

電子檔案技術應用

檔案管理局
檔案資訊組

課程目標

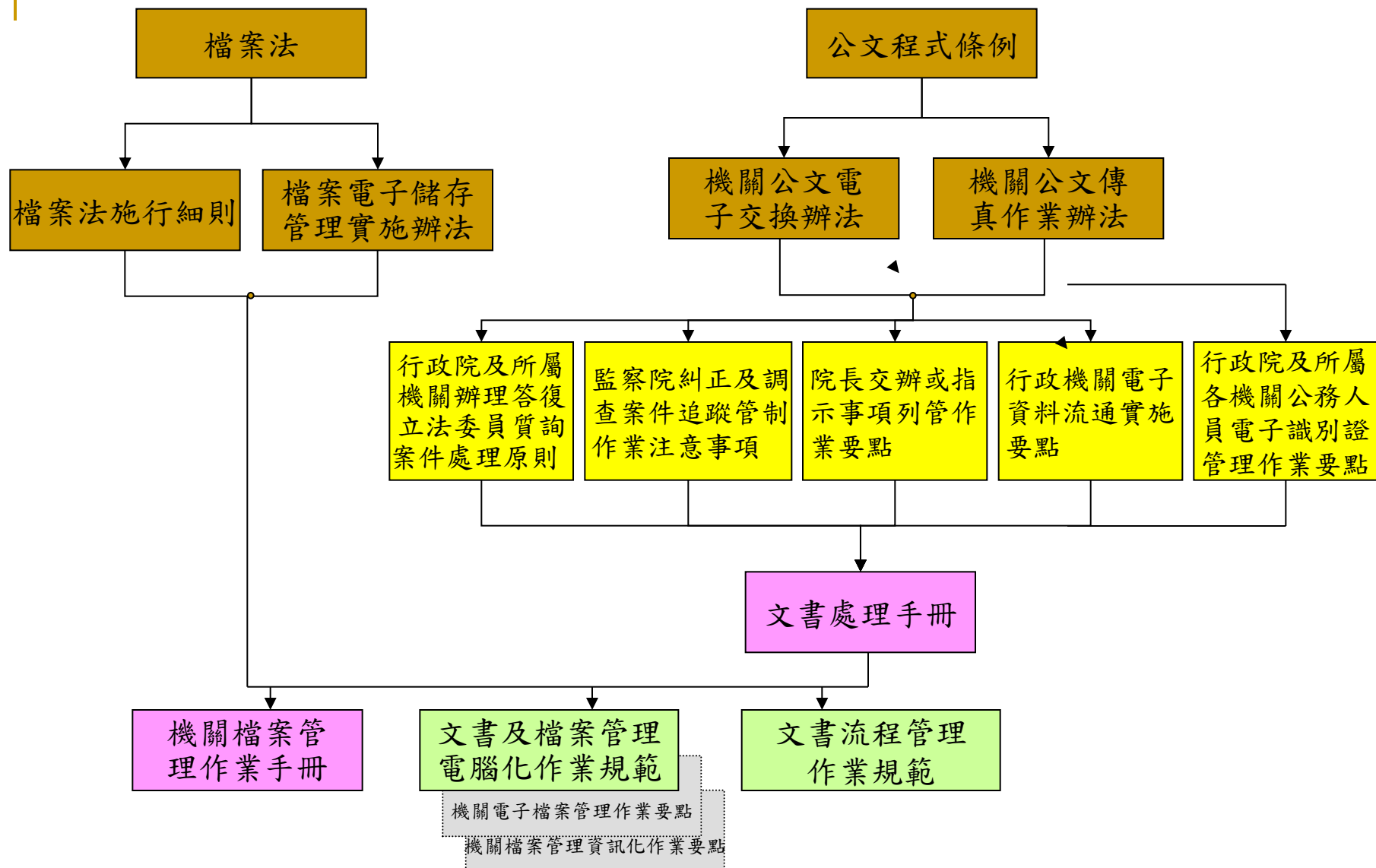
- 協助機關檔案管理及資訊人員了解公文線上簽核及電子檔案應用技術，介紹電子檔案格式、XML技術、數位簽章及轉置概念，並說明公文線上簽核、檔管點收、移轉(交)封裝實作概念及電子檔案轉置理機制，以便能運用適當的資訊技術，妥善管理電子檔案，確保其真實性、完整性與可及性。

大綱

- 電子檔案法規與定義
- 電子檔案格式
- XML與簽章技術
- 封裝處理技術
- 實作範例介紹
- 電子檔案轉置
- 電子公文檔案清理工具
- 結語

電子檔案法規與定義

文書及檔案電腦化作業相關法規架構圖



文書及檔案管理電腦化作業規範架構

壹、總則

依據、適用範圍、功能...

貳、業務管理規範

收文、發文、線上簽核、
電子檔案管理等處理程序及
注意事項

參、系統管理規範

線上簽核、檔管系統、稽
核作業紀錄保存等作業規
定

肆、系統技術規範

線上簽核、檔管系統建置、
電子檔案清查作業等技術
規定

附件

文書流程

傳輸檔案格式

代碼清冊

交換架構

中文字碼

附件格式

檔案管理系統功能說明

電子檔案格式表

電子媒體規格表

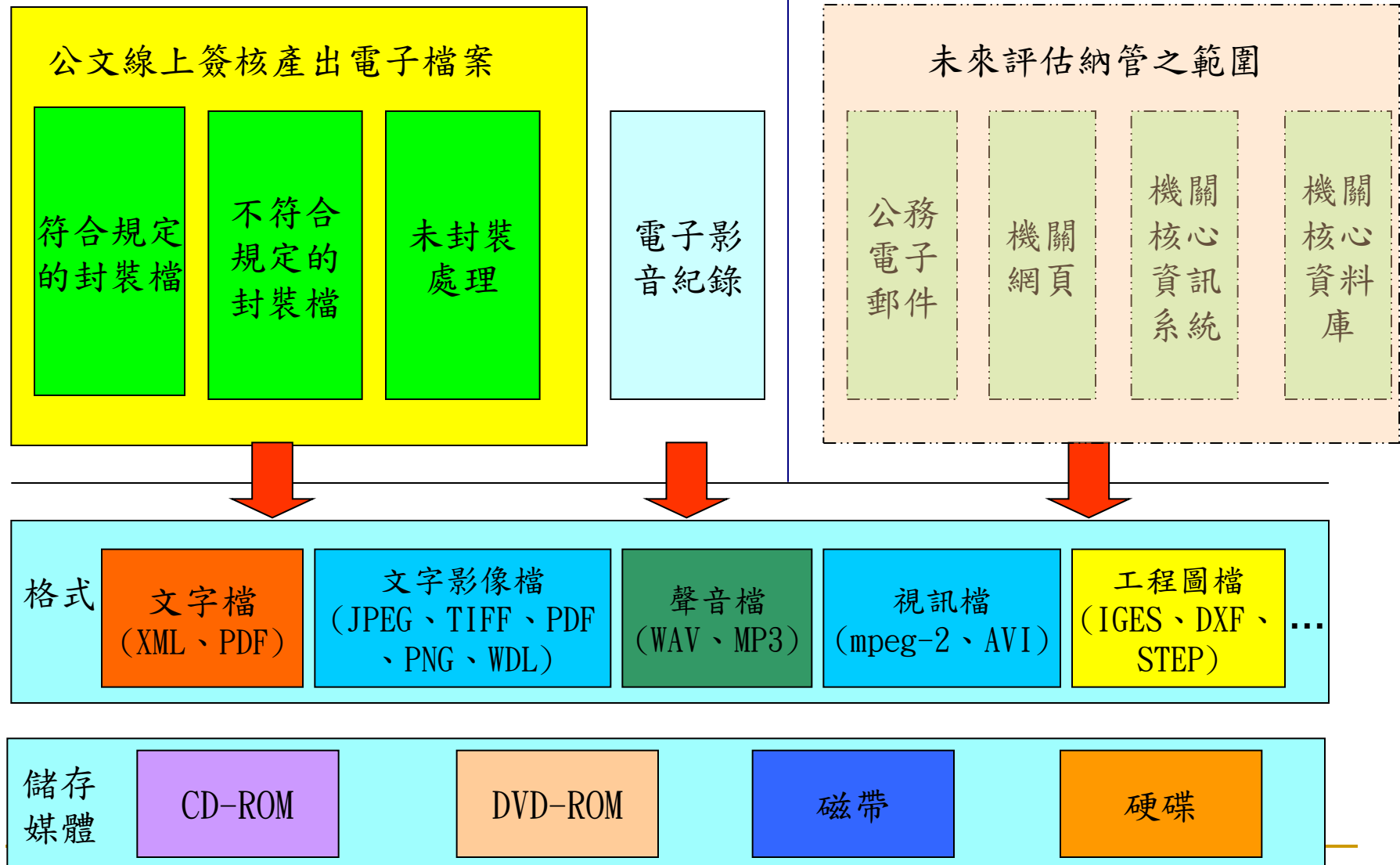
機關電子檔案統一命名原則

用詞定義

- 線上簽核係指公文以電子方式在安全之網路作業環境下，進行線上傳遞、簽核工作。
- 電子檔案係指指電腦可處理之文字或非文字資料，且符合檔案法及相關法令規定等。
- 詮釋資料 (metadata)：指用以描述電子檔案有關資料背景、內容、關聯性及資料控制等相關資訊。
- 封裝檔：指將電子檔案及其詮釋資料與驗證檔案真實性、完整性之資訊，以包裹方式儲存之檔案。

註:文書及檔案管理電腦化作業規範第六點

電子檔案範圍



電子檔案格式

電子檔案格式

■ 電子檔案格式

- 係指檔案內容以資訊編碼成位元組後儲存在電腦的一種表示方法。
- 對於任何電腦來說，有效的資訊就是0和1，必須將肉眼可以辨識有意義的資訊轉換成對應的0和1，故不同的資訊有不同的儲存格式。
- 每一種資訊可能有一種或多種檔案格式儲存電腦中，例如文字影像檔有 jpeg、pdf、png 等檔案格式，視訊檔有 mpeg-2、avi 等檔案格式。
- 通常軟體設計以電子檔案的副檔名來標示檔案類型。

■ 基於商業、智慧產權等因素，軟體有其特定檔案格式，不同的電子檔案格式，須有不同的軟體才能開啟閱讀。

■ 讀取舊紀錄需使用對應之軟體開啟，因應新技術更迭，舊紀錄必須不斷轉換成新的紀錄格式。

電子檔案保存格式考慮因素

■ 選擇格式的重要關鍵因子

- 開放式國際標準(例:PDF/A)
- 獲大眾經常使用的格式
- 是否會受限於專利保護
- 格式的穩定性
- 支持詮釋資料註記

■ 檔案格式

- 保存資料本體與格式結構，惟資料本體保存以TEXT為宜，解釋環境資料以影像檔表示，減少結構問題。
- 保存、應用、預覽採用不同格式
- 經擇選的檔案格式，需定期監測，提供轉置機制
- 儘量減少檔案格式，限制檔案格式量

選擇格式必需能支持檔案產生者、使用者及管理者的工作方便進行，並應定期評估

電子檔案用途區分

- 長期保存檔案 (Archive Image): 非失真、高解析度版本，確有必要才使用
 - 解析度: 300 dpi
 - 顏色深度: 全彩
 - 格式: Tiff
 - 不壓縮
- 線上應用檔案 (Reference Image): 日常展示應用、加值處理
 - 用 jpeg 壓縮
 - 掃描後降階
- 預覽檔案 (Thumbnail Image): 用於網路檢索等用途
 - 解析度: 72 dpi
 - 顏色深度: 全彩
 - 掃描後降階

電子檔案格式表

類型	格式	說明
文字檔	XML	一、開放性標準。 二、電子公文傳遞交換格式。
	PDF	業界認定可攜性文件格式。
圖片檔	JPEG	一、如檔案係以影像掃描製作，一律採全彩，壓縮品質為75%以上，解析度300 DPI以上。 二、開放性標準。
	SVG	一、國際標準（ISO/IEC26300:2006）。 二、XML開放性架構，具可攜性文件格式。
聲音檔	MP3	開放性標準。
	WAV	開放性標準。
視訊檔	MPEG-2	開放性標準。
	AVI	專屬軟體。
	H. 264	開放性標準。

電子檔案格式表(續)

類型	格式	說明
工程圖檔	IGES	美國國家標準 (ANSI Y14.26M) 。
	DXF	開放性標準。
	STEP	國際標準 (ISO/IEC10303) 。
文字影像檔	JPEG	一、彩色影像：採全彩，壓縮品質為75%以上，解析度200 DPI以上。 二、開放性標準。
	TIFF	灰階影像：採解析度200 DPI以上。
	TIFF	一、黑白影像：採CCITT G4標準，解析度300 DPI以上。 二、業界認定開放性標準。
	PDF	業界認定可攜性文件格式。
	WDL	國內開發之可攜性文件格式。
	PNG	一、索引色影像：採256色ZIP非破壞性壓縮，解析度300DPI以上。 二、線上簽核使用追蹤修訂功能時，採用本格式產生簽核頁面。
	ODF	開放性標準。
數位墨水	ISF	一、手寫簽核資料採用本格式以筆跡方式存檔。 二、筆跡檔案業界認定開放性標準。

儲存格式說明

■ 執行線上簽核檔案得包含以下內容：

□ 文書本文檔

- 內容以XML語法所組成，另稱DI（Document Instance）檔。
- 包括令、函、簽等公文本文，內容結構依文書及檔案管理電腦化作業規範，呈現格式依文書處理手冊

內容結構

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- 99_2_utf8.dtd 函 2008.10.1 修改日期:2010.01.08 -->
<|ENTITY % 基本標籤 SYSTEM "99_basic_utf8.ent">
%基本標籤;
<|ENTITY % 電子交換標籤 SYSTEM "99_exchange_utf8.ent">
%電子交換標籤;
<|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 -->
```

di檔

呈現格式

行政院研究發展考核委員會 函

地址：10051台北市中正區廣南路1段2之2
5樓
承辦人：黃書儀
電話：02-23419066#822
電子信箱：syihuang@rdcc.gov.tw

發文日期：中華民國98年3月30日
發文字號：會研字第0982460308號
類別：普通件
留置及解密條件或保密期限：普通
附件：活動說明

主旨：本會謹定於98年4月17日假台南市政府6樓會議室辦理「機關電子公布欄推廣經驗分享座談會」，請派員參加，請 查照。

說明：

- 一、本會自96年8月起推廣機關電子公布欄，為持續推廣與擴大機關電子公布欄使用效益，爰辦理「機關電子公布欄推廣經驗分享座談會」。
- 二、本會邀請使用成效良好之縣市政府，分享其電子公布欄推廣經驗與應用方式(如前置作業、相關張貼規則訂定、政策宣導做法等)，活動議程及說明如附件。

正本：宜蘭縣政府、花蓮縣政府、南投縣政府、屏東縣政府、苗栗縣政府、桃園縣政府、高雄市政府、高雄縣政府、雲林縣政府、新竹市政府、新竹縣政府、嘉義市政府、嘉義縣政府、彰化縣政府、金門縣政府、福建省連江縣政府、臺中市政府、臺中縣政府、臺北市政府、臺北縣政府、臺東縣政府、臺南市政府、臺南縣政府、澎湖縣政府、基隆市政府
副本：

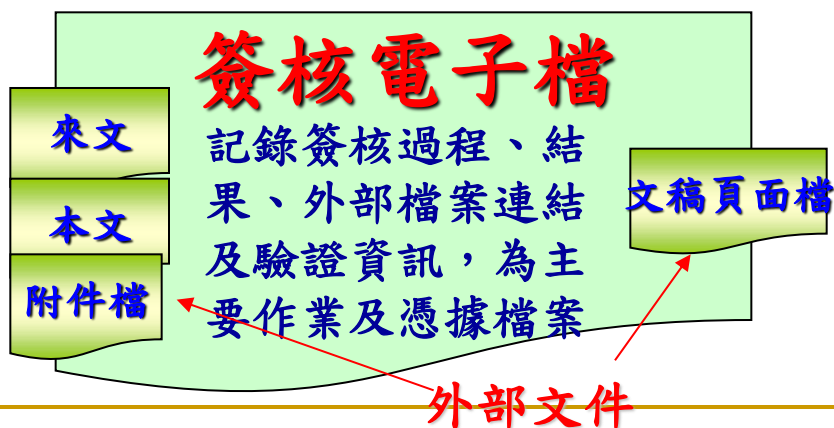
儲存格式說明(續)

■ 附件檔

- 附件檔類型含文字檔、靜態圖形檔、工程圖檔、動畫檔、聲音檔、動態影像檔等電子或電子影音檔案。

■ 簽核電子檔

- 線上簽核之文字化記錄工具，內容以XML語法所組成，用以記錄各簽核點之簽核結果及過程，為主要作業及憑據檔案，另稱SI（Sign Instance）檔。



```
<?xml version="1.0" encoding="utf-8"?>
<!-- 99_sign_utf8.ent 線上簽核(簽核電子檔) 2010.1.08 -->
<!ELEMENT 線上簽核流程 (簽核流程+)>
<!ATTLIST 線上簽核流程
  Id ID #REQUIRED
>
<!ELEMENT 簽核流程 (分會點|流程點)*
<!ATTLIST 簽核流程
  Id ID #REQUIRED
  異動別 CDATA #REQUIRED
>
```

si檔

儲存格式說明(續)

□ 文稿頁面檔

- 為線上簽核之視覺化記錄工具，因考量多元化之輔助工具技術產生及為免文字誤會，以影像方式記錄各簽核點人員作業完成後於清稿前之稿面，輔助重現文稿之原文原意(包含各簽核點簽核意見)。

文稿頁面檔

視覺化影像檔 (Tiff/Jpeg..)

呈現文稿頁面

輔助原貌重現

理。

2樓研討室

二、本案焦點會議業於98年8月20日日假本局3樓會議室召開，計邀請吳委員宗成等5位委員出席，並請本局檔案徵集組及檔案典藏組列席，審查本案第2期交付文件。

三、本案如奉 核後，擬將會議紀錄以電子郵件發送與會人員。

敬請

核示

訂

承辦單位
檔案資訊組

0911
1025
分析師 林玉美

0911
1133
科長 李殷

決行

可

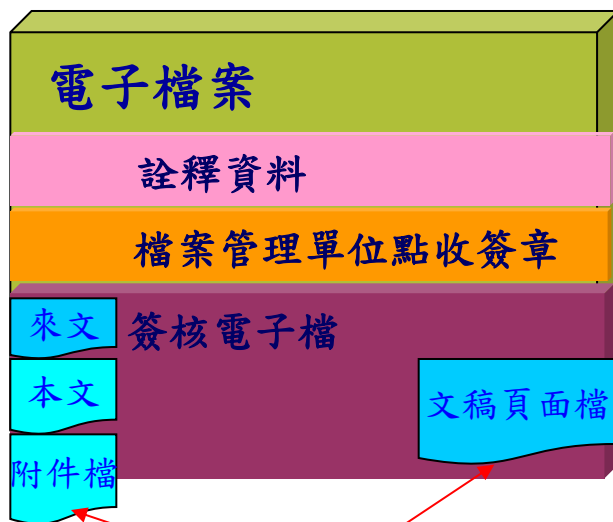
0911
1141
檔案資訊組
組長 張文熙

線

儲存格式說明(續)

電子檔案封裝檔

- 公文線上簽核電子檔案：內容以XML語法所組成，以簽核電子檔為基礎，歸檔點收時以機關憑證加簽，年度封裝詮釋資料。
- 紙本檔案數位化之電子影音檔案：以機關憑證加簽。



外部文件

```
<電子封裝檔>+
<封裝檔內容 Id="Wrap">+
  <封裝檔資訊>電子檔案<封裝檔資訊>+
  <電子檔案>+
    <檔案管理單位點收簽章>+
    <Signature Id="CheckSignGCA">+
    <SignedInfo>+
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">+
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">+
      <Reference URI="#FlowInfo">+
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">+
      <DigestValue>ADKDS+WuPeobYGFY7sbDIJ85CMs=</DigestValue>+
    </Reference>+
    <Reference URI="#Sol">+
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">+
    <DigestValue>aCBtv+TVs91GsFdfElxq04ajH+4=</DigestValue>+
    </Reference>+
    <SignedInfo>+
    <Signature Value>c2I24xp/4Ei2ufbBdC17SQD3aDDXcIDSL213Cn+mnvqFZLmWp1vRrAT3eGJzL0VxWid1V7DabdVQ9Iu0jW4pFEC969rDe85LZpJBrg/4D+GjHIQ7jZIDfc2W58QPEaM09/FAAbNysDezOm2KjGhHIY YX2HGkbTVmAvuCz8UQM=</SignatureValue>+
    <KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">+
    <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">+
    <X509Certificate>MIID7zCCAtegAwIbAgIQUi6ux4wdnafUf7Ad+tpXD1DANBgkqhkiG9w0BAQUFADBKMQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KG M5pS6ZmMScwJQYDVQQQLDB7mLLfupzmukZzoqabmhpHorYnraqHnkfbkuC3I
```

XML與簽章技術

電子檔案管理目標

原則	說明	對應做法
完整性 (integrity)	確保儲存電子檔案的內容、詮釋資料及儲存結構之完整，未遭到竄改或偽造。	運用雜湊值計算
真實性 (authenticity)	可鑑別及確保電子檔案產生、蒐集及修改過程的合法性。	運用數位憑證加簽
可及性 (accessibility)	指藉由電子檔案保存機制，配合法定保存年限，維持電子檔案及其管理系統的可用性。	制定一致性的線上簽核電子檔案格式、限縮電子檔案格式之使用
不可否認性 (Non-repudiation)	發送端不能否認經其同意送出的資料，亦即簽核者不可否認其所完成的簽核行為。	運用電子憑證加簽
機密性 (Confidentiality)	防止非法使用者(指未獲授權者)得知已保護之敏感資料的內容。	採對稱式或非對稱式加密處理、權限控管

電子檔案生命週期相關技術

電子檔案管理流程

檔案蒐集與產生

檔案保管與維護

檔案清理

檔案檢調與應用

稽核與安全

使用時機及運用技術、工具及方法

公文簽核

檔管點收

數位簽章

詮釋資料
封裝

數位簽章

檔案移轉(交)

數位簽章、數位
信封、封裝工具

應用申請
(認證授權)

數位簽章、權限控管

檔案傳輸

檔案儲存

加密

檔案保存

轉置、模擬、封裝、系統保存、更新

檔案清查

技術鑑定工具

智慧財產
權保護

浮水印

檔案銷毀

實體銷毀、邏
輯銷毀

XML技術

- XML(eXtensible Markup Language)是一種標示語言，也是一種「元語言」(meta-language)，使用者可依需求自行定義標籤描述文件結構。
 - 具擴展性、結構性與可驗證性(validation)等優點，利於資訊的交換及處理。
 - W3C提出的標準，具備跨平台、可長期保存、可再利用、能直接瀏覽等特性。
- DTD(Document Type Definition)：提供正式的文法規範，說明XML文件結構與可允許的值，提供機器自動剖析。
 - Well-formed XML文件：沒有參引DTD。
 - Valid XML文件：參引DTD。
- XML簽章：資料格式是以XML為基礎，支援部分區段簽章與多人簽章。

XML技術（續）

■ 以表格方式呈現學籍資料

姓名	學號	性別	出生日期	住家電話	手機
陳品潔	09600101	女	65.10.22	02-25112036	0918-204303
李心怡	09600102	女	66.2.13	02-28974411	
吳百莉	09600103	女	65.12.08	02-28996013	0918-3579
張功行	09600104	男	66.6.24	02-28964458	0916-4483

“?” 表示可選用
“,” 表示連接
“*” 表示可不選用或多次選用
“+” 表示至少一次或多次選用
“|” 表示任取其一

■ 以XML呈現學籍資料

DTD

<學籍資料>
<學員>
<姓名>陳品潔</姓名>
<學號>09600101</學號>
<性別>女</性別>
<出生日期>0651022</出生日期>
<住家電話>02-25112036</住家電話>
<手機>0918-204303</手機>
</學員>
.....

XML文件

```
<?xml version="1.0" encoding="utf-8" ?>  
<!ELEMENT 學籍資料 (學員*)>  
<!ELEMENT 學員 (姓名,學號,性別,出生日期,住家電話,手機?)>  
<!ELEMENT 姓名 (#PCDATA)>  
<!ELEMENT 學號 (#PCDATA)>  
<!ELEMENT 性別 (#PCDATA)>  
<!ELEMENT 出生日期 (#PCDATA)>  
<!ELEMENT 住家電話 (#PCDATA)>  
<!ELEMENT 手機 (#PCDATA)>
```

說明XML文件結構與可允許
的值，提供機器自動剖析

XML技術應用

■ 檔案傳輸格式

□ 機關內部傳輸及儲存

- 公文線上簽核：簽核電子檔
- 電子檔案歸檔點收：電子檔案封裝檔

□ 跨機關間資料交換

- 公文電子交換：函、開會通知單等DI檔。
- 機關定期彙送之檔案目錄彙送格式。
- 機關間移轉或移交時之移轉(交)電子媒體封裝檔。

□ 其他常見應用

- 線上購物、RSS訂閱等。

標籤集說明

共用

基本標籤集

線上簽核標籤集

內部用標籤集

公文交換標籤集

檔案管理標籤集

含公文交換、公文管理及公文製作

係以「欄位」為基礎，以XML語法定義相關欄位及內容結構。

標籤集說明(續)

■ XML文件實例(函)

基本標籤集

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- 基本標籤集 99_basic_utf8.ent 1999.12.1 修改日期:2010.01.08 -->
<!ELEMENT 年月日 (#PCDATA)>
<!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 時分 (#PCDATA)>
<!ELEMENT 文字 (#PCDATA)>
<!ELEMENT 姓名 (#PCDATA)>
<!ELEMENT 職稱 (#PCDATA)>
<!ELEMENT 全銜 (#PCDATA)>
<!ELEMENT 機關代碼 (#PCDATA)>
<!ELEMENT 單位代碼 (#PCDATA)>
<!ELEMENT 收發處理本別 EMPTY>
```

DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- 99_2_utf8.dtd 函 2008.10.1 修改日期:2010.01.08 -->
<!ENTITY % 基本標籤 SYSTEM "99_basic_utf8.ent" >
%基本標籤;
<!ENTITY % 電子交換標籤 SYSTEM "99_exchange_utf8.ent" >
%電子交換標籤;
<!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+,連別?,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 -->
```

函之DI

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE 函 SYSTEM "99_2_utf8.dtd" [
<!ENTITY 表單 SYSTEM "g2b2c.sw" NDATA DI>
<!NOTATION DI SYSTEM "">
<!NOTATION_X SYSTEM "">
]>
<函>
<發文機關>
<單位名>行政院研考會資訊管理處</單位名>
<機關代碼>TEST34100A</機關代碼><單位代碼>U010050</單位代碼>
</發文機關>
<函類別 代碼="函"/>
<地址>台北市濟南路1段2之2號8樓</地址>
<聯絡方式>承辦人:王上安</聯絡方式>
<聯絡方式>電話:(02)2788-8888#888</聯絡方式>
<聯絡方式>傳真:(02)2788-8888</聯絡方式>
<受文者><交換表 交換表單="表單">如正副奉行文單</交換表></受文者>
<發文日期><年月日>中華民國93年7月21日</年月日><發文日期>
```

欄位定義

欄位名稱	內部格式	說明
職稱	X(n)	人員的職稱
全銜	X(n)	機關全稱

標籤集說明(續)

■ XML文件實例(檔案目錄彙送)

檔案標籤集

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- 檔案標籤集(檔案用) 99_records_utf8.ent 修改日期:2010.01.08 -->
<!ELEMENT 檔案目錄傳送名稱 EMPTY>
<!ATTLIST 檔案目錄傳送名稱 代碼 (A|B|C|D|E|F|G|I|X) "A">
<!ELEMENT 系統名稱 EMPTY>
<!ATTLIST 系統名稱 代碼 (1|2) "1">
<!ELEMENT 月份 (PCDATA)>
<!ELEMENT 應用註記 (PCDATA)>
<!ELEMENT 複製註記 EMPTY>
<!ATTLIST 複製註記 代碼 (Y|N|C) "Y">
<!ELEMENT 應用方式 EMPTY>
<!ATTLIST 應用方式 代碼 (1|2|3|4) "1">
```

DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- 99_recatalog_utf8.dtd 檔案目錄彙送格式 -->
<!ENTITY % 基本標籤 SYSTEM "99_basic_utf8.ent">
%基本標籤;
<!ENTITY % 檔案標籤 SYSTEM "99_records_utf8.ent">
%檔案標籤;
<!ELEMENT ROWSET (案卷|案件)*>
<!ELEMENT 案卷 (檔案目錄傳送名稱,功能,案名,並列案名?,其他案名?,
檔案產生及管有機關,檔案有關機關?,密等,保存年限,調整後之保存年限?,
保存年限調整原因?,應用限制?,應用註記?,複製限制?,媒體型式*,基準項目
編號*,年度號,分類號,案次號,其他編號*,案卷檔案起始日期之年制?,案卷
檔案起始日期,案卷檔案迄止日期之年制?,案卷檔案迄止日期,數量+,計量
單位+,外觀細節*,案情摘要+,可參照之有關案卷*,主題,附註*,核准銷毀文
號?,銷毀日期?,移轉註記?,延長移轉屆滿日期?,移轉日期?,移交日期?,接管
機關代碼?,移交機關代碼?,分類號啟用日期?,史政機關代碼*)>
```

欄位定義

欄位名稱	內部格式	說明
檔案目錄傳送名稱	X(1)	代碼:該單紀錄之檔案係屬: <u>A</u> 案卷之檔案目錄彙送、 <u>B</u> 案卷之檔案移轉目錄、 <u>C</u> 案件之檔案目錄彙送、 <u>D</u> 案件之檔案銷毀目錄、 <u>E</u> 案件之檔案移交目錄、 <u>F</u> 案卷之檔案銷毀目錄、 <u>G</u> 案卷之檔案移交目錄、 <u>I</u> 案件之檔案移轉目錄、 <u>X</u> 分類表。
系統名稱	X(1)	代碼:指資料來源之系統名稱。1:公文管理系統 2:檔案管理系統

XML文件

```
<案卷>
<檔案目錄傳送名稱 代碼="A"/>
<功能 代碼="N"/>
<案名>各類語言教學資料</案名>
<檔案產生機關>X.X縣政府</檔案產生機關>
<檔案有關機關>教育部、內政部、國立師範大學等</檔案有關機關>
<密等 代碼="1"/>
<保存年限>3</保存年限>
<應用限制 代碼="Y"/>
<媒體型式 代碼="1"/>
<年度號>0095</年度號>
<分類號>010101</分類號>
<案次號>1</案次號>
<案卷檔案起始日期>0950101</案卷檔案起始日期>
<案卷檔案迄止日期>0950820</案卷檔案迄止日期>
```

範例1說明

■ 實作練習

- 以XML EDITOR工具檢核XML文件
- 修改XML文件
- 修改內容結構(DTD)
- 操作步驟詳附錄

■ 目的

- 讓學員瞭解如何檢核XML文件
- 瞭解XML文件與內容結構(DTD)之關聯

電子簽章相關定義

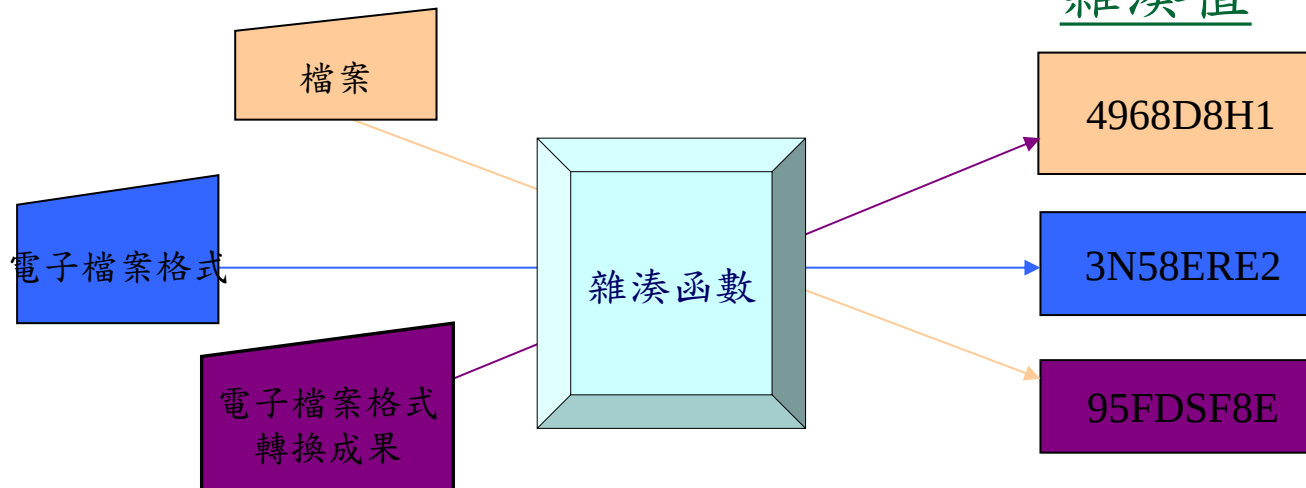
- 電子文件：指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。
- 電子簽章：指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。
- 數位簽章：指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。
- 加密：指利用數學演算法或其他方法，將電子文件以亂碼方式處理。
- 憑證機構：指簽發憑證之機關、法人。
- 憑證：指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。
- 憑證實務作業基準：指由憑證機構對外公告，用以陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則。

雜湊值概念

■ 雜湊值 (Hash Value)

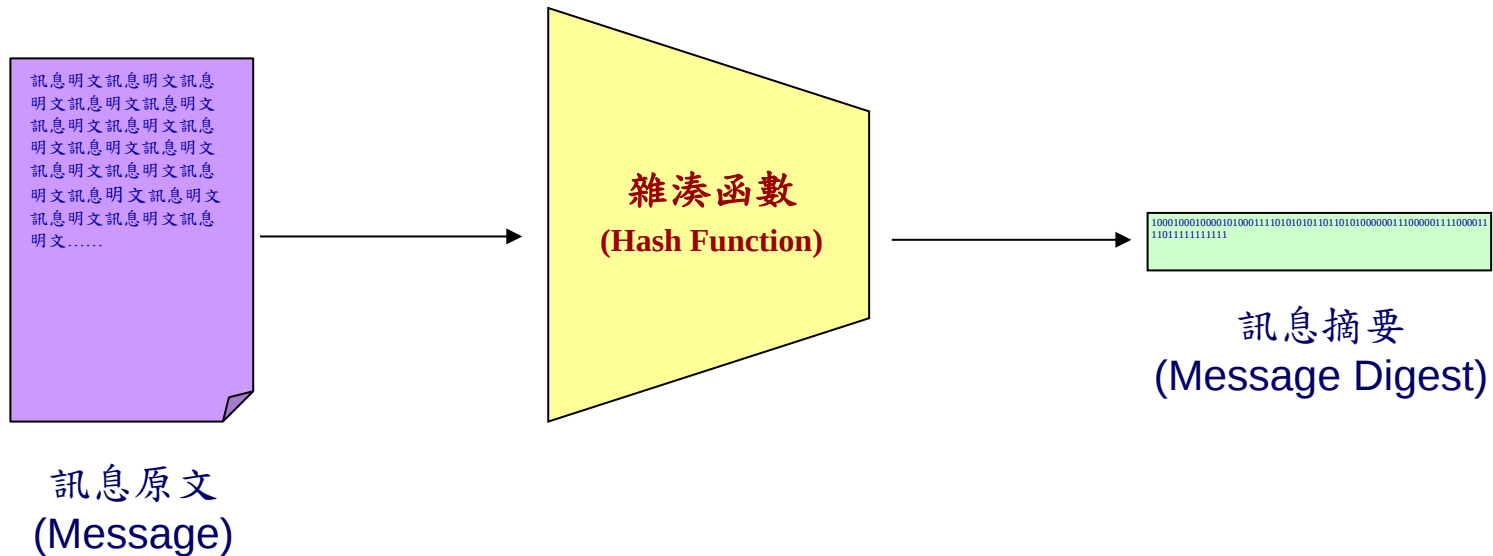
- 此函數會將任意長度訊息對應到固定長度雜湊值
- M：訊息 H:雜湊函數 雜湊值： $h=H(M)$

輸入



雜湊函數的功能

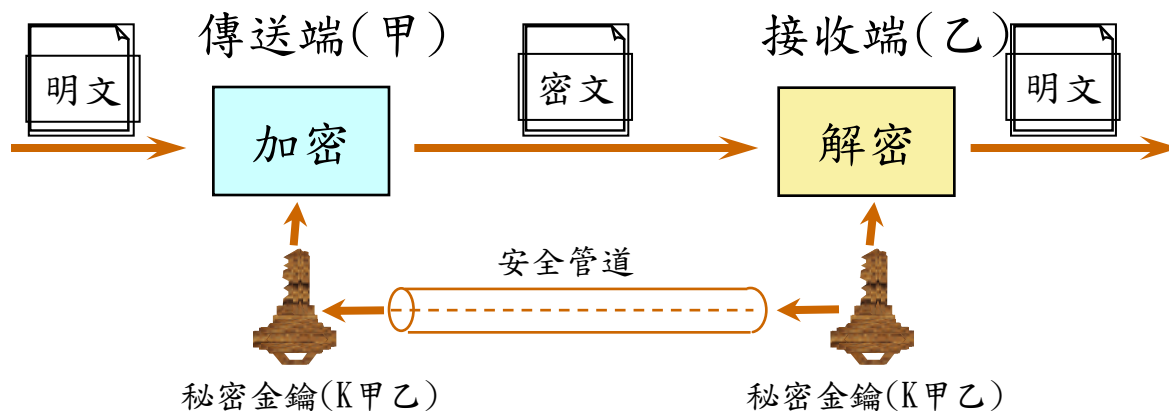
- 可以處理任意大小的資料區段
- 產生固定長度的輸出，即訊息摘要(Message Digest)
- 單向(one-way)，為不可逆
- 碰撞機率低
- 計算速度快
- 常見的雜湊函數演算法有MD5、SHA1



加密機制

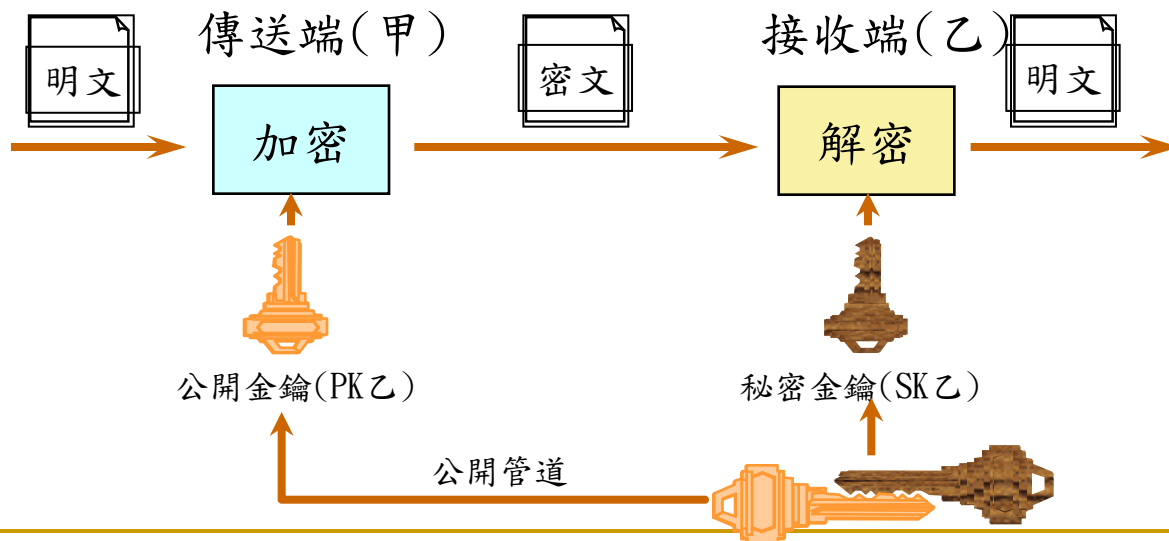
對稱性
加密法

DES
3-DES
AES

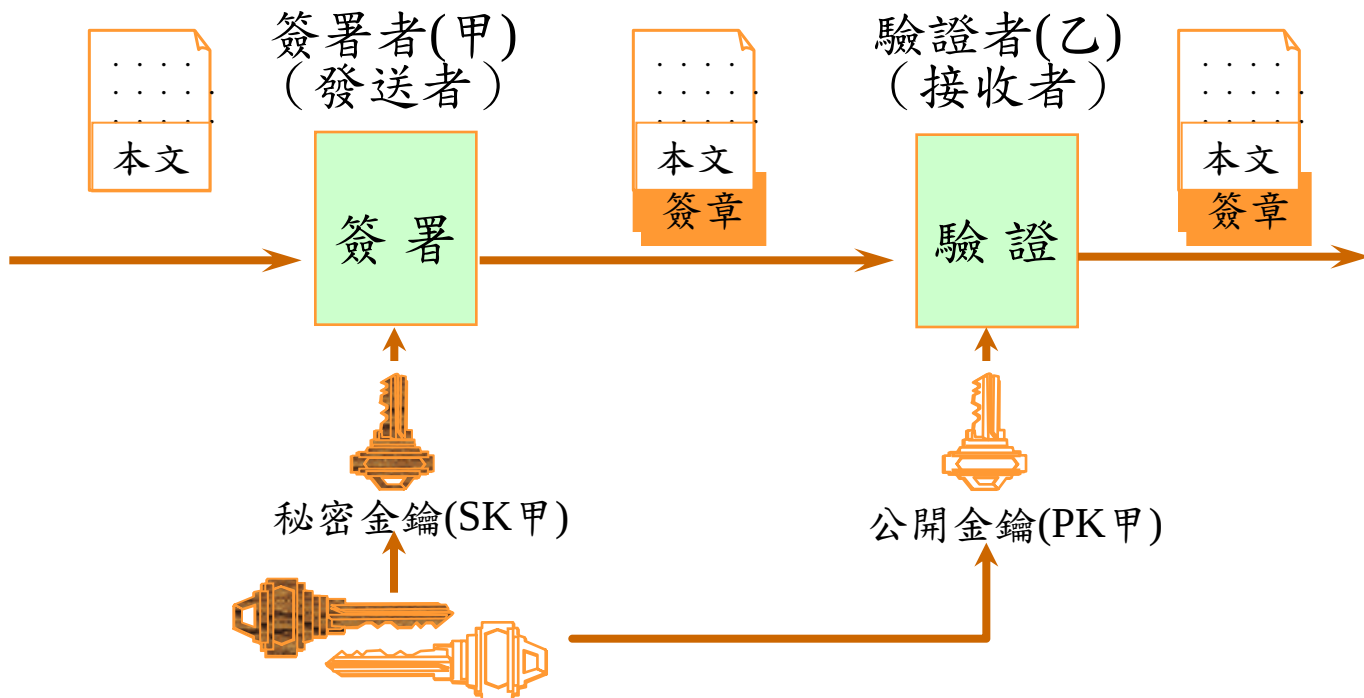


非對稱性
加密法

RSA
ECC
DL-Based



數位簽章



數位簽章方法

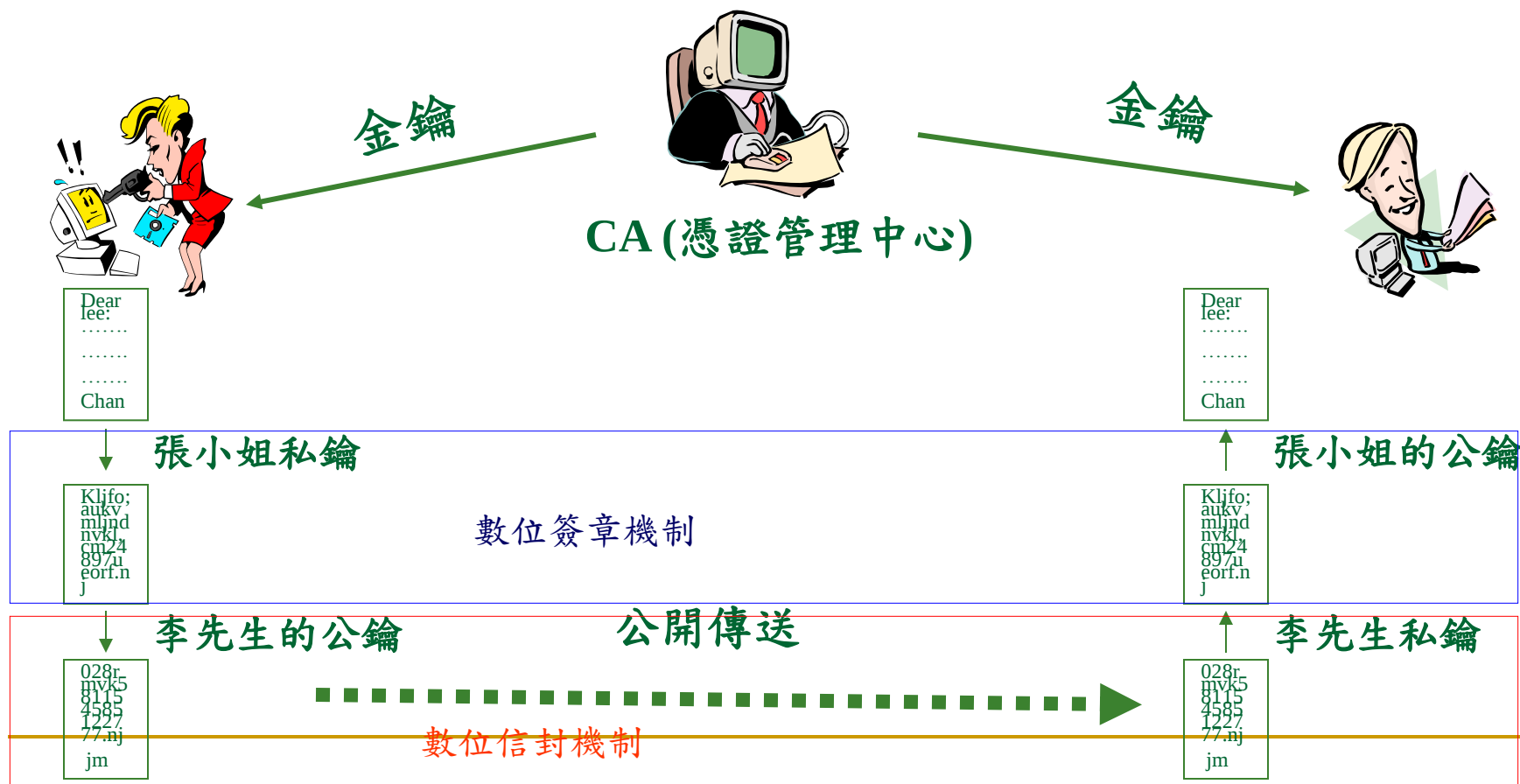
- RSA
- ElGamal
- DSA (digital signature algorithm)

安全保護功能

- 完整性
- 鑑別性
- 不可否認性

非對稱式密碼系統

❖ 張小姐寫封信給李先生



封裝處理技術與作法

電子檔案與封裝處理

- 封裝：將電子檔案及詮釋資料，以包裹方式儲存之。
- 封裝目的
 - 建立電子檔案管理標準化，便利機關間檔案相互移轉(交)作業。
 - 封裝檔案與資訊系統個自獨立，可透過共通性軟體瀏覽、驗證檔案內容，降低不同系統間之轉換成本。
 - 將電子檔案、詮釋資料與驗證資訊併同封裝，可確保電子檔案真實性、完整性。
 - 封裝檔案格式符合電子檔案格式表規定，避免檔案格式過多造成轉置的複雜度，利於電子檔案長期保存與應用。

封裝檔格式

■ 電子檔案封裝檔：

- 公文線上簽核電子檔案：將本文、附件、各層級簽核者憑證公鑰、簽核意見、簽體、簽核時間封裝處理。每一簽核流程點以個人憑證加簽，歸檔點收以機關憑證加簽，並得加附檔管人員之個人憑證。
- 紙本簽核公文數位化之電子影音檔案：以機關憑證加簽。
- 詮釋資料封裝處理：進行案件、案卷詮釋資料封裝處理，以機關憑證加簽。

■ 電子媒體封裝檔：

- 電子檔案儲存備份至媒體時之產出格式。
- 進行詮釋資料的封裝處理，以機關憑證加簽。

■ 移轉（交）電子媒體封裝檔：

- 機關間移轉或移交電子檔案時產出格式。
- 進行詮釋資料的封裝處理，以機關憑證加簽。

■ 封裝檔係採XML簽章規範，以 XML 格式呈現。

公文線上簽核流程設計示意圖



承辦人



主管



結案

最終簽核結果清
稿前文稿影像檔
(含簽核意見等)

作業處理層

簽核記錄層

資訊系統
(XML/資料庫)
(輔助工具)

提供彈性
簽核作業處理

資訊系統
(XML/資料庫)
(輔助工具)

提供彈性
簽核作業處理

資訊系統
(XML/資料庫)
(輔助工具)

文稿
頁面檔
(檔管格式)

輸出必要簽核結果

輸出必要簽核結果

輸出必要簽核結果

輸出

簽核電子檔
(標準格式)
(輔助工具
為選項紀錄)

簽核電子檔
(標準格式)
(輔助工具
為選項紀錄)

簽核電子檔
(標準格式)
(輔助工具
為選項紀錄)

文稿
頁面檔
(檔管格式)

驗證

歸檔

文稿頁面檔設計示意圖

留存清稿前內容，記錄方式擬採單頁式及堆疊式2種



承辦

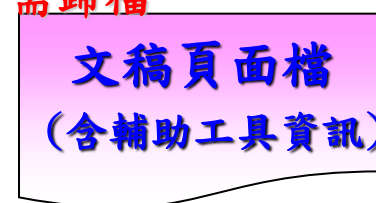


核閱



決行

需歸檔



單頁式

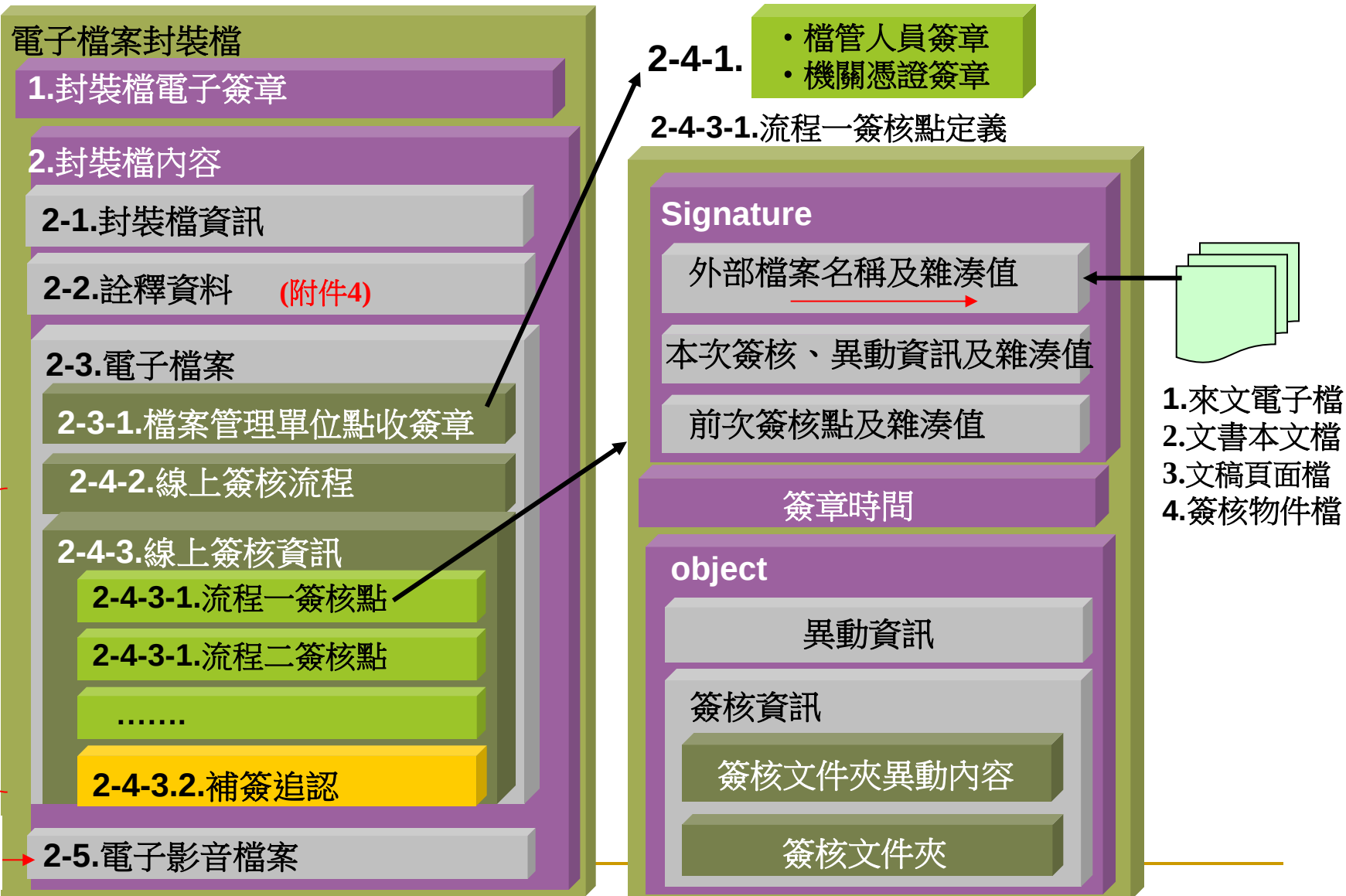
2擇1

堆疊式

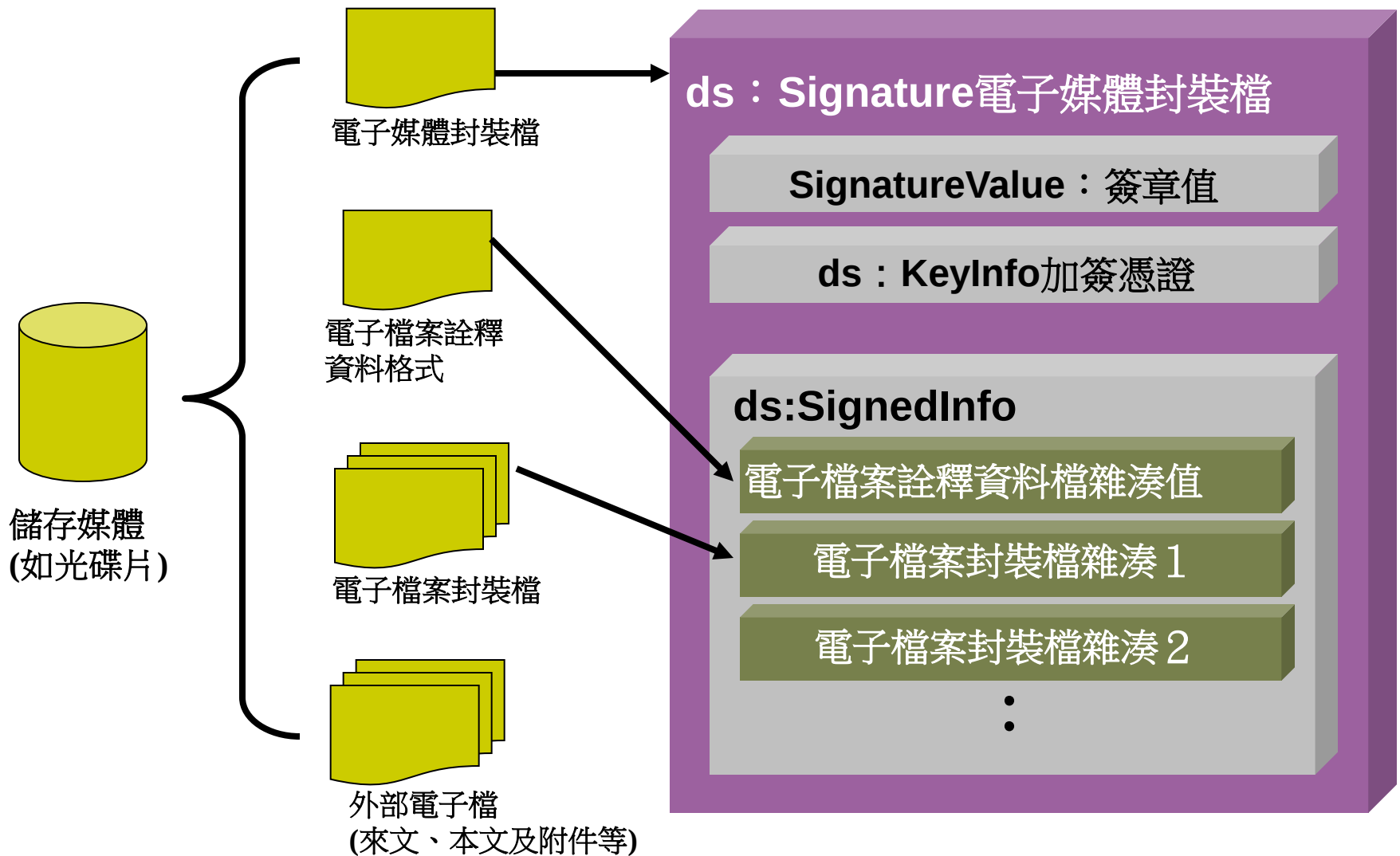


註1-輔助工具：章戳、文字意見、圖檔等

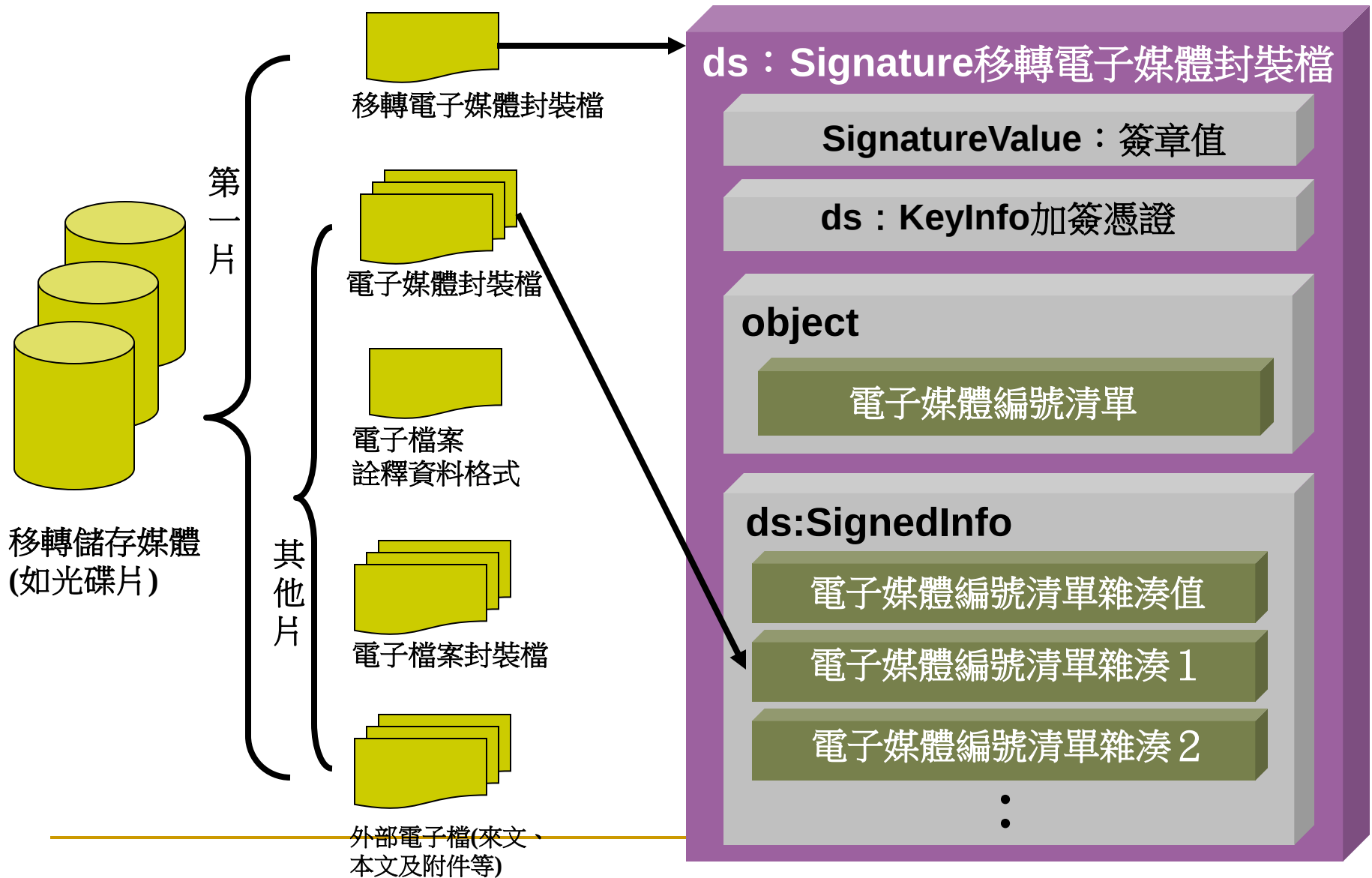
電子檔案封裝檔示意圖



電子媒體封裝檔示意圖



移轉(交)電子媒體封裝檔示意圖



實作範例介紹

實作範例說明

■ 公文線上簽核－簽核電子檔

```
<線上簽核>
<線上簽核流程 Id="FlowInfo">
  <簽核流程 Id="FLOW_分文" 異動別="分文"/>
  <簽核流程 Id="FLOW_承辦" 異動別="呈核"/>
  <簽核流程 Id="FLOW_科長" 異動別="核閱"/>
  <簽核流程 Id="FLOW_高分" 異動別="決行"/>
</線上簽核流程>
<線上簽核資訊>
  <簽核點定義 URI="#FLOW_承辦" Id="sign_承辦">
    <Signature Id="ds_user_0">
      <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010315"/>
        </CanonicalizationMethod>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        </SignatureMethod>
        <Reference URI="函1來文-0970000022.di">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          </DigestMethod>
          <DigestValue>ounPg12wSr57UIttAFdWk1tEdaU=</DigestValue>
        </Reference>
        <Reference URI="簽98110001v1.di">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          </DigestMethod>
          <DigestValue>NybKuw7TLC9wqavT2J71/GHpoD0=</DigestValue>
        </Reference>
        <Reference URI="簽-文稿頁面檔-原始頁面.tifff">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          </DigestMethod>
          <DigestValue>ounPg12wSr57UI3CAfddk1tEdaU=</DigestValue>
        </Reference>
        <Reference URI="#Sign_承辦">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          </DigestMethod>
          <DigestValue>FUuygSacYTRmPWUagptN0jbNe0c=</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>WlWWF6gg4kQUNZdjC/m/ssy07b/Fx3zty3mjyCJsD6y0Kahiso1BL3Q/KwSQEpuNQPzKFvYr/jLY
      4aY7QZK66PGL+ahuJy9GrU1gPU6/bpFXGN/+8yha7XoXB92u+uYH3KY5UzU0aGw9khW5Up/oL049
      4U+5voNDyWMAaxPTDk=</SignatureValue>
```

簽核流程 Id="Flow_分文" 不在線上簽核資訊中，故此簽核流程不需加簽

外部關聯檔案之雜湊值

"Flow_承辦" 簽核流程之雜湊值

"Flow_承辦" 簽核流程之簽章值

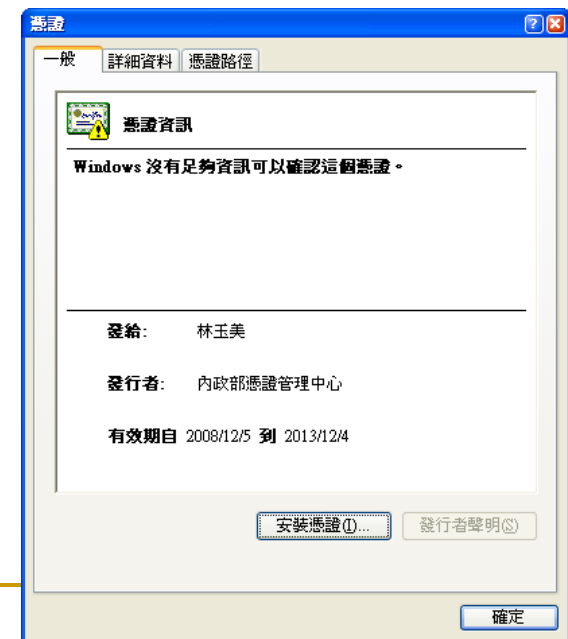
實作範例說明(續)

■ 公文線上簽核－簽核電子檔

```
<KeyInfo>
  <X509Data>
    <X509Certificate>MIID6jCCATKgAwIBAgIRA0298dbIChCJGAdUdy01D5cwDQYJKoZIhvcNAQEFBQAwSjELMAkGA1UE
    BHMCFVcxEjaQBGNUBAOMCeiHj0aUv+mZojEnMCUGA1UECwwe5pS/5bqc5ris6Kmm5oaR6K2J566h
    55CG5Lit5b+DMB4XDTA3MDUyNzA3NTQyMUoXDTA3MDcyNjA3NTQyMUowQzELMAkGA1UEBHMCFVcx
    GTAXBGNUBAMME0a4r0ippuiHqueEtuS6ujExGTAXBGNUBAUTEDJmZTQwYzI2NzkW0WM3ODYwgZ8w
    DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALh6xWu1i9PATLI/UYdiDjJukkCLibZTfstZuAHvW8PM
    YSQFCBmr49B8UwUmVukCLs90BL0Kb3ypN0xZtTzEptj8X0oF6g2Z560SW2b1laL5bjRPAiPmFijov
    +vn210MucCsoI3u+ru5US9AnikcFr2RkTv1IchigC7Umu1NGrbNagMBAAGjggFUMIIBUDBGbGnu
    HR8EPzA9MDug0a3hjUodHRwOi8vZ3Rlc3RjY5S5uYXQuZ292LnR3L3JlcG9zaXRvcnkvdQ1JML2Nu
    bXB5ZXR1LmNybdBtBgggrBgEFBQcBAQRHMEUwQWYIKwYBBQUHMAKGN2h0dHA6Ly9ndGUzdGNNhLm5h
    dC5nb3YudHcvcmUwb3NpdG9yeS9Jc3N1ZWVub1RoXNDQ55wN2IwFAYDVR0gBA0wCzAJBgdnhZ1
    AAMAMC8GA1UdCQoMCYwFQYHYI2ZAWQCATEKBghghnYBZAMBATANBgdnhYBZAIZMQIMADAdBgNU
    HQ4EFgQUQqHk8mUsuXAsT9o14d8iUzn4/QQwGgYDVR0RBBAwEVEPdgUzdEBjaHQuY29tLnR3MA4G
    A1UdDwEB/wQEAwIHGDAFBGnuHSMEDAwgBRL9kp3aNOUx001YNwOG++punv2UZANBgkqhkiG9w0B
    AQUFAAOCAQEAiWtEt+N5hc+cPN9sFerhbKmwY2TERG+ov6+P1kTQxSSEab0WU00yuvZFQgg51XUa2
    NjC4EEBSPL/y9r5Cj0NdrEhocovZf1/0GeU8WuihgG4/Orguv1jbFxaGr0t9F8KIMw1gdZfLU479
    nHe0HDkUzI2UgZe1HkwfY47M1gd/S1kUP1ygnX3oHph92Y3QGKFNH9HnZsmmd3Wsv9mtw3dYxI2
    rH/UE49tXrIUZU/F/qzyx57FmUB2RuBQ/xPDuV30IJsXfatpNtkcsPvJ009220RMvXYMsyQ21sHD
    4Q4KFTkwxUCjhLPuYfUrIqzhNynMAfUF7EJzZ15JFrhVukP25g==</X509Certificate>
  </X509Data>
</KeyInfo>
</Signature>
<Object Id="Sign_info_0">
  <異動資訊>
    <簽核人員>
      <單位>規劃科</單位>
      <職稱>科員</職稱>
      <姓名>王小民</姓名>
      <帳號>CAESAR1</帳號>
      <角色>承辦人員</角色>
    </簽核人員>
    <異動別>呈核</異動別>
    <簽核意見>敬呈簽辦</簽核意見>
    <簽核時間>09605271823</簽核時間>
    <次位簽核人員>
      <簽核人員>
        <單位>規劃科</單位>

```

“Flow_承辦”簽
核流程採用之憑證



實作範例說明(續)

■ 公文線上簽核－簽核電子檔

```
<簽核點定義 URI="#Flow_高分" Id="sign_高分" >
  <Signature Id="ds_user_2">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/></CanonicalizationMethod>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/></SignatureMethod>
      <Reference URI="函1來文-0970000022.di">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
          </DigestMethod>
          <DigestValue>ounPg12wSr57UIttAFdWk1tEDaU=</DigestValue>
        </Reference>
        <Reference URI="簽98110001v2.di">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </DigestMethod>
            <DigestValue>NybkW7TLC9wqavT2J71/GHpoD0=</DigestValue>
          </Reference>
          <Reference URI="函稿附件1v1.doc">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
              </DigestMethod>
              <DigestValue>ounPg12wSr57UI3CAhhWk1tEDaU=</DigestValue>
            </Reference>
            <Reference URI="簽-文稿頁面檔-高分.tiff">
              <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                </DigestMethod>
                <DigestValue>ounPg12wSr57UI3CAhhWk1RRDaU=</DigestValue>
              </Reference>
              <Reference URI="#Sign_科長">
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                  </DigestMethod>
                  <DigestValue>FU11gSacYTRmPWvagptN0jbNe0c=</DigestValue>
                </Reference>
                <Reference URI="#sign_高分">
                  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                    </DigestMethod>
                    <DigestValue>cvuygSacYTRmPWvagptN0jbNe0c=</DigestValue>
                  </Reference>
                </SignedInfo>
```

前一簽核流
程之雜湊值

“Flow_高分”
簽核流程之
雜湊值

實作範例說明

■ 電子檔案封裝檔-公文線上簽核電子檔案

```
<電子封裝檔>
<封裝檔內容 Id="Wrap">
  <封裝檔資訊>電子檔案</封裝檔資訊>
  <電子檔案>
    <檔案管理單位點收簽章>
      <Signature Id="CheckSignGCA">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <Reference URI="#FlowInfo">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>ADKDS+WuPEobYGfY7sbDIJ85CMs</DigestValue>
          </Reference>
          <Reference URI="#Sol">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>aCBtv+TVs91GsFdfElxq04ajH+4</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>c2I24xp4Ei2ufbBdC17SQD3aDDXcIDSI213Cn+nmqFZLmWp
          1vRrAT3sGJzL0VxWtJiV7DabdVQ
          9Iu0jW4pFEC969rDe8SLZpJBrg/4D+fGjHIQ7jZIDfcI2W58QPEmM09/PAAbNysD
          ezOm2KiGhHIY YX2HGkbTVmAvCz8UQM=
        </SignatureValue>
        <KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Certificate>MIID7zCCAtegAwIBAgIQUi6ux4wdmfUf7Ad+tpXD1DANBgk
              qhkiG9w0BAQUFADBKMQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KG
              M5pS6ZmMScwJQYDVQQQLDB7mLlupzmuKzoqabmhpHorYnnrqHnklbkuK3l
            </X509Certificate>
          </X509Data>
        </KeyInfo>
      </Signature>
    </檔案管理單位點收簽章>
  </電子檔案>
</封裝檔內容>
</電子封裝檔>
```

此為檔案管理人員以
GCA機關副卡進行點收
加簽所產生之簽章

"SignatureValue"存放
電子簽章簽體

實作範例說明

■ 電子檔案封裝檔-電子影音檔

```
<封裝檔內容 Id="Wrap"> ↵
<封裝檔資訊>電子影音檔案</封裝檔資訊> ↵
<電子影音檔案 文號="0950004978"> ↵
<歸檔掃描影像 群組數="3" 總頁數="7"> ↵
<頁面群組 頁數="3" 檔案數="3" 群組名稱="本文" 群組型別="本文"> ↵
<電子影音檔案資訊> ↵
<檔案名稱>0950004978.0001</檔案名稱> ↵
<檔案大小>20647</檔案大小> ↵
<檔案格式>TIF</檔案格式> ↵
</電子影音檔案資訊> ↵
<電子影音檔案資訊> ↵
<檔案名稱>0950004978.0002</檔案名稱> ↵
<檔案大小>29985</檔案大小> ↵
<檔案格式>TIF</檔案格式> ↵
</電子影音檔案資訊> ↵
<電子影音檔案資訊> ↵
<檔案名稱>0950004978.0003</檔案名稱> ↵
<檔案大小>52794</檔案大小> ↵
<檔案格式>TIF</檔案格式> ↵
</電子影音檔案資訊> ↵
</頁面群組> ↵
<頁面群組 頁數="2" 檔案數="2" 群組名稱="AA" 群組型別="附件"> ↵
<電子影音檔案資訊> ↵
<檔案名稱>0950004978.0004</檔案名稱> ↵
<檔案大小>31903</檔案大小> ↵
<檔案格式>TIF</檔案格式> ↵
</電子影音檔案資訊> ↵
```

電子影音檔對應
之文號

影像檔總頁數7
頁，本文3頁

實作範例說明

■ 電子媒體封裝檔

```
<媒體封裝檔>
  <Signature>
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="電子媒體檔案詮釋資料.xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>Zj4LXFIsjFV5E5arekW1L4PGzs=</DigestValue>
      </Reference>
      <Reference URI="0950000001O.XML">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>wq2nrhWXdYMMPGgKL2r7unqCYs=</DigestValue>
      </Reference>
      <Reference URI="0950000002O.XML">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>Q8oS+h8XC5hz0F0P3LTz5+IuX+0=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>rtM...gl4H/fb xmQ==</SignatureValue>
    <KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Certificate>MIIEIT...A==</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</媒體封裝檔>
```

1.對媒體詮釋資料明細計算雜湊值

2.對媒體內每1筆電子檔案封裝檔均計算雜湊值

以機關憑證加簽，於”SignatureValue”存放電子簽章簽體

實作範例說明

■ 移轉(交)電子媒體封裝檔

```
<移轉封裝檔>
  <Signature>
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="V0950001.xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>5xL6wST6Gw7ZIIYFFhJympEYg=</DigestValue>
      </Reference>
      <Reference URI="V0950002.xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>kkKdggQekwSGxt5evalGLVXDmYY=</DigestValue>
      </Reference>
      <Reference URI="#MediaObjId">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>PZ7WKxZtEMhT7GyqVhJaEToOLx0=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>BcNVBAMIMCem...</SignatureValue>
    <KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Certificate>MIIBOTC...Q0M=</X509Certificate>
      </X509Data>
    </KeyInfo>
    <Object Id="MediaObjId">
      <電子媒體編號清單>
        <電子媒體編號>V0950001</電子媒體編號>
        <電子媒體編號>V0950002</電子媒體編號>
      </電子媒體編號清單>
    </Object Id>
  </Signature>
</移轉封裝檔>
```

- 1.對每1片媒體均計算雜湊值
- 2.對媒體編號清單計算雜湊值

以機關憑證加簽，
於”SignatureValue”存
放電子簽章簽體

電子檔案轉置

電子檔案轉置

- 轉置(Migration)：電子檔案管理系統之軟硬體過時或失效需進行軟硬體格式轉換，以便日後可讀取之作業程序。
- 電子檔案限制：須經由應用程式才能呈現，各種應用程式也須在作業系統上執行，某些作業系統更只能執行在特定的硬體架構上。
- 面臨轉置原因：
 - 因應保存需求，轉置為適合長期保存格式。
 - 電子檔案應用需求。
 - 電子檔案格式可能過時。
 - 支援電子檔案之應用程式、相依的作業系統或硬體架構無法繼續取得。
 - 配合法令規定。

電子檔案轉置(續)

■ 轉置注意事項

- 格式轉置前應評估相關應用系統是否需要一併調整或更新。
- 格式轉置應建立標準作業程序與產出標準作業文件，以備日後查核及作業改善之依據。
- 轉置後之目的格式必須符合長期保存要求。
- 訂定轉置品質檢驗方式。
- 轉置工具名稱與版本、轉置參數、品質驗證結果及歷史版本資訊等轉置相關資訊應納入詮釋資料，應與轉置後檔案一併保存。

電子檔案轉置(續)

■ 轉置品質

- 任何形式的轉置都存在資訊流失的風險，因此須建立一個評量機制以確保轉置的品質。

□ 轉置品質評量方式

- 客觀準則：以計算轉置前後的量化指標來評估影像品質。
- 主觀準則：以人類肉眼的觀察來比較轉置前後影像品質。

電子公文檔案清理工具

電子公文檔案清理工具

■ 移轉（交）工具

- 將指定路徑之影像檔及目錄詮釋資料（附件七），依移轉（交）媒體封裝檔格式封裝處理，並附加機關憑證，產出移轉（交）電子媒體封裝檔。
- 後續將蒐集機關移交業務需求，評估批次修正分類號及加註附註項「典藏歷史註」欄位之需求。

■ 技術鑑定工具

- 批次檢核指定路徑之電子檔案封裝檔及其外部檔案，確認格式、簽章等資訊之正確性，可輸入抽樣條件，並自動產出技術鑑定報告。
- 現階段僅針對符合規定格式之封裝檔進行檢測及統計，後續將蒐集機關需求，擴充工具功能。

■ 瀏覽及檢測工具

- 單筆或批次檢測指定之電子檔案封裝及外部檔案，確認格式、簽章等資訊之正確性

電子檔案清理工具(續)



移轉（交）封裝作法

- ❑ 封裝時機：機關間電子檔案移轉或移交。
- ❑ 執行前須備妥機關憑證及下列資料：
 - 目錄詮釋資料檔案格式
 - ❑ 可依機關需求選擇採電子檔案詮釋資料格式或檔案目錄彙送格式(新版或舊版格式)之案件層級電子檔。
 - 設定目錄詮釋資料與影像檔對應規則
 - ❑ 依收文號或發文號
 - ❑ 依檔號
 - ❑ 依使用者自建之對照檔
- ❑ 封裝作法：
 - 進行目錄詮釋資料封裝。
 - 產出移轉（交）電子媒體封裝檔。
 - ❑ 計算本次移轉(交)所有儲存媒體中電子媒體封裝檔之雜湊值，再以機關憑證加簽處理，確保移轉(交)內容完整性。

移轉（交）封裝工具

電子公文檔案清理工具

移轉(交)工具

電子檔案檢測與瀏覽工具 電子檔案技術鑑定工具 檔案移轉(交)工具 關於本程式 回首頁

檔案封裝 | 檢視封裝紀錄檔 | 批次加入附註項 軟體使用說明

系統參數設定

檔案移出機關代碼 341020000A 儲存媒體容量大小 200 MB

檔案移出機關名稱 檔案管理局

紀錄檔路徑 C:\Documents and Settings\250221\桌面\990618 瀏覽

詮釋資料檔案型式 ☒ XML ☐ CSV

檔案詮釋資料與影像檔對應規則 ☒ 依收文號或發文號 ☐ 依檔號 ☐ 依使用者自建之對照表檔案(格式：收文號，影像檔路徑)

☒ 影像檔數量不一致時,是否一併進行封裝

詮釋資料格式 ☐ 附件四 ☐ 檔案目錄(案卷與案件整合) ☒ 檔案目錄(案卷與案件分離) ☐ 附表三

詮釋資料路徑(案卷) WHpsv8\檔案資訊組共用區\第1科\講義\電子檔案技術應用\安裝程式及資料 瀏覽

詮釋資料路徑(案件) WHpsv8\檔案資訊組共用區\第1科\講義\電子檔案技術應用\安裝程式及資料 瀏覽

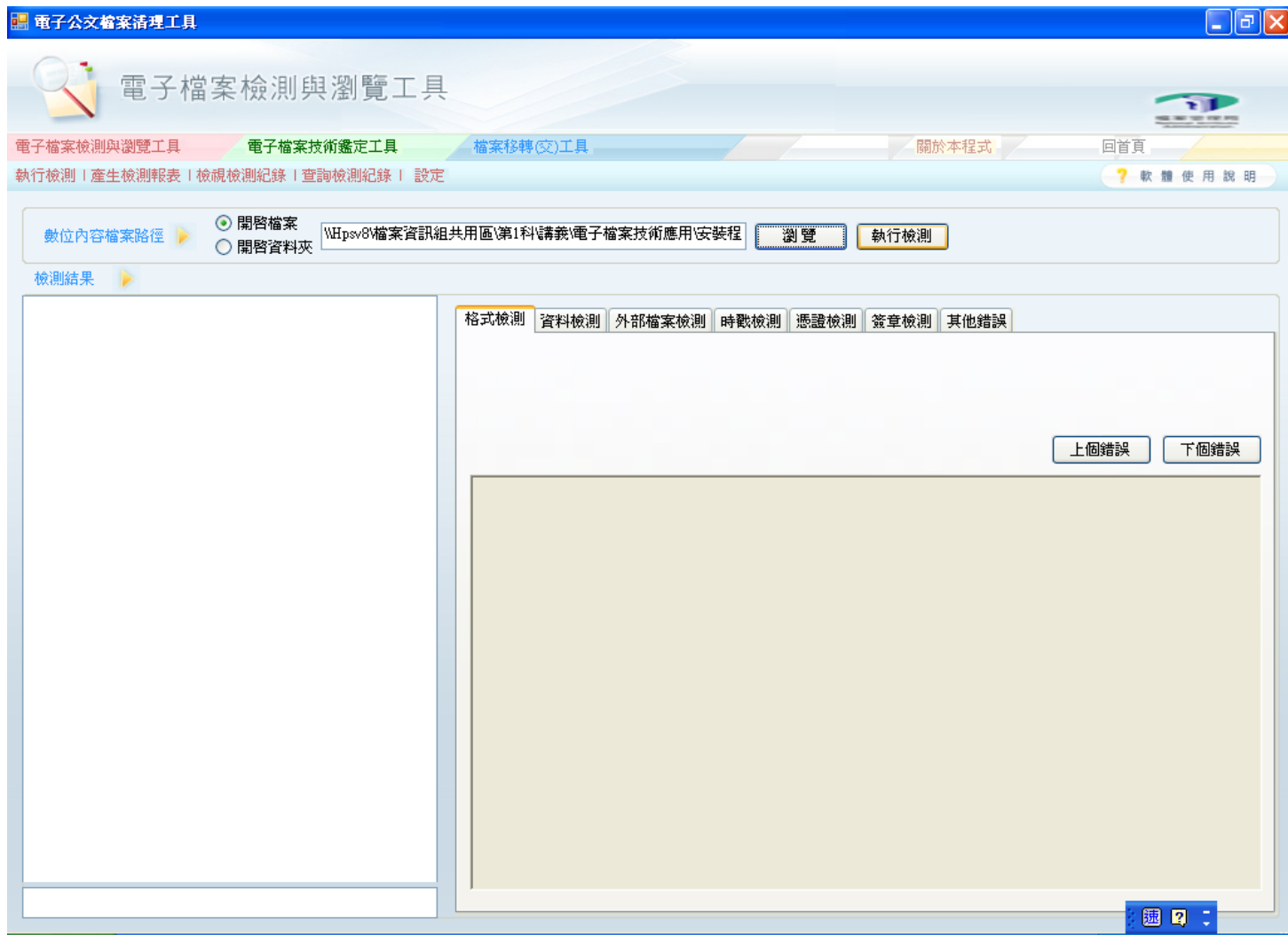
待封裝數位內容檔案路徑 WHpsv8\檔案資訊組共用區\第1科\講義\電子檔案技術應用\安裝程式及資料 瀏覽

封裝完成數位內容產出路徑 C:\Documents and Settings\250221\桌面\990618 瀏覽 執行封裝

封裝檔瀏覽與檢測

- 以離線工具瀏覽及檢測數位內容檔案
 - 格式檢測
 - 內容檢測（電子簽章、金鑰、憑證效期）
 - 外部檔案驗測（符合電子檔案格式表）
 - 簽章驗測（雜湊值驗算、驗章比對）
 - 產出檢測報表

封裝檔瀏覽與檢測（續）



封裝檔瀏覽與檢測（續）



封裝檔瀏覽與檢測（續）

電子公文檔案清理工具

電子檔案檢測與瀏覽工具

電子檔案檢測與瀏覽工具 | 電子檔案技術鑑定工具 | 檔案移轉(交)工具 | 關於本程式 | 回首頁

執行檢測 | 產生檢測報表 | 檢視檢測紀錄 | 查詢檢測紀錄 | 設定

軟體使用說明

數位內容檔案路徑 ☐ 開啟檔案 ☒ 開啟資料夾

\\Hpsv8\檔案資訊組共用區\第1科\講義\電子檔案技術應用\安裝程

瀏覽 執行檢測

檢測結果

0980008050-X.XML

格式檢測 資料檢測 外部檔案檢測 時戳檢測 憑證檢測 簽章檢測 其他錯誤

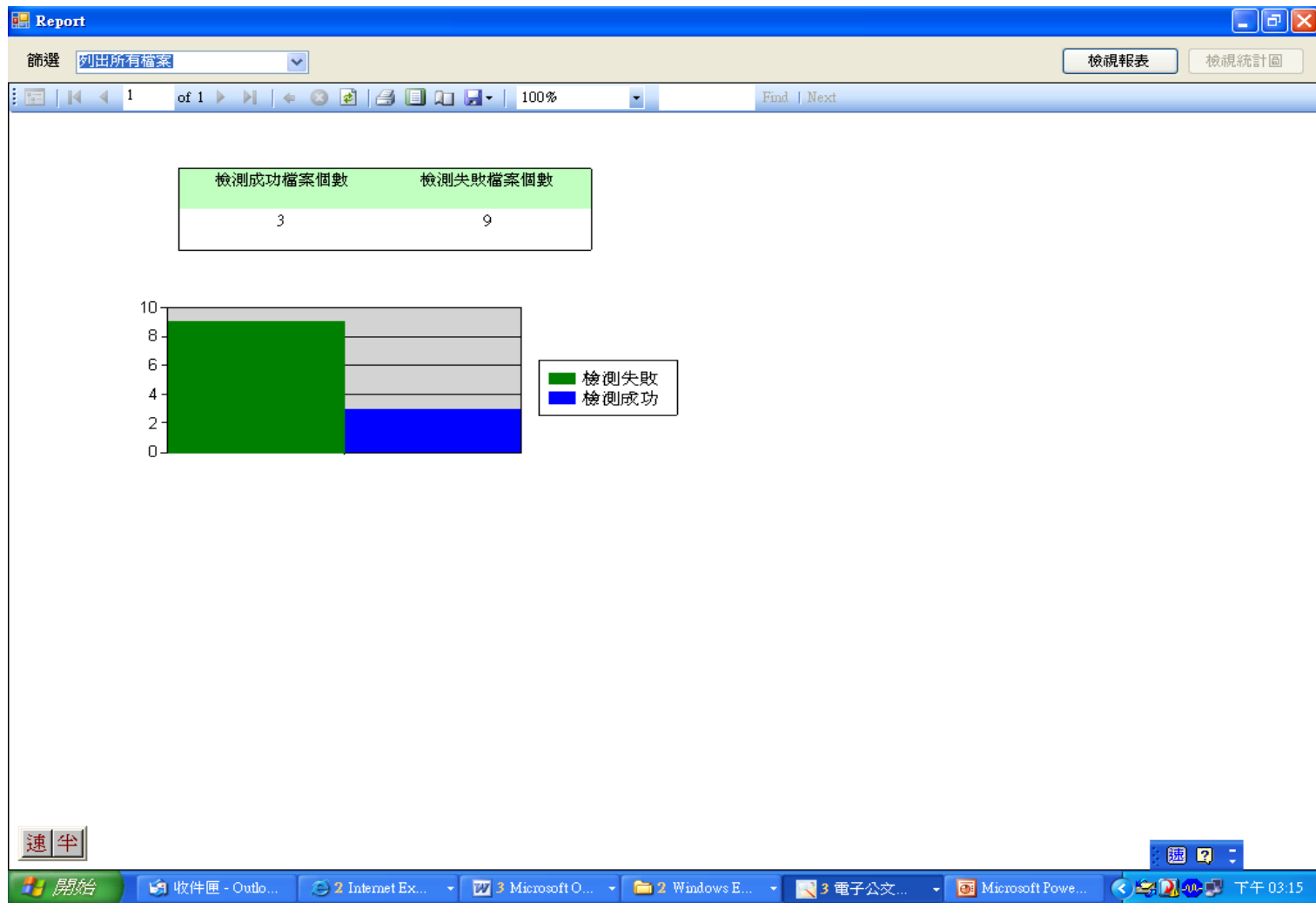
DTD驗證格式正確

上個錯誤 下個錯誤

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE 電子封裝檔 SYSTEM "附件三 DTD"[
  <!ENTITY % 基本標籤 SYSTEM "94_檔案基本標籤.ent">
  <!ENTITY % 交換用標籤 SYSTEM "94_檔案交換用標籤.ent">
  <!ENTITY % 內部用標籤 SYSTEM "94_檔管內部用標籤.ent">
]>
<電子封裝檔>
  <封裝檔內容 Id="Wrap">
    <封裝檔資訊>電子檔案</封裝檔資訊>
    <電子檔案>
      <線上簽核流程 Id="FlowInfo"><簽核流程 URI="#FLOW_106"/><簽核流程 URI="#FLOW_846489"/><簽核流程 URI="#FLOW_846491"/><簽核流程 URI="#FLOW_846492"/><簽核流程 URI="#FLOW_846493"/><簽核流程 URI="#FLOW_846494"/><簽核流程 URI="#FLOW_846495"/><簽核流程 URI="#FLOW_846496"/></線上簽核流程>
      <線上簽核資訊 Id="Sol"><簽核點定義 Id="FLOW_106"><Signature Id="ds_user_106">
        <SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
          </CanonicalizationMethod><SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></SignatureMethod>
          <Reference URI="0980008050-00-01V0003-t:xml"><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </DigestMethod><DigestValue>cnuQadBgicvqsBU7wvxzNGHUsN8</DigestValue></Reference>
          <Reference URI="0980008050-P-0001.TIF"><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            </DigestMethod><DigestValue>...</DigestValue></Reference>
        </SignedInfo></Signature></簽核點定義></線上簽核資訊>
    </電子檔案>
  </封裝檔內容>
</電子封裝檔>
```

速 半

封裝檔瀏覽與檢測（續）



範例2說明

■ 實作練習

□ 輸入資料

- 影像檔儲存路徑
- 案件詮釋資料

□ 輸出資料

- 移轉(交)電子媒體封裝檔

□ 檢測封裝結果

□ 操作步驟詳附錄

■ 目的

- 讓學員熟悉移轉(交)封裝工具操作方式
- 轉置後如何驗證轉置後結果

結語

結語

- 規劃電子檔案相關機制應注意事項：
 - 系統效能：雜湊值運算、加簽及檔案下載等。
 - 標準交換格式：檔案傳輸交換採標準格式，便利機關間檔案移轉（交）及電子檔案保管及維護。
 - 簽核時間：以伺服器主機為基準，定期校時，確保正確性及一致性。
- 電子檔案生命週期各階段均應注意資訊安全議題，應定期進行電子檔案備份作業，避免電子檔案遭竄改、破壞，或因人為操作不當等因素，造成電子檔案毀損或遺失。
- 開發電子檔案保存及清理共用元件、工具，協助解決機關電子檔案長期保存問題，避免工具重複開發人力及成本。

謝謝聆聽，敬請指教

檔案資訊諮詢服務中心

02-27751580#101

免付費網路電話

<https://online.archives.gov.tw>