辦法」或「國家檔案移轉辦法」之規定編製檔案銷毀目錄或檔案移轉目錄，送請檔案中央主管機關審核通過後，辦理檔案銷毀或移轉。

6、前述第三點及第五點之檔案目錄、檔案銷毀目錄及檔案移轉目錄傳輸

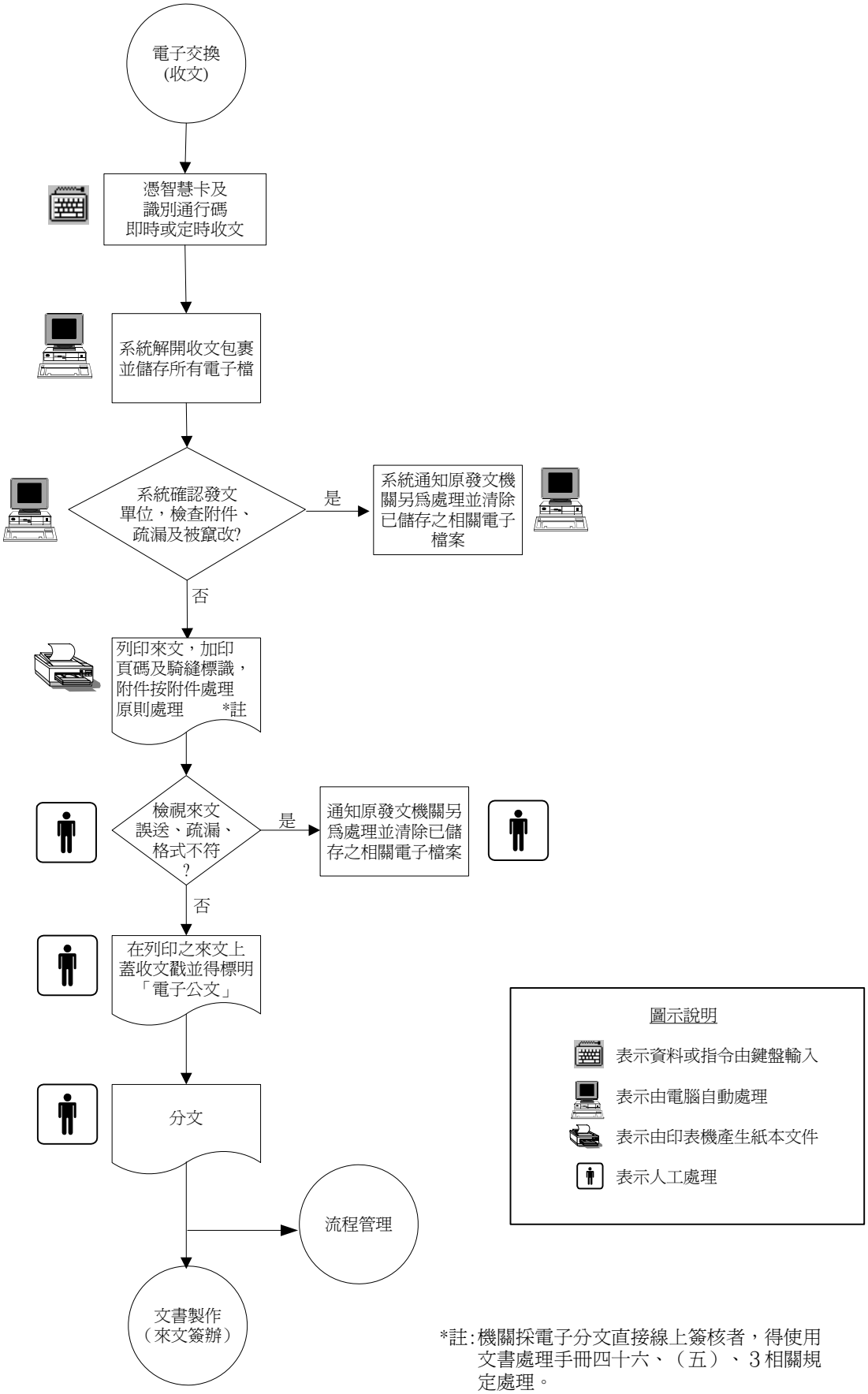
格式，依「機關檔案管理資訊化作業要點」附表三辦理。

7、檔案目錄應提供全文檢索查詢功能，以便利檔案檢調及應用事項。

8、檔案管理各項作業結果宜提供統計功能，以掌握檔案管理及應用狀態。

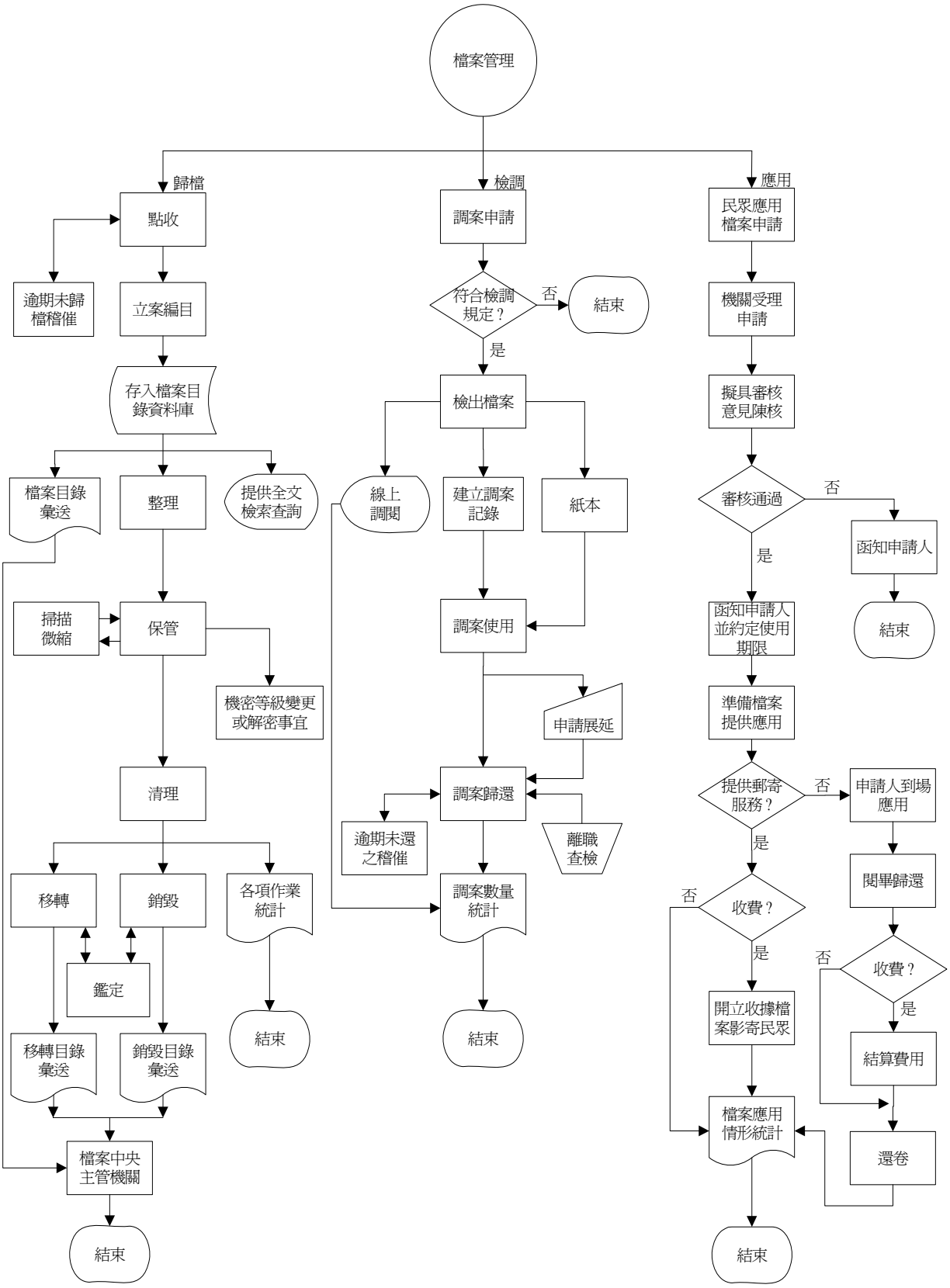


圖五　傳遞交換(發文)流程示意圖



*註:機關採電子分文直接線上簽核者，得使用文書處理手冊四十六、（五）、3 相關規定處理。

圖六　傳遞交換(收文)流程示意圖


檔案管理
歸檔
點收
逾期未歸
檔稽催
立案編目
存入檔案目
錄資料庫
檔案目錄
彙送
整理
提供全文
檢索查詢
掃描
微縮
保管
機密等級變更
或解密事宜
清理
移轉
銷毀
各項作業
統計
鑑定
移轉目錄
彙送
銷毀目錄
彙送
結束
檔案中央
主管機關
結束
檢調
調案申請
符合檢調
規定？
否
結束
是
檢出檔案
線上
調閱
建立調案
記錄
紙本
調案使用
申請展延
調案歸還
逾期未還
之稽催
離職
查檢
調案數量
統計
結束
應用
民眾應用
檔案申請
機關受理
申請
擬具審核
意見陳核
審核通過
否
函知申請人
結束
是
函知申請人
並約定使用
期限
準備檔案
提供應用
提供郵寄
服務？
否
申請人到場
應用
閱畢歸還
是
收費？
否
是
開立收據檔
案影寄民眾
檔案應用
情形統計
結束
收費？
否
是
結算費用
還卷

圖七　檔案管理示意圖

五、相關規定

- 檔案法及其相關法令規定
- 公文程式條例
- 事務管理規則中有關「文書處理」篇
- 機關公文電子交換作業辦法
- 文書處理手冊
- 文書流程管理手冊
- 其他機關公文電子交換作業相關法令

六、欄位定義

文書及檔案管理電腦化作業所應用之資料皆以「欄位」描述之，欄位之組成單元，最基本者為文字與數字之組合，如「字」、「文號」等，此等欄位本身並無應用上之意義，但可用以定義更高層次之欄位，故統稱為「基本欄位」。有些欄位如「發文字號」、「收文字號」、「來文字號」，雖然同是由「字」與「文號」組成，在應用上卻有特定之意義，此類欄位凡是與公文電子交換、檔案目錄彙送作業相關者，統稱為「交換用欄位」；其他用於文書及檔案管理電腦化作業或機關單位自訂以供內部使用之欄位，則歸類於「內部用欄位」，詳見表一至表三。表一所列之「基本欄位」及表二所列之「交換用欄位」因與公文電子交換、檔案目錄彙送有關，請按所列欄位名稱及屬性應用，至於表三之「內部用欄位」則僅供參考，個別機關若有需要，可比照既列欄位自行增訂。

交換用欄位資料項目內容空白時，收文機關應將欄位名稱依照文書處理手冊規定呈現。

各欄位之內容格式分內部及外部兩種：前者為便於電子儲存與處理，故明示其最大長度及資料型態；後者為便於閱讀，故無長度與資料型態之限制，即任何文字、數字及符號之組合皆可。其他各業務系統主管機關可參照基本及交換用欄位增訂，如民意代表質詢答復系統、監察

案件管理資訊系統、人事資訊系統等，惟應注意各業務系統與公文字號及公文時效管制之整合。

表一　基本欄位定義

註：　(1)　9 代表數字；　X 代表文字或數字；　( )內之數字代表字數,若為 n 代表不定長
　　(2)　“?”　表示可選用
　　(3)　“,”　表示連接
　　(4)　“*”　表示可不選用或多次選用
　　(5)　“+”　表示至少一次或多次選用
　　(6)　“|”　表示任取其一

欄位名稱	內部格式	說　　明
年月日	9(7)	中華民國〔0-999〕年,[1-12]月,〔1-31〕日
字	X(n)	不含年度
文號		(年度＋流水號＋支號)為 11 位***英數字半形(0123456789)***，其中年度為 3 位數字,流水號為 7 位數字,支號為 1 位英數字,流水號與支號可互用，使支號形同擴增(即支號擴增時擴增使用之流水號部分仍為數字，支號為英數字)；另若未使用支號則取消支號之 tag，在公文列印時支號前無須加印“｜”。
年度	X(3)	3 位數字,不足部分補零
流水號	X(7)	7 位數字,不足部分補零
支號	X(1)	支號供做雙稿、多稿公文用，得以 1－9、A－Z、a－z 方式表示。
月份	9(2)	[01-12]
星期	9(1)	[1-7]
時分	9(4)	時[00-23],分[00-59]
件數	9(n)	
天數	9(n)	
年數	9(n)	
公文頁數	X(4)	指該件公文總頁數，包括本文、簽陳及隨文裝訂附件
電話	X(n)	包括區號?,門號,分機?
聯絡方式	X(n)	可為傳真電話、聯絡人、聯絡電話或電子郵件資料，各機關視業務狀況彈性運用，若此欄位為空白時，欄位名稱不顯示。
地址	X(n)	
段落		文字?,條列*；其段名包含說明、辦法、擬辦、經過、原因、建議、請求、核示事項、依據、公告事項等，或亦可以空白取代段名
條列		文字?,條列*；段落內表示分項條列之序號，如”一、”
文字	X(n)	
姓名	X(n)	可前接機關全銜及單位名，另可併同職稱應用，如ＯＯＯ、Ｏ處長ＯＯ、ＯＯＯ處長、資管處Ｏ處長ＯＯ、行政院研考會Ｏ處長ＯＯ、行政院研考會資管處Ｏ處長ＯＯ
職稱	X(n)	
全銜	X(n)	
單位名	X(n)	可前接機關全銜
總稱	X(n)	行文群組，如行政院所屬內政部等一級機關
署名	X(n)	包括全銜?,單位名?,(姓名，職稱),代行之(姓名，職稱)

欄位名稱	內部格式	說　　明
機關代碼	X(10)	採人事行政局編訂之十位數機關代碼
單位代碼	X(7)	第一碼為 U，第二、三碼為內部一級單位碼，第四至七碼為 0;內部一級單位碼請洽各機關人事單位，依據銓敘部「各機關訂定職務說明書及辦理職務、歸系作業注意事項」職務編號說明原則填寫，若未編碼請自行編列，切勿重複。請參照本規範附錄二之四(一)規定
百分比	9(5)	整數三位,小數二位
平均日數	9(5)	整數三位,小數二位
收發處理本別	9(1)	代碼 ； 參見「貳之七、代碼清冊」
公文類別	X(1)	代碼 ； 參見「貳之七、代碼清冊」
函類別	X(1)	代碼 ； 參見「貳之七、代碼清冊」
速別	9(1)	代碼 ； 參見「貳之七、代碼清冊」
密等	X(1)	代碼 ； 參見「貳之七、代碼清冊」; 按國家機密保護法規辦理
解密條件***或保密期限***	X(40)	指機密檔案其機密等級解密條件之標示
附件	X(50)	有關附件之說明
含附件	X(n)	說明副本收受者是否含附件等處理,提供交換表單使用時內容為含附件或不含附件。 例：含附件：<含附件>含附件</含附件> 不含附件：<含附件>不含附件</含附件> 其他:無此 tag 則表含附件,其他非上述情形者表不含附件。
數位簽章	X(n)	有關數位簽章之說明
保存年限	X(2)	99 表示永久保存，?表示未判定，定期則以數字表示之
功能	X(1)	代碼 ； 參見「貳之七、代碼清冊」
應用限制	X(1)	代碼 ； 參見「貳之七、代碼清冊」
檔案來源別	X(1)	代碼 ； 參見「貳之七、代碼清冊」
年度號	X(4)	指該案卷(件)之年份號碼
分類號	X(20)	指公文依檔案分類表所載類目名稱之文、數字組合號碼
案次號	X(12)	指區分同類不同案次之號碼
卷次號	X(4)	指區分同案不同卷次之號碼
目次號	X(3)	指區分同一卷不同案件次序之號碼
媒體型式	X(1)	代碼 ； 參見「貳之七、代碼清冊」
檔案目錄傳送名稱	X(1)	代碼 ； 參見「貳之七、代碼清冊」
保存狀況	X(1)	代碼 ； 參見「貳之七、代碼清冊」
保存年限調整原因	X(20)	依機關檔案管理作業手冊相關規定辦理，採代碼方式，A：經微縮電子或其他方式儲存，B：仍具參考價值，C：其他
移轉註記	X(1)	代碼 ； 參見「貳之七、代碼清冊」

表二　交換用欄位定義

註：　(1)　“?”　表示可選用
　　(2)　“,”　表示連接
　　(3)　“*”　表示可不選用或多次選用
　　(4)　“+”　表示至少一次或多次選用
　　(5)　“|”　表示任取其一

欄位名稱	說　　明
發文機關	((全銜,機關代碼)|(單位名,(機關代碼,單位代碼)))
填表機關	(全銜,機關代碼?)
機關	(全銜,機關代碼?)
單位	(單位名,單位代碼?)
發文日期	(年月日)
填表日期	(年月日)
發文字號	((字,文號)|(文字)),最多 X(40),其中文字係提供各機關傳送舊有檔案時使用
單位發文字號	(字,文號)
交換表單	(((姓名,機關代碼,單位代碼?)|(單位名,機關代碼,單位代碼)|(全銜,機關代碼)),含附件？)+，若為正本，在交換表一律含附件
受文者	(((姓名,職稱?,機關代碼,單位代碼?)|(全銜,機關代碼)|(單位名,機關代碼,單位代碼?)),含附件?|交換表) 紙本發文時，受文者郵遞區號及地址可由資訊系統產生
正本	((姓名,職稱?)|全銜|單位名|總稱)+
副本	(((姓名,職稱?)|全銜|單位名|總稱),含附件?)*
聯絡人及電話	((姓名,職稱?),電話)+
主持人	(姓名,職稱?)+
機關首長	(姓名,職稱?)
單位主管	(姓名,職稱?)
填表人	(姓名,職稱?)
敬陳	(職稱,姓名?)+
出席者	((姓名,職稱?)|全銜|單位名|總稱)+
列席者	((姓名,職稱?)|全銜|單位名|總稱)*
密等及解密條件或保密期限	(密等,解密條件***或保密期限***)
開會時間	(年月日,星期,時分)
開會事由	文字
開會地點	文字
主旨	文字，最多 X(300)
備註	段落

欄位名稱	說　　明
附件數	件數
送達機關	(全銜,機關代碼?)
資料時間	(年度,月份)
發文者	((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)，最多 X(60)
來文者	((姓名,職稱?)|單位|機關)+ ，最多 X(60)
文別	(公文類別,函類別?) ，最多 X(2)
本別	收發處理本別，最多 X(1)
收文字號	((字,文號)|(文字)) ，最多 X(40)
來文字號	((字,文號)|(文字)) ，最多 X(40)
併案文號	((字,文號)|(文字)) ，最多 X(40)
電子檔案路徑	文字，指電子檔案之路徑，最多 X(50)
電子檔案名稱	文字，指電子檔案之檔名，最多 X(50)
辦畢日期	年月日，最多 X(7)
收文日期	年月日，最多 X(7)
來文日期	年月日，最多 X(7)
附件名稱	附件，最多 X(50)
附件媒體型式	媒體型式，最多 X(1)
承辦單位	單位名，最多 X(46)
承辦人	姓名，最多 X(20)
案由	文字，最多 X(300)，主旨或主旨摘由
並列案由	文字，最多 X(200)，外文案由
其他案由	文字，最多 X(300)，補充說明案由
案名	文字，最多 X(100)
相關案件	文字，最多 X(100)，相關案名、案由或檔號
主要發文者	((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)，最多 X(60)
主要來文者	((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)，最多 X(60)
次要發文者	((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)，最多 X(60)
次要來文者	((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)，最多 X(60)
發文者之補正	((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)，最多 X(60)
來文者之補正	((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)，最多 X(60)
調整後之保存年限	保存年限
核准銷毀文號	((字,文號)|(文字)) ，最多 X(40)
銷毀日期	年月日，最多 X(7)
解密日期	年月日，最多 X(7)
延長移轉屆滿日期	年月日，最多 X(7)
移轉日期	年月日，最多 X(7)
電子媒體編號	文字，最多 X(25)
微縮編號	文字，最多 X(25)
文件產生日期	((年月日)|文字)，最多 X(30)
數量	((公文頁數)|(件數))，最多 X(4)
計量單位	文字，最多 X(4)，如：頁、件、張、捲、幅或(其他)
附件數量	附件之數量，X(4)
附件單位	文字，最多 X(4)，如：頁、件、張、捲、幅或(其他)
類目名稱	文字，最多 X(40)
主題	文字，最多 X(50)，格式為(代碼)_文字
附註	文字，最多 X(50)，格式為(代碼)_文字

欄位名稱	說　　明
全宗號	(檔案來源別, 機關代碼)
檔號	(年度號, 分類號, 案次號, 卷次號, 目次號)
一般_本月新收件數	件數
一般_截至上月待辦件數	件數
一般_本月創稿數	件數
一般_本月應辦公文總數	件數
一般_六日內辦結	件數
一般_六日內辦結比例	百分比
一般_六至三十日辦結	件數
一般_六至三十日辦結比例	百分比
一般_三十日以上辦結	件數
一般_三十日以上辦結比例	百分比
一般_發文件數	件數
一般_存查件數	件數
一般_辦結件數總計	件數
一般_辦結件數總計比例	百分比
一般_發文平均使用日數	平均日數
一般_待辦件數	件數
一般_待辦件數比例	百分比
一般_未逾辦理期限待辦件數	件數
一般_已逾辦理期限待辦件數	件數
立委_本月新收件數	件數
立委_截至上月待辦件數	件數
立委_本月應辦件數	件數
立委_依限辦結件數	件數
立委_依限辦結件數比例	百分比
立委_逾限辦結件數	件數
立委_逾限辦結件數比例	百分比
立委_逾限五日內辦結件數	件數
立委_逾限五日內辦結件數比例	百分比
立委_逾限五至十日辦結件數	件數
立委_逾限五至十日辦結件數比例	百分比
立委_逾限十至十五日辦結件數	件數
立委_逾限十至十五日辦結件數比例	百分比
立委_逾限十五日以上辦結件數	件數
立委_逾限十五日以上辦結件數比例	百分比
立委_發文平均使用日數	平均日數
立委_待辦件數	件數
立委_待辦件數比例	百分比
立委_未逾辦理期限待辦件數	件數
立委_已逾辦理期限待辦件數	件數
申請_本月新收件數	件數
申請_截至上月待辦件數	件數
申請_本月應辦件數	件數
申請_依限辦結件數	件數

欄位名稱	說　　明
申請_依限辦結件數比例	百分比
申請_逾限辦結件數	件數
申請_逾限辦結件數比例	百分比
申請_辦結案件總數	合計
申請_辦結案件總數比例	百分比
申請_待辦件數	件數
申請_待辦件數比例	百分比
申請_未逾辦理期限待辦件數	件數
申請_已逾辦理期限待辦件數	件數
訴願_本月新收件數	件數
訴願_截至上月待辦件數	件數
訴願_本月應辦件數	件數
訴願_依限辦結件數	件數
訴願_依限辦結件數比例	百分比
訴願_逾限辦結件數	件數
訴願_逾限辦結件數比例	百分比
訴願_辦結案件總數	件數
訴願_辦結案件總數比例	百分比
訴願_待辦件數	件數
訴願_待辦件數比例	百分比
訴願_未逾辦理期限待辦件數	件數
訴願_已逾辦理期限待辦件數	件數
陳情_本月新收件數	件數
陳情_截至上月待辦件數	件數
陳情_本月應辦件數	件數
陳情_依限辦結件數	件數
陳情_依限辦結件數比例	百分比
陳情_六日內辦結件數	件數
陳情_六日內辦結件數比例	百分比
陳情_六至十五日辦結件數	件數
陳情_六至十五日辦結件數比例	百分比
陳情_十五至三十日辦結件數	件數
陳情_十五至三十日辦結件數比例	百分比
陳情_逾限辦結件數	件數
陳情_逾限辦結件數比例	百分比
陳情_辦結件數	件數
陳情_辦結件數比例	百分比
陳情_待辦件數	件數
陳情_待辦件數比例	百分比
陳情_未逾辦理期限待辦件數	件數
陳情_已逾辦理期限待辦件數	件數
專案_本月新增專案數	件數
專案_截至上月待辦專案數	件數
專案_本月應辦件數	件數
專案_依限辦結件數	件數
專案_逾限辦結件數	件數

欄位名稱	說　　明
專案_已辦結件數	件數
專案_已辦結件數比例	百分比
專案_待辦件數	件數
專案_待辦件數比例	百分比
專案_未逾辦理期限待辦專案數	件數
專案_已逾辦理期限待辦專案數	件數

表三　內部用欄位定義

註：　(1) “?” 表示可選用
(2) “,” 表示連接
(3) “*” 表示可不選用或多次選用
(4) “+” 表示至少一次或多次選用
(5) “|” 表示任取其一

欄位名稱	說　　明
收文機關	((全銜,機關代碼?) |(單位名,(機關代碼,單位代碼)?))
承辦單位	單位名
受會單位	單位名
協辦單位	單位名
調卷單位	單位名
分文日期	(年月日,時分?)
改分日期	(年月日,時分?)
延辦日期	(年月日,時分?)
收會時間	(年月日,時分?)
會畢時間	(年月日,時分?)
創簽稿日期	年月日
限辦日期	年月日
歸檔日期	年月日
調卷日期	年月日
應還日期	年月日
展延日期	年月日
催卷日期	年月日+
歸還日期	年月日
起日期	年月日
止日期	年月日
決行	(姓名,職稱?)
審核	(姓名,職稱?)
承辦	(姓名,職稱?)
會辦	(姓名,職稱?)
繕打	(姓名,職稱?)
校對	(姓名,職稱?)
監印	(姓名,職稱?)
調卷人	(姓名,職稱?)
創簽稿字號	(字,文號)
單位收文字號	(字,文號)
會核意見	段落
辦理情形	段落
會稿	(單位名,文字,(姓名,職稱?))
會簽	(單位名,文字,(姓名,職稱?))

欄位名稱	說　　明
續存	年數
展延天數	天數
會辦機關	(全銜, 決行, 審核, 承辦, 會辦, 收文日期, 收文字號, 發文日期, 發文字號)
主辦機關	(全銜, 決行, 審核, 承辦, 會辦, 收文日期, 收文字號, 發文日期, 發文字號)
電子交換處理機制類別	可依據機關需要區分第一、二、三類
戳印	有關戳印之說明

七、代碼清冊

(一)公文類別

代　碼	內　　容
1	令
2	函(詳下(二)說明)
3	公告
4	開會通知單
5	簽
6	簽稿會核單
7	會銜公文會辦單
8	公文時效統計
9	呈
A	咨
Z	其他(詳下(三)說明)

(二)函類別

代　碼	內　　容
1	函
2	書函
3	交辦案件通知單
4	交議案件通知單
5	催辦案件通知單
6	移文單
7	機密文書機密等級變更或註銷建議單
8	機密文書機密等級變更或註銷通知單

(三)其他類別

代碼	內容
1	公務電話紀錄
2	手令或手諭
3	報告
4	箋函或便簽
5	聘書
6	證明書
7	證書或執照
8	契約書
9	提案
A	紀錄
B	節略

代碼	內容
C	說帖
D	代電
E	*原本*
F	*判決書*
G	*起訴書*
H	*處分書*
I	*定型化表單*
Z	非屬以上各類文書

(四)速別

代　碼	內　　容
1	普通件
2	速件
3	最速件

(五)機密等級

代　碼	內　　容
1	普通
2	密
3	機密
4	極機密
5	絕對機密

(六)收發處理本別

代　碼	內　　容
1	正本
2	副本
3	抄本
4	影本
5	譯本
A	稿本
B	草稿
C	定稿
D	底圖
E	藍圖

(七)機關代碼

採行政院人事行政局所編訂之「機關暨學校代碼」。

(八)單位代碼

請參照第 17 頁規定。

(九)檔案來源別

代　碼	內　　容
A	人事行政局機關學校代碼
B	人事行政局代碼本未列之政府機關
C	人事行政局代碼本未列之私人團體
D	個人檔案

(十)功能

代　碼	內　　容
N	新增
M	修改
D	刪除

(十一)應用限制

代　碼	內　　容
Y	開放
N	不開放
R	限制開放

(十二)媒體型式

代　碼	內　　容
1	紙本
2	底片
3	微縮片
4	幻燈片
5	磁片
6	磁帶
7	光碟
8	錄音帶
9	錄影帶
A	工程圖
B	照片
C	圖表
D	電影片
E	地圖
F	*硬式磁碟*

代　碼	內　　容
Z	其他

(十三)檔案目錄傳送名稱

代　碼	內　　容
A	案卷之檔案目錄彙送
B	案卷之檔案移轉目錄
C	案件之檔案目錄彙送
D	案件之檔案銷毀目錄
F	案卷之檔案銷毀目錄
G	案卷之擬移轉目錄
H	案卷之擬銷毀目錄
P	案件之擬移轉目錄
V	案件之擬銷毀目錄
T	案件之檔案移轉目錄

(十四)保存狀況

代　碼	內　　容
A	良好
B	蟲蛀霉蝕
C	檔案散落
D	檔案破損
E	不在架上
F	無法修護
G	遺失
Z	其他

(十五)移轉註記

代　碼	內　　容
1	移轉
2	原機關續管
3	受託保管
4	不移轉
5	延長移轉期限

其他有需用之代碼或未盡事宜由相關主管機關另訂之。

參、技術規範

文書處理及檔案管理之電腦化作業，必須有共通規範使開放環境中任何電腦平台(包括電腦設備、作業系統、應用軟體等)都知道如何處理這些文書，管理這些檔案，而共通規範之基礎就是機器和人類都可以辨識之公文電子交換共同傳輸檔案格式。共同檔案格式既然要機器能夠辨識，其定義就必須精簡明確，最有效之作法即為利用國際標準、國家標準或業界標準作為定義之工具，本技術規範即參考比較各種標準而研訂。有了明確共通規範，各界即能應用或開發符合共通規範之公文電腦化作業系統。

決定各種標準是否適用於定義公文電子交換之共同傳輸檔案格式，係參考以下十二個評估準則：

- 規範共識程度
- 產品可獲得性
- 規範穩定性
- 規格完整性
- 技術成熟性
- 業界使用狀況
- 使用自由度
- 作業之效率性
- 資料之再用性
- 格式之可擴充性
- 系統之整合性
- 文件之呈現方式

經過審慎評估，決定採用 XML（eXtensible Markup Language, 可擴充之標示語言）以定義公文電子交換之共同傳輸檔案格式，並據以制定公文電子交換和處理之技術規範。

一、共同傳輸檔案格式

電子公文之共同傳輸檔案格式係以「貳之六、欄位定義」為基礎，以 XML 語法定義出「基本標籤集」、「交換用標籤集」及「內部用標籤集」，再用「基本標籤集」與「交換用標籤集」為基礎，以 XML 語法定義出各種制式公文類型內容結構，茲舉數例說明之：

例一、<!ELEMENT 字 (#PCDATA)>
表示「字」是由文字、數字和特殊符號任意組合而成,其中不含年度敘述。

例二、<!ELEMENT 文號 (年度,流水號,支號?)>
表示「文號」係由「年度」、「流水號」及「支號」結合而成，且「支號」可有可無。

例三、<!ELEMENT 受文者 ((姓名,職稱?,機關代碼,單位代碼?)|(全銜,機關代碼)|(單位名,機關代碼,單位代碼)|交換表)
表示「受文者」可以是「姓名,職稱?,機關代碼,單位代碼?」、「全銜,機關代碼」、「單位名,機關代碼,單位代碼」或「交換表」中之任何一種。

例四、<!ELEMENT 條列 (項目*)>
表示「項目」在「條列」中可以完全不出現，也可出現多次。

例五、<!ELEMENT 主持人 ((姓名,職稱?)+)>
表示「(姓名,職稱?)」在「主持人」中可以重覆出現，且至少須出現一次。

例六、<!ELEMENT 速別 EMPTY>
表示「速別」不標示任何內容，但標籤本身具有意義。

例七、<!ATTLIST 速別 代碼 (普通件|速件|最速件) 普通件>
「ATTLIST」是個關鍵詞，表示「速別」具有「代碼」屬性，「代碼」可以是「普通件」、「速件」或「最速件」，其預設值則是「普通件」。

例八、<!ELEMENT 附件 (文字,附件檔名?)>
<!ELEMENT 附件檔名 EMPTY>
<!ATTLIST 附件檔名 附件名 ENTITIES #REQUIRED>

表示「附件」之說明為文字和數字組合，且以「附件名」這個屬性作補充說明。「附件名」屬性值是附件在收發文兩端通用之附件名稱，必須註明，而且可以有多個。至於附件在發文端電子公文系統中之檔案名和檔案型態則是以「ENTITY」和「NOTATION」宣告之，請參見「參之二、附件採用格式」中之舉例說明。

例九、<!ELEMENT 數位簽章 EMPTY>
<!ATTLIST 數位簽章 簽章名 ENTITY #IMPLIED>

表示「數位簽章」以「簽章名」這個屬性作補充說明。「簽章名」屬性值是簽章在收發文兩端通用之簽章名稱，連同相關簽章檔案都可以由系統提供而毋須註明。

例十、<!ENTITY % 基本標籤 SYSTEM "基本標籤.ent" >
%基本標籤;
表示「基本標籤」是一個巨集，其內容在一個名為「基本標籤.ent」檔案中。呼叫「%基本標籤;」即可將之展開。又「交換用標籤」及「內部用標籤」之表示方法亦同。

公文及檔案管理標籤集

==========

```
<?xml version="1.0" encoding="BIG5"?>
<!--  公文標籤集（基本層）    93_基本標籤.ent   1999.12.1  修改日期:2004.1.1  -->

<!ELEMENT  年月日                  (#PCDATA)>
<!--  例:<年月日>中華民國九十年十二月一日</年月日>  -->

<!ELEMENT  字                      (#PCDATA)>
<!ELEMENT  文號                    (年度,流水號,支號?)>
<!ELEMENT  年度                    (#PCDATA)>
<!ELEMENT  流水號                  (#PCDATA)>
<!ELEMENT  支號                    (#PCDATA)>

<!ELEMENT  月份                    (#PCDATA)>

<!ELEMENT  星期                    (#PCDATA)>
<!--  例:<星期>三</星期>  -->

<!ELEMENT  時分                    (#PCDATA)>
<!--  例:<時分>八時三十分</時分>  -->
<!--  例:<時分>上午八時三十分</時分>  -->
<!--  例:<時分>下午二十時三十分</時分>  -->

<!ELEMENT  件數                    (#PCDATA)>
<!ELEMENT  天數                    (#PCDATA)>
<!ELEMENT  年數                    (#PCDATA)>
<!ELEMENT  公文頁數                (#PCDATA)>

<!ELEMENT  電話                    (#PCDATA)>
<!ELEMENT  聯絡方式                (#PCDATA)>
<!ELEMENT  地址                    (#PCDATA)>

<!ELEMENT  段落                    (文字?,條列*) >
<!ATTLIST  段落  段名   CDATA   "">
<!ELEMENT  條列                    (文字?,條列*)>
<!ATTLIST  條列  序號   CDATA   "">
<!ELEMENT  文字                    (#PCDATA) >

<!ELEMENT  姓名                    (#PCDATA)>
<!ELEMENT  職稱                    (#PCDATA)>
<!ELEMENT  全銜                    (#PCDATA)>
<!ELEMENT  單位名                  (#PCDATA)>
<!ELEMENT  總稱                    (#PCDATA)>
<!ELEMENT  署名                    (#PCDATA)>
<!ELEMENT  機關代碼                (#PCDATA)>
<!ELEMENT  單位代碼                (#PCDATA)>

<!ELEMENT  百分比                  (#PCDATA)>

<!ELEMENT  平均日數                (#PCDATA)>
```

```
<!ELEMENT  收發處理本別        EMPTY>
<!ATTLIST  收發處理本別  代碼     (正本|副本|抄本|影本|譯本|稿本|草稿|定稿|底圖|藍圖)  "正本">


<!ELEMENT  公文類別            EMPTY>
<!ATTLIST  公文類別  代碼   (令|函|公告|開會通知單|簽|簽稿會核單|會銜公文會辦單|
                            公文時效統計|其他)  "函">

<!ELEMENT  函類別              EMPTY>
<!ATTLIST  函類別    代碼   (函|書函|交辦案件通知單|交議案件通知單|
                            催辦案件通知單|移文單|
                            機密文書機密等級變更或註銷建議單|
                            機密文書機密等級變更或註銷通知單)      "函">
<!ELEMENT  其他類別            EMPTY>
<!ATTLIST  其他類別    代碼   (公務電話紀錄|手令或手諭|報告|箋函或便簽|聘書|證明書|證書或執照|契
                            約書|提案|紀錄|節略|說帖|代電 | 原本|判決書|起訴書|處分書|定型化表單)
                                 "公務電話紀錄">

<!ELEMENT  速別                EMPTY>
<!ATTLIST  速別  代碼   (普通件|速件|最速件)   "普通件">

<!ELEMENT  密等                EMPTY>
<!ATTLIST  密等  代碼   (普通|密|機密|極機密|絕對機密)   "普通">
<!ELEMENT  解密條件或保密期限      (#PCDATA)>

<!ELEMENT  附件          (文字,附件檔名?)>
<!ELEMENT  附件檔名        EMPTY>
<!ATTLIST  附件檔名  附件名    ENTITIES  #REQUIRED>

<!ELEMENT  含附件        (#PCDATA)>
<!ELEMENT  內含本文與附件之可攜式文件檔名 (#PCDATA)>

<!ELEMENT  數位簽章            EMPTY>
<!ATTLIST  數位簽章  簽章名    ENTITY  #IMPLIED>

<!ELEMENT  保存年限            (#PCDATA)>

<!ELEMENT  功能                EMPTY>
<!ATTLIST  功能  代碼   (新增|修改|刪除)   "新增">
<!ELEMENT  應用限制            EMPTY>
<!ATTLIST  應用限制  代碼   (開放|不開放|限制開放)   "開放">
<!ELEMENT  檔案來源別          EMPTY>
<!ATTLIST  檔案來源別  代碼   (人事行政局機關學校代碼|人事行政局代碼本未列之政府機關|人事行政局
                            代碼本未列之私人團體|個人檔案)   "人事行政局機關學校代碼">
<!ELEMENT  年度號              (#PCDATA)>
<!ELEMENT  分類號              (#PCDATA)>
<!ELEMENT  案次號              (#PCDATA)>
<!ELEMENT  卷次號              (#PCDATA)>
<!ELEMENT  目次號              (#PCDATA)>
<!ELEMENT  媒體型式            EMPTY>
<!ATTLIST  媒體型式  代碼   (紙本|底片|微縮片|幻燈片|磁片|磁帶|光碟|錄音帶|錄影帶|工程圖|照片|圖
                            表|電影片|地圖|硬式磁碟|其他)   "紙本">
```

<!ELEMENT 檔案目錄傳送名稱 EMPTY>
<!ATTLIST 檔案目錄傳送名稱 代碼 （*案卷之檔案目錄彙送|案卷之檔案移轉目錄|案件之檔案目錄彙送|案卷之檔案銷毀目錄|案卷之擬移轉目錄|案卷之擬銷毀目錄|案件之擬移轉目錄|案件之擬銷毀目錄|案件之檔案銷毀目錄）"案件之檔案目錄彙送"*>
<!ELEMENT 保存狀況 EMPTY>
<!ATTLIST 保存狀況 代碼（良好|蟲蛀霉蝕|檔案散落|檔案破損|不在架上|無法修護|遺失|其他） "良好">
<!ELEMENT 保存年限調整原因 (#PCDATA)>
<!ELEMENT 移轉註記 EMPTY>
<!ATTLIST 移轉註記 代碼 （移轉|原機關續管|受託保管|不移轉|延長移轉期限） "移轉">

註：為便於電子交換處理，轉換為 XML 格式之年月日及時分，請以國字小寫全形方式處理。

```
<?xml version="1.0" encoding="BIG5"?>
<!--  公文標籤集（交換用）  93_交換用標籤.ent    1999.12.1  修改日期:2004.7.1  -->

<!ELEMENT  發文機關          ((全銜,機關代碼)|(單位名,(機關代碼,單位代碼)))>
<!ELEMENT  填表機關          (全銜,機關代碼?)>
<!ELEMENT  機關              (全銜,機關代碼?)>
<!ELEMENT  單位              (單位名,單位代碼?)>

<!ELEMENT  發文日期          (年月日)>
<!ELEMENT  填表日期          (年月日)>

<!ELEMENT  發文字號          ((字,文號)|(文字)>
<!ELEMENT  單位發文字號      (字,文號)>

<!ELEMENT  受文者        ((((姓名,職稱?,機關代碼,單位代碼?)|(全銜,機關代碼)|(單位名,機關代
                          碼,單位代碼)),含附件?,內含本文與附件之可攜式文件檔名?)|交換表)>

<!ELEMENT  交換表            (#PCDATA)>
<!ATTLIST  交換表  交換表單   ENTITY  #REQUIRED>

<!ELEMENT  正本              ((姓名,職稱?)|全銜|單位名|總稱)+>
<!ELEMENT  副本              (((姓名,職稱?)|全銜|單位名|總稱),含附件?)*>

<!ELEMENT  聯絡人及電話((姓名,職稱?),電話)+>

<!ELEMENT  主持人            ((姓名,職稱?)+)>
<!ELEMENT  機關首長          (姓名,職稱?)>
<!ELEMENT  單位主管          (姓名,職稱?)>
<!ELEMENT  填表人            (姓名,職稱?)>
<!ELEMENT  敬陳              ((職稱,姓名?)+)>

<!ELEMENT  出席者            ((姓名,職稱?)|全銜|單位名|總稱)+>
<!ELEMENT  列席者            ((姓名,職稱?)|全銜|單位名|總稱)*>

<!ELEMENT  密等及解密條件或保密期限  (密等,解密條件或保密期限)>

<!ELEMENT  開會時間          (年月日,星期,時分)>

<!ELEMENT  開會事由          (文字)>
<!ELEMENT  開會地點          (文字)>
<!ELEMENT  主旨              (文字)>
<!ELEMENT  備註              (段落)>

<!ELEMENT  附件數            (件數)>

<!ELEMENT  送達機關          (全銜,機關代碼?)>
<!ELEMENT  資料時間          (年度,月份)>

<!ELEMENT  發文者            ((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)>
<!ELEMENT  來文者            ((姓名,職稱?)|單位|機關)>
<!ELEMENT  文別              (公文類別,函類別?) >
```

```
<!ELEMENT  本別              (收發處理本別)>
<!ELEMENT  收文字號          ((字,文號)|(文字))>
<!ELEMENT  來文字號          ((字,文號)|(文字))>
<!ELEMENT  併案文號          ((字,文號)|(文字))>
<!ELEMENT  電子檔案路徑      (文字)>
<!ELEMENT  電子檔案名稱      (文字)>
<!ELEMENT  辦畢日期          (年月日)>
<!ELEMENT  收文日期          (年月日)>
<!ELEMENT  來文日期          (年月日)>
<!ELEMENT  附件名稱          (附件)>
<!ELEMENT  附件媒體型式      (媒體型式)>
<!ELEMENT  承辦單位          (單位名)>
<!ELEMENT  承辦人            (姓名)>
<!ELEMENT  案由              (文字)>
<!ELEMENT  並列案由          (文字)>
<!ELEMENT  其他案由          (文字)>
<!ELEMENT  案名              (文字)>
<!ELEMENT  相關案件          (文字)>
<!ELEMENT  主要發文者        ((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)>
<!ELEMENT  主要來文者        ((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)>
<!ELEMENT  次要發文者        ((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)>
<!ELEMENT  次要來文者        ((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)>
<!ELEMENT  發文者之補正      ((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)>
<!ELEMENT  來文者之補正      ((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?)|姓名)>
<!ELEMENT  調整後之保存年限  (保存年限)>
<!ELEMENT  核准銷毀文號      ((字,文號)|(文字))>
<!ELEMENT  銷毀日期          (年月日)>
<!ELEMENT  解密日期          (年月日)>
<!ELEMENT  延長移轉屆滿日期  (年月日)>
<!ELEMENT  移轉日期          (年月日)>
<!ELEMENT  電子媒體編號      (文字)>
<!ELEMENT  微縮編號          (文字)>
<!ELEMENT  文件產生日期      ((年月日)|文字)>
<!ELEMENT  數量              ((公文頁數)|(件數))>
<!ELEMENT  計量單位          (文字)>
<!ELEMENT  附件數量          (件數)>
<!ELEMENT  附件單位          (文字)>
<!ELEMENT  類目名稱          (文字)>
<!ELEMENT  主題              (文字)>
<!ELEMENT  附註              (文字)>

<!ELEMENT  全宗號            (檔案來源別,機關代碼)>
<!ELEMENT  檔號              (年度號,分類號,案次號,卷次號,目次號)>

<!ELEMENT  一般_本月新收件數          (件數)>
<!ELEMENT  一般_截至上月待辦件數      (件數)>
<!ELEMENT  一般_本月創稿數            (件數)>
<!ELEMENT  一般_本月應辦公文總數      (件數)>
<!ELEMENT  一般_六日內辦結            (件數)>
<!ELEMENT  一般_六日內辦結比例        (百分比)>
<!ELEMENT  一般_六至三十日辦結        (件數)>
<!ELEMENT  一般_六至三十日辦結比例    (百分比)>
```

<!ELEMENT 一般_三十日以上辦結 (件數)>
<!ELEMENT 一般_三十日以上辦結比例 (百分比)>
<!ELEMENT 一般_發文件數 (件數)>
<!ELEMENT 一般_存查件數 (件數)>
<!ELEMENT 一般_辦結件數總計 (件數)>
<!ELEMENT 一般_辦結件數總計比例 (百分比)>
<!ELEMENT 一般_發文平均使用日數 (平均日數)>
<!ELEMENT 一般_待辦件數 (件數)>
<!ELEMENT 一般_待辦件數比例 (百分比)>
<!ELEMENT 一般_未逾辦理期限待辦件數 (件數)>
<!ELEMENT 一般_已逾辦理期限待辦件數 (件數)>

<!ELEMENT 立委_本月新收件數 (件數)>
<!ELEMENT 立委_截至上月待辦件數 (件數)>
<!ELEMENT 立委_本月應辦件數 (件數)>
<!ELEMENT 立委_依限辦結件數 (件數)>
<!ELEMENT 立委_依限辦結件數比例 (百分比)>
<!ELEMENT 立委_逾限辦結件數 (件數)>
<!ELEMENT 立委_逾限辦結件數比例 (百分比)>
<!ELEMENT 立委_逾限五日內辦結件數 (件數)>
<!ELEMENT 立委_逾限五日內辦結件數比例 (百分比)>
<!ELEMENT 立委_逾限五至十日辦結件數 (件數)>
<!ELEMENT 立委_逾限五至十日辦結件數比例 (百分比)>
<!ELEMENT 立委_逾限十至十五日辦結件數 (件數)>
<!ELEMENT 立委_逾限十至十五日辦結件數比例 (百分比)>
<!ELEMENT 立委_逾限十五日以上辦結件數 (件數)>
<!ELEMENT 立委_逾限十五日以上辦結件數比例 (百分比)>
<!ELEMENT 立委_發文平均使用日數 (平均日數)>
<!ELEMENT 立委_待辦件數 (件數)>
<!ELEMENT 立委_待辦件數比例 (百分比)>
<!ELEMENT 立委_未逾辦理期限待辦件數 (件數)>
<!ELEMENT 立委_已逾辦理期限待辦件數 (件數)>

<!ELEMENT 申請_本月新收件數 (件數)>
<!ELEMENT 申請_截至上月待辦件數 (件數)>
<!ELEMENT 申請_本月應辦件數 (件數)>
<!ELEMENT 申請_依限辦結件數 (件數)>
<!ELEMENT 申請_依限辦結件數比例 (百分比)>
<!ELEMENT 申請_逾限辦結件數 (件數)>
<!ELEMENT 申請_逾限辦結件數比例 (百分比)>
<!ELEMENT 申請_辦結案件總數 (件數)>
<!ELEMENT 申請_辦結案件總數比例 (百分比)>
<!ELEMENT 申請_待辦件數 (件數)>
<!ELEMENT 申請_待辦件數比例 (百分比)>
<!ELEMENT 申請_未逾辦理期限待辦件數 (件數)>
<!ELEMENT 申請_已逾辦理期限待辦件數 (件數)>

<!ELEMENT 訴願_本月新收件數 (件數)>
<!ELEMENT 訴願_截至上月待辦件數 (件數)>
<!ELEMENT 訴願_本月應辦件數 (件數)>
<!ELEMENT 訴願_依限辦結件數 (件數)>
<!ELEMENT 訴願_依限辦結件數比例 (百分比)>

<!ELEMENT 訴願_逾限辦結件數 (件數)>
<!ELEMENT 訴願_逾限辦結件數比例 (百分比)>
<!ELEMENT 訴願_辦結案件總數 (件數)>
<!ELEMENT 訴願_辦結案件總數比例 (百分比)>
<!ELEMENT 訴願_待辦件數 (件數)>
<!ELEMENT 訴願_待辦件數比例 (百分比)>
<!ELEMENT 訴願_未逾辦理期限待辦件數 (件數)>
<!ELEMENT 訴願_已逾辦理期限待辦件數 (件數)>

<!ELEMENT 陳情_本月新收件數 (件數)>
<!ELEMENT 陳情_截至上月待辦件數 (件數)>
<!ELEMENT 陳情_本月應辦件數 (件數)>
<!ELEMENT 陳情_依限辦結件數 (件數)>
<!ELEMENT 陳情_依限辦結件數比例 (百分比)>
<!ELEMENT 陳情_六日內辦結件數 (件數)>
<!ELEMENT 陳情_六日內辦結件數比例 (百分比)>
<!ELEMENT 陳情_六至十五日辦結件數 (件數)>
<!ELEMENT 陳情_六至十五日辦結件數比例 (百分比)>
<!ELEMENT 陳情_十五至三十日辦結件數 (件數)>
<!ELEMENT 陳情_十五至三十日辦結件數比例 (百分比)>
<!ELEMENT 陳情_逾限辦結件數 (件數)>
<!ELEMENT 陳情_逾限辦結件數比例 (百分比)>
<!ELEMENT 陳情_辦結件數 (件數)>
<!ELEMENT 陳情_辦結件數比例 (百分比)>
<!ELEMENT 陳情_待辦件數 (件數)>
<!ELEMENT 陳情_待辦件數比例 (百分比)>
<!ELEMENT 陳情_未逾辦理期限待辦件數 (件數)>
<!ELEMENT 陳情_已逾辦理期限待辦件數 (件數)>

<!ELEMENT 專案_本月新增專案數 (件數)>
<!ELEMENT 專案_截至上月待辦專案數 (件數)>
<!ELEMENT 專案_本月應辦件數 (件數)>
<!ELEMENT 專案_依限辦結件數 (件數)>
<!ELEMENT 專案_逾限辦結件數 (件數)>
<!ELEMENT 專案_已辦結件數 (件數)>
<!ELEMENT 專案_已辦結件數比例 (百分比)>
<!ELEMENT 專案_待辦件數 (件數)>
<!ELEMENT 專案_待辦件數比例 (百分比)>
<!ELEMENT 專案_未逾辦理期限待辦專案數 (件數)>
<!ELEMENT 專案_已逾辦理期限待辦專案數 (件數)>

表單之內容結構

```
<?xml version="1.0" encoding="BIG5"?>
<!-- 93_roster.dtd  交換表  2004.7.1  -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "93_交換用標籤.ent" >
%交換用標籤;
<!ELEMENT  交換表單  (((姓名,職稱?,機關代碼,單位代碼?) |
                       (單位名,機關代碼,單位代碼) |
                       (全銜,機關代碼)),含附件?,內含本文與附件之可攜式文件檔名?)+>
<!/ 交換表單>
```

```
<?xml version="1.0" encoding="BIG5"?>
<!--      公文標籤集（內部用）    93_內部用標籤.ent    1999.12.1  修改日期:2004.7.1 -->

<!ELEMENT  收文機關     ((全銜,機關代碼?)|(單位名,(機關代碼,單位代碼)?))>

<!ELEMENT  承辦單位     (單位名)>
<!ELEMENT  受會單位     (單位名)>
<!ELEMENT  協辦單位     (單位名)>
<!ELEMENT  調卷單位     (單位名)>

<!ELEMENT  分文日期     (年月日,時分?)>
<!ELEMENT  改分日期     (年月日,時分?)>
<!ELEMENT  延辦日期     (年月日,時分?)>
<!ELEMENT  收會時間     (年月日,時分?)>
<!ELEMENT  會畢時間     (年月日,時分?)>

<!ELEMENT  創簽稿日期   (年月日)>
<!ELEMENT  限辦日期     (年月日)>
<!ELEMENT  歸檔日期     (年月日)>
<!ELEMENT  調卷日期     (年月日)>
<!ELEMENT  應還日期     (年月日)>
<!ELEMENT  展延日期     (年月日)>
<!ELEMENT  催卷日期     (年月日+)>
<!ELEMENT  歸還日期     (年月日)>
<!ELEMENT  起日期       (年月日)>
<!ELEMENT  止日期       (年月日)>

<!ELEMENT  決行         (姓名,職稱?)>
<!ELEMENT  審核         (姓名,職稱?)>
<!ELEMENT  承辦         (姓名,職稱?)>
<!ELEMENT  會辦         (姓名,職稱?)>
<!ELEMENT  繕打         (姓名,職稱?)>
<!ELEMENT  校對         (姓名,職稱?)>
<!ELEMENT  監印         (姓名,職稱?)>
<!ELEMENT  調卷人       (姓名,職稱?)>

<!ELEMENT  創簽稿字號   (字,文號)>
<!ELEMENT  單位收文字號 (字,文號)>

<!ELEMENT  案情摘要     (文字)>

<!ELEMENT  會核意見     (段落)>
<!ELEMENT  辦理情形     (段落)>

<!ELEMENT  會稿         (單位,文字,(姓名,職稱?))>
<!ELEMENT  會簽         (單位,文字,(姓名,職稱?))>

<!ELEMENT  續存         (年數)>

<!ELEMENT  展延天數     (天數)>

<!ELEMENT  會辦機關(全銜,決行,審核,承辦,會辦,收文日期,收文字號,發文日期,發文字號)>
```

<!ELEMENT 主辦機關(全銜,決行,審核,承辦,會辦,收文日期,收文字號,發文日期,發文字號)>

<!ELEMENT 電子交換處理機制類別 (#pcdata)>
<!ELEMENT 戳印 (#pcdata)>

公文及報表之內容結構

電子交換類別

代　碼	內　　容	已進行交換項目（截至 90.12）
1	令	
2	函	V
3	公告	
4	開會通知單	V
5	簽	
6	簽稿會核單	
7	會銜公文會辦單	
8	公文時效統計	V
9	公文欄位轉換格式表	V
A	檔案目錄傳輸格式表	V
B	機關檔案分類表傳輸格式表	V

==========

```
<?xml version="1.0" encoding="BIG5"?>
<!--      93_1.dtd_     令      2004.7.1      -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "93_交換用標籤.ent" >
%交換用標籤;
<!ELEMENT  令 (發文機關,發文日期,發文字號,附件?,主旨,段落?,署名*)>
<!-- /令 -->
```

```
<?xml version="1.0" encoding="BIG5"?>
<!--      93_2.dtd      函      2004.7.1      -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "93_交換用標籤.ent" >
%交換用標籤;
<!ELEMENT  函 (發文機關+,函類別,地址,聯絡方式+,受文者,發文日期,發文字號+,速別?,密等及解密條件或
            保密期限?,附件?,主旨,段落*,正本,副本?,署名*)>
<!-- /函 -->
```

```
<?xml version="1.0" encoding="BIG5"?>
<!--      93_3.dtd      公告      2004.7.1      -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "93_交換用標籤.ent" >
```

```
%交換用標籤;
<!ELEMENT  公告    (發文機關,發文日期,發文字號,附件?,主旨,段落*)>
<!-- /公告 -->
```

```
<?xml version="1.0" encoding="BIG5"?>
<!--      93_4.dtd      開會通知單      2004.7.1      -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "93_交換用標籤.ent" >
%交換用標籤;
<!ELEMENT  開會通知單  (發文機關,受文者,聯絡人及電話?,發文日期,發文字號,速別?,密等及解密條件或保
                        密期限?,附件?,開會事由,開會時間,開會地點,主持人,出席者,列席者?,副本?,備
                        註?,署名*)>
<!-- /開會通知單 -->
```

```
<?xml version="1.0" encoding="BIG5"?>
<!--      93_5.dtd      簽      2004.7.1      -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "93_交換用標籤.ent" >
%交換用標籤;
<!ELEMENT  簽  ((機關|單位),受文者?,主旨,段落*, 署名,年月日)>
<!-- /簽 -->
```

```
<?xml version="1.0" encoding="BIG5"?>
<!--      93_6.dtd      簽稿會核單      2004.7.1      -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 內部用標籤  SYSTEM "93_內部用標籤.ent" >
%內部用標籤;
<!ELEMENT  簽稿會核單        (受文者?,全銜,案情摘要,承辦單位,收文字號?, (受會單位,會核意見,
                              收會時間,會畢時間)+)>
<!-- /簽稿會核單 -->
```

```
<?xml version="1.0" encoding="BIG5"?>
<!--      93_7.dtd      會銜公文會辦單      2004.7.1      -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "93_交換用標籤.ent" >
%交換用標籤;
<!ENTITY  % 內部用標籤  SYSTEM "93_內部用標籤.ent" >
%內部用標籤;
<!ELEMENT  會銜公文會辦單        (發文機關+,公文類別,承辦單位,會辦機關+,主辦機關,受文者?)>
<!-- /會銜公文會辦單 -->
```

```
<?xml version="1.0" encoding="BIG5"?>
<!--      93_8.dtd      公文時效統計      2004.7.1      -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "93_交換用標籤.ent" >
%交換用標籤;
<!ELEMENT  公文時效統計      (送達機關,填表機關,填表日期,資料時間,一般公文統計,
      立法委員質詢案件統計?,人民申請案件統計?,訴願案件統計?,人民陳情案件統計?,
      專案管制案件統計?,機關首長?,單位主管?,填表人?,電話?)>

<!ELEMENT  一般公文統計      (一般_本月新收件數,一般_截至上月待辦件數,
      一般_本月創稿數,一般_本月應辦公文總數,一般_六日內辦結,一般_六日內辦結比例,
      一般_六至三十日辦結,一般_六至三十日辦結比例,一般_三十日以上辦結,
      一般_三十日以上辦結比例,一般_發文件數,一般_存查件數,一般_辦結件數總計,
      一般_辦結件數總計比例,一般_發文平均使用日數,一般_待辦件數,一般_待辦件數比例,
      一般_未逾辦理期限待辦件數,一般_已逾辦理期限待辦件數)>
<!ELEMENT  立法委員質詢案件統計      (立委_本月新收件數,立委_截至上月待辦件數,
      立委_本月應辦件數,立委_依限辦結件數,立委_依限辦結件數比例,立委_逾限辦結件數,
      立委_逾限辦結件數比例,立委_逾限五日內辦結件數,立委_逾限五日內辦結件數比例,
      立委_逾限五至十日辦結件數,立委_逾限五至十日辦結件數比例,
      立委_逾限十至十五日辦結件數,立委_逾限十至十五日辦結件數比例,
      立委_逾限十五日以上辦結件數,立委_逾限十五日以上辦結件數比例,
      立委_發文平均使用日數,立委_待辦件數,立委_待辦件數比例,
      立委_未逾辦理期限待辦件數,立委_已逾辦理期限待辦件數)>
<!ELEMENT  人民申請案件統計  (申請_本月新收件數,申請_截至上月待辦件數,
      申請_本月應辦件數,申請_依限辦結件數,申請_依限辦結件數比例,申請_逾限辦結件數,
      申請_逾限辦結件數比例,申請_辦結案件總數,申請_辦結案件總數比例,申請_待辦件數,
      申請_待辦件數比例,申請_未逾辦理期限待辦件數,申請_已逾辦理期限待辦件數)>
<!ELEMENT  訴願案件統計      (訴願_本月新收件數,訴願_截至上月待辦件數,
      訴願_本月應辦件數,訴願_依限辦結件數,訴願_依限辦結件數比例,訴願_逾限辦結件數,
      訴願_逾限辦結件數比例,訴願_辦結案件總數,訴願_辦結案件總數比例,訴願_待辦件數,
      訴願_待辦件數比例,訴願_未逾辦理期限待辦件數,訴願_已逾辦理期限待辦件數)>
<!ELEMENT  人民陳情案件統計  (陳情_本月新收件數,陳情_截至上月待辦件數,
      陳情_本月應辦件數,陳情_依限辦結件數,陳情_依限辦結件數比例,陳情_六日內辦結件數,
      陳情_六日內辦結件數比例,陳情_六至十五日辦結件數,陳情_六至十五日辦結件數比例,
      陳情_十五至三十日辦結件數,陳情_十五至三十日辦結件數比例,陳情_逾限辦結件數,
      陳情_逾限辦結件數比例,陳情_辦結件數,陳情_辦結件數比例,陳情_待辦件數,
      陳情_待辦件數比例,陳情_未逾辦理期限待辦件數,陳情_已逾辦理期限待辦件數)>
<!ELEMENT  專案管制案件統計  (專案_本月新增專案數,專案_截至上月待辦專案數,
      專案_本月應辦件數,專案_依限辦結件數,專案_逾限辦結件數,專案_已辦結件數,
      專案_已辦結件數比例,專案_待辦件數,專案_待辦件數比例,
      專案_未逾辦理期限待辦專案數,專案_已逾辦理期限待辦專案數)>
<!-- /公文時效統計 -->


<?xml version="1.0" encoding="BIG5"?>
<!--      93_9.dtd      公文欄位轉換格式      2004.7.1  -->
<!ENTITY  % 基本標籤  SYSTEM "93_基本標籤.ent" >
%基本標籤;
<!ENTITY  % 交換用標籤  SYSTEM "交換用標籤.ent" >
%交換用標籤;
<!ELEMENT  公文欄位轉換格式  (功能?,主旨?,發文者?,來文者*,文別?,本別?,密等?,解密條件或保密期限?,
```

保存年限?,應用限制?,發文字號?,收文字號?,來文字號?,併案文號?,分類號?,電子檔案路徑?,電子檔案名稱*,媒體型式?,辦畢日期?,發文日期?,收文日期?,來文日期?,附件名稱*,附件媒體型式*,附件數量*,公文頁數?,承辦單位?,承辦人?)+>

<!-- /公文欄位轉換格式 -->

<?xml version="1.0" encoding="BIG5"?>

<!--93_A.dtd 檔案目錄傳輸格式表 2004.7.1 -->

<!ENTITY % 基本標籤 SYSTEM "93_基本標籤.ent" >

%基本標籤;

<!ENTITY % 交換用標籤 SYSTEM "93_交換用標籤.ent" >

%交換用標籤;

<!ELEMENT 檔案目錄傳輸格式 (檔案目錄傳送名稱,功能,案由,並列案由?,其它案由?,案名?,相關案件?,主要發文者?,主要來文者?,次要發文者?,次要來文者?,發文者之補正?,來文者之補正?,文別?,本別?,密等,解密條件或保密期限?,保存年限,應用限制?,保存狀況?,調整後之保存年限?,保存年限調整原因?,核准銷毀文號?,銷毀日期?,解密日期?,移轉註記?,延長移轉屆滿日期?,移轉日期?, 發文字號?,收文字號?,來文字號?,年度號,分類號,案次號,卷次號,目次號,電子媒體編號?,電子檔案路徑?,電子檔案名稱*,微縮編號?,文件產生日期,媒體型式?,數量?,計量單位?,附件名稱*,附件媒體型式*,附件數量*,附件單位*,主題*,附註*)+>

<!-- /檔案目錄傳輸格式-->

<?xml version="1.0" encoding="BIG5"?>

<!-- 93_B.dtd 機關檔案分類表傳輸格式表 2004.7.1 -->

<!ENTITY % 基本標籤 SYSTEM "93_基本標籤.ENT" >

%基本標籤;

<!ENTITY % 交換用標籤 SYSTEM "93_交換用標籤.ENT" >

%交換用標籤;

<!ELEMENT 機關檔案分類表傳輸格式表 (分類號, 類目名稱, 保存年限?, 備註?)+>

<!-- /機關檔案分類表傳輸格式表-->

二、附件採用格式

附件來源種類繁多，經廣泛分析後，歸納出六種附件檔案類型：文字檔、靜態圖形檔、工程圖檔、動畫檔、聲音檔及動態影像檔。這些檔案類型大都有國際標準、國家標準或業界標準之檔案格式，也都有支援呈現之軟體工具。基於傳輸效率及普及性考量，本技術規範明訂以上附件類型採用之格式，惟若發文端與收文端另有一致之呈現軟體工具，或發文端確定收文端能從適當管道解讀其所傳送之格式，雙方可直接進行傳遞交換，無須採用所訂定之格式，但發文端需註明軟體名稱，以供收文端參考。本技術規範所明訂採用之附件格式如下(詳細說明請參考附錄一)：

(一)文字檔案附件

1、文書處理軟體製成之文字檔，以可攜式文件傳遞交換，惟若確知收文端有同樣之文書處理軟體，雙方可直接進行傳遞交換，但發文端需註明軟體名稱，以供收文端參考。

2、傳送資料時，若能攜帶字體，可連帶字體一起傳送。

3、若無法攜帶字體，則收文端之軟體以 True Type(或收文端預選之字體)顯示文字資料。

4、若無法攜帶字體，且已知收文端之軟體無法以 True Type 顯示文字資料，則將資料轉成靜態圖形格式傳送之。

(二)靜態圖形檔案附件

1、靜態圖形可隨可攜式文件格式傳送，至單獨之靜態圖形製成 JPEG 格式傳送。

2、圖表製成 JPEG 格式傳送。

(三)工程圖檔案附件

工程圖檔案採用 IGES 格式。

(四)動畫檔案附件

動畫檔案採用 MPEG 格式。

(五)聲音檔案附件

聲音檔案採用 WAV 格式。

(六)動態影像檔案附件

動態影像檔案採用 MPEG 格式。

附件在電子公文中之表達方式如下例：

```
<?xml version="1.0" encoding="BIG5"?>
<!DOCTYPE 函 SYSTEM "2.dtd" [
<!ENTITY 第一件 SYSTEM "copy.jpg" NDATA JPEG>
<!NOTATION JPEG SYSTEM  “” >
<!ENTITY 第二件 SYSTEM "attachment#5.doc" NDATA Word>
<!NOTATION Word SYSTEM  “” >
]>
…
<附件><文字>檢附原函影本暨附件一份</文字><附件檔名  附件名="第一件 第
        二件">
</附件檔名></附件>
…
```

其中：

- 「檢附原函影本暨附件一份」是有關附件之說明。
- 「附件名="第一件 第二件"」賦予兩個附件在發文端與收文端可以通用之名稱。
- 「SYSTEM "copy.jpg"」中之檔名是供發文端系統存取該檔案用。
- 「NDATA JPEG」說明該檔案為 JPEG 格式。
- 「NOTATION JPEG SYSTEM “” 」說明呈現 JPEG 檔案格式之軟體在系統中的某處。
- 有關「SYSTEM "attachment#5.doc"」之說明類同。

(七)其他常用附件格式參見電子公文網站

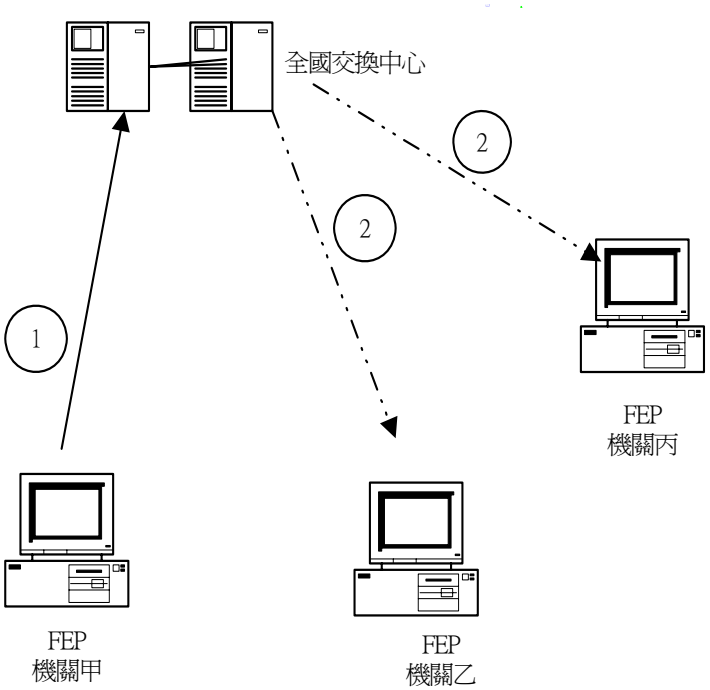
http://www.good.nat.gov.tw/08.htm

三、電子公文傳遞交換作業規範

(一)公文傳遞交換方式簡述如下:

1、第一類公文傳遞交換處理機制:機關公文經公文電子交換中心傳遞,並由中心提供公文傳遞通訊紀錄儲存者,稱為第一類公文傳遞交換處理機制,傳遞方式如下:

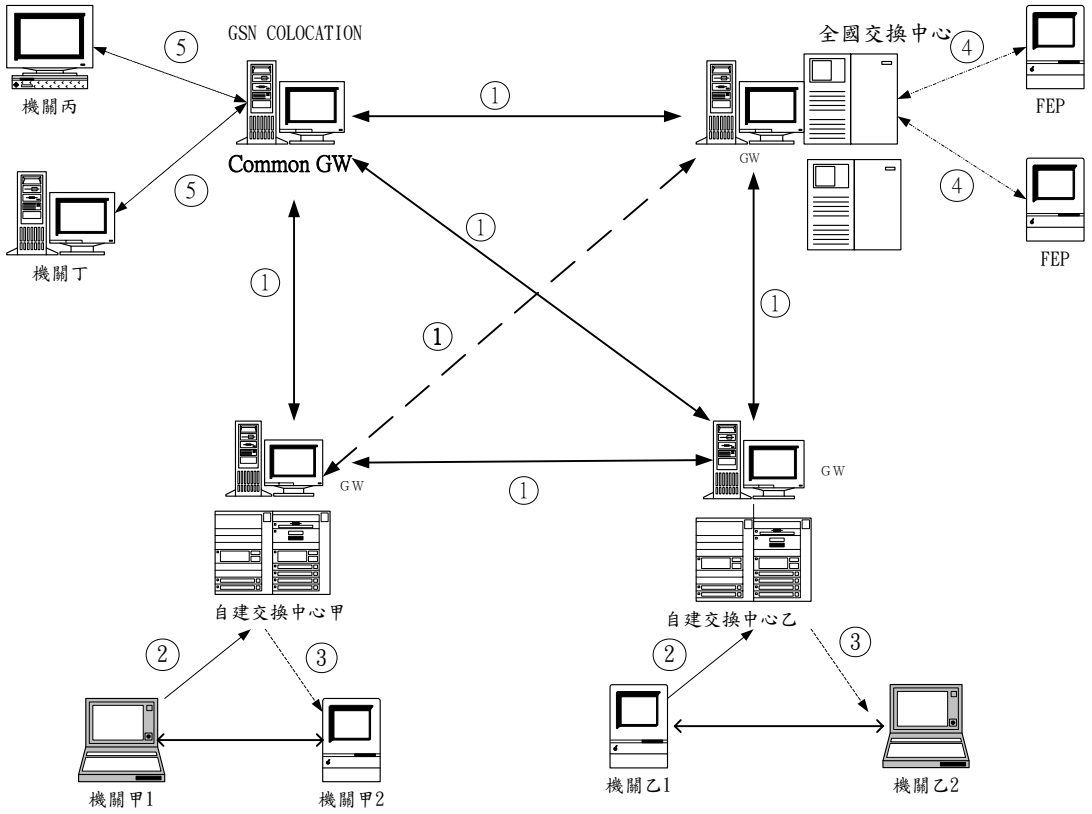
(1)機關使用交通部委外開發傳遞交換之前置處理器(Front End Processor,以下簡稱FEP,細部規範詳參、三、(二))經全國公文電子交換中心相互傳遞電子公文者,示意圖如下:



①→發文機關將公文透過FEP傳送至全國公文電子交換中心

②→各收文機關透過FEP至全國公文電子交換中心收文。

(2)各機關自建公文交換中心，所屬機關經該交換中心，相互傳遞電子公文，自建交換中心，與外部機關傳遞電子公文時，需使用公文閘道系統(Gateway，以下簡稱GW，細部規範詳參、三、(三))，轉送公文封，其傳遞交換紀錄，由發文機關所經之交換中心負責儲存，示意圖如下：



(3)FEP:前置處理器　GW:公文閘道系統　COMMON GW:共用閘道系統

①◄►　不同交換中心間或與共用閘道系統之傳遞交換

②►　發文機關甲1將公文傳送至自建交換中心甲

③----►　收文機關甲2至自建交換中心收文

①◄--►　自建交換中心甲透過GW將公文傳送到全國公文電子交換中心

④◄··►　各使用FEP之機關至全國公文電子交換中心收發文

⑤◄····►　未建置公文閘道系統之機關透過COMMON GW收發文

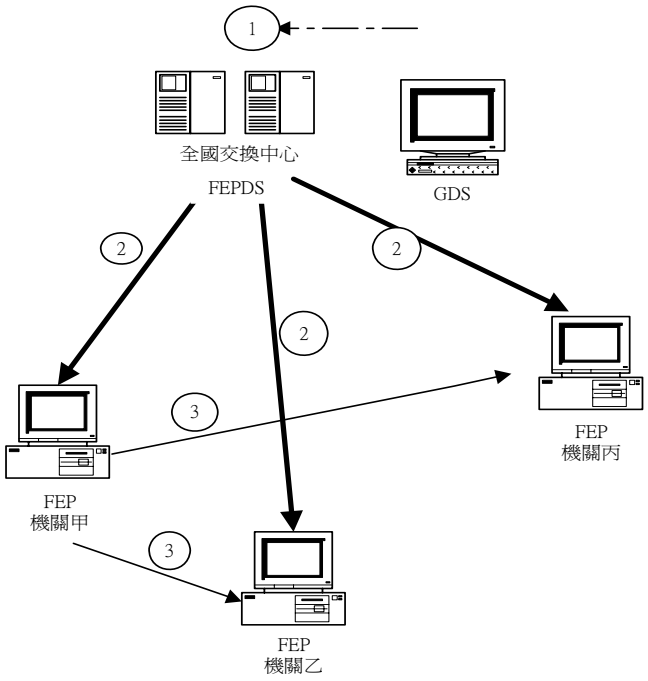
反之，採FEP之機關丙將公文傳送至全國公文電子交換中心，全國公文電子交換中心透過GW將公文傳送至機關甲2之自建交換中心，並由機關甲2至自建交

換中心收文。

備註: 共用閘道系統提供自建交換中心缺少公文閘道系統或機關暨所屬規模小尚未建置公文閘道系統者透過共用閘道系統與其他交換中心傳遞交換。

2、第二類公文傳遞交換處理機制：機關公文採點對點(Point to Point)不經交換中心傳遞者，稱為第二類公文傳遞交換處理機制，傳遞方式如下:

(1)機關使用 FEP，直接以點對點傳遞交換公文者，其通訊紀錄，由發文機關負責儲存，示意圖如下：



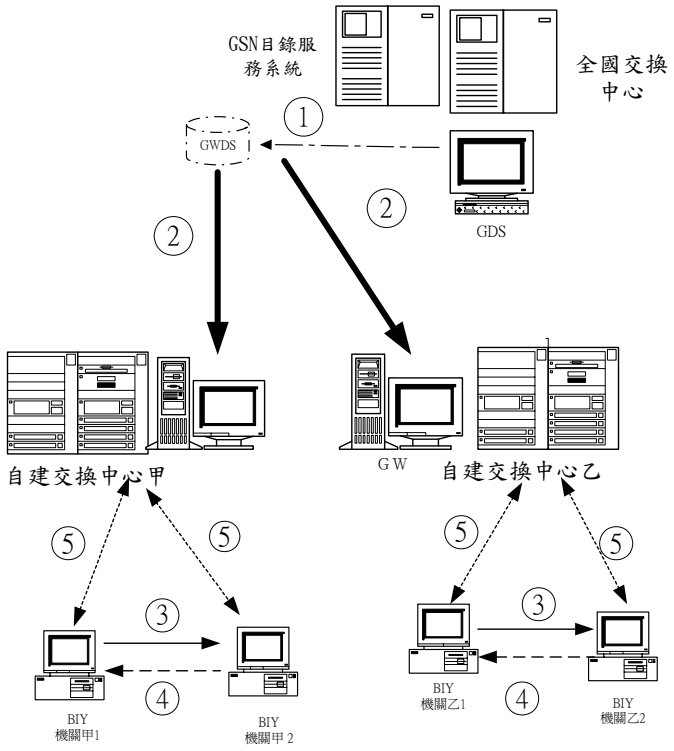
FEPDS:公文電子交換目錄服務　　GDS:GSN 所建置之政府機關目錄服務

① -·-▶　全國公文電子交換中心定期至 GDS 下載政府機關最新資料，並建置公文交換目錄服務 FEPDS。

② ▬▶　各使用 FEP 端，應同步複製 FEPDS。

③ ——▶　機關甲為發文機關，使用 FEPDS 取得收文機關公開資訊，其公文經簽章後，分別視需要使用各收方資訊加密後，以點對點方式傳送機關乙、丙。機關乙、丙使用 FEPDS 取得發文方公開資訊，進行查驗，並回復相關訊息。

(2)各機關非使用 FEP,自建交換中心或自行委外開發公文交換前置處理系統者(Build It Yourself，以下簡稱 BIY)，其內部機關間公文採點對點電子交換，應參照本規範自行訂定傳遞交換及管理事項，對外部機關電子交換時,則需經公文閘道系統直接以點(中心)對點(中心)傳遞電子公文，其通訊紀錄由發文機關負責儲存，示意圖如下：



GWDS:公文閘道目錄服務

① ┄┄▶ 公文閘道系統定期至 GDS 下載政府機關最新資料，並建置公文閘道目錄服務 GWDS。

② ━━▶ 自建交換中心使用 GW 同步複製 GWDS

③ ──▶ 機關甲 1、乙 1 為發文機關，分別使用 GWDS 取得收文機關甲 2、乙 2 公開資訊，其公文經簽章後，視需要使用收方資訊加密後，分別以點對點方式傳送給機關甲 2、乙 2。機關甲 2、乙 2 使用私鑰收文後，透過 GWDS 取得發文方公開資訊，進行查驗，並回復收文訊息。

④ ┈┈▶ 同③發文機關為甲 2、乙 2，收文機關為甲 1、乙 1。

⑤ ┈┈┈▶ 機關甲1、乙1及甲2、乙2分別至所屬交換中心收發第一類電子文。

通訊紀錄之存證得由自建交換中心甲或機關甲1負責。

機關甲1及自建交換中心甲可使用GWDS即時得知收文公開資訊。

3、第三類公文傳遞交換處理機制：機關對於發文通報週知性質公文應登載電子公布欄，並指派權責人員管理。第三類公文，依使用對象分類，包括下列方式:

(1)對象為通報全國各機關者，由行政院指定機關建置全國電子公布欄，各機關應指定專人負責瀏覽，並轉載至機關內電子公布欄。全國電子公布欄所登載事項，應建立分類開放各界查閱，並提供相關檢索等服務。刊登全國電子公布欄事項由各權責機關負責登載，如人事訊息由行政院人事行政局負責，法規命令由法務部負責。登載於全國電子公布欄之公文，如對某些特定對象有所影響，或需其有所作為者，應結合GDS目錄服務，輔以電子郵遞告知前述登載訊息，以利其配合辦理，訊息中應明確告知登載之位址及內容概要。

(2)對象為機關(含所屬機關)內部人員，其通報週知事項登載電子公布欄者，稱為機關內電子公布欄，至於各部會或各地方政府及所屬機關學校，亦可自建跨機關之內部電子公布欄。

機關所建置機關內電子公布欄系統，除提供機關內部人員查詢，並可視需要另設專區，將應公開資訊提供外部人員查詢之用，其基本功能包括:

- 提供機關內部人員張貼內部電子公布欄功能，將各類電子收文(含第一、二類公文電子交換者)及屬於通報週知公文，於網站電子公布欄區分類管理，即各機關應具備動態更新機關內部電子公布欄功能之網站。
- 按專人瀏覽或接獲登載訊息之電子郵遞時，具備自動至全國電子

公布欄轉載服務，而能將全國電子公布欄系統中，轉載有關本機關單位應週知之事項，包括公文及附件。

- 提供整合 GDS 目錄服務及電子郵遞告知登載訊息之功能。
- 提供不特定對象查詢列印:提供不特定機關人員、民眾，依據發文機關、收文者、公布時間、主旨內容關鍵字等條件複合式查詢檢索機關電子公布欄。
- 各機關建置機關電子公布欄，必要得提供主動發送資訊機制。
- 除應登載電子公布欄之公文外，機關可於網站另設專區提供各項訊息服務供各界參閱。

(二)前置處理訊息傳輸規範

前置處理器與全國公文電子交換中心傳遞電子公文時，其交換訊息採用兩種途徑傳送，公文、附件等資料量大之訊息使用 SMTP 方式傳輸；控制訊息則使用 FTP 方式傳輸，利用雙向傳輸方式，達到立即確認之目的。全國公文電子交換中心之 FTP 伺服器為結合安控之特殊功能軟體,使用者 FTP 連線程序未依本規範執行或資料不符，將被立即斷線。以點對點方式傳遞之電子公文及電子公務訊息郵遞，則僅使用 SMTP 方式傳輸，詳細說明如附錄二。

(三)公文閘道系統傳輸規範

公文閘道系統採 TCP/IP 連結方式，以 Two-Way 之 Request-and-Response 方式與公文管理系統間進行 Client-Server 形態之資料傳輸作業，傳輸過程中，公文閘道系統為 Server，其通訊埠預設為 18088，公文管理系統為 Client，其傳輸方式詳如附錄三。

四、中文字碼處理原則

(一)公文以電子方式傳遞時，若需經公文交換中心，則交換之公文需轉換為 CNS11643 中文標準交換碼(以下簡稱國標碼)。

(二)各機關(構)應有中文字碼管理人員管理、維護各機關 (構)內共用之使用者造字區字集與前置處理軟體建置之單位自用(造)字對照檔之正確性。

(三)各機關(構)中文碼管理人員可視下列需要應用國標碼全字庫網站(http://www.cns11643.gov.tw)提供之機制。

1、清查機關(構)內各使用者造字區字集。

2、整合機關(構)內各使用者造字區字集。

3、下載機關(構)內共用之自用(造)字字形與輸入法。

4、提供機關(構)內共用之使用者造字區字集給機關(構)內使用者使用。

(四)公文管理系統(收文、發文)之傳遞交換中，均需具備以下功能：

1、處理 BIG5、BIG5E、UNICODE、國標碼。

2、具備 BIG5 與國標碼對照檔(簡稱 CNS_B5.tbl)、BIG5E 與國標碼對照檔(簡稱 CNS_B5E.tbl)、UNICODE 與國標碼對照檔(簡稱 CNS_UCS.tbl)，供轉碼程式使用。

3、建置單位自用(造)字對照檔：依據用戶端之各機關(構)內共用之使用者造字區字集建置「自用(造)字碼與國標碼對照表」檔(以下簡稱單位自用(造)字對照檔或 CNS_B5U.tbl)，供轉碼程式使用。

4、收文端接收之 XML 格式公文，若經轉碼，收文機關(構)之 CNS_B5U.tbl 沒有對照之字碼時，應通知機關內部中文字碼管理人員於 CNS_B5U.tbl 中新增自用(造)字，提供機關(構)內使用者使用，以確保收文端之電子檔能正確表達發文端所發公文之中文字形。

五、政府憑證管理中心相關規範

(一)技術標準

政府憑證管理中心(Government Certification Authority, GCA)有關電子憑證之命名、加密演算、數位簽章演算、憑證格式、憑證編碼、私密金鑰加密格式等所採用之標準與格式如下：

1、命名(Naming):採 X.509 命名方式。其他標準包括電子郵件 E-mail(RFC 822)、網域名稱服務 Domain Name Service Name(RFC 1035)、Originator/Recipient Address O/R Address(X.400, 1988)、 目錄名稱 DirectoryName(X.501,1993)、電子文件交換 EDI part Name、 全球資訊網網址 Uniform Resource Locator URL(RFC 1630)、網際網路位址 IP address(RFC 791)及註冊識別碼 Registered ID(X.660)等。

2、對稱金鑰加解密演算法 ：採 Triple DES CBC 演算法。

3、非對稱金鑰數位簽章演算法:採 RSA 演算法,其金鑰長度為 1024 bits,並配合雜湊函數 SHA-1 作訊息摘要，補白(padding)方法採 SET 規範。

4、憑證公佈(Certificate Distribution)：採用 HTTP 協定。

5、憑證格式(Certificate Format)：採用 X.509(V3，1997)標準。

6、憑證廢止清冊(Certificate Revocation List):採用 X.509(V2,1997)標準。

7、憑證編碼方式，請參閱政府憑證管理中心網站，

http://www.pki.gov.tw

8、私密金鑰: 採用 PKCS#5 (PKCS: Public Key Cryptographic Standard)公開金鑰密碼標準加密格式。

(二)電子憑證格式

有關 GCA 憑證格式及其 ASN.1 格式說明如下：

1、GCA 憑證格式(X.509 v3)

2、憑證內容說明如下：

(1)版本：該憑證製作所依據之 X.509 版序(V3)

(2)憑證序號：由憑證管理中心所給定之唯一憑證序號

(3)簽章演算法：憑證管理中心簽署該憑證所用之演算法

(4)簽發單位名稱：簽署該憑證之憑證管理中心名稱

(5)憑證有效期限：該憑證生效日期與截止日期

(6)持有者識別名稱：依據 X.500 命名方式所命名之用戶名稱

(7)持有者公鑰：公開金鑰值與演算法名稱

(8)簽發者唯一識別碼：簽署該憑證之憑證管理中心獨有之識別號碼

(9)持有者唯一識別碼：持有者獨有唯一識別碼

3、憑證擴充欄位(Certificate Extensions) 說明 如下：

(1)金鑰用途(Key Usage):係說明此金鑰對之用途，如:簽章、資料加密等。

(2)憑證政策(Certificate Policies)

(3)持有者別名(Alternative Name)

(4)基本限制(Basic Constraints):指此憑證係簽給CA或一般使用者。

(5)CA簽章：憑證管理中心對以上資料所作之數位簽章

4、憑證ASN.1格式說明詳如政府憑證管理中心網站，

http://www.pki.gov.tw

(三)伺服器應用軟體(Server Application Certificate)憑證內容及查詢說明

GCA所核發伺服器應用軟體憑證內容有三項資料說明:

1、持有者識別名稱 (Subject Name)

c=tw，o=政府，ou=主管機關及本機關及伺服主機名稱、編號、服務埠等，cn=Domain Name或IP位址

2、持有者唯一識別碼 (Subject Unique ID)

本欄位不編號

3、持有者別名(Alternative Name)

本欄為伺服器之URL。

(四)機關/單位憑證內容及查詢說明

GCA所核發政府機關/單位憑證有兩項資料內容說明:

1、持有者識別名稱 (Subject Name)

c=tw，o=政府，ou=主管機關、上級機關、本機關、單位名稱等，cn=機關/單位全稱。

2、持有者唯一識別碼 (Subject Unique ID)

依據人事行政局編訂之機關代碼及各機關人事單位依據銓敘部「各機關訂定職務說明書及辦理職務歸系作業注意事項」職務編號原則自訂之單位代碼。

註:country(c), organization(o), organization unit(ou), common name(cn)

註:憑證查詢時輸入URL或機關/單位代碼

(五)GCA 憑證及簽章格式

GCA 簽章內容分成兩部分，其依循之標準為 X.509v3(1997 年)以上及 RFC2459，PKCS#1 V1.5 或 V2.1。

1、Algorithm ID of RSAwithSHA_1

含DER Tag及Length(各為一位元組)，和OID：sha-1 With RSA Encryption資料，故總長度為11位元組。即：

```
30 09       ---- signature algorithm OID
 06 05      ---- OBJECT IDENTIFIER sha-1 With RSA
Encryption (1 3 14 3 2 29)
 2b 0e 03 02 1d  ---- NULL
       05 00
```

2、 Signature of data of signed by RSA private key

因key length為128位元組，再加上Bit string ”00”一個位元組，所以總長度為129位元組。

名稱	Appending	Algorithm ID	Hash value
內容說明	PKCS #1 format	SHA_1	Hash of X.509v3 to be signed data
以 RSA public key 解密後得原來實際資料內容	00:01:ff:ff:…..ff:00:	30:21 30:09 06:05 2b:0e:03:02:1a 05:00 04:14	SHA_1 output
資料長度(位元組)	93	15	20

```
03 81 81 ---- signature tag and length
         ---- signature(BIT STRING)
00 42 2e 40 ef 3c b8 cb a4 2b c8 b4 60 4c 7e 0c d5 57 f3 8d 74 09
2b
```

註: bit string data 必須補成 8 的倍數, 所以會多加一個 byte 來記錄所補充之位元數, 而本列中為 128bytes 資料, 故所補長度為 0。

註：GCA 憑證 DER code 範例詳如政府憑證管理中心網站，

http://www.pki.gov.tw

(六)憑證廢止清冊

憑證廢止清冊(Certificate Revocation List, CRL)係用來公告已經有安全顧慮之憑證資料，。GCA 憑證管理中心之目錄伺服器會依憑證實作準則，公布憑證廢止清冊，以便降低有安全顧慮金鑰遭冒用之機會。

1、本憑證管理中心所使用之憑證廢止清冊內容及架構說明如下：

(1) 版序(Version)：指 X.509 CRL 格式版本(第二版)

(2) 簽章演算法(Signature Algorithm)：指對 CRL 簽章者(憑證管理中心)採用之演算法

(3) 憑證管理中心名稱(CRL Issuer)

(4) 本次發佈時間(This Update)：包括日期、時間

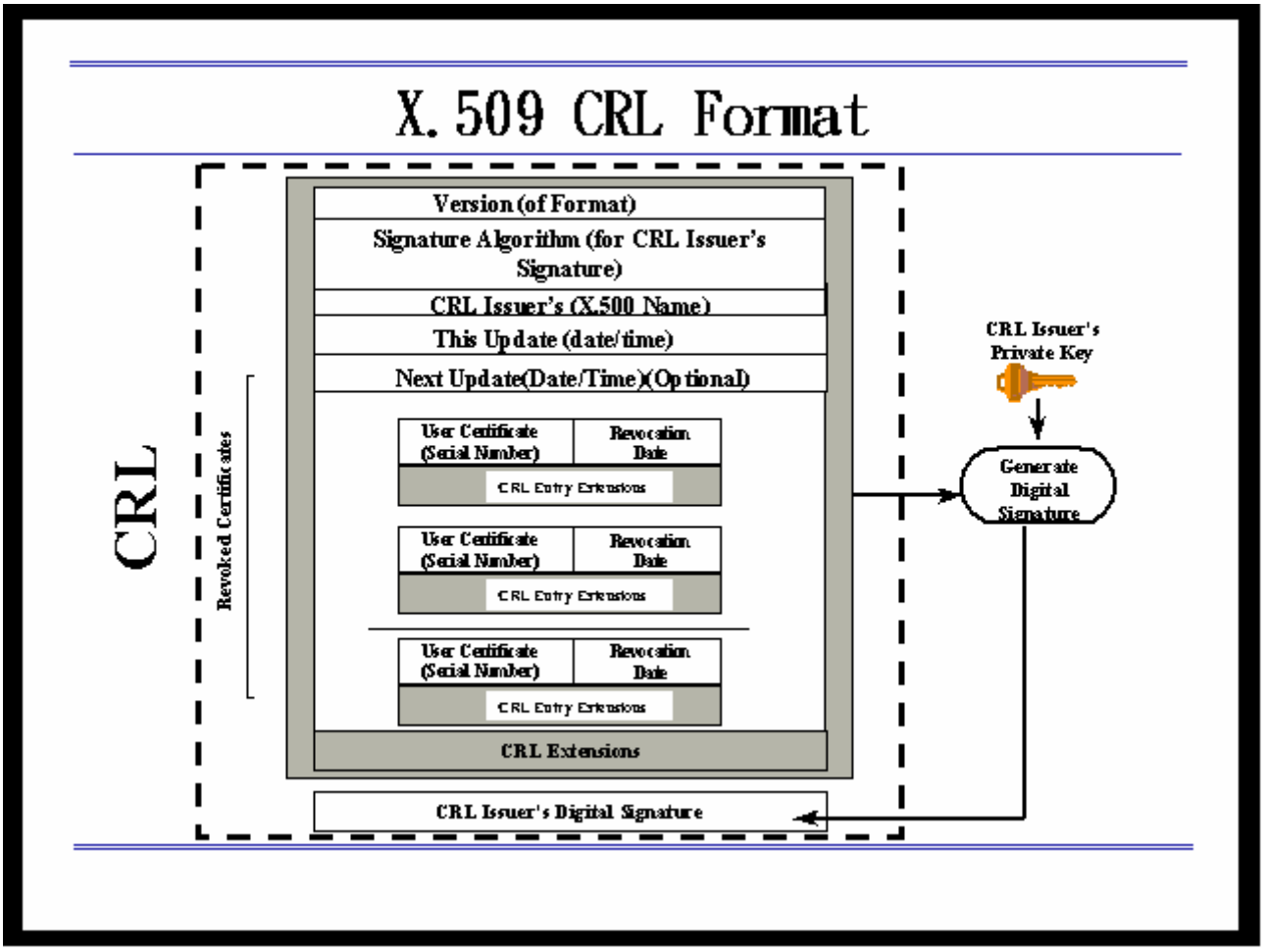
(5) 下次發佈時間(Next Update) ：包括日期、時間(Option)

(6) 廢止憑證串列: 包括憑證序號(User Certificate)、廢止時間(Revocation Date)、廢止憑證串列項目之擴充資料(CRL Entry Extensions)(如：廢止原因等)

(7) 廢止憑證清冊擴充資料(CRL Extensions)

(8) 憑證管理中心簽章(CRL Issuer’s Digital Signature)：憑證管理中心對以上資料所做之數位簽章。

註:過期憑證，其序號是不刊在 CRL 中



圖一、CRL格式

2、憑證廢止清冊 ASN.1 說明詳如附錄四。

(七)私密金鑰格式

GCA 私密金鑰格式是依照 PKCS #5: Password-Based Encryption Standard 以及 PKCS #8: Private-Key Information Syntax Standard 所規範或符合 PKCS #12 或使用 RSA IC 卡。

(八)使用 HTTP 查詢下載 CRL 說明

1、目前 GCA CRL 是公佈在政府憑證管理中心網站上，必須輸入憑證序號當作查詢條件，而採 HTTP 當作 CRL 檔下載協定。

2、傳送憑證廢止清冊協定

(1)連線到 www.pki.gov.tw

(2)http method 為: “POST /ows-bin/crlcgi HTTP/1.0”

(3)參數為 serial=憑證序號

(4)DS 傳回 html 資料

3、如所 post 之憑證序號和 ID 正確，DS 將會傳以下 HTML 資料:

<HTML><HEAD>
<TITLE>查詢下載憑證廢止清冊</TITLE></HEAD>
<BODY BGCOLOR=#CCF7DA><title>憑證廢止清冊</title><CENTER><IMG SRC=/gca.jpg vspace=10 border=0 align=bottom><HR></CENTER><FONT COLOR=#FF0000>注意事項:
<LI>憑證廢止清冊檔案名稱係根據建檔日期所命名(GCA+YYYYMMDDHHMM.crl)</FONT>
<MENU TYPE=SQUARE> <h2>憑證廢止清冊：</H2><!hr size=5><table border width=90><tr><th>GCA 憑證廢止清冊</th><th>檔案長度</th></tR><tr><th><a href=/ows-doc/crl/GCA199812290000.crl>GCA199812290000.crl</th><td>647 bytes</td></tr></table> <hr size=5><FONT COLOR=#0000FF> 已廢止憑證人數：0
</BODY></HTML>

4、此時僅需 search 到 a href=/ows-doc/crl/ 字串即可取出可供下載之 CRL 檔名（此例為 GCA199812290000.crl)。若所 post 之憑證序號和 ID 不對，DS 將會傳回:

<HTML><HEAD>
<TITLE>查詢下載憑證廢止清冊</TITLE></HEAD>
<BODY BGCOLOR=#CCF7DA> <FONT COLOR=#FF0000><H3>無此憑證資料，請重新輸入查詢條件</FONT> </H3><!hr size=5>
</BODY></HTML>

因此無法 search 到 *a href=/ows-doc/crl/* 字串。

5、根據 parse 出之 CRL 檔名以 http 到 DS 去 GET 這個 CRL 檔案。必須注意 HTTP 應採 octet-string 模式來接收 CRL 檔，才能夠正確獲得這個 DER 編碼之檔案。

(九)政府機關憑證申請作業

1、憑證註冊受理機關

行政院研考會為各機關(單位)之憑證註冊受理窗口(RA)，應指定專人專責辦理相關業務。

2、主管機關(院、部會行處局署、省市及縣市政府)申請憑證

各主管機關填妥憑證申請書並加蓋機關印信，再函送指定之憑證註冊受理窗口辦理。

申請伺服器應用軟體憑證，必須先製作私密金鑰及憑證申請磁片，一併送交憑證註冊受理窗口辦理。

3、各主管機關之所屬機關(單位)申請憑證

各申請機關(單位)填妥使用者憑證申請書並加蓋機關印信，統一送交主管機關彙整、核對，再函送指定之憑證註冊受理窗口辦理。

申請伺服器應用軟體憑證，必須先製作私密金鑰及憑證申請磁片，一併送交主管機關彙整、核對，再函送指定之憑證註冊受理窗口辦理。

4、機關(單位)專責人員取得憑證作業流程

(1)憑證註冊受理窗口受理憑證申請書後，審查申請書內容，如為機關/單位憑證，將產製金鑰對，並轉入IC卡，再連同密碼送回申請機關。

(2)如申請機關/單位憑證,機關(單位)專責人員將收到兩張RSA ＩＣ卡，一為正卡、一為副卡。如申請伺服器應用軟體憑證，可從GCA網站下載憑證，並依安全需求，選擇以磁片、硬碟或高速保密器作為私密金鑰儲存媒體。

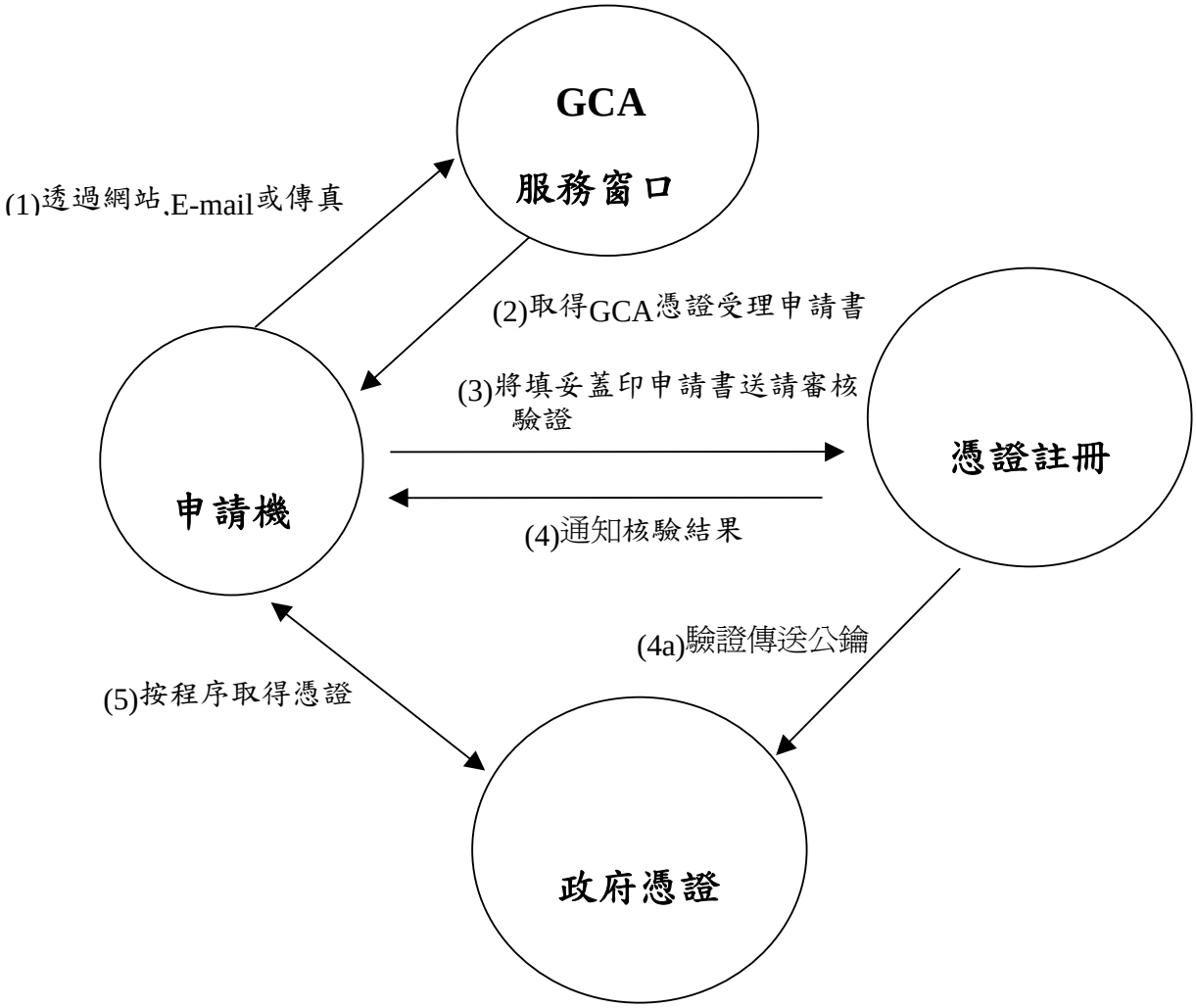
5、政府憑證管理中心認證服務窗口

(1)網站窗口--http://www.pki.gov.tw

(2)電子郵件窗口--nisc@pki.gov.tw

(3)傳真窗口--TEL:(02)23518961

6、申請作業流程圖



7、相關表單

GCA 憑證申請書及 GCA 認證服務功能需求表等詳如政府憑證管理中心所訂格式。

8、RSA ＩＣ卡、讀卡機之安裝介紹暨憑證之申請將併於教育訓練時實施。

(十)政府機關憑證之展延、廢止、變更等作業，請參考 GCA 網站之憑證實務作業基準(http://www.pki.gov.tw)

(十一)政府機關憑證安全保密函式庫申請作業

1、安全保密函式庫申請

(1)受理窗口為行政院研考會。

(2)各機關開發應用系統(含委外)，如需使用 GCA 憑證，必須以公文函請研考會同意後，再向政府憑證管理中心申請使用；不受理廠商直接申請。

2、安全保密函式庫內容介紹，請參閱 GCA 網站

(網址 http://www.pki.gov.tw)

3、安全保密函式庫說明

(1) API 主要分為七大類：API 起始函式、數位簽章與數位信封函式、憑證應用服務函式、憑證狀況查詢函式、加解密函式、高速保密器相關函式及其他函式。

A. API 起始函式：於系統起始及結束時使用，並提供 API 所需參數設定函式。

B. 數位簽章與數位信封函式：提供確保資料隱密性、完整性及不可否認性相關函式。

C. 憑證應用服務函式：提供下載、驗證憑證及讀取憑證資料相關函式。

D. 憑證狀況查詢函式：提供憑證廢止清單下載、驗證相關函式。

E. 加解密函式：對稱式加解密演算法及單向函數演算法相關函式。

F. 高速保密器相關函式。

G. 其他函式。

(2)政府憑證管理中心安全保密函式庫分為版本 A 及版本 B，其中版本 A 可免費提供各機關使用，版本 B 需向政府憑證管理中心(GCA)服務廠商洽購，版本 A 與 B 內容說明如下：

函式名稱	功能說明	版本 A	版本 B
ＡＰＩ起始函式			
InitializeLib	保密及憑證函式庫之起始登記。	☆	☆
GetAPIEnv	讀取函式庫之版本、發行日期及相關加解密方法資訊	☆	☆

函式名稱	功能說明	版本 A	版本 B
SetSymMethod	設定函式庫之對稱式金鑰加解密方法之密鑰儲存媒體		☆
SetCurMedium	設定函式庫之加解密方法之密鑰儲存媒體		☆
SetHWRsa_Samkeyid	設定高速保密器簽章以及解密時所需之 RSA_SAM 金鑰 ID		☆
CloseLib	函式結束終止函式。	☆	☆
數位簽章與數位信封函式(公鑰私鑰格式)			
MakeSignature	使用標準 PKCS #7 語法對輸入資料產生數位簽章封包。	☆	☆
VerifySignature	檢驗遵從 PKCS #7 語法之簽體格式是否正確。	☆	☆
VerSign_GetMessage	檢驗遵從 PKCS #7 語法之簽體格式是否正確，並取出原本被簽章之資料。	☆	☆
MakeSignature_OLD	使用 SHA-1 (FIPS 180-1)及 1024-bit RSA 演算法對任何訊息產生簽章	☆	☆
VerifySignature_OLD	使用 SHA-1 (FIPS 180-1)及 1024-bit RSA 演算法來檢驗資料簽章值是否正確。	☆	☆
SealDE	將輸入資料包成數位信封格式	☆	☆
UnsealDE	解數位信封	☆	☆
SignDE	將輸入資料包成含數位簽章之數位信封格式。	☆	☆
UnSignDE	處理含數位簽章之數位信封封包。	☆	☆
數位簽章與數位信封函式(PKCS #12 格式)			
PFX_MakeSignature	使用標準 PKCS #7 語法對輸入資料產生數位簽章封包，不過將輸入部分由原本簽署者加密後，私密金鑰以及憑證檔案改為經由 PKCS #12 封包成之簽署者 PFX 檔案。	☆	☆
PFX_MakeSignature_OLD	使用 SHA-1 (FIPS 180-1)及 1024-bit RSA 演算法對資料產生簽章，不過將輸入部分由原本簽署者加密後，私密金鑰檔案改為經由 PKCS #12 封包成之簽署者 PFX 檔案。	☆	☆

函式名稱	功能說明	版本 A	版本 B
PFX_UnSealDE	處理數位信封封包，不過將輸入部分由原本接收者加密後，私密金鑰檔案改為經由 PKCS #12 封包成之接收者 PFX 檔案	☆	☆
PFX_SignDE	將輸入資料包成含數位簽章之數位信封格式，不過將輸入部分由原本寄送者加密後，私密金鑰以及憑證檔案改為經由 PKCS #12 語法封包成之寄送者 PFX 檔案。	☆	☆
PFX_UnSignDE	處理含簽章之數位信封封包，不過將輸入部分由原本接收者加密後，私密金鑰檔案改為經由 PKCS #12 語法封包成之接收者 PFX 檔案。	☆	☆
憑證應用服務函式			
GetCertificate	下載政府憑證管理中心之憑證	☆	☆
VerifyCert	藉由檢查憑證使用期限來驗證使用者憑證以及用 CA 公開金鑰(從 CA 憑證得來)來驗證 CA 憑證上之簽章。	☆	☆
VerifyKeyPair	驗證 RSA 金鑰對。	☆	☆
GetIntSerialNumber	從憑證得出憑證序號(只適用目前 GCA 憑證)。	☆	☆
GetSerialNumber	從憑證得出憑證序號。	☆	☆
GetIssuerName	從憑證得出憑證製發單位國家名稱、組織名稱、組織單位名稱及一般名稱等資料。	☆	☆
GetCertName	從憑證得出該憑證持有人之國家名稱、組織名稱、組織單位名稱及一般名稱等資料。	☆	☆
GetCertSubjectUID	得到憑證所有人之唯一識別碼(身份證字號)。	☆	☆
GetCitiZenID	得到憑證個人身分證號碼(為雜湊值)。	☆	☆
GetCertPolicyID	得到憑證之等級狀況。	☆	☆
GetCertValidity	得到憑證之啟用及廢止時間。	☆	☆
憑證狀況查詢函式			
GetCRL	查詢並下載 GCA 憑證廢止清冊	☆	☆

函式名稱	功能說明	版本 A	版本 B
VerifyCRL	驗證 GCA CRL 檔之正確性並取得 CRL 相關資訊	☆	☆
SearchCRL	檢查某一憑證是否列於 GCA CRL 檔中，並取得廢止相關資訊	☆	☆
QueryOCS	線上查詢憑證狀態資訊。		☆
加解密函式			
GenSessionKey	隨機產生一個對稱加密演算法所需要之共用金鑰。		☆
SymEncryption	使用對稱式金鑰加解密演算法來對資料作加密動作		☆
SymDescription	使用對稱式金鑰加解密演算法來對加密資料作解密動作。		☆
HashFunction	使用雜湊函數來對任何訊息產生訊息摘要。	☆	☆
HashFile	使用雜湊函數來對輸入檔案產生訊息摘要。		☆
高速保密器相關函式			
Write_Priv_to_HW	將私密金鑰寫入高速保密器。		☆
getHWsamkeyid	一個提供 API 得到高速保密器運算時所需之 SAMKEY 及其 ID 值介面(由檔案讀取)。		☆
writeSAMkey2	將 SAMKEY 資料鑰寫入高速保密器。		☆
其他函式			
ChangeKeyPassword	修改私密金鑰使用密碼。		☆
PublicKeyEncode	由憑證中取出公開金鑰對資料作 RSA 金鑰演算法加密動作。		☆
PrivateKeyDecode	使用非對稱式私密金鑰對加密資料作解密動作。		☆
PrivateKeyEncode	使用非對稱式私密金鑰對資料作 RSA 金鑰演算法加密動作。		☆
PublicKeyDecode	由憑證中取出公開金鑰對加密資料作解密動作。		☆
checkGCAcert	檢驗輸入憑證是否為GCA政府憑證管理中心所簽發之憑證。	☆	☆
KeySplit	將輸入資料分解為 N 份，且只需要 M 份就可以回復原資料。		☆
KeyCombine	將分持之各個資料結合為原本未分持前之資料。		☆

函式名稱	功能說明	版本 A	版本 B
KeyGeneration	產生 RSA 金鑰對		☆

註 1:雖然版本 B 之功能較版本 A 來得多，不過以使用 API 來發展一套 PKI 應用服務系統而言，版本 A 已提供足夠之基本功能。舉例來說，如果要達到資料隱密性，則可以使用 API 提供之產生數位信封相關函式(包括有 SealDE、UnsignDE、SignDE、UnsealDE、PFX_UnSealDE、PFX_SignDE、PFX_UnSignDE 等七個函式)；如果要達到資料完整性，則可以使用 API 所提供之數位簽章及雜湊函數相關函式(包括有 PFX_MakeSignature、VerifySignature、MakeSignature、PFX_MakeSignature_OLD、MakeSignature_OLD、VerifySignature_OLD、HashFunction、HashFile 等八個函式)；如果要達到資料不可否認性，則是利用 API 提供之數位簽章函式。

註 2：防止第三者以假冒身分方式進行資料竊取，API 提供憑證之驗證函式來檢驗憑證真確性，進而辨識對方真實身份。檢驗憑證製發單位或是使用期限是否到期，可以使用 API 提供之 VerifyCert；檢驗該憑證是否已遭廢止使用，可以使用 API 提供之憑證狀況查詢相關函式。憑證內容資料，可利用 API 提供之憑證應用服務相關函式。

註 3:下表為 PKI 服務與 API 函式對應關係。應用系統開發者只要依據本身需求，參考本表即可得到正確解決方案。

資料完整性	雜湊函數	HashFunction、HashFile、SetHashMethod
資料完整性、來源確認及不可否認性	數位簽章	MakeSignature、VerifySignature、MakeSignature_OLD VerifySignature_OLD、PFX_MakeSignature PFX_MakeSignature_OLD
資料隱密性	加解密演算法	SymEncrypt、SymDecrypt、SetSymMethod
	數位信封	SealDE、UnsealDE、SignDE、UnsignDE PFX_UnSealDE、PFX_SignDE、PFX_UnSignDE
憑證驗證	來源	VerifyCert
	有效期限	VerifyCert、GetCertValidity
	憑證廢止清單檢驗	SearchCRL

六、智慧卡設備規範

(一)IC 智慧卡

於簽章、加密時所使用之 IC 智慧卡將於各機關(單位) 申請憑證時，由政府憑證管理中心或由憑證註冊受理窗口發給。

(二)IC 智慧卡讀卡機

1、概說

本 IC 卡讀卡機，係配合ＰＣ使用之 IC 卡讀卡機，其分為外接型和 PC 內接型兩種，可透過 RS-232、Keyboard(PS/2)、USB、PCI 等介面和 PC 連接。

2、電氣規格

(1)符合 PC/SC Specification 1.0 規格

(2)讀卡機和電腦通信介面：(通信介面於採購時指定之)

- 外接式讀卡機介面為: RS-232、Keyboard(PS/2)、USB 介面
- 內接式讀卡機介面為:PCI 介面
- RS-232 介面，讀卡機和 PC 通信速率，至少應提供 9.6K bps 等通信速率

(3)讀卡機電源

讀卡機可使用下列三種電源。(採用何種電源，於採購時指定之)

A、使用 PS/2 介面 5V 電源

- 耗電量應 ≦ 100mA
- 讀卡機使用 PS/2 介面電源時，應附電源連接用轉接頭，接頭應採用小型 PS/2。

B、使用 AC 110V 電源

- 電源供應器須符合 IEC 1000-4-5 或 FCC Part 68 之規定保護裝

置，以保護讀卡機和相關設備，免遭雷擊之損害。

C、使用 PC 內部電源

- 內裝型讀卡機才可使用ＰＣ內部電源。
- 介面符合ＰＣ電源規範。

(4)讀卡機使用壽命

- IC 卡連接插座，應允許卡片插拔 10 萬次以上。
- 整體讀卡機使用壽命，應保用五年以上。

(5)讀卡保護功能要求

- 卡片使用時，讀卡機不得刮傷卡片，或傷害卡片晶片。
- 插入具有凸字 IC 卡，無論正面或反面插入讀卡機，卡片都應可順利插入與取出，且不可對卡片和讀卡機造成刮傷。
- 電源或讀卡機故障時，仍應可順利取出卡片。

(6)讀卡機保護要求

- 將金屬板插入讀卡機，使讀卡機內ＩＣ卡讀卡接觸點短路時，讀卡機應具備保護機能，不會造成讀卡機損壞。

(7)讀卡機顯示機能

- 讀卡機至少應具備下列顯示燈號
- IC 卡定位指示燈，卡片正確插定位時指示燈應亮。
- IC 卡操作指示燈，讀卡機對卡片讀寫資料時，該燈應閃爍。

(8)電磁特性

- 應符合 CNS 13438-C6357 標準。

(9)安全規範

- 應符合 UL 1950 或 IEC 60950。

(10)工作環境:

- 溫度：2℃ ~ 45℃；

- 相對濕度：40%~95%
- AC110V 電源：117V±20%; 60Hz±10%；

3、軟體功能

(1)讀卡機應同時支援下列功能：

- 讀寫 ISO-7816　T=0，T=1 Protocol 智慧卡
- 作業系統 Plug & Play 功能

(2)讀卡機供應廠商，應同時提供下列軟體(數量於採購時指定之)

- 提供 Reader PC/SC Component Library for VB、C、C++ 等程式發展工具軟體
- 作業系統之 PC/SC 驅動程式

4、機械特性

(1)讀卡機外型尺寸

廠商可依美觀、實用、安全、符合人體工學及易維護等原則來設計讀卡機外型，但外型尺寸應符合採購要求。

- 外接式機型: 高 ≦10 cm; 寬≦10 cm ;深≦15 cm。
- PC 內裝型: 應配合 5.25”或 3.5”磁碟機槽尺寸，可順利牢固裝於 PC 內部。(內裝型應使用ＰＣ內部電源。)
- 機殼上應具有生產公司名稱。

(2)各機構零件須遵照本規範中規定。

(3)各零件應裝置牢靠，不得有螺絲鬆脫、零件鬆動或端子接觸不良之現象。

(4)設計及製造時須注意使用者及維護者之安全與方便，不可有任何銳角毛邊等易造成傷害之現象。

(5)讀卡機外殼材質應採用具充分強度、高硬度且耐衝擊之材料製造如金屬、ABS、PVC 等材質製成。所有金屬零件均應予適當之表面防蝕

處理。

附錄一：附件補充說明

為能有效推動公文電子交換作業，便利公文處理電腦化作業之整體發展，特就附件格式之採用，詳予分析補充說明如次。

參酌一般公文附件處理需求，本說明係基於以下原則：

- 附件用紙尺寸除法令另有規定者外，以採用國家標準總號五號用紙尺度 A4 為原則
- 大量附件如：研究報告、書籍等，以於本文中敘明檔案儲存位置，如：網址，由收方按存取控制機制自行下載為原則；第一類公文電子交換之附件大小，以不超過 500K 為原則，超過者應改置於共用附件下載區供收文方下載使用。
- 附件以提供顯示及列印為目的，收文時，不以要求發文端提供原製作工具用以複製傳送之資料再利用。
- 附件應以不改變原文字內容為原則，而不宜要求原貌重現。

一、附件傳送原則

經廣泛分析及歸納，公文附件檔案格式分為文字檔、靜態圖形檔、工程檔、動畫檔、動態影像檔、聲音檔、紙本文件及無法電子化之實物等，其傳送原則可分類如下：

- 實體－無法電子化之實體附件，連同公文本文仍以傳統方式傳送為宜。
- 已電子化－符合交換規範之電子附件可直接傳送。
- 可電子化－紙本文件、錄音帶、錄影等可轉換成電子附件者，轉換後傳送之。

二、各類檔案格式之分析比較

(一)文字（Text）檔案格式

1、格式說明

格　式	說　　明
RTF	RTF (Rich Text format)
DOC	Microsoft Word 所使用之文書處理檔案格式
可攜式文件	可攜式文件 (Portable Document Format)為業界普遍使用發展之可攜式文件格式

2、格式特性之比較

比較項目	可攜式文件	DOC	RTF
支援平台	DOS、Windows Apple、Unix	Windows、Apple	Windows、Apple Unix
編輯文件之軟體	任何軟體 如 MS-Word、Word-Perfect、Photoshop 等	MS-Word	有限 如 MS-Word 等
整篇文章資料儲存方式	文件產生時圖文共有八種壓縮方式	無法壓縮	無法壓縮
檔案壓縮	一般檔案通常可壓縮至原來的數十到數百分之一	不支援	不支援
支援多媒體	圖形、影像、聲音	圖形、影像、聲音	圖形、影像、聲音
超連結	可以指定一個 WWW 瀏覽器來顯示文中的 URL	MS-Word 本身可充當 WWW 瀏覽器	MS-Word 本身可充當 WWW 瀏覽器
閱讀方式	先下載能 plug-in 的可攜式文件 reader，安裝後始能閱讀。reader 可配合 WWW 瀏覽器使用	使用 MS-Word 或 Internet Explorer 瀏覽	使用 MS-Word 等軟體瀏覽
內崁字型	可	否	否
安全性	文件擁有者及調閱者可對文件列印、複製、編修及備註功能設定使用權	MS-Word 支援文件之唯讀存取、密碼設定及備份	MS-Word 支援文件之唯讀存取、密碼設定及備份

註：可攜式文件透過相關之處理工具可以原貌重現，並可作有限度的編輯和檢索。可攜式文件並具有下列文件傳送時之優越特性：

1. Page at a time downloading：文件過大時，可不用全部傳送完畢，即可顯示。
2. Progressive display：可攜式文件之最適格式每頁可先顯示文字(text)和圖像(picture)，然後才顯示字型(fonts)，即利用 perceived speed 與 actual speed 之視覺差異現象。
3. Byte serving:即可快速檢視跳頁資料(如從頁 1 直接跳至頁 73，skip

to byte 1,237,549，即頁 73 之開始，並存取 17,307Bytes，即頁 73 之資料內容長度)。

產生可攜式文件有兩種方式：

1. 應用程式利用模擬印表機驅動程式(Writer)直接產生可攜式文件檔案。
2. 應用程式利用 PostScript 印表機驅動程式間接產生可攜式文件檔案。

(二)靜態圖形 (Graphics) 檔案格式

1、格式說明

格　式	說　　明
GIF	CompuServe 及 BBS 系統經常使用之圖形檔案交換格式 (Graphical Interchange Format)
JPEG	JPEG (Joint Photographic Experts Group)是一相當有效的壓縮過的圖形檔案，亦可指定不同解析度儲存，是大部分 Web Browser 內建支援之圖形檔案格式
BMP	Microsoft Windows 所使用之位元圖形檔案格式
PCX	ZSOFT 首先在其 Paintbrush 程式中發展之格式，是諸多圖形軟體共用之圖形檔案格式，大部分之 Scanner 及 Fax 亦支援此格式
JBIG	JBIG (Joint Bi-level Image Group) 是一種不失真之黑白圖檔壓縮方式。JBIG 由 ITU (CCITT)及 ISO/IEC JTCI/SC29 共同贊助
TIFF	TIFF (Tagged Image File Format) 用於巨大且需高解析度之黑白圖形。由 Adobe Systems 提供維護。

2、格式特性之比較

比較項目	GIF	JPEG	BMP	PCX	JBIG	TIFF
壓縮比	中	高	無	低	中	高
失真度	中	高	不失真	不失真	不失真	不失真
最多顯示顏色	256 色	全彩	256 色全彩 (新格式)	全彩	黑白	黑白
顯示速度	快	快	最快	慢	傳輸速度快	快
廣泛度	高	高	中	中	低	高
瀏覽器內建圖形格式	是	是	否	否	否	否
平台	Windows Unix	Windows Unix	Windows OS/2	Windows	Unix	Windows Unix

	Macintosh	Macintosh		Macintosh		Macintosh

(三)工程圖 (Drawing) 檔案格式

1、格式說明

格　式	說　　明
IGES	IGES (Initial Graphics Exchange Specification) 是異質 CAD/CAM 系統交換格式。IGES 為美國國家標準 (ANSI Y14.26M)
STEP	STEP (Standard for the Exchange of Product Model Data) 是一種獨立於系統之產品模組交換格式。STEP 為國際標準(ISO 10303)
CGM	CGM (Computer Graphics Metafile) 是一種 2D 圖形儲存及交換標準。為國際標準 (ISO/IEC 8632:1992 version 3)
DXF	DXF (Drawing eXchange Format) 是一種業界支援之開放性資料交換格式，用於 CAD 工程圖之檔案交換

2、格式特性之比較

比較項目	IGES	STEP	CGM	DXF
標準性	美國國家標準 (ANSI Y14.26M)	ISO 標準 (ISO/IEC 10303)	ISO 標準 (ISO 8632:1992)	Autodesk 之開放性標準
支援 3D	是	是	否 (2D)	是
支援此格式之軟體	AuotCAD, ICEMDDN, CADAM ANVIL 5000, Intergraph, ComputerVision, Unigraphics, Pro Engineer, 及 Mechanical Desktop	AuotCAD, 及 Mechanical Desktop 等工具	Microsoft Word, Harvad Graphics, Interleaf, HSIview, IsoDraw, IsoView 及 FrameMaker 等工具	AutoCAD, Word processor, desktop publishing, 及 illustrator 等工具
廣泛度	高	中	低	低
應用領域	CAD 在機械方面之應用	CAD 在機械、電子、建築方面之應用 模擬 電腦輔助製造 結構化分析	CAD 在機械、電子方面之應用 GIS 桌上排版 地球物理探討	CAD 在機械方面之應用 桌上排版

		系統間資料交換		
支援 WEB	否	否	是	否

註:目前有 38 個國家在從事 STEP 之發展,STEP 似乎於未來有可能取代 IGES。

(四)動畫 (Animation) 檔案格式

1、格式說明

格　式	說　　明
GIF	CompuServer 及其它 BBS 系統經常使用之圖形檔案交換格式，GIF89A format 支援 Animation
FLC/FLI	FLC/FLI 為 Autodesk's "Flick" (影像) 格式
MOV	Apple's QuickTime Movie 格式是最早出現之影像格式
AVI	Microsoft Video for Windows，可將聲音及動畫混合在一起，但無法在 Macintosh 上使用
MPEG	MPEG (Motion Picture Expert Group) 專門用於動態影像壓縮

2、格式特性之比較

比較項目	GIF	FLC/FLI	MOV	AVI	MPEG
支援 3D	否 (2D)	否 (2D)	是	是	是
支援聲音	否	否	是	是	是
影像品質	中	中	中	中	高
廣泛度	高	低	中	高	高

(五)聲音 (Sound) 檔案格式

1、格式說明

格　式	說　　明
WAV	Windows 之聲音檔案格式
MIDI	MIDI (Musical Instrument Digital Interface)並非真正聲音檔案，而是儲存能在音效卡上演奏之一串音符

2、格式特性之比較

比較項目	WAV	MIDI
製作難易度	簡單	難
儲存空間	很大	很小
音源	任何聲音皆可	只允許樂器
硬體需求	少	多(聲音的品質完全取決發聲設備)

(六)動態影像（Movie）檔案格式

1、格式說明

格　式	說　　明
MOV	Apple’s QuickTime Movie 格式是最早出現之影像格式
AVI	Microsoft Video for Windows，可將聲音及動畫混合在一起，無法在 Macintosh 上使用
MPEG	MPEG（Motion Picture Expert Group）專門用於動態影像壓縮

2、格式特性之比較

比較項目	MOV	AVI	MPEG
壓縮	有	否	有
儲存空間	中	大	小
製作難易度	中	易	中
廣泛度	中	高	高
影像品質	中	中	高
硬體需求	中	低，祇需要一般影像擷取卡	高，需要專業擷取卡

三、附件傳送方式之建議

(一)文字檔案附件

1、由於可攜式文件格式之跨平台特性、高壓縮比、可攜性、可支援任何軟體、及安全性，所以建議以其他文書處理軟體製成之電子檔應轉成可攜式文件格式，連帶本文之 XML 檔一起傳送。

2、傳送之資料若能攜帶字體，則連帶字體一起傳送。

3、傳送之資料若無法攜帶字體，則收文端之軟體應以 True Type 顯示文字資料。

4、傳送之資料若無法攜帶字體，而且收文端之軟體無法以 True Type 顯示文字資料，則應將資料轉成圖形格式以傳送之。

(二)靜態圖形檔案附件

1、靜態圖形固然可隨可攜式文件傳送，但單獨之靜態圖形宜製成 JPEG 圖形檔傳送。

2、由於 JPEG 格式壓縮比高、顯示顏色可達全彩、顯示速度快、被廣泛使用、且跨平台，所以建議將圖表製成 JPEG 格式。

(三)工程圖檔案附件

由於 IGES 為美國國家標準且為全球業界廣泛使用，所以建議工程圖檔案採用 IGES 格式。

(四)動畫檔案附件

由於 MPEG 可支援 3D 動畫、可結合影像及聲音、影像品質高、且廣泛使用，所以建議動畫檔案採用 MPEG 格式。

(五)聲音檔案附件

由於 WAV 格式製作容易、可使用任何音源、且硬體需求少，所以建議聲音檔案採用 WAV 格式。

(六)動態影像檔案附件

由於 MPEG 可壓縮、儲存空間小、影像品質高、且廣泛使用，所以建議影像檔案採用 MPEG 格式。

附錄二：前置處理訊息傳輸方式補充說明

（本附錄提供自建交換中心時參考，至全國電子交換中心之實際作業以交通部網站公布資料為準）

一、SMTP 傳輸方式

遵循 Simple Mail Transfer Protocol(RFC821) 與 Standard for the Format of Internet Text Message(RFC822)等標準處理。

以下說明 SMTP 訊息的各種格式內容：

(一)公文電子交換(經由交換中心)的 SMTP 訊息格式

1、文件內容(Document)部份

(1) SMTP Header

依據 SMTP 標準訂定的電子郵件傳送必備表頭，Mail Subject 一律定為”OD Exchange (Encrypt)”或”OD Exchange (None Encrypt)”。

(2) Exchange Data

交換中心執行交換工作或由符合本節規範之前置處理軟體 FEP 執行收文工作所需要之文件內容描述資料檔案遵循 Multipurpose Internet Mail Extensions (RFC1521)的編碼方式，置於電子郵件的第一附加檔案。

(3)公文

XML 格式電子公文資料檔案，先經 gzip(GNU zip)壓縮、視需要以 Triple-DES CBC 模式加密，再遵循 MIME 的編碼方式，置於電子郵件的第二附加檔案(GNU zip 資訊詳如交通部網站、Triple-DES CBC 資訊詳如政府憑證管理中心網站)。

(4)附件

電子附件資料檔案，先經 gzip(GNU zip)壓縮、視需要以 Triple-DES CBC 模式加密，再遵循 MIME 的編碼方式，置於電子郵件的第三附加檔案和後續附加檔案。

公文以加密處理時，附件則必須以加密處理。

2、控制(Control)部份

(1) SMTP Header

依據 SMTP 標準訂定的電子郵件傳送必備表頭，Mail Subject 一律定為”OD Exchange (None Encrypt)”。

(2) Exchange Data

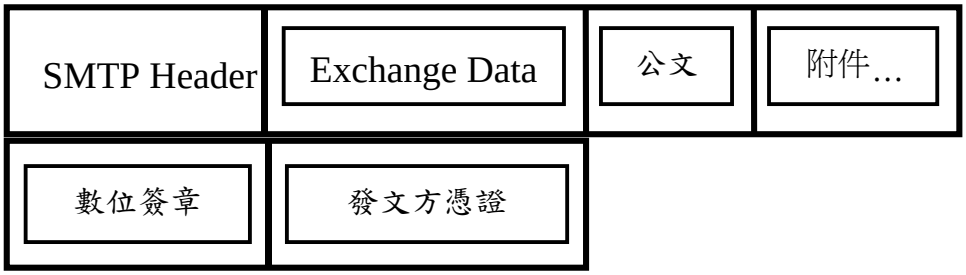
交換中心執行交換管理工作或 FEP 執行交換管理工作所需要之控制資料檔案遵循 MIME 的編碼方式，置於電子郵件的第一附加檔案。

(3)數位簽章

將 Exchange Data 使用政府憑證管理中心 GCA(相關規範詳參之五)提供之簽章方式，以發送方密鑰產生數位簽章檔案遵循 MIME 的編碼方式，置於電子郵件的第二附加檔案。

(二)電子公文交換(以點對點方式)的 SMTP 訊息格式

1、文件內容(Document)部份



(1) SMTP Header

依據 SMTP 標準訂定的電子郵件傳送必備表頭，Mail Subject 一律定為”OD Mail (Encrypt)” 或”OD Mail (None Encrypt)”。

(2) Exchange Data

收文 FEP 執行電子公文交換(以點對點方式)收文工作所需要之文件內容描述資料檔案遵循 MIME 的編碼方式，置於電子郵件的第一附加檔案。

(3)公文

XML 格式電子公文資料檔案，先經 gzip(GNU zip)壓縮、視需要以 Triple-DES CBC 模式加密，再遵循 MIME 的編碼方式，置於電子郵件的第二附加檔案。

(4)附件

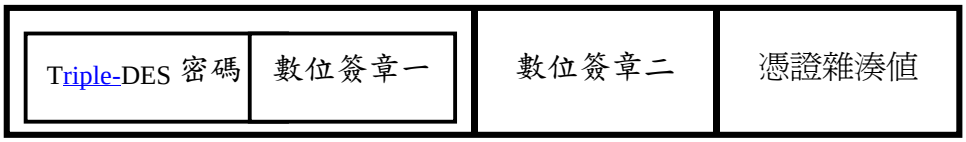
電子附件資料檔案，先經 gzip(GNU zip)壓縮、視需要以 Triple-DES CBC 模式加密，再遵循 MIME 的編碼方式，置於電子郵件的第三附加檔案和後續附加檔案。

公文以加密處理時，附件則必須以加密處理。

(5)數位簽章

將 Exchange Data 使用 GCA 提供之簽章方式，以發文方密鑰產生數位簽章檔案遵循 MIME 的編碼方式，置於電子郵件的最後第二附加檔案。

如需加密則改為以下格式：



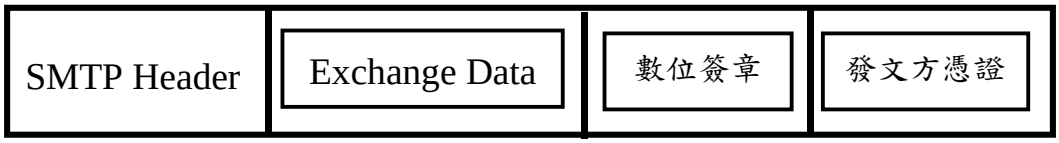
前 128 位元組以收文方公鑰加密。

(6)發文方憑證

GCA 發放之有效發文方憑證檔案，先經 gzip (GNU zip)壓縮，再

遵循 MIME 的編碼方式，置於電子郵件的最後第一附加檔案。

2、控制(Control)部份



(1) SMTP Header

依據 SMTP 標準訂定的電子郵件傳送必備表頭，Mail Subject 一律定為”OD Mail (None Encrypt)”。

(2) Exchange Data

收文 FEP 執行電子公文郵遞收文工作所產生之回覆控制資料檔案遵循 MIME 的編碼方式，置於電子郵件的第一附加檔案。

(3)數位簽章

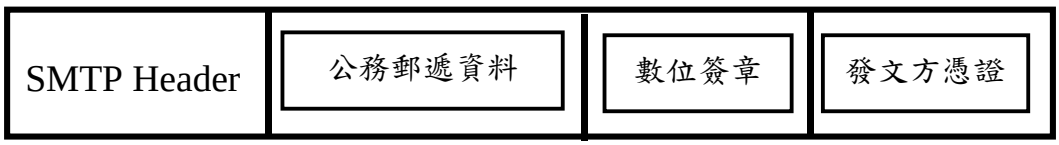
將 Exchange Data 使用 GCA 提供之簽章方式，以發文方密鑰產生數位簽章檔案遵循 MIME 的編碼方式，置於電子郵件的第二附加檔案。

(4)發文方憑證

將 GCA 發放之有效發文方憑證檔案遵循 MIME 的編碼方式，置於電子郵件的第三附加檔案。

(三)電子公務訊息郵遞的 SMTP 訊息格式

1、文件內容(Document)部份



(1) SMTP Header

依據 SMTP 標準訂定的電子郵件傳送必備表頭，Mail Subject 定為”郵遞編號：業務代碼〈業務名稱〉：發文機關代號〈發文機關(單位、人)〉：收文機關代號〈收文機關(單位、人)〉，收文機關代號〈收

文機關(單位、人)〉…：檔案名稱：Encrypt 或 None Encrypt”。

- 郵遞編號：由十位數字組成，由發文機關自訂，不得重複。
- 業務代碼：由收送雙方約定之業務處理代碼，如公文時效統計資料之傳送使用 DS，另代碼為“ZZ”時，表示為其他業務，可為臨時性之傳遞需求。約定事宜，請洽行政院研考會。
- 發文機關代號：可為十碼之機關代碼或為十七碼之機關代碼＋單位代碼。
- 收文機關代號：可為十碼之機關代碼或為十七碼之機關代碼＋單位代碼。可為多個接收機關。
- 檔案名稱：實際傳送之檔案名稱。
- 加解密註記：以加密方式傳送時註記為” Encrypt”，未以加密方式傳送時註記為”None Encrypt”。
- 〈…〉:〈 〉內註記之資訊為說明參考用。

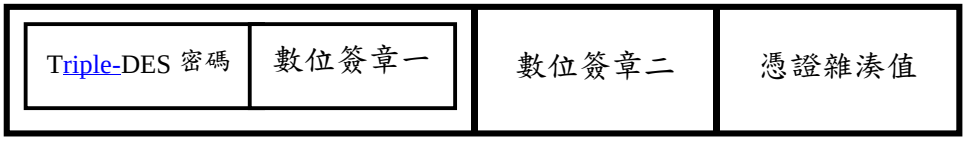
FEP 需要以收文機關代號為查詢依據，取得各收文機關(人)的電子郵件地址放入 TO 欄位內，分別寄出。

(2)公務郵遞資料

將公務郵遞資料檔案，先經 gzip(GNU zip)壓縮、視需要以 Triple-DES CBC 模式加密，再遵循 MIME 的編碼方式，置於電子郵件的第一附加檔案。

(3)數位簽章

將公務郵遞資料檔案使用 GCA 提供之簽章方式，以發文方密鑰產生數位簽章檔案遵循 MIME 的編碼方式，置於電子郵件第二附加檔案。如需加密則改為以下格式：



前 128 位元組以收文方公鑰加密。

(4)發送方憑證

GCA 發放之有效發文方憑證檔案遵循 MIME 的編碼方式，置於電子郵件的第三附加檔案。

2、控制(Control)部份

(1) SMTP Header

依據 SMTP 標準訂定的電子郵件傳送必備表頭，MailSubject 定為”郵遞編號：業務代碼〈業務名稱〉：發文機關代號〈發文機關(單位、人)〉：收文機關代號〈收文機關(單位、人)〉：回條：None Encrypt”。FEP 需要以收文機關代號為查詢依據，取得收文機關(人)的電子郵件地址放入 TO 欄位內寄出。

(2)數位簽章

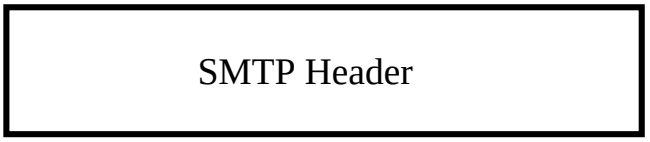
接收機關將收到之公務郵遞資料檔案使用 GCA 提供之簽章方式，以發文方密鑰產生數位簽章檔案遵循 MIME 的編碼方式，置於電子郵件的第一附加檔案。

(3)發文方憑證

將 GCA 發放之有效發文方憑證檔案遵循 MIME 的編碼方式，置於電子郵件的第二附加檔案。

(四)查詢憑證的 SMTP 訊息格式

1、查詢部份



- SMTP Header

依據 SMTP 標準訂定的電子郵件傳送必備表頭，Mail Subject 定為”Certificate Query”。FEP 需將欲取得收文機關(人)的電子郵件地址放入 TO 欄位內寄出。

2、回應部份

(1) SMTP Header

依據 SMTP 標準訂定的電子郵件傳送必備表頭，Mail Subject 定為”發文機關代號〈發文機關(單位、人)〉：Certificate Reply”。FEP 將查詢憑證電子郵件之發送地址放入 TO 欄位內寄出。

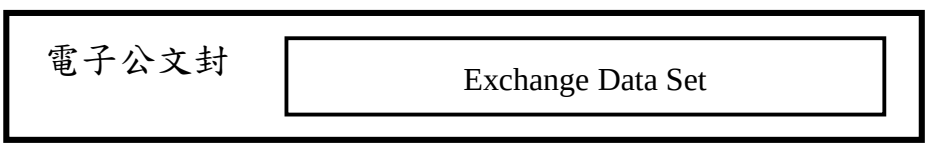
(2)發文方憑證

將 GCA 發放之有效發文方憑證檔案遵循 MIME 的編碼方式，置於電子郵件的第一附加檔案。

二、FTP 傳輸方式

完全遵循 FTP 通信協定。以下說明電子公文的 FTP 訊息格式控制(Control)部份：

各機關需要與交換中心傳送有保密需求的控制訊息時，交換中心提供一特殊 FTP 伺服器(簡稱安控 FTP 伺服器)讓各機關傳送以電子公文封包裝之 Exchange Data Set 至交換中心，並由交換中心取得以電子公文封包裝之 Exchange Data Set，電子公文封參考行政院研考會「政府機關公文電子交換作業安全協定」2.4 電子公文防竊視(電子公文封)的驗核協定及其訊息格式。



Exchange Data Set 之格式如下：

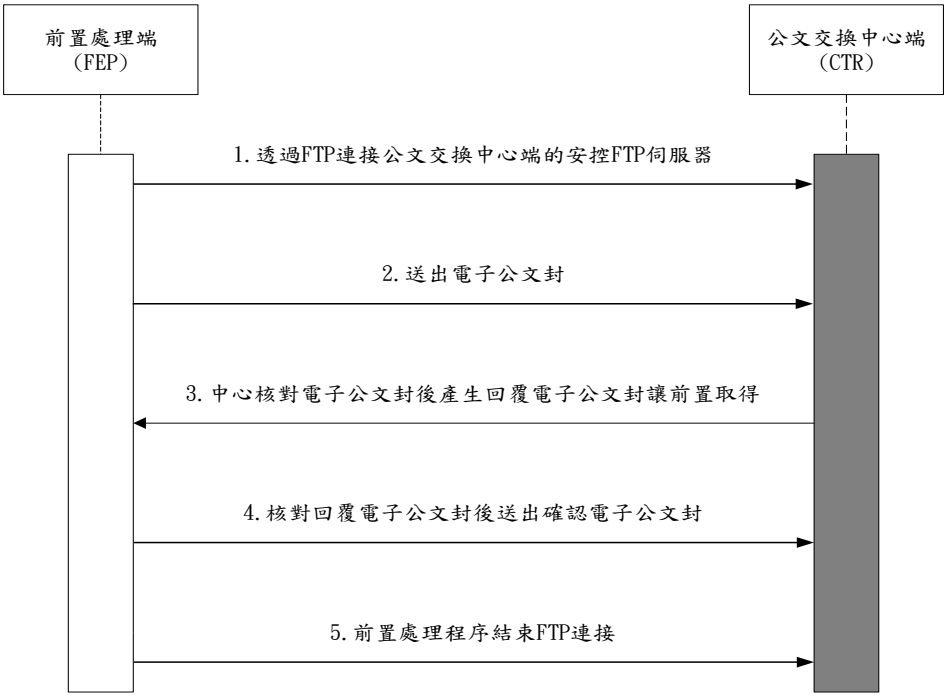
長度	Exchange Data

1、以上圖之資料組重覆組成 Exchange Data Set。

2、長度佔 4Bytes，位元組順序為由高至低，值為 Exchange Data 的 Byte 數。

三、FTP 傳輸步驟

安控 FTP 伺服器：



1、FEP 使用 FTP 通訊協定連線到交換中心安控 FTP 伺服器(使用"USER anonymous"、"PASS 單位代碼@odedi.gov.tw"指令)。

2、FEP 送出電子公文封檔案(內含 Exchange Data Set)到交換中心（使用"put 檔案名稱"指令)。

3、交換中心核對收到之電子公文封檔案正確後，產生回覆電子公文封檔案(內含 Exchange Data Set)讓 FEP 取得(使用"get 檔案名稱"指令)。

4、FEP 核對收到之回覆電子公文封檔案正確後，如非空電子公文封檔案則送空電子公文封檔案到交換中心確認(使用"put 檔案名稱"指

令），空電子公文封為只包一件檢查(Check)訊息之電子公文封。

5、FEP 結束 FTP 連線(使用”quit”指令)。

四、公文電子交換訊息傳輸資料格式

(一)交換資料(Exchange Data)

需符合下列定義之需求：

1、各欄位每列最大長度不得大於 1023Bytes(含欄位名稱及 CR-LF 字元)，並以 CR-LF 結束該欄內容之描述，若該欄位內容超過長度限制時，應以 CR-LF 字元分列，且第二列以後之起始字為△，表示該列續上列的內容；各欄位之順序不硬性規定。

2、Digits 表示為阿拉伯數字之組合。

3、ChineseCharacterString 表示中文字串。

4、CharacterString 表’A’…’Z’，’a’…’z’，’0’…’9’之組合。

5、Date 表示日期；格式為 YYYY/MM/DD，YYYY 表西曆年，如：1999，MM 為月份，DD 為日。

6、Time 表示時間，格式為 HH：MM：SS，HH 表時，為 24 小時制。MM 表分鐘，SS 表秒數，如 19：17：10。

7、機關代號共 17 碼，分述如下：

機關代碼(10 碼)	單位代碼(7 碼)			
	U (1 碼)	內部一級單位碼 (2 碼)	000 (3 碼)	0 (1 碼)

第 1-10 碼：機關代碼，請依據人事行政局編訂之機關代碼填寫。

第 11-17 碼：單位代碼，其中第 12-13 碼是內部一級單位碼，請洽各機關人事單位依據銓敘部「各機關訂定職務說明書及辦理職務歸系作業注意事項」職務編號說明原則填寫，若未編碼，請自行編列，切勿重複；機關憑證請填 00。

8、｜表示多取一。

9、“　“表示內容，須完全符合。

10、[　]表示該項可有可無。

11、CR-LF 表示 Carriage-Return(0DH)及 Line-Feed(0AH)。

(二)、SMTP Header 格式

採用 E-Mail 方式傳送訊息，需有 SMTP Header，其格式如下：

編號	項　　目	說　　明	範　　例
1	Date:	發送 E-Mail 日期時間	Thu, 29 Apr 1999 12:35:03 +0800
2	From:	發送 E-Mail Address	315000000H<odedi@motc.gov.tw>
3	To:	接收 E-Mail Address	CENTER0001<odctr@motc.gov.tw >
4	Subject:	交換與非交換公文 E-Mail 標示	OD Exchange OD Mail
5	Message-ID:	E-Mail 識別碼	<042999123503.0@motc.gov.tw>
6	MIME-Version:	E-Mail MIME 版本	1.0
8	Content-Type:	多重本文 E-Mail 內容型別標示	multipart/mixed; boundary= "------------ 0BF7A8E88B23B7A3AB3D3 4E5"
9	Content-Type:	多重本文 E-Mail 子內容型別標示	application/exchange-data; name=”om01" application/office-document; name=”od870430.1" application/attachment- document; name="cvtoldoc.obj" application/signature-data ;

			name=” signature" application/certificate-data; name=” certificate"
10	Content-Transfer-Encoding:	E-Mail 內容編碼方式標示	Base64

(三)交換資料(Exchange-Data)

Exchange-Header	CR-LF	Exchange-Message

1、交換表頭(Exchange-Header)

交換表頭提供交換中心基本交換控制資料，例如：版本別、訊息別、傳送序號、收送單位代碼、收送時間等。

2、交換訊息(Exchange-Message)

交換訊息分為文件內容(Document)與控制(Control)兩大類，Document 用於公文本文及附件檔資料之傳送，Control 則為達到確認及資料查詢等功能而設計。檢查(Check)訊息只有交換表頭，用於當作 Exchange Data Set 必備內容。

3、交換表頭的欄位分文件內容(Document)、控制(Control)和檢查(Check)等三類對欄位需求如下表所示：

欄　位	文件內容	控制	檢查	意　義
X-Type：	V	V	V	內容為："Document"、"Control"或” Check”
X-Version：	V	V	V	版本："1.0"
X-Sender：	V	V	--	內容為發文機關代碼
X-To：	V	V	--	內容為收文機關代碼
X-Document-Id：	V	--	--	內容為公文文號
X-Document-Date：	V	--	--	公文日期，例如："1999/04/29"
X-Send-Time：	V	V	V	發送日期及時間，例如："1999/04/29 11:55:12"
X-Serial-No：	V	V	--	交換序號，值為 1 至 999999999
X-Received：	#	#	--	接收時間(由公文交換中心填入) ，例如："1999/04/29 accept 12:35:03"

符號說明：V：必須具備之欄位。

--：可有可無之欄位，交換中心不檢查亦不處理。

#：交換中心必須加入之欄位。

五、訊息格式說明

(一)訊息分類

交換資料(Exchange Data)中交換訊息(Exchange Message)之文件內容/控制分類，描述如下：

1、電子公文封收發

OM00：Exchange Data Set 必備內容，包含序號、時間等檢查資料。

2、公文訊息收發

(1)OM01：公文共同傳輸檔案格式資料，為行政院發佈「文書及檔案管理電腦化作業規範(九十年修訂版)」中之「共同傳輸檔案格式(XML)」及第二類點對點交換 Triple-DES 密碼及憑證雜湊值資料。

(2)OM02：Triple-DES 密碼及憑證雜湊值資料。

(3)OM03：交換中心或收文端回覆發文端確認接收電子公文訊息或收文方回覆中心或發文端確認接收電子公文訊息。

3、收發文記錄查詢

(1)OM11：用戶端向交換中心查詢收發文清單資料。

(2)OM12：交換中心回覆用戶端查詢收發文清單資料。

4、下載用戶資料

(1)OM21 ：用戶端向交換中心要求下載用戶資料。

(2)OM22 ：交換中心回覆下載用戶端之用戶資料。

5、重複傳送公文的申請

(1)OM31：用戶端向交換中心要求重覆發文之請求訊息。

(2)OM32：交換中心回覆用戶端之重覆發文請求訊息。

6、下載代擬代判授權資料

(1)OM41：用戶端向交換中心要求下載代擬代判授權資料。

(2)OM42：交換中心回覆下載用戶端之代擬代判授權資料。

7、異常處理

OM90：處理錯誤訊息。

各類訊息之傳送方式如下表所列：

		FTP	SMTP
電子公文封收發	OM00	V	
公文訊息收發	OM01		V
	OM02	V	
	OM03	V	V
收發文記錄查詢	OM11	V	
	OM12		V
下載用戶資料	OM21	V	
	OM22		V
重複傳送公文的申請	OM31	V	
	OM32		V
下載代擬代判資料	OM41	V	
	OM42		V
異常處理	OM90	V	

第一類經由交換中心傳遞所使用訊息為

FTP:OM00、OM02、OM03、OM11、OM21、OM31、OM90

SMTP:OM01、OM12、OM22、OM32

第二類點對點方式傳遞所使用訊息為

SMTP:OM01、OM03

(二)各項訊息描述

在 Exchange-Header X-Type 欄若為：

1、"Document"，則 Exchange-Message 為公文文件訊息(Document-Message)

2、"Control"，則 Exchange-Message 為控制訊息(Control-Message)

3、"Check"，則無 Exchange-Message

以下為各訊息的所有相關格式：

1、OM00 訊息代碼

(1)訊息說明

- 使用時機：每一電子公文封 Exchange Data Set 之必備內容，於發送前產生，供交換中心檢查 FEP 端是否時間設定差異過大。
- 傳送方式：FTP。

(2)訊息格式：

- OM00 交換表頭

項次	項　　目	說　　明
1	“X-Type:”△”Check”	訊息類別，內容為："Check"
2	“X-Version:”△”1.0”	版本別，內容為： "1.0"
4	“X-Send-Time:”△Date △Time	發送日期及時間，如：1999/04/29 11:55:12

- OM00 傳輸結構

- OM00 範例

X-Type: Check

X-Version: 1.0

X-Send-Time: 1998/06/25 14:11:10

2、OM01 訊息代碼

(1)訊息說明

- 使用時機：傳送公文本文資料與附件電子檔。
- 傳送方式：SMTP。

(2)訊息格式：

- OM01 交換表頭

項次	項　　目	說　　明
1	“X-Type:” △” Document”	訊息類別，內容為："Document"
2	“X-Version:” △” 1.0”	版本別，內容為："1.0"
3	“X-Sender:” △機關代號	內容為：傳送機關代碼
4	“X-To:” △機關代號	內容為：接收機關代碼
5	“X-Document-ID:” △ Digits	內容為：公文文號
6	“X-Document-Date:” △ Date	公文日期，如：1999/04/29
7	“X-Send-Time:” △Date △Time	發送日期及時間，如：1999/04/29 11:55:12
8	“X-Serial-No:” △ Digits	傳送流水號為 0~999999999 的值，不可重覆
9	“X-Received:” △機關代號△ “accept” △Date△ Time	交換中心收到日期及時間，如：CENTER0001 accept 1999/04/29 11:55:12

- OM01 表頭

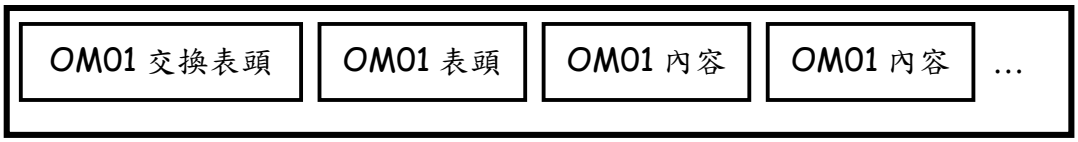
項次	項　　目	說　　明
1	“Type:” △” OM01”	訊息代碼
2	“Record-Count:” △Digits	資料總筆數

- OM01 內容

項次	項　　目	說　　明
1	“File-Name:” △ CharacterString [“.” CharacterString]	電子公文檔案名稱
2	“File-Type:” △ ” exchange-data” | “office-document” |	電子公文檔案類別包括：交換資料、公文、附件、簽章、憑證

	“attachment-document” | “signature-data” | “certificate-data”	
3	“Content-Length:” △Digits	傳送內容長度
4	“Content-Hash:” △CharacterString	對轉碼後的公文或附件檔案作雜湊值運算所得的值，以 16 進制表示，如 0xA1B24CF3

- OM01 傳輸結構



- OM01 範例

X-Type: Document

X-Version: 1.0

X-Sender: 315000000H

X-To: 375090000H

X-Document-Id: 8800004715

X-Document-Date: 1996/07/19

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 1

X-Received: CENTER0001 accept 1998/05/29 09:50:12

Type: OM01

Record-Count: 2

File-Name: od870430.1

File-Type: office-document

Content-Length: 1029

Content-Hash: 0x0B85F6E22D3353A731D0

A9302EB71C7C0774866B

File-Name: cvtoldoc.obj

File-Type: attachment-document

Content-Length: 2200

Content-Hash: 0x71C5378F312C5DC203BD
2B5892FA26DB4EB0F377

3、OM02 訊息代碼

(1)訊息說明

- 使用時機：傳送密碼及雜湊值資料。
- 傳送方式：FTP。

(2)訊息格式：

- OM02 交換表頭

項次	項　　目	說　　明
1	“X-Type:” △” Control”	訊息類別
2	“X-Version:” △” 1.0”	版本別
3	“X-Sender:” △機關代號	傳送機關
4	“X-To:” △機關代號	接受機關
5	“X-Send-Time:” △Date △Time	訊息送出日期及時間，如：1999/04/29 11:55:12
6	“X-Serial-No:” △ Digits	傳送流水號為 0~999999999 的值，不可重覆
7	“X-Received:” △機關代號△ “accept” △Date△ Time	交換中心收到日期及時間，如：CENTER0001 accept 1999/04/29 11:55:12

- OM02 表頭

項次	項　　目	說　　明
1	“Type:” △” OM02”	訊息代碼
2	“Document-Id:” △ Digits	公文文號
3	“Document-Date:” △ Date	公文日期
4	“Serial-No:” △Digits	為 OM01 的傳送流水號
5	“Record-Count:” △ Digits	資料總筆數

- OM02 內容：

項次	項　　目	說　　明
1	“File-Name:” △ CharacterString [“.” CharacterString]	電子公文檔案名稱
2	“File-Type:” △ ” exchange-data” |	電子公文檔案類別包括：交換資料、公文、附件、簽章、憑證

	“office-document” | “attachment-document” | “signature-data” | “certificate-data”	
3	“Content-Length:” △ Digits	傳送內容長度
4	“Content-Hash:” △ CharacterString	對轉碼後的公文或附件檔案作壓縮再加密後，作第二次雜湊值運算所得的值，以 16 進制表示，如 0xA1B24CF3
5	“Decry-Key:” △ CharacterString	對公文或附件檔案加密所用的對稱式金鑰，以 16 進制表示，如 0xA1B24CF3

- OM02 傳輸格式

- OM02 範例

X-Type: Control

X-Version: 1.0

X-Sender: 315000000H

X-To: 375090000H

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 2

X-Received: CENTER0001 accept 1998/05/29 09:50:12

Type: OM02

Document-Id: 8800004715

Document-Date: 1996/07/19

Serial-No: 1

Record-Count: 2

File-Name: od870430.1

File-Type: office-document

Content-Length: 1029

Content-Hash: 0x0B85F6E22D3353A731D0A9
302EB71C7C0774866B

Decry-Key: 0xA731D0A9302EB7

File-Name: cvtoldoc.obj

File-Type: attachment-document

Content-Length: 2200

Content-Hash: 0x71C5378F312C5DC203BD2B
5892FA26DB4EB0F377

Decry-Key: 0x312C5DC203BD2B

4、OM03 訊息代碼

(1)訊息說明

- 使用時機:傳送回交換中心回覆發文端確認訊息資料或收文方回覆中心確認訊息資料。
- 傳送方式：FTP(經由交換中心傳遞)或 SMTP(點對點方式傳遞)。

(2)訊息格式：

- OM03 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送機關
4	"X-To:"△機關代號	接收機關
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間，如：1999/04/29 11:55:12
6	“X-Serial-No:” △Digits	傳送流水號為 0~999999999 的值，不可重覆
7	“X-Received:” △機關代號△ “accept” △Date△Time	交換中心收到日期及時間，如：CENTER0001 accept 1999/04/29 11:55:12

- OM03 表頭

項次	項　　目	說　　明
1	"Type:"△"OM03"	訊息代碼
2	"Sender:"△機關代號	發文機關
3	"Receiver:"△機關代號	接收機關
4	"Document-Id:"△Digits	公文文號
5	"Document-Date:"△Date	公文日期
6	"Serial-No:"△Digits	為 OM01 的傳送流水號
7	"Send-Time:"△Date△Time	發文機關傳送日期及時間
8	“Auth-Time:” △機關代號△ “accept” △Date△Time	交換中心收到日期及時間，如：CENTER0001 accept 1999/04/29 11:55:12
9	"Receive-Time:"△Date△Time	收文機關收到日期及時間

- OM03 傳輸格式

- OM03 範例

X-Type: Control

X-Version: 1.0

X-Sender: 375090000H

X-To: 315000000H

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 3

X-Received: CENTER0001 accept 1998/05/29 09:50:12

Type: OM03

Sender: 315000000H

Receiver: 375090000H

Document-Id: 8800004715

Document-Date: 1996/07/19

Serial-No: 1

Send-Time: 1998/05/29 09:47:52

Auth-Time: CENTER0001 accept 1998/05/29 09:50:12

Receive-Time: 1998/05/29 09:47:52

5、OM11 訊息代碼

(1)訊息說明

- 使用時機：用戶端向交換中心要求查詢收發文清單資料。
- 傳送方式：FTP。

(2)訊息格式：

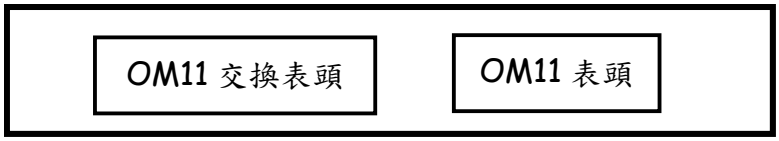
- OM11 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送機關
4	"X-To:"△機關代號	接收之交換中心
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間
6	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

- OM11 表頭：

項次	項　　目	說　　明
1	"Type:"△"OM11"	訊息代碼
2	"List-Type:"△”1”|”2”	清單類別，”1”代表發文清單，”2”代表收文清單
3	"Document-Date-Start:"△Date	開始日期
4	“Document-Date-End:”△Date	結束日期

- OM11 傳輸格式



- OM11 範例

X-Type: Control

X-Version: 1.0

X-Sender: 315000000H

X-To: CENTER0001

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 3

Type: OM11

List-Type: 1

Document-Date-Start: 1998/05/29

Document-Date-End: 1998/05/29

- 備註：

  “Document-Date-Start “與” Document-Date-End”兩欄位均需具備，且” Document-Date-Start “之值不能大於” Document-Date-End” 之值。

6、OM12 訊息代碼

(1)訊息說明

- 使用時機：交換中心回覆用戶端查詢收發文端資料。
- 傳送方式：SMTP。

(2)訊息格式：

- OM12 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送之交換中心
4	"X-To:"△機關代號	接收機關
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間
6	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

- OM12 表頭

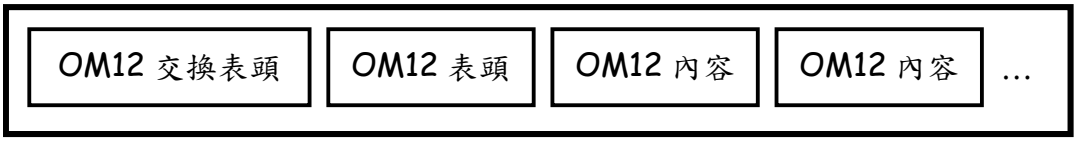
項次	項　　目	說　　明
1	"Type:"△" OM12"	訊息代碼
2	"List-Type:"△”1” | “2”	清單類別，”1”代表發文清單，”2”代表收文清單
3	"Document-Date-Start:"△Date	開始日期
4	“Document-Date-End:”△Date	結束日期
5	"Serial-No:"△Digits	為 OM11 傳送流水號，交換中心主動傳送之收發文清單無此一欄位
6	"Record-Count:"△Digits	OM12 資料總筆數

- OM12 內容：

項次	項　　目	說　　明
1	" Sender:"△機關代號	發文機關
2	"Receiver:"△機關代號	接收機關
3	"Document-Id:"△Digits	公文文號
4	"Document-Date:"△Date	公文日期
5	"Serial-No:"△Digits	為 OM01 的傳送流水號
6	"Send-Time:"△Date△Time	發文機關傳送日期及時間

項次	項　　目	說　　明
7	“Auth-Time:” △ 機關代號△ “accept” △Date △Time	交換中心收到日期及時間，如：CENTER0001 accept 1999/04/29 11:55:12
8	"Receive-Time:"△Date △Time	收文機關收到日期及時間

- OM12 的傳輸結構



- OM12 範例

X-Type: Control

X-Version: 1.0

X-Sender: CENTER0001

X-To: 315000000H

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 1

Type: OM12

List-Type: 1

Document-Date-Start: 1998/05/29

Document-Date-End: 1998/05/29

Serial-No: 3

Record-Count: 4

Sender: 315000000H

Receiver: 375090000H

Document-Id: 8800004715

Document-Date: 1996/07/19

Serial-No: 1

Send-Time: 1998/05/29 09:47:52

Auth-Time: CENTER0001 accept 1998/05/29 09:50:12

Receive-Time: 1998/05/29 09:47:52

Sender: 315000000H

Receiver: 315150000H

Document-Id: 8800004716

Document-Date: 1996/07/19

Serial-No: 8

Send-Time: 1998/05/29 09:47:52

Auth-Time: CENTER0001 accept 1998/05/29 09:50:12

Receive-Time: 1998/05/29 09:47:52

Sender: 315000000H

Receiver: 315100000H

Document-Id: 8800004718

Document-Date: 1996/07/19

Serial-No: 18

Send-Time: 1998/05/29 09:47:52

Auth-Time: CENTER0001 accept 1998/05/29 09:50:12

Receive-Time: 1998/05/29 09:47:52

Sender: 315000000H

Receiver: 315000000HA340000

Document-Id: 8800004720

Document-Date: 1996/07/19

Serial-No: 12

Send-Time: 1998/05/29 09:47:52

Auth-Time: CENTER0001 accept 1998/05/29 09:50:12

Receive-Time: 1998/05/29 09:47:52

7、OM21 訊息代碼

(1)訊息說明

- 使用時機：用戶端向交換中心要求下載用戶資料。
- 傳送方式：FTP。

(2)訊息格式：

- OM21 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送機關
4	"X-To:"△機關代號	接收之交換中心
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間
6	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

- OM21 表頭：

項次	項　　目	說　　明
1	"Type:"△"OM21"	訊息代碼
2	"Update-Type:" △ ”1” | “2”	更新類別，”1” 代表全部更新，”2” 代表部份更新
3	"Update-Start-Date:" △ Date	更新開始日期，全部更新無此一欄位

- OM21 傳輸格式

- OM21 範例

X-Type: Control

X-Version: 1.0

X-Sender: 315000000H

X-To: CENTER0001

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 3

Type: OM21

Update-Type: 2

Update-Start-Date: 1998/05/29

8、OM22 訊息代碼

(1)訊息說明

- 使用時機：交換中心回覆下載用戶端之用戶資料。
- 傳送方式：SMTP。

(2)訊息格式：

- OM22 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送之交換中心
4	"X-To:"△機關代號	接收機關
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間
6	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

- OM22 表頭

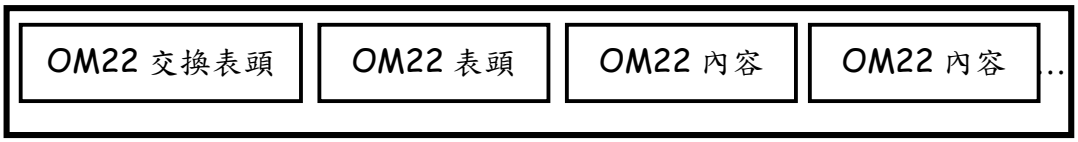
項次	項　　目	說　　明
1	"Type:"△" OM22"	訊息代碼
2	"Update-Type:"△”1” | “2”	更新類別，”1”代表全部更新，”2”代表部份更新
3	"Update-Start-Date:"△Date	更新開始日期，全部更新無此一欄位
5	"Serial-No:"△Digits	同 OM21 傳送流水號，交換中心主動傳送之用戶異動資料無此一欄位
6	"Record-Count:"△Digits	OM22 資料總筆數

- OM22 內容：

項次	項　　目	說　　明
1	"Update-Method:"△"New" |"Change" |"Delete"	異動類別包括：新增、修改、刪除
2	"Org-Id:"△機關代號	機關代碼
3	"Org-Name:"△ChineseCharacterString	機關全名，以 CNS11643 中文標準交換碼表示
4	"Active-Status:"△”Active” | “Suspend”	使用狀態包括:使用中、暫停
5	"Org-Email:"△	機關電子郵件信箱，以完整的電子郵件位

項次	項　　目	說　　明
	CharacterString	址當做內容
6	“Relate-Org-Id”	群組代表之機關代碼
7	“Relate-Attribute:” △"Group" ｜"Member"	群組屬性包括群組代表或群組成員
8	“Certify-No:”	憑證序號

- OM22 的傳輸結構



- OM22 範例

X-Type: Control

X-Version: 1.0

X-Sender: CENTER0001

X-To: 315000000H

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 1

Type: OM22

Update-Type: 2

Update-Start-Date: 1998/05/29

Serial-No: 3

Record-Count: 2

Update-Method: New

Org-Id: 375090000H

Org-Name: →F:}$R\QIM4G()W)(

Active-Status: Active

Org-Email:odmail@motc.gov.tw

Relate-Org-Id: 375090000H

Relate-Attribute:Group

Certify-No:700002616

Update-Method: Change

Org-Id: 315100000H

Org-Name: →G()W)eg*rSRfK6MT

Active-Status: Suspend

Org-Email:odmail@rdec.gov.tw

Relate-Org-Id: 315100000H

Relate-Attribute:Group

Certify-No:700002610

9、OM31 訊息格式

(1)訊息說明

- 使用時機：用戶端向交換中心要求重覆發文之請求訊息。
- 傳送方式：FTP。

(2)訊息格式：

- OM31 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送機關
4	"X-To:"△機關代號	接收之交換中心
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間
6	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

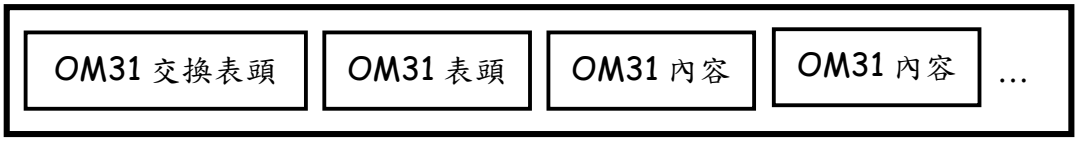
- OM31 表頭：

項次	項　　目	說　　明
1	"Type:"△"OM31"	訊息代碼
2	"Record-Count:"△Digits	OM31 資料總筆數

- OM31 內容：

項次	項　　目	說　　明
1	" Sender:"△機關代號	發文機關
2	"Receiver:"△機關代號	接收機關
3	"Document-Id:"△Digits	公文文號
4	"Document-Date:"△Date	公文日期
5	"Serial-No:"△Digits	為 OM01 的傳送流水號

- OM31 傳輸格式



- OM31 範例

X-Type: Control

X-Version: 1.0

X-Sender: 315000000H

X-To: CENTER0001

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 3

Type: OM31

Record-Count: 4

Sender: 315000000H

Receiver: 375090000H

Document-Id: 004715

Document-Date: 1996/07/19

Serial-No: 1

Sender: 315000000H

Receiver: 315150000H

Document-Id: 004715

Document-Date: 1996/07/19

Serial-No: 8

Sender: 315000000H

Receiver: 315100000H

Document-Id: 004715

Document-Date: 1996/07/19

Serial-No: 18

Sender: 315000000H

Receiver: 315002200

Document-Id: 004715

- 備註：

  “Sender”、”Receiver” 、”Document-Id” 、”Document-Date” 、”Serial-No”五欄位均需具備。

10、OM32 訊息代碼

(1)訊息說明

- 使用時機：交換中心回覆用戶端的 OM31 訊息。
- 傳送方式：SMTP。

(2)訊息格式：

- OM32 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送之交換中心
4	"X-To:"△機關代號	接收機關
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間
6	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

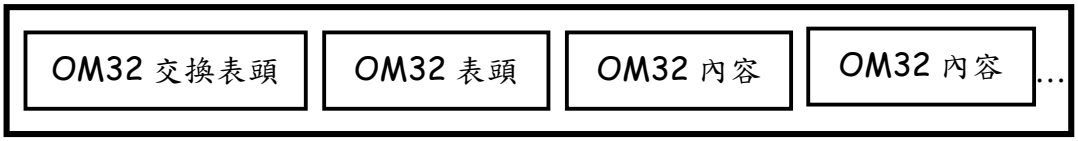
- OM32 表頭：

項次	項　　目	說　　明
1	"Type:"△"OM32"	訊息代碼
5	"Serial-No:"△Digits	為 OM31 傳送流水號
2	"Record-Count:"△Digits	OM32 資料總筆數

- OM32 內容：

項次	項　　目	說　　明
1	" Sender:"△機關代號	發文機關
2	"Receiver:"△機關代號	接收機關
3	"Document-Id:"△Digits	公文文號
4	"Document-Date:"△Date	公文日期
5	"Serial-No:"△Digits	為 OM01 的傳送流水號
6	"Retrieval-Status:"△"Ok" | "Error"	重送狀況包括:完成、錯誤

- OM32 傳輸格式



- OM32 範例

X-Type: Control

X-Version: 1.0

X-Sender: 315000000H

X-To: CENTER0001

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 3

Type: OM32

Record-Count: 4

Sender: 315000000H

Receiver: 375090000H

Document-Id: 004715

Document-Date: 1996/07/19

Serial-No: 1

Retrieval-Status: Ok

Sender: 315000000H

Receiver: 315150000H

Document-Id: 004715

Document-Date: 1996/07/19

Serial-No: 8

Retrieval-Status: Ok

Sender: 315000000H

Receiver: 315100000H

Document-Id: 004715

Document-Date: 1996/07/19

Serial-No: 18

Retrieval-Status: Error

Sender: 315000000H

Receiver: 315000000HU340000

Document-Id: 004715

Document-Date: 1996/07/19

Serial-No: 12

Retrieval-Status: Ok

11、OM41 訊息代碼

(1)訊息說明

- 使用時機：用戶端向交換中心要求下載代擬代判授權資料。
- 傳送方式：FTP。

(2)訊息格式：

- OM41 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送機關
4	"X-To:"△機關代號	接收之交換中心
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間
6	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

- OM41 表頭：

項次	項　　目	說　　明
1	"Type:"△"OM41"	訊息代碼

- OM41 傳輸格式

- OM41 範例

X-Type: Control

X-Version: 1.0

X-Sender: 315000000H

X-To: CENTER0001

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 3

Type: OM41

12、OM42 訊息代碼

(1)訊息說明

- 使用時機：交換中心回覆下載用戶端之代擬代判授權資料，或由交換中心主動傳送代擬代判授權資料。
- 傳送方式：SMTP。

(2)訊息格式：

- OM42 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送之交換中心
4	"X-To:"△機關代號	接收機關
5	"X-Send-Time:"△Date△Time	訊息送出日期及時間
6	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

- OM42 表頭

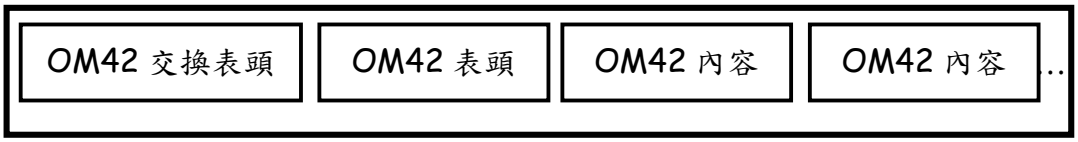
項次	項　　目	說　　明
1	"Type:"△" OM42"	訊息代碼
2	"Serial-No:"△Digits	同 OM41 傳送流水號，交換中心主動傳送之代擬代判授權資料無此一欄位
3	"Record-Count:"△Digits	OM42 資料總筆數

- OM42 內容：

OM42 內容範圍僅包括各連線機關之代擬代判被授權資料

項次	項　　目	說　　明
1	" Aut-Org-Id-Encry :"△加密授權機關代號	加密授權機關代號，以十六進位制表示
2	Update-Date:”△Date	異動日期
3	“Ctr-Signature:”△簽章	計算密文的 Hash 值，用中心的憑證加簽
4	“Word-Encry-Count:” △Digits	加密代字號筆數
5	“Word-Encry:”△加密代字號	加密代字號，以十六進位制表示，以‘OM42’作為分隔

- OM42 的傳輸格式



- OM42 內容安全處理做法

1.加密的授權機關代碼

來源：交換中心資料庫的授權機關代碼

產生方式：以訊息接收機關的公鑰加密

2.數位簽章：

來源：加密的授權機關代碼

產生方式：計算授權機關代碼密文的雜湊值，用中心密鑰產生數位簽章

3.加密的發文代字號：

來源：交換中心資料庫的授權機關發文代字號資料

產生方式：以訊息接收機關的公鑰加密

- OM42 範例

X-Type: Control

X-Version: 1.0

X-Sender: CENTER0001

X-To: 315000000H

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 1

Type: OM42

Serial-No: 3

Record-Count: 1

Aut-Org-Id-Encry: :←ㄩ‘?芋\?n↕赶]⊥⊥　　扶　W?%?s 湟)??[@

匐]摜??"e¶x ?‘ n 盞 鼏啟錕←F 叟葭　1?瑲↑/棻?!

覾 aw???塶焰　鐊?筐?

App-Date: 1999/07/19

Ctr-Signature:

Word-Encry: W?%?s 湟)??[@;1?瑲↑/棻?! 覾 aw

13、OM90 訊息代碼

(1)訊息說明

- 使用時機：傳送處理錯誤訊息。
- 傳送方式：FTP。

(2)訊息格式：

- OM90 交換表頭

項次	項　　目	說　　明
1	"X-Type:"△"Control"	訊息類別
2	"X-Version:"△"1.0"	版本別
3	"X-Sender:"△機關代號	傳送之交換中心
4	"X-To:"△機關代號	接收機關
5	"X-Document-ID:"△Digits	公文文號
6	"X-Send-Time:"△Date△Time	訊息送出日期及時間
7	"X-Serial-No:"△Digits	傳送流水號為 0~999999999 之值，不可重覆

- OM90 表頭

項次	項　　目	說　　明
1	"Type:"△"OM90"	訊息代碼
2	“Document-Id:” △Digits	公文文號
3	“Document-Date:” △Date	公文日期
4	"Serial-No:"△Digits	錯誤 OM 訊息的傳送流水號
5	"Error-Code:"△ErrorNo	錯誤代碼
6	"Error-Content:"△CharacterString	錯誤訊息內容

- OM90 傳輸格式

- OM90 錯誤代碼表

最新錯誤代碼於交通部網站公佈表，其範例說明如下：

錯誤代碼	錯誤內容
1001	Hash 1 Error
1002	Hash 2 Error
1003	RSA Error
1004	機關代碼錯誤
1005	壓縮檔案錯誤
1006	發文機關未獲授權
1007	收文機關停用
1008	系統時差過大
1009	中文碼錯誤
1010	XML 格式錯誤
1011	資料總筆數與實際內容筆數不符合
1012	OM01 未收到
1013	OM02 未收到
1014	OM01 格式錯誤
1015	OM02 格式錯誤
1016	OM11 格式錯誤
1017	OM21 格式錯誤
1018	OM31 格式錯誤
1019	OM41 格式錯誤

- OM90 範例

X-Type: Control

X-Version: 1.0

X-Sender: 375090000H

X-To: 315000000H

X-Send-Time: 1998/05/29 09:47:52

X-Serial-No: 3

Type: OM90

Document-Id: 8800004715

Document-Date: 1996/07/19

Serial-No: 1

Error-Code: 1007

Error-Content: 收文機關 xxxxxxxxxx 停用

六、軟體功能說明

（以下各項傳遞交換功能或可與文書製作、流程管理等作業相整合）

(一)電子收發文管理

電子收發文其處理過程中必須完成下列事項。方法如下：

1、中文轉碼：處理公文檔案中文轉碼的工作。

(1)CNS11643 與 BIG5、BIG5E 中文碼的轉碼功能。

(2)使用者自造字內碼與 CNS11643 的轉碼功能。

(3)可設定、維護使用者自造字內碼與 CNS11643 之對照。

2、代碼轉換：可自動執行機關內部代碼與標準代碼轉換。

(1)可自動執行機關內部代碼與標準代碼轉換。

(2)可設定、維護機關內部代碼與標準代碼轉換之對照。

3、收送記錄：記錄電子公文收送相關資訊。

(1)記錄電子公文收送日期及時間功能。

(2)記錄電子公文收/發文機關及收文回復功能。

4、傳輸對象管理：可接收及查詢交換中心的用戶資料檔。

(1)查詢用戶功能。

(2)列印用戶資料檔功能。

5、確認回覆：收文經確認程序後自動回覆 OM03 格式訊息予交換中心。

(二)通信管理

通信管理的主要功能在處理前置軟體與電子公文交換系統間的通信。以下說明通信管理提供的功能：

1、通訊等級設定

(1)快遞件級：優先權最高，為立即傳送。

(2)掛號件級：優先權介於快遞件級與普通件級之間，依照所設定的文件

傳輸間隔傳送。

(3)普通件級：優先權最低，集中在夜間減價時段一次傳送當天所有普通級件，可避開通信尖峰時間。

2、傳輸設定

(1)設定時間間隔功能：可設定文件收送之時間或間隔。

(2)計算文件輸送量功能：計算郵件大小，當郵件大小超過設定值時，可自動降低郵件通信等級，或安排在夜間傳送。

3、網路連線設定

(1)網路中斷提示功能

(2)資料續傳功能

(3)自動撥接功能

(三)收文列印

列印前需先比對雜湊值正確後，方依「文書處理手冊」公文格式印出並加印頁碼、騎縫標識，文末需有「電子公文交換戳記」，並可視需要加印電子收文日期時間。

列印前需先比對雜湊值若為不正確，應於公文明顯位置標示著名字樣，以資識別。

1、騎縫標識可依自訂公式製作防偽校對字組，其基本原則如下：

(1)每兩頁公文之間加印騎縫標識乙次。

(2)騎縫標識切割後分別列印於相鄰兩頁公文之左右邊。

(3)騎縫標識列印位置及分割原則可隨機改變。

(4)僅一頁之公文不印騎縫標識。

(5)電子騎縫章蓋印位置及角度說明，每一頁蓋印的角度及位置由電腦隨機產生於不同位置。

2、騎縫標識可為『騎縫章』、『防偽押花』或其他任何由收文機關自行

採擇之標識。

3、附件列印頁頁碼及騎縫標識之處理方式亦同。

(四)管理功能

管理功能主要針對終端用戶提供使用者人機介面,供使用者方便於維護管理電子公文。

其作業方式如下：

1、自動化處理功能：可設定自動處理時段，自動確認所接收之文件，依IC 智慧卡(相關規範詳後說明)上之 Private Key 自動解密，並直接列印於系統印表機上。

(1)自動處理時段設定功能。

(2)自動解密功能。

(3)自動列印公文功能。

(4)自動公文處理記錄功能。

2、資料維護功能：可備份、回復(Restore)及清檔的功能。

(1)備份資料功能。

(2)回復資料功能。

(3)清檔功能。

3、狀況顯示功能：可即時顯示目前機器處理狀況。

(1)已收公文顯示功能。

(2)待發公文顯示功能。

(3)處理中公文顯示功能。

(4)錯誤資料顯示(警示)功能。

4、系統備份/回復功能。

(1)系統備份功能。

(2)系統回復功能。

(3)自動備份設定功能。

5、資料安全功能：應具備使用者安全檢驗機制，如：

(1)作業系統檢核使用者功能。

(2)應用軟體檢核使用者功能。

(3)設定資料讀取權限功能。

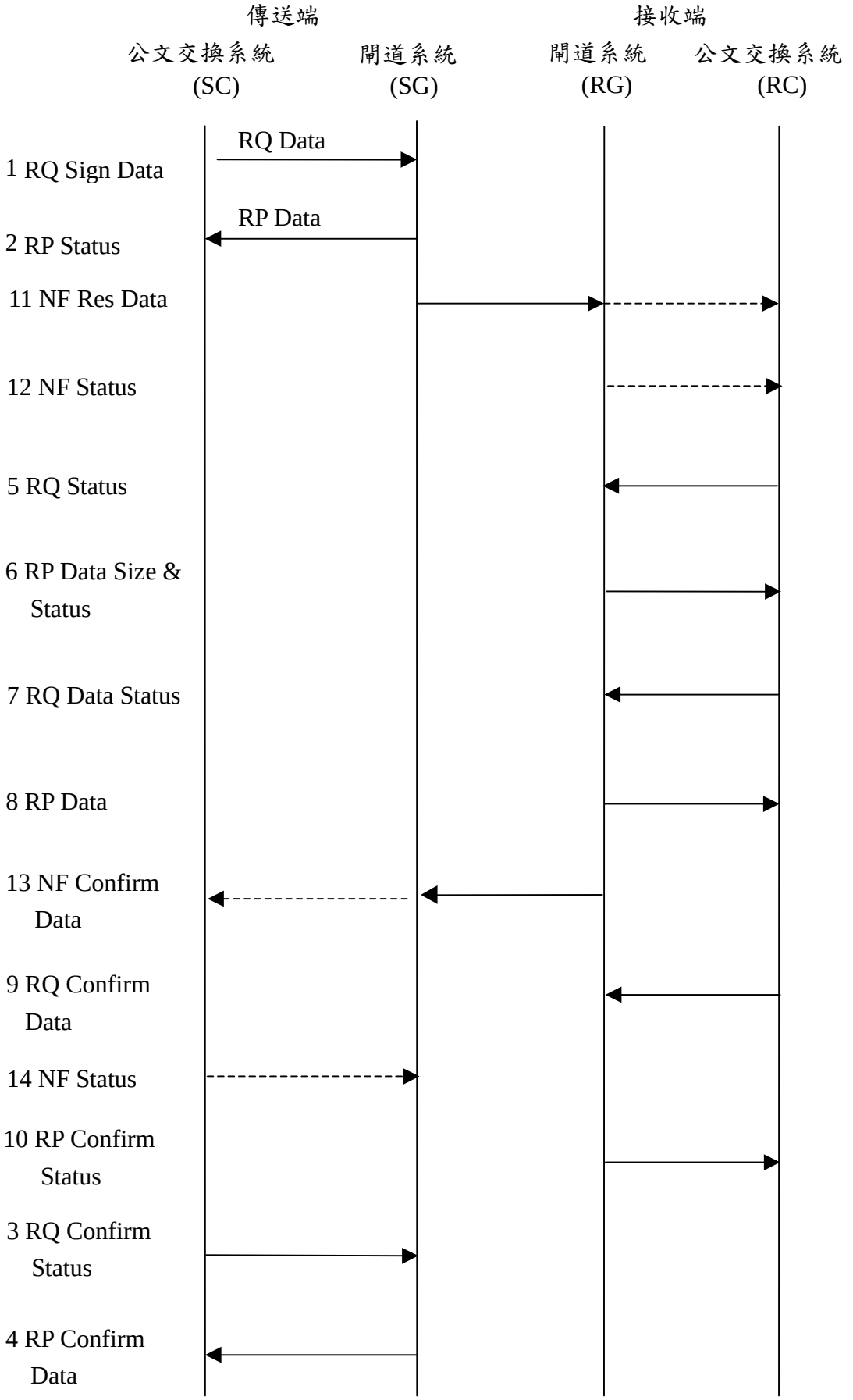
6、使用者識別功能：應提供使用者權限管理之功能。

7、系統應有校時功能。

附錄三：公文閘道系統補充說明(草案，系統建置案完成視需要更新)

進行公文電子交換前,首先公文交換系統須向閘道系統請求建立一TCP連結後，在該連結中將編碼後之資料完整送至閘道系統，並於閘道系統回覆結果後關閉該連結。

當接收端公文交換系統（以下簡稱RC）支援閘道系統（以下簡稱RG）Notification模式時，由RC提供TCP/IP連結方式與RG間之通訊作業。RC以Two-Way之Request-and-Response方式與RG間進行Client-Server形態之資料交換過程中，RC作為Server，其通訊埠預設為18089；RG作為Client。RG須向RC請求建立TCP連結後，在該連結中將編碼之Notification訊息完整送至RC端，並於RC回覆結果後關閉該連結。有關閘道系統API語法演譯說明如下：


傳送端
接收端
公文交換系統
(SC)
閘道系統
(SG)
閘道系統
(RG)
公文交換系統
(RC)
RQ Data
1 RQ Sign Data
RP Data
2 RP Status
11 NF Res Data
12 NF Status
5 RQ Status
6 RP Data Size & Status
7 RQ Data Status
8 RP Data
13 NF Confirm Data
9 RQ Confirm Data
14 NF Status
10 RP Confirm Status
3 RQ Confirm Status
4 RP Confirm Data

一、公文交換系統使用閘道系統 API 作業規範

閘道系統為一項提供公文交換系統間轉送服務之軟體，閘道系統需設置一部電腦稱為閘道器(以下簡稱 GWP)，當公文交換系統依一定傳輸編碼規範，將公文送入 GWP 後，由閘道系統負責轉送，此轉送之收文端需具備 GWP。

（一）當發文端公文交換系統透過閘道系統傳送公文時，處理方式如下:

1、由 SC　RG 下達 RQ Sign Data，其介面程式為 SC2SG_Data。

2、當 SG 收到 SC 之 RQ 後，必須回復 RP status，其介面程式為 SG2SC_Data_Response。

3、其後由 SG 2 RG 及 RG 2 RC 對發文端而言，沒有任何動作。

4、發文端公文交換系統，必須定時向 SG 請求 confirm，即收取收文端收文回條，即由 SC to SG 下達 RQ confirm status，其 API 為 SC2SG_Query

5、當 SG 收而 SC 之 RQ 後，必須回復，RPconfirmData，其介面程式為 SG2SC_Query_Response。

（二）SG to RG 間資料傳送，由閘道系統負責，包括轉送過程簽章，加密等另外規範。

（三）公文交換系統依系統本身特性，定時向所屬 GWP，請求接收資料，當收文端公文交換系統，向其 GWP 請求接收資料時，依下列步驟處理:

1、由 RC to RG 下達 RQ status，其 API 為 RC2RG_Query。

2、當 RG 收到 RC 之 RQ 後，必須回復 RP Datasize & status，其 API 為 RG2RC_Query_Response。

3、當 RG 回復之 status 表示有資料時，同時會回復資料大小，因此 RC 依收到資訊，以 RQ Data & status 向 RG 請求傳送 Data，其 API 為

RC2RG_Data。

4、當 RG 收到 RC 之 RQ 時，RG 必須回復 Data，其 API 為 RG2RC_Data_Response。

5、當 RC 收到 RG 之 Data，並檢查無誤後，由公文交換系統製作回條，必須向 RG 確認，即由 RC to RG 下達 RQ confirm Data，其 API 為 RC2RG_Data_confirm。

6、當 RG 收到 RC 之 Confirm，會自動將 confirm Data 轉送至發文端公文交換系統。

7、同時 RG 必須向 RC 回復，即 RP confirm status，其 API 為 RG2RC_Data_confirm_Response。

(四)以上語法縯繹係考慮由公文交換系統為 client，閘道系統為 sever，即由公文交換系統以 Batch 方式，將欲轉送之資料主動請 GWP 轉送，並以 Batch 方式，定時向 GWP 請求接收資料，較合乎目前各機關公文收發之習慣，且不易產生系統死結。

(五)對於時效性公文，為達到即時傳送之目的，另增加兩組介面程式，由 GWP 通知公文交換系統，即 GWP 為 client，公文交換系統為 sever，稱為 Notification。

(六)當 RG 接收到 SG 轉來之 Data，如為特急件時，為使 RC 立即接收 Data，由 RG to RC 下達 NF resData 之請求，其 API 為 RG2RC_Notification。

(七)當 RG 發送通知後，原則上 RC 應回復 status，但 RG 於發送後，3 秒內未收到回復，應再次通知，再通知以三次為限。

(八)當 RC 收到 RG 之通知時，應先回復 RG　NF status，其 API 為 RC2RG_Notification confirm。

(九)當 SG 收到 RG 轉來之 confirm Data 時，為使 SC 立即得到 confirm，

由 SG to SC 下達 NF confirm 之請求，其 API 為 SG 2 SC Notification。

(十)當 SG 發送通知後，原則上 SC 應回復 status，但 SG 於發送後，3 秒內未收到回復，應再通知，再通知以三次為限。

(十一)當 SC 收到 SG 之通知時應先回復 SG NF status，其 API 為 SC2SG_Notification_confirm。

二、公文本文、附件及數位簽章資料傳輸編碼原則

公文本文及其附件產生數位簽章簽體格式及檔案相互關連方式，原則採用 ASN.1 規範之 DER 方式產生唯一編碼，且其 TAG 皆採 Explicit。

傳輸使用檔案資料 ASN.1 編碼規範如下:

```
Package ::= SEQUENCE {
version          INTEGER,                          -- 0 代表第一版本
mainDoc          MainDoc,                          -- 公文本文
attachments      SEQUENEC OF Attachment            -- 公文附件序列，當無
                 附件時編碼之長度資訊使用 0x00
attachmentCount INTEGER                            --附件數量
}
MainDoc ::= CHOICE {
doc              [0] EXPLICIT Doc                  -- 未加密之公文
encryptedDoc     [1] EXPLICIT EnvelopedData        -- 即 pkcs#7
                    envelopedData 之加密公文
}
Doc ::= SEQUENCE {
type                 INTEGER,                      -- xml(0)
data                 OCTET STRING,                 -- 公文資料串，
                      OCTET STRING 方式編碼
signature            SEQUENCE OF AttachmentSignature
 -- 本文之簽體序列，可支援多個簽章，無簽體時以長度為 0x00 填入
}
-- Attachment 為附件資料
Attachment ::= SEQUENCE {
filename          Utf8string,                       -- 附件檔案名稱
message           Utf8string,                       -- 附件檔案額外說明
type              SEQUENCE {
    majorType        INTEGER,
    subType          INTEGER
},

data         OCTET STRING,
             -- 附件內容，以 OCTET STRING 編碼
signature    SEQUENCE OF AttachmentSignature
            -- 附件之簽章序列，可支援多個簽章，無簽體時長度須為 0x00
}
-- majorType 之定義如下：
-- text(0)       - 以文字為主之檔案
-- image(1)      - 以影像、多媒體表現之檔案
```

```
-- package(2)    - 公文附件可以來文為附件
-- sigData(3)    - 公文及附件之數位簽章與文件分離，並另以附件方式傳送

-- 當 majorType 為(0)時，subType 之定義
-- xml(0)
-- pdf(1)
-- wdl(2)
-- other(3)

-- 當 majorType 為(1)時，subType 之定義
-- jpeg(0)       - 靜態圖形檔案格式
-- iges(1)       - 工程圖形檔案格式
-- mpeg(2)       - 動態檔案格式
-- wav(3)        - 聲音檔案格式
-- mpeg(4)       - 動態影像格式
-- AttachmentSignature 為以某指定文件之檔案內容做簽章之資訊
  AttachmentSignature ::= SEQUENCE {
    signerDn          GeneralName,
          -- 簽章者 dn, 用以識別簽章者
   signerSN           INTEGER,
          -- 簽章者之憑證序號，配合 signerDn 可唯一識別簽章者
   signerKeyId        OCTET STRING
          -- RFC 2459 規範之公鑰以識別多個憑證中某一簽章之公鑰
   signatureAlg       algorithmIdentifier,
          -- 簽章使用之演算法
   attachFilename     UTF8string
          -- 對附件檔案之簽體，其長度為 0 時以 0x00 為代表,檔案名稱同附件檔
             名,簽章附件檔名以”.sig”作為延伸檔名對公文主體 MainDoc 之簽
             章,檔案名稱同公文檔名,簽章附件檔名以”.sig”作為延伸檔名
    signatureContent BIT STRING
          -- 簽體內容，以 BIT STRING 方式將簽體編碼
}
其中之 AlgorithmIdentifier 為定義簽章者所使用之簽章演算法，參考
[RFC2459]之定義如下：
AlgorithmIdentifier::=  SEQUENCE {
    Algorithm     ALGORITHM-ID.&id({SupportedAlgorithms}),
    parameters    ALGORITHM-ID.&Type({SupportedAlgorithms}
                              { @algorithm}) OPTIONAL }
ALGORITHM-ID ::= CLASS {
    &id           OBJECT IDENTIFIER UNIQUE,
    &Type         OPTIONAL
} WITH SYNTAX { OID &id [PARMS &Type] }
目前[RFC2459]定義支援之簽章演算法包括：
```

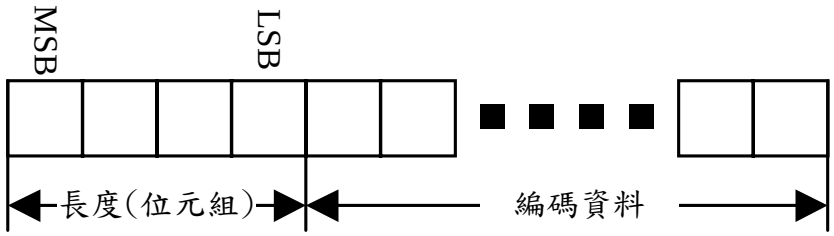
```
SupportedAlgorithms ALGORITHM-ID::= {
    , -- extensible
    rsaPublicKey |
    rsaSHA-1  |
    rsaMD5 |
    rsaMD2 |
    dssPublicKey |
    dsaSHA-1 |
    dhPublicKey }
```

其中各項簽章演算法之 OID 定義如下：

```
rsaPublicKey ALGORITHM-ID ::=
    { OID rsaEncryption PARMS NULL }
rsaSHA-1 ALGORITHM-ID ::=
    { OID sha1WithRSAEncryption PARMS NULL }
rsaMD5 ALGORITHM-ID ::=
    { OID md5WithRSAEncryption PARMS NULL  }
rsaMD2 ALGORITHM-ID ::=
    { OID md2WithRSAEncryption PARMS NULL  }
dssPublicKey ALGORITHM-ID ::=
    { OID id-dsa PARMS Dss-Parms }
dsaSHA-1 ALGORITHM-ID ::=
    { OID id-dsa-with-sha1 }
dhPublicKey ALGORITHM-ID ::=
    {OID dhpublicnumber PARMS DomainParameters}
```

三、公文交換系統使用閘道系統資料傳輸 API，ASN.1 編碼規範

公文交換系統與 GWP 間之資料傳送協定規範以位元組(Byte)為基本單位，所有傳輸均為先傳送四位元組之資料，代表其後資料長度資訊(DataLength)。資料長度以 Big-Endian 方式編碼，即第一位元組為權值(Weight)最大之位元組(Most Significant Byte, MSB)，第四位元組為權值(Weight)最小之位元組(Least Significant Byte, LSB)。DataLength 其後之資料總長度仍以位元組為單位，共 DataLength 位元組數。資料之編碼原則須遵循 ASN.1(X.680 以及 X.690)之方式，並採用 ASN.1 規範之 DER 方式產生唯一編碼。資料之組成簡示如下：



version	INTEGER,	-- 0 代表第一版本
type	INTEGER,	
content	ANY DEFINED BY type	-- 詳述於後

}

本語法(Data)中，version 為版本識別用，此版本為 0，代表第一版。相同版本中之語法固定，本規範中各系統於實作通訊協定時，須先檢驗版本是否正確；如系統無法處理不同之版本時，須遵循本規範回覆無法支援該版本之訊息。本文件中，為進一步簡化閘道器及公文交換系統於運作中之不同表示，將以 SC 代表發文端公文交換系統、SG 代表發文端閘道器、RC 代表收文端公文交換系統、RG 代表收文端閘道器、Data 代表傳輸資料、Query 代表狀態查詢、Response 代表回覆資訊、Notification 代表資料備妥通知、Confirm 代表資料確認。

Type 值代表各種不同用途，與 content 配合使用。content 之定義

依 type 值而異，其值內容說明如下：

2 代表 SC2SG_Data，

3 代表 SG2SC_Data_Response，

4 代表 SC2SG_Query，

5 代表 SG2SC_Query_Response，

6 代表 RC2RG_Query，

7 代表 RG2RC_Query_Response，

8 代表 RC2RG_Data，

9 代表 RG2RC_DataR_esponse，

10 代表 RC2RG_Data_Confirm，

11 時代表 RG2RC_Data_Confirm_Response，

12 時代表 RG2RC_Notification，

13 時代表 RC2RG_Notification_Confirm，

14 時代表 SG2SC_Notification，

15 時代表 SC2SG_Notification_Confirm。

上述 content 各種資料編碼規範細節詳述如下。

(一)SC 至 SG 發送請求編碼規範

```
SC2SGData ::= SEQUENCE{
  version   INTEGER,              -- 0 代表第一版本
  mID       PrintableString,      --由 SC 決定之唯一訊息識別
  status    INTEGER,              -- SC 之狀態，保留暫不使用
  message   UTF8String,           -- 額外告知 SG 訊息
  orgID     PrintableString,      -- 該資料目的地機關代碼
  ouID      PrintableString,      -- 該資料目的地單位代碼
  SCIP      PrintableString,      -- SC 之 IP
  SGIP      PrintableString,      -- SG 之 IP
  RCIP      PrintableString,      -- RC 之 IP
  RGIP      PrintableString,      -- RG 之 IP
  package           Package       -- 傳送資料包，
                                  -- 包括公文以及附件
```

}

本語法用以支援 SC 向 SG 請求將資料透過 RG 轉送至 RC 中。

version 為版本識別用，此版本為 0(0x02 0x01 0x00)，代表第一版。

mID 為由 SC 決定之一亂數，用以識別某一請求以及 SG 回覆是否一致用。

status 為 SC 告知 SG 之目前狀態，於此版本並未使用，應以 0 值填入(0x02 0x01 0x00)。

message 為 SC 對於該資料之額外說明；於此版本中，若該檔案存在於 SC 中，可為該資料於該 SC 檔案系統中之完整路徑，包括檔案名稱以及延伸檔名。如該資料於 SC 中並未以檔案形式存在，SC 可以長度為零之空字串填入(0x13 0x00)。

OrgID 以及 ouID 為資料目的地機關以及單位代碼，若 RCIP 以及 RGIP 已經提供，orgID 以及 ouID 所從屬之 RC 與 RG 須與 RCIP 以及 RGIP 一致。(orgID, ouID)以及(RCIP, RGIP)兩對資料不得同時為空資料。如 SC 以 RCIP 以及 RGIP 指定 RG 以及 RC 時，得以長度為零之空字串填入 orgID 以及 ouID 欄位(0x13 0x00)。

SCIP 為 SC 之 IP

SGIP 為 SG 之 IP

RCIP 以及 RGIP 為 RC 以及 RG 之 IP，若 orgID 以及 ouID 已經提供，RCIP 以及 RGIP 所負責之 orgID 與 ouID 須與提供 orgID 以及 ouID 之一致。

Package 為實際發送資料，須依據規範並採公文本文、附件及數位簽章 ASN.1 編碼原則，制作成 Octet String 資料型態，並於傳

送資料前先行完成編碼。

(二)SG 至 SC 發送請求回覆結果編碼規範

```
SG2SCDataResponse ::= SEQUENCE {
version     INTEGER,            -- 0 代表第一版本
mID         INTEGER,            -- 由 SC 決定之數
status      INTEGER,            -- SID 該資料之發送狀態
message     UTF8String,         -- 返回訊息
orgID       PrintableString,    -- 該資料目的地機關代碼
ouID        PrintableString,    -- 該資料目的地單位代碼
SCIP        PrintableString,    -- SC 之 IP
SGIP        PrintableString,    -- SG 之 IP
RCIP        PrintableString,    -- RC 之 IP
RGIP        PrintableString,    -- RG 之 IP
SID         PrintableString,    -- 發送識別碼
RID         PrintableString,    -- 接收識別碼
}
```

本語法中之目的為提供 SG 回覆 SC 對於某一資料轉送請求之結果。

version 為版本識別用，於此版本為 0，代表第一版。

mID 須為原 SC 請求之相同 mID 值。

status 之值詳附錄三之一，於本語法中，status 之可能值包括：

GW_OK	接受語法，進行指定作業。
GW_VERSION	不支援指定語法版本
GW_SG_RG_AUTH	SG 無法完成對 RG 之鑑別
GW_SG_RG_SYN	SG 無法解析 RG 之語法
GW_SG_RG_TIMEOUT	SG 等待 RG 回應逾時
GW_SG_PENDING	SG 尚未將資料轉送出 RG
GW_SG_SENDING	SG 正在將資料轉送至 RG 中
GW_SG_RG_CONFIRMED	RG 已經確認收到 SG 轉送資料
GW_SG_RC_CONFIRMED	RC 已經確認收到 RG 轉送資料
GW_RG_SG_AUTH	RG 無法完成對 SG 之鑑別
GW_RG_SG_SYN	RG 無法解析 SG 之語法

GW_RG_RC_SYN　　RG 無法解析 RC 之語法

GW_RG_RC_TIMEOUT　　RG 等待 RC 回應逾時

message 為 SC 傳回之返回訊息，指出處理狀況之額外說明。

OrgID 以及 ouID 為資料目的地機關以及單位代碼，若 RCIP 以及 RGIP 已經提供，orgID 以及 ouID 所從屬之 RC 與 RG 須與 RCIP 以及 RGIP 一致。(orgID, ouID)以及(RCIP, RGIP)兩對資料不得同時為空資料。如 SC 以 RCIP 以及 RGIP 指定 RG 以及 RC 時，得以長度為零之空字串填入 orgID 以及 ouID 欄位(0x13 0x00)。

SID 為發送識別碼，若 status 不為錯誤訊息時，由 SG 指定。SID 之格式規範定義於附錄三之六中。

RID 為接收識別碼，若 status 為：

GW_SG_RG_CONFIRMED　　RG 已經確認收到 SG 轉送資料

GW_SG_RC_CONFIRMED　　RC 已經確認收到 RG 轉送資料

GW_RG_RC_SYN　　RG 無法解析 RC 之語法

GW_RG_RC_TIMEOUT　　RG 等待 RC 回應逾時

RID 即為 RG 對該資料所賦予之接收識別碼；若 status 為其他值時，RID 之值為未定義。SID 之格式規範定義於附錄三之六中。

SCIP 代表原 SC 之 IP。

SGIP 代表 SG 之 IP。

RCIP 代表 RC 之 IP，得由 SG 提供。

RGIP 代表 RG 之 IP，得由 SG 提供。

(三)SC 至 SG 查詢請求編碼規範

```
SC2SGQuery ::= SEQUENCE {
version     INTEGER,            -- 0 代表第一版本
mID         INTEGER,            -- 由 SC 決定之數
status      INTEGER,            -- SC 之狀態，保留用
```

```
message     UTF8String,          -- 額外告知 SG 訊息
SCIP        PrintableString,     -- SC 之 IP
SGIP        PrintableString,     -- SG 之 IP
SID         PrintableString,     -- 發送識別碼
RID         PrintableString,     -- 接收識別碼
}
```

本語法中由 SC 向 SG 發出查詢某一已經傳遞之資料之轉送狀態。

version 為版本識別用，於此版本為 0，代表第一版。

mID 為一由 SC 決定之一亂數，用以識別某一請求以及 SG 回覆是否一致用。

status 為 SC 告知 SG 之目前狀態，若於此版本並未使用，應以 0 值填入。

message 為 SC 告知 SG 之額外文字訊息，供 SG 提供稽核時查詢使用，於此版本並未使用，得以長度為零之空字串值填入。

SCIP 為 SC 之 IP。

SGIP 為 SG 之 IP。

SID 為發送識別碼，即 SC 因以向 SG 查詢資料轉送狀態之唯一識別。

RID 為接收識別碼，如 SC 於查詢時無法提供，得以長度為零之空字串值填入。若 RID 為查詢時已知，則 RID 與 SID 必須與轉送之結果一致。

(四)SG 至 SC 查詢請求回覆結果編碼規範

```
SG2SCQueryResponse ::= SEQUENCE {
version     INTEGER,             -- 0 代表第一版本
mID         INTEGER,             -- 由 SC 決定之數
status      INTEGER,             -- SID 指定之資料轉送狀態
message     UTF8String,          -- 返回訊息
SCIP        PrintableString,     -- SC 之 IP
SGIP        PrintableString,     -- SG 之 IP
RCIP        PrintableString,     -- RC 之 IP
RGIP        PrintableString,     -- SG 之 IP
SID         PrintableString,     -- 發送識別碼
RID         PrintableString,     -- 接收識別碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 為一發送端閘道器回覆 SC 之亂數，用以識別同一請求以及回覆。

status 之值定義於附錄三之六中，於本語法中，status 之可能值包括：

GW_OK	接受語法，進行指定作業。
GW_VERSION	不支援指定語法版本
GW_SG_RG_AUTH	SG 無法完成對 RG 之鑑別
GW_SG_RG_SYN	SG 無法解析 RG 之語法
GW_SG_RG_TIMEOUT	SG 等待 RG 回應逾時
GW_SG_PENDING	SG 尚未將資料轉送出 RG
GW_SG_SENDING	SG 正在將資料轉送至 RG 中
GW_SG_RG_CONFIRMED	RG 已經確認收到 SG 轉送資料
GW_SG_RC_CONFIRMED	RC 已經確認收到 RG 轉送資料
GW_RG_SG_AUTH	RG 無法完成對 SG 之鑑別
GW_RG_SG_SYN	RG 無法解析 SG 之語法
GW_RG_RC_SYN	RG 無法解析 RC 之語法
GW_RG_RC_TIMEOUT	RG 等待 RC 回應逾時

message 為 SC 傳回之返回訊息，指出處理狀況之額外說明。

SCIP 代表 SC 之 IP。

SGIP 代表 SG 之 IP。

SID 為發送識別碼，即 SC 向 SG 指定之唯一資料。

RID 為接收識別碼，若 status 為：

GW_SG_RG_CONFIRMED	RG 已經確認收到 SG 轉送資料
GW_SG_RC_CONFIRMED	RC 已經確認收到 RG 轉送資料
GW_RG_RC_SYN	RG 無法解析 RC 之語法
GW_RG_RC_TIMEOUT	RG 等待 RC 回應逾時時，RID 即為 RG

對該資料所賦予之接收識別碼；若 status 為其他值時，RID 之值為未定

義。

(五)RC 至 RG 查詢請求編碼規範

```
RC2RGQuery ::= SEQUENCE {
version     INTEGER,              -- 0 代表第一版本
mID     INTEGER,                  -- 由 SC 決定之數
status      INTEGER,              -- RC 之狀態，保留
message     UTF8String,           -- RC 額外提供訊息
orgID       PrintableString,      -- 該資料目的地機關代碼
ouID        PrintableString,      -- 該資料目的地單位代碼
RCIP        PrintableString,      -- RC 之 IP
RGIP        PrintableString,      -- RG 之 IP
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 由 RC 決定之一亂數，用以識別某一請求以及 RG 回覆用。

status 為 RC 告知 RG 之目前狀態，於此版本並未使用，應以 0 值填入(0x02 0x01 0x00)。

message 為 RC 對於該資料之額外說明。如 RC 並未有資料提供，應以長度為零之空字串填入(0x13 0x00)。

OrgID 以及 ouID 為資料目的地機關以及單位代碼，該資訊用以過濾指定收取之資料。如 RC 並未指定，得以長度為零之空字串填入 orgID 以及 ouID 欄位(0x13 0x00)。本版本規範並未強制於此版本中必須提供是項過濾功能。

RCIP 為 RC 之 IP。

RGIP 為 RG 之 IP。

(六)RG 至 RC 查詢請求回覆結果編碼規範

```
RG2RCQueryResponse ::= SEQUENCE {
version         INTEGER,          -- 0 代表第一版本
mID             INTEGER,          -- 由 RC 決定之數
status          INTEGER,          -- 該 RG 之接收狀態
message         UTF8String,       -- 返回訊息
RCIP            PrintableString,  -- RC 之 IP
```

```
RGIP            PrintableString, -- RG之IP
packageCount    INTEGER,         -- 查詢所得資料筆數
packageSet      SEQUENCE OF package
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 為一接收端道器回覆 RC 之亂數，用以識別同一請求以及回覆。

status 之值定義於附錄三之六中，於本語法中，status 之可能值包括：

GW_OK　　接受語法，進行指定作業。

GW_VERSION　　不支援指定語法版本

GW_RG_RC_SYN　　RG 無法解析 RC 之語法

message　為 RG 傳回之返回訊息，指出處理狀況之額外說明。

RCIP 代表 RC 之 IP。

RGIP 代表 RG 之 IP。

packageCount 為 packageSet 中資料筆數。

packageSet 為 RG 對於該 RC 所能存取之清單表列。每一筆記錄代表一筆資料之資訊，其內之資料項目規範如下：

version 為 packageSet 版本資訊

SCIP 該資料之 SC 之 IP

SGIP 該資料之 SG 之 IP

SID　該資料之發送識別碼

RID 該資料之接收識別碼

message 為 SC 對於該資料之額外說明，現階段之規範為該資料於該 SC 之完整路徑，包括檔案名稱以及延伸檔名。

size　該資料之大小，以位元組為單位

(七)RC 至 RG 接收請求編碼規範

```
RC2RGData ::= SEQUENCE {
version     INTEGER,            -- 0 代表第一版本
```

```
mID          INTEGER,              -- 由 RC 決定之數
status       INTEGER,              -- RC 之狀態，保留
message      UTF8String,           -- RC 額外提供訊息
RCIP         PrintableString,      -- RC 之 IP
RGIP         PrintableString,      -- RG 之 IP
RID          PrintableString,      -- 接收識別碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 由 RC 決定之一亂數，用以識別某一請求以及 RG 回覆用。

status 為 RC 告知 RG 之目前狀態，於此版本並未使用，應以 0 值填入(0x02 0x01 0x00)。

message 為 RC 對於該資料之額外說明。如 RC 並未有資料提供，應以長度為零之空字串填入(0x13 0x00)。

RCIP 代表 RC 之 IP。

RGIP 代表 RG 之 IP。

RID 為 RC 指定取得之資料識別碼。

(八)RG 至 RC 接收請求回覆結果編碼規範

```
RG2RCDataResponse ::= SEQUENCE {
version          INTEGER,           -- 0 代表第一版本
mID              INTEGER,           -- 原 RC 指定決定之數
status           INTEGER,           -- 該 RG 傳回之接收狀態
message          UTF8String,        -- 返回訊息
RCIP             PrintableString,   -- RC 之 IP
RGIP             PrintableString,   -- RG 之 IP
RID              PrintableString,   -- 接收識別碼
packageCount     INTEGER,           -- 資料大小
package          OctetString        -- 傳送資料，以 octet string 編碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 為一由接收系統端決定之一亂數，用以識別某一請求以及回覆用。

status 之值定義於附錄三之六中，於本語法中，status 之可能值包括：

GW_OK　　接受語法，進行指定作業。

GW_VERSION　　不支援指定語法版本

GW_RG_RC_SYN　　RG 無法解析 RC 之語法

GW_RG_NODATA　　RG 無法提供資料

message　為 RC 傳回之返回訊息，指出處理狀況之額外說明。

RCIP 代表 RC 之 IP。

RGIP 代表 RG 之 IP。

packageCount 為該筆資料之大小，以位元組為單位。PackageCount 並不包含 package 欄位中之標籤與長度資訊。

package 即為 RG 傳回 RC 之資料內容，以 OctetString 方式編碼。實際資料須除去標籤以及資料長度。

(九)RC 至 RG 確認資料編碼規範

```
RC2RGDataConfirm ::= SEQUENCE {
version     INTEGER,              -- 0 代表第一版本
mID         INTEGER,              --原 RC 指定決定之數
message     UTF8String,           -- 返回訊息
RCIP        PrintableString,      -- RC 之 IP
RGIP        PrintableString,      -- RG 之 IP
RID         PrintableString,      -- 接收識別碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 為一由發送系統端決定之一亂數，用以識別某一請求以及回覆用。

message　為 RC 提供 RG 之額外說明。

RCIP 代表 RC 之 IP。

RGIP 代表 RG 之 IP。

RID 為 RC 指定取得之資料識別碼。表示該資料已經由 RC 取回。

(十)RG 至 RC 確認請求結果編碼規範

```
RG2RCDataConfirmResponse ::= SEQUENCE {
version     INTEGER,              -- 0 代表第一版本
mID         INTEGER,              -- 原 RC 指定決定之數
```

```
status      INTEGER,            -- 該 RC 傳回之接收狀態
message     UTF8String,         -- 返回訊息
RCIP        PrintableString,    -- RC 之 IP
RGIP        PrintableString,    -- RG 之 IP
RID         PrintableString,    -- 接收識別碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 為一由接收系統端決定之一亂數，用以識別某一請求以及回覆用。

status 之值定義於附錄三之六中，於本語法中，status 之可能值包括：

GW_OK	接受語法，進行指定作業。
GW_VERSION	不支援指定語法版本
GW_RG_RC_SYN	RG 無法解析 RC 之語法
GW_RG_NODATA	RG 無法提供資料

message　為 RC 傳回之返回訊息，指出處理狀況之額外說明。

RCIP 代表 RC 之 IP。

RGIP 代表 RG 之 IP。

(十一)RG 至 RCNotification 資料編碼規範

```
RG2RCNotification ::= SEQUENCE {
version     INTEGER,            -- 0 代表第一版本
mID         INTEGER,            -- 由 RG 決定之數
status      INTEGER,            -- RID 指定之資料轉送狀態
message     UTF8String,         -- 返回訊息額外說明
SCIP        PrintableString,    -- 與 SID 相關之 SC 之 IP
SGIP        PrintableString,    -- 與 SID 相關之 SG 之 IP
RCIP        PrintableString,    -- 與 RID 相關之 RC 之 IP
RGIP        PrintableString,    -- 與 RID 相關之 RG 之 IP
SID         PrintableString,    -- 發送識別碼
RID         PrintableString,    -- 接收識別碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 為一發送端道器回覆 SC 之之亂數，用以識別同一請求以及回覆。

status 之值定義於附錄三之六中。

message　為 RG 傳回之額外說明。

SCIP 代表 SC 之 IP。

SGIP 代表 SG 之 IP。

SID 為發送識別碼，即 SG 向 SC 指定之唯一資料。

RID 為接收識別碼，即 RG 向 RC 指定之唯一資料。

(十二)RC 至 RGNotification 確認資料編碼規範

```
RC2RGNotificationComfirm ::= SEQUENCE {
version     INTEGER,              -- 0 代表第一版本
mID         INTEGER,              -- 原 RG 指定之辨識碼
message     UTF8String,           -- RC 端額外訊息
RID         PrintableString,      -- 接收識別碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 由 RG 指定，RC 於確認時傳回。

message　為 RC 提供 RG 之額外說明。

RID 為 RG 指定取得之資料識別碼。表示該資料已經 RC 確認。

(十三)SG 至 SCNotification 資料編碼規範

```
SG2SCNotification ::= SEQUENCE {
version     INTEGER,              -- 0 代表第一版本
mID         INTEGER,              -- 由 SG 決定之數
status      INTEGER,              -- SID 指定之資料轉送狀態
messageUTF8String,                -- 返回訊息額外說明
SCIP        PrintableString,      -- 與 SID 相關之 SC 之 IP
SGIP        PrintableString,      -- 與 SID 相關之 SG 之 IP
RCIP        PrintableString,      -- 與 RID 相關之 RC 之 IP
RGIP        PrintableString,      -- 與 RID 相關之 RG 之 IP
SID         PrintableString,      -- 發送識別碼
RID         PrintableString,      -- 接收識別碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 為一發送端道器回覆 SC 之之亂數，用以識別同一請求以及回覆。

status 之值定義於附錄三之六中 message　為 SC 傳回之返回訊息，指

出處理狀況之額外說明。

SCIP 代表 SC 之 IP。

SGIP 代表 SG 之 IP。

SID 為發送識別碼，即 SG 向 SC 指定之唯一資料。

(十四)SC 至 SGNotification 確認資料編碼規範

```
SC2SGNotificationComfirm ::= SEQUENCE {
version     INTEGER,              -- 0 代表第一版本
mID         INTEGER,              -- 原 SG 指定之辨識碼
message     UTF8String,           -- SC 端額外訊息
SID         PrintableString,      -- 發送識別碼
}
```

本語法中，version 為版本識別用，於此版本為 0，代表第一版。

mID 由 SG 指定，SC 於確認時傳回。

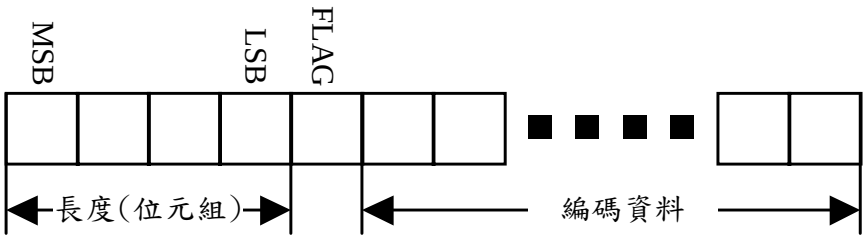
message　為 SC 提供 SG 之額外說明。

SID 為 SG 指定之資料識別碼。

四、閘道器間資料傳輸與編碼規範

閘道器間以 TCP/IP 連結方式，進行資料交換作業，其通訊協定採用 Three-Way 之 Request-Response-Confirm 方式確認資料傳輸雙方皆已完成。在資料轉送過程中，採取 Client-Server 方式進行資料傳輸：RG 作為 Server，其通訊埠預設為為 18091；SG 則為 Client。SG 須向 RG 請求(Request)成功建立一 TCP 連結後，在該連結中，將編碼後之資料完整送至 RG 端；並於閘道器回覆(Response)結果後，判讀該結果是否為預期之回覆資料，以便製作確認(Confirm)訊息回送 RG，之後由 SG 關閉該連結。

閘道器間之資料傳送協定規範為先傳送四位元組之資料，代表其後資料長度資訊。資料長度以 Big-Endian 方式編碼，即第一位元組為權值最大之位元組，其後之資料總長度以位元組為單位。資料之編碼原則須遵循 ASN.1(X.680 以及 X.690)之方式，並採用 ASN.1 規範之 DER 方式產生唯一編碼。資料之組成簡示如下：



其中 FLAG 之意義如下

編碼資料	FLAG 值	編碼資料語法
eGWMsg	'80'H	EnvelopedData(eGWMessage)
finaleGWMsgRep	'85'H	EnvelopedData (eGWMessage)
errorMsgRep	'06'H	human readable error message

閘道器間傳輸加密資料 ASN.1 編碼規範參考 PKCS#7 之定義，說明如下：

```
GWData ::= SEQUENCE {
```

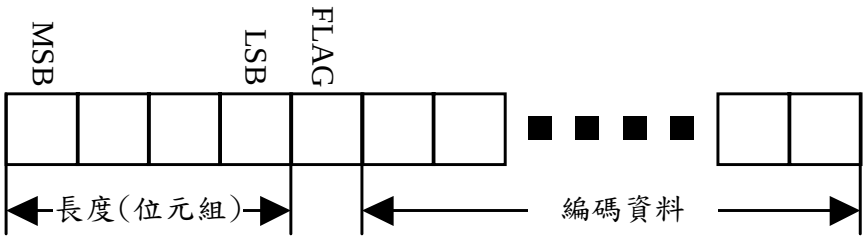
```
version     INTEGER,                -- 0 代表第一版本
content     ContentInfo             -- DEFINED BY PKCS7
}
ContentInfo ::= SEQUENCE {
contentType ContentType,
content                 [0]     EXPLICIT ANY DEFINED
BY contentType OPTIONAL }
ContentType ::= OBJECT IDENTIFIER
```

本系統採用 EnvelopedData 形態作為資料傳輸時資料加密之語法。其中資料須先簽章後，再加密傳送。

五、閘道管理者與轉送閘道器管理者間資料傳輸與編碼規範

MG 與 SG/RG 間以 TCP/IP 連結方式，進行資料交換作業。其通訊協定採用 Three-Way 之 Request-Response-Confirm 方式確認資料傳輸雙方皆已完成。在通訊過程中，採取 Client-Server 方式進行資料傳輸：SG/RG 作為一 Server,其通訊埠預設為為 18090;MG 則作為一 Client 向各 SG/RG 發出管理請求。MG 須向 SG/RG 請求(Request)成功建立一 TCP 連結後，在該連結中將編碼後之資料完整送至 SG/RG；並於 SG/RG 回覆(Response)結果後，判讀該結果是否為預期之回覆資料，以便製作確認(Confirm)訊息回送 SG/RG，之後由 MG 關閉該連結。

MG 與 SG/RG 間之資料傳送協定規範為先傳送四位元組之資料，代表其後資料長度資訊。資料長度以 Big-Endian 方式編碼，即第一位元組為權值最大之位元組，其後之資料總長度以位元組為單位。資料之編碼原則須遵循 ASN.1(X.680 及 X.690)之方式，並採用 ASN.1 規範之 DER 方式產生唯一編碼。資料之組成簡示如下：



其中 FLAG 之意義如下：

編碼資料	FLAG 值	編碼資料語法
eGWMsg	'80'H	EnvelopedData(eGWMessage)
finaleGWMsgRep	'85'H	EnvelopedData (eGWMessage)
errorMsgRep	'06'H	human readable error message

MG 與 SG/RG 間傳輸加密資料的 ASN.1 編碼規範參考 PKCS 7 之定義如下：

```
MGData ::= SEQUENCE {
version     INTEGER,                -- 0 代表第一版本
content     ContentInfo             -- DEFINED BY PKCS7
}
ContentInfo ::= SEQUENCE {
contentType ContentType,
content                 [0]     EXPLICIT ANY DEFINED
                                 BY contentType OPTIONAL }
ContentType ::= OBJECT IDENTIFIER
```

本系統採用 SignedData 資料以及 EnvelopedData 形態作為資料傳輸時 Request、Response、Confirm 之語法。其中資料須先經 SignedData 語法編碼後，再以 EnvelopedData 語法加密。

閘道器管理者(於本規範中簡稱 MG)，透過 GSN 存取 DMZ 中另一轉送閘道器之管理組態，以便提供遠端管理維護機制以及版本控制、更新與佈署功能。本規範中之 MG 對於 SG/RG 之管理功能包括：

1．以 RSA 1024 位元元以及 SHA1 演算法提供 SG/RG 間之鑑別

2．建立 SG/RG 轉送閘道器網路

3．偵測 SG/RG 是否運作

4．測試 SG/RG 之運作狀況

5．取得該 SG/RG 之軟體版本資訊

6．協助 SG/RG 取得下載新版本安裝程式

7．取得該 SG/RG 之閘道轉送表資訊

8．取得該 SG/RG 之轉送稽核記錄

9．指定該 SG/RG 之閘道轉送表資訊

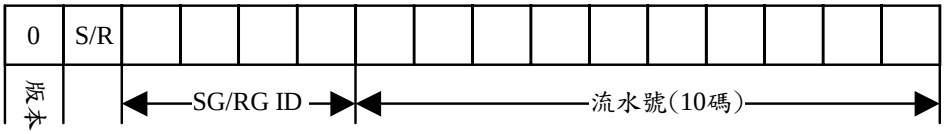
10．新增/刪除一 SG/RG 於轉送閘道器網路中

11．提供 SG/RG 以及 orgID/ouID 之目錄服務

六、閘道系統各項訊息彙編

(一)SID 與 RID 格式規範

SID 與 RID 以三欄位、共 16 位元組表示如下圖：



其中第一位元組為版本識別用，於本規範為第一版，定為‘0’；第二位元組為‘S’或‘R’代表該閘道器作為 SG 或 RG 時，並識別該資料為 SID 或 RID 用；第三至第六位元組共四位元組為 MG 指定之 SG/RG 唯一編號;第七至第十六位元組共十位元組為 SG/RG 賦予之唯一號碼,由‘0000000000’開始,各位元組須為 ASCII 碼中之‘0’~‘9’。

(二)編碼規範中之 status 欄位定義

值	代碼	狀況說明
0x0000	GW_OK	接受語法，進行指定作業
0x0001	GW_VERSION	不支援指定語法版本
0x0101	GW_MG_SG_AUTH	MG 無法完成對 SG 之鑑別
0x0102	GW_MG_RG_AUTH	MG 無法完成對 RG 之鑑別
0x0103	GW_MG_SG_SYN	MG 無法解析 SG 之請求語法
0x0104	GW_MG_RG_SYN	MG 無法解析 RG 之請求語法
0x0105	GW_MG_SG_TIMEOUT	MG 等待 SG 回應逾時
0x0106	GW_MG_TIMEOUT	MG　等待 RG 回應逾時

0x0201	GW_SG_MG_AUTH	SG 無法完成對 MG 之鑑別
0x0202	GW_SG_RG_AUTH	SG 無法完成對 RG 之鑑別
0x0203	GW_SG_MG_SYN	SG 無法解析 MG 之語法
0x0204	GW_SG_RG_SYN	SG 無法解析 RG 之語法
0x0205	GW_SG_MG_TIMEOUT	SG 等待 MG 回應逾時
0x0206	GW_SG_RG_TIMEOUT	SG 等待 RG 回應逾時
0x0207	GW_SG_PENDING	SG 尚未將資料轉送出 RG
0x0208	GW_SG_SENDING	SG 正在將資料轉送至 RG 中
0x0209	GW_SG_RG_CONFIRMED	RG 已經確認收到 SG 轉送資料
0x0210	GW_SG_RC_CONFIRMED	RC 已經確認收到 RG 轉送資料
0x0301	GW_RG_MG_AUTH	RG 無法完成對 MG 之鑑別
0x0302	GW_RG_SG_AUTH	RG 無法完成對 SG 之鑑別
0x0303	GW_RG_MG_SYN	RG 無法解析 MG 之語法
0x0304	GW_RG_SG_SYN	RG 無法解析 SG 之語法
0x0305	GW_RG_RC_SYN	RG 無法解析 RC 之語法
0x0306	GW_RG_MG_TIMEOUT	RG 等待 MG 回應逾時
0x0307	GW_RG_SG_TIMEOUT	RG 等待 SG 回應逾時
0x0308	GW_RG_RC_TIMEOUT	RG 等待 RC 回應逾時
0x0309	GW_RG_NODATA	RG 無法提供資料

附錄四：憑證 ASN.1 格式補充說明

一、格式說明

憑證 ASN.1 格式詳細如下：

```
 Certificate     ::= SEQUENCE {
    tbsCertificate              TBSCertificate,
    signatureAlgorithm AlgorithmIdentifier,
    signature                   BIT STRING    }

TBSCertificate      ::= SEQUENCE {
    version                 [0] EXPLICIT Version,
    serialNumber              CertificateSerialNumber,
    signature                 AlgorithmIdentifier,
    issuer                        Name,
    validity                      Validity,
    subject                       Name,
    subjectPublicKeyInfo    SubjectPublicKeyInfo,
    issuerUniqueID        [1] IMPLICIT
                                  UniqueIdentifier OPTIONAL,
    SubjectUniqueID [2] IMPLICIT
                                  UniqueIdentifier OPTIONAL,
    extensions              [3] EXPLICIT Extensions OPTIONAL
    }

Version   ::= INTEGER { v3(2) }

CertificateSerialNumber ::= INTEGER

Validity   ::= SEQUENCE {
    notBeforeTime,
    notAfter  Time      }

Time      ::= CHOICE   {
    utcTime         UTCTime,
    generalTime   GerneralizedTime   }

UniqueIdentifier    ::= BIT STRING

SubjectPublicKeyInfo    ::= SEQUENCE {
    algorithm             AlgorithmIdentifier,
    subjectPublicKey   BIT STRING  }

Extensions     ::= SEQUENCE SIZE (1..MAX) OF EXTENSION

Extension::= SEQUENCE     {
    exnID           OBJECT IDENTIFIER,
```

```
        critical     BOOLEAN DEFAULT FALSE,
        extnValue      OCTET STRING      }

AlgorithmIdentifier::=    SEQUENCE {
        algorithm        OBJECT IDENTIFIER,
        parameters              ANY DEFINED BY algorithm OPTIONAL }

Name      ::=    CHOICE {
        RDNSequence }

RDNSequence::=SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName   ::=
        SET OF AttributeTypeAndValue

AttributeTypeAndValue  ::= SEQUENCE {
        type         AttributeType,
        value              AttributeValue }

AttributeType  OBJECT IDENTIFIER ::= { joint-iso-ccitt (2) ds(5) attributeType (4) }

AttributeValue::= ANY DEFINED BY AttribeType

-- country type
countryName  ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX
                PrintableString (SIZE(2) )-- IS 3166 codes only
        MATCHES FOR EQUALITY
        SINGLE  VALUE
        ::= { attributeType 6 }

-- organization type
organizationName   ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX
                caseIgnoreStringSyntax
                        (SIZE(1..ub-organization-Name) )
        ::= { attributeType 10 }

-- organization unit type
organizationUnitName    ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX
                caseIgnoreStringSyntax
                        (SIZE(1..ub-organizational-unit-Name) )
        ::= { attributeType 11 }

-- common name type
commonName ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX
                caseIgnoreStringSyntax
```

```
                (SIZE(1..ub-common-Name) )
        ::= { attributeType 3 }

-- extensions
-- key usage extension
id-ce-keyUsage      OBJECT IDENTIFIER ::=     { id-ce 15 }

KeyUsage       ::= BIT STRING{
        DigitalSignature        (0)
        NonRepudiation          (1)
        KeyEncipherment         (2)
        dataEncryption          (3)
        keyAgreement            (4)
        keyCertSign             (5)
        cRLSign                 (6)
        encipherOnly            (7)
        decipherOnly            (8)       }

-- policy extension
id-ce-certificatePolicies  OBJECT IDENTIFIER  ::= { id-ce 32 }

certificatePolicies   ::=   SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation   ::= SEQUENCE {
        policyIdentifier        CertPolicyId,
        policyQualifiers        SEQUENCE SIZE (1..MAX) OF
        PolicyQualifierInfo OPTIONAL }

CertPolicyId    OBJECT IDENTIFIER

id-cht-cp-1             OBJECT IDENTIFIER ::= {1 2 tw(886) cht(1) cp(2) policy-1(1) }

PolicyQualifierInfo ::=   SEQUENCE {
        policyQualifierId           PolicyQualifierId,
        qualifier           ANY DEFUNED BY policyQualifierId }

-- subject alternative name extension
id-ce-subjectAltName    OBJECT IDENTIFIER ::= {id-ce 17 }

SubjectAltName     ::=   GeneralNames

GeneralNames::= SEQUENCE SIZE (1..MAX) OF GernalName

GernalName   ::= CHOICE {
        otherName                       [0]             OtherName
        rfc822Name                      [1]             IA5String
        dNSName                         [2]             IA5String
        x400Name                        [3]             ORAddress
        directoryName                   [4]             Name
```

```
    ediPartyName                [5]         EDIPartyName
    uniformResourceIdentifier   [6]         IA5String
    iPAddress                   [7]         OCTET STRING,
    reqisterdID                 [8]         OBJECT IDENTIFIER }

OtherName   ::=  SEQUENCE  {
    type-id             OBJECT IDENTIFIER,
    value                           [0]   EXPLICIT ANY DEFIED BY type-id }

id-taiwanPersonalID     OBJECT IDENTIFIER  ::= { 1 2 tw(886) cht(1) id(1) }

TaiwanPersonID    IA5String

-- basic constraints entensions
id-ce-basicConstraints    OBJECT IDENTIFIER  ::= { id-ce 19 }

BasicConstraints    ::=  SEQUENCE {
    cA                  BOOLEAN DEFAULT FALSE,
    pathConstraint INTEGER (..MAX) OPTIONAL }
```

二、GCA 憑證 DER code 範例

以下描述某一份 GCA 憑證的 DER 編碼：

```
30 82 02 93                         ---- certificate tag and length
   30 82 02 00                      ---- tag and length of to-be-signed part
      a0 03                         ---- tag and length of certificate version
         02 01                      ---- integer with 1-byte length for version 3
            02                      ---- version 3
      02 04                         ---- integer with 4-byte length for serial number
           0f 7f 49 02              ---- serial number
      30 09                         ---- signature algorithm OID
         06 05
            ( 1 3 14 3 2 29 )
            2b 0e 03 02 1d
         05 00
      30 57                         ---- (issuer) tag and length of Name
         31 0b
            30 09
               06 03                ---- (issuer) countryName OID
                  ( 2 5 4 6 )
                  55 04 06
               13 02
                  'TW'
                  54 57
         31 0f
            30 0d
               06 03                ---- (issuer) localityName OID
                  ( 2 5 4 8 )
```

```
            55 04 08
        14 06
            '臺灣省'
            bb 4f c6 57 ac d9
    31 0f
        30 0d
            06 03                   ---- (issuer) organizationName OID
            ( 2 5 4 10 )
            55 04 0a
            14 06
            '行政院'
            a6 e6 ac 46 b0 7c
    31 0f
        30 0d
            06 03                   ---- (issuer)
                                         organizationUnitName OID
            ( 2 5 4 11 )
            55 04 0b
            14 06
            '研考會'
            ac e3 a6 d2 b7 7c
    31 15
        30 13
            06 03                   ---- (issuer) commonName OID
            ( 2 5 4 3 )
            55 04 03
            14 0c
            '憑證管理中心'
            be cc c3 d2 ba de b2 7a a4 a4 a4 df
30 1e                               ---- Validity tag and length
    17 0d
        '980219091852Z'
        39 38 30 32 31 39 30 39 31 38 35 32 5a ---- NotBefore
    17 0d
        '000219091852Z'
        30 30 30 32 31 39 30 39 31 38 35 32 5a---- NotAfter

30 5d                               ---- (Subject) tag and length
    31 0b
        30 09
            06 03                   ---- (Subject) countryName OID
            ( 2 5 4 6 )
            55 04 06
            13 02
            'TW'
            54 57
    31 0f
        30 0d
            06 03                   ---- (Subject) localityName OID
```

```
                ( 2 5 4 8 )
                55 04 08
            14 06
                '臺灣省'
                bb 4f c6 57 ac d9
        31 17
            30 15
                06 03                   ---- (Subject) organizationName OID
                ( 2 5 4 10 )
                55 04 0a
                14 0e
                '中華電信研究所'
                a4 a4 b5 d8 b9 71 ab 48 ac e3 a8 73 a9 d2
        31 13
            30 11
                06 03                   ---- (Subject) OrganizationUnitName OID
                ( 2 5 4 11 )
                55 04 0b
                14 0a
                '應用科技室'
                c0 b3 a5 ce ac ec a7 de ab c7
        31 0f
            30 0d
                06 03                   ---- (Subject) commonName OID
                ( 2 5 4 3 )
                55 04 03
                14 06
                '王上安'
                a7 f5 ab d8 bd f7

    30 81 9e                            ---- Subject PubliceKeyInfo tag and length
        30 0d                           ---- Algorithm OID
            06 09
            ( 1 2 840 113549 1 1 1 )
            2a 86 48 86 f7 0d 01 01 01
            05 00
        03 81 8c                        ---- Public Key:參照 X.509 規範存入
                                             128byte 的 n 以及 3 byte 的 e

00 30 81 88 02 81 80 16 91 e0 a7 b6 52 f5 d0 5f b4 c2 00 bd bd
18 b7 8c e7 67 a0 65 d2 4e 42 1c c2 66 c2 1e cb e6 20 70 93 00
ab c8 14 f0 6d fc 17 40 6e 90 ba 51 37 d3 2f 7a 07 98 87 79 89
90 98 99 d4 42 6a ef 07 d2 9a 08 11 82 ae 56 a5 16 f4 d5 14 1b
a4 60 7e e3 81 f1 70 2c bd de c1 9d 4b 4b 24 0d db 50 3a c8 ea
e8 c6 8a d0 86 cf 74 b6 ea 6d 3c e7 9a 60 fb eb a5 17 a3 09 b2
04 ad bf ea c9 a2 bd 09 6d 02 03 01 00 01 82 1a        ---- UniqueIdentifier tag and length
    03 18
        00
```

30 15
06 05 ---- id-taiwanPersonalID OID
2a 86 76 01 01
a0 0c
16 0a
55 31 32 30 30 39 37 36 37 38 ---- ID Number
a3 53
30 51
30 0b
06 03 ---- keyUsage OID
(2 5 29 15)
55 1d 0f
04 04 ---- KeyUsage(BIT STRING)
03 02 07 80
30 09
06 03 ---- basicConstraints OID
(2 5 29 19)
55 1d 13
04 02
30 00
30 22
06 03 ---- subjectAltName OID
(2 5 29 17)
55 1d 11
04 1b
30 19 a0 17 30 15 06 05 2a 86 76 01 01 a0 0c 16 0a 55 31
32 30 30 39 37 36 37 38
30 13
06 03 ---- certificatePolicy OID
(2 5 29 32)
55 1d 20
04 0c ---- id-cht-cp-1 tag and length
30 0a 30 08 06 06 2a 86 76 01 02 01 ---- id-cht-cp-1
30 09
06 05 ---- signature Algorithm OID
(1 3 14 3 2 29)
2b 0e 03 02 1d
05 00
03 81 81 ---- signature tag and length
---- signature(BIT STRING)
00 42 2e 40 ef 3c b8 cb a4 2b c8 b4 60 4c 7e 0c d5 57 f3 8d 74 09 2b
4a 73 02 cf dd 06 0a da 85 90 ec 78 6a 6f 06 c5 70 1d 1c b3 6f bd d8
34 11 49 e6 40 9d dc 35 e7 18 5b 43 7d 98 93 0a e5 fc e2 66 5e 48 22
16 8a 99 a3 25 bd 76 da c8 f9 e2 92 15 1e 5b ad 42 4e f7 77 d3 ed 1b
21 ee c8 fb ee 9d d6 4c 38 1b 6b a2 b9 33 36 09 85 93 fb ca de 4b 37
8e 6b 6f e7 d2 99 18 1c 70 3b 71 b8 84 37

簽章中取 hash 的範圍及內容

以下描述憑證中簽章的資料範圍：

由

30 82 02 00 ---- tag and length of to-be-signed part

到

30 0a 30 08 06 06 2a 86 76 01 02 01 ---- id-cht-cp-1

之 DER code

三、憑證廢止清冊的 ASN.1 格式

格式詳如下所列：

```
CertificateRevokationList ::=   SIGNED{    SEQUENCE   {
version        Version OPTIONAL-- if present, must be v2
signature              AlgorithmIdentifier,
Issuer                      Name,
thisUpdate                  Time,
nextUpdate                        Time OPTIONAL ,
      revokedCertificates       SEQUENCE OF SEQUENCE{
 userCertificate       CertificateSerialNumber,
 revocationDate              Time,
 crlEntryExtensions Extensions OPTIONAL
                            -- if present, must be v2 } OPTIONAL,
crlExtensions          [0] EXPLICIT Extensions OPTIONAL
                            -- if present, must be v2 }}}
                            -- crl entry extension : revoke reason
id-ce-cRLReason     OBJECT IDENTIFIER  ::= { id-ce 21 }
                            -- reasonCode ::= {CRLReason }
CRLReason     ::=   ENUMERATE {
unspecified                 (0),
keyCompromise               (1),
cACompromise                (2),
affiliationChanged          (3),
superseded                  (4),
cessationOfOperation        (5),
certificateHold             (6),
removeFromCRL               (8)   }
SIGNED { ToBeSigned }       ::= SEQUENCE {
 toBeSigned                       ToBeSigned,
 COMPONENTS OF                          SIGNATURE{ ToBeSigned} }
SIGNATURE{ OfSignature }::= SEQUENCE {
 algorithmIdentifier          AlgorithmIdentifier,
 encrypted                    ENCRYPTED{ HASHED { OfSignature }}}
```

四、GCA 憑證廢止清冊 DER code 範例

以下描述某一份 GCA 的憑證廢止清冊的 DER 編碼：

```
30 82 490: SEQUENCE {
30 82 343:   SEQUENCE {
02    1:     INTEGER 1
30    9:     SEQUENCE {
06    5: OBJECT IDENTIFIER sha-1WithRSAEncryption (1 3 14 3 2 29)
05    0:       NULL
        :       }
30   87:     SEQUENCE {
31   11:       SET {
30    9:         SEQUENCE {
06    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
13    2:           PrintableString 'TW'
                 :           }
                 :         }
31   15:       SET {
30   13:         SEQUENCE {
06    3:           OBJECT IDENTIFIER stateOrProvinceName
                       (2 5 4 8)
14    6:           TeletexString '臺灣省'
           :           }
           :         }
31   15:       SET {
30   13:         SEQUENCE {
06    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
14    6:           TeletexString '行政院'
```

```
          :           }
          :         }
   31   15:       SET {
   30   13:         SEQUENCE {
   06    3:           OBJECT IDENTIFIER organizationalUnitName
                        (2 5 4 11)
   14    6:           TeletexString '研考會'
          :           }
          :         }
   31   21:       SET {
   30   19:         SEQUENCE {
   06    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
   14   12:           TeletexString '憑證管理中心'
          :           }
          :         }
          :       }
   17   13:     UTCTime '981217160001Z'
   17   13:     UTCTime '981218160001Z'
30 82 204:     SEQUENCE {
   30   33:       SEQUENCE {
   02    2:         INTEGER 10001
   17   13:         UTCTime '980225010741Z'
   30   12:         SEQUENCE {
   30   10:           SEQUENCE {
   06    3:             OBJECT IDENTIFIER cRLReason (2 5 29 21)
```

```
04    3:              OCTET STRING
          :                 0A 01 03
          :               }
          :             }
          :           }
30   35:        SEQUENCE {
02    4:          INTEGER 313701459
17   13:          UTCTime '980307041848Z'
30   12:          SEQUENCE {
30   10:            SEQUENCE {
06    3:              OBJECT IDENTIFIER cRLReason (2 5 29 21)
04    3:              OCTET STRING
          :                 0A 01 01
          :               }
          :             }
          :           }
30   35:        SEQUENCE {
02    4:          INTEGER 313701454
17   13:          UTCTime '980307041848Z'
30   12:          SEQUENCE {
30   10:            SEQUENCE {
06    3:              OBJECT IDENTIFIER cRLReason (2 5 29 21)
04    3:              OCTET STRING
          :                 0A 01 01
          :               }
```

```
            :            }
            :          }
    30    9:     SEQUENCE {
    06    5:       OBJECT IDENTIFIER sha-1WithRSAEncryption (1 3 14 3 2
                   29)
    05    0:       NULL
            :       }
            :     }
    03  129:   BIT STRING 0 unused bits
            :     60 F7 68 92 63 ED DE 56 E3 E4 C0 47 A2 2C 0E E9
            :     00 11 8F B8 9D CD 2C 55 59 A2 7A 94 A6 8D F3 D7
            :     23 A8 55 D8 BC 7E 83 2F 4E 05 7F B9 6B 55 00 BA
            :     ED 0B 3C 25 41 13 FA FB A3 DC 18 1A 9B 08 97 6F
            :     BF 8D 05 85 DD B6 43 9D 12 2E C8 0F 92 49 A8 F0
            :     02 14 8D 59 67 E4 97 62 44 B7 97 FF A4 6D 70 98
            :     49 D4 6C AF 46 6D 6F CC 29 FE 31 1F 4C 53 0A 9F
            :     21 2B 39 A0 B8 6E 42 88 A4 64 23 50 BD 76 47 B2
            :   }
```