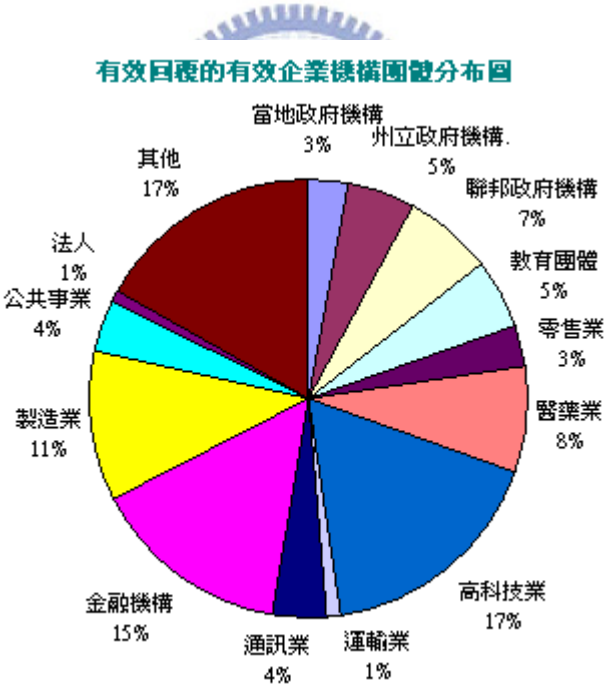
第一章 緒論

1.1 前言

根據電腦安全協會(CSI, Computer Security Institute)與位於芝加哥的美國聯邦調查局(FBI)連續八年對美國內部與資訊安全領域相關機構的調查，研究對象包含：企業、政府機關、財經機構、醫療機構與各公私立大學(見圖 1-1)，所發布的電腦犯罪與安全報告主要是以在電腦網路的犯罪頻繁性與其所帶來的損害程度為訴求。在其最新發表的 2003 年 CSI/FBI 電腦犯罪與安全報告[1]有些數據值得資訊安全研究者注意的。



（圖 1-1）受訪企業與機構的產業分布圖[1]

在 530 份有效的回收資料中，指出受非法攻擊的威脅並未減少。但值得注意的是這些非法攻擊的威脅程度與所花的成本卻是自 1999 年以來第一次減少的。這似乎意謂著，由於網路的普及導致獲取攻擊程式的便利性與病毒原始碼傳播容易很快就會有

變種病毒的產生，這是一個對資訊安全的危險信號。

另一方面，從防堵的技術性角度來看，在 1999 年到 2003 年間的資料明顯看出其變化。在侵入偵測的採用比率中，由 60%左右提升到 73%顯見外部的侵入層出不窮，導致為了能有效防堵非法入侵而被迫提昇網路的偵測使用的迫切性。而另一方面，在身份鑑別方面也有明顯的變化。數位身份認證的技術從 40%左右提昇至 49%，主要原因除了數位身份認證技術的成熟與基礎建設的輪廓逐漸健全外，另外一項關鍵就是美國在 2003 年 4 月 14 日公佈實施的醫療資料保密通知書(HIPPA, Health Insurance Portability and Accountability Act)對個人資料保密性的完整定義與其他相關的電子簽章法的頒布後，使數位身份認證廣受各單位採用，未來其使用的比率預期也將逐漸提高。而台灣也在 2002 年 4 月 1 日公佈實施電子簽章法提供使用者於使用電子文件與電子簽章的法律保護，目前民眾使用網路報稅與健保 IC 卡的使用上，個人資料也得以有法律的保護效用。

在其報告中，還有一項值得探討的項目的資料數據。很多資訊安全的從業者都有一種迷思，甚至欲套用 80/20 理論來使它的認知合理化，認為說只要防堵外部非法侵入的侵害就可以達到 80%的達成率。但其所做的調查(見表 1-1)卻讓人驚訝，沒想到竟然內部與外部的非法侵害的比率是相差不多。

發生的事件次數?

依百分比(%)	1~ 5%	6~ 10%	11~ 30%	31~ 60%	超過 60%	不知道
2003	38	20	多於 16%	0	0	26
2002	42	20	8	2	5	23
2001	33	24	5	1	5	31

2000	33	23	5	2	6	31
1999	34	22	7	2	5	29

2003 年共回覆 356 份 佔總比率 67%
2002 年共回覆 321 份 佔總比率 64%
2001 年共回覆 348 份 佔總比率 65%
2000 年共回覆 392 份 佔總比率 61%
1999 年共回覆 327 份 佔總比率 63%

有多少次數是遭受外部攻擊?

依百分比(%)	1~ 5%	6~ 10%	11~ 30%	31~ 60%	超過 60%	不知道
2003	46	10	13	0	0	31
2002	49	14	5	0	4	27
2001	41	14	3	1	3	39
2000	39	11	2	2	4	42
1999	43	8	5	1	3	39

2003 年共回覆 336 份 佔總比率 63%
2002 年共回覆 301 份 佔總比率 60%
2001 年共回覆 316 份 佔總比率 59%
2000 年共回覆 341 份 佔總比率 53%
1999 年共回覆 280 份 佔總比率 54%

有多少次數是遭受內部攻擊?

依百分比(%)	1~ 5%	6~ 10%	11~ 30%	31~ 60%	超過 60%	不知道
2003*	45	11	12	0	0	33
2002	42	13	6	2	1	35
2001	40	12	3	0	4	41
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35

2003 年共回覆 328 份 佔總比率 62%
2002 年共回覆 289 份 佔總比率 57%
2001 年共回覆 348 份 佔總比率 65%
2000 年共回覆 392 份 佔總比率 61%
1999 年共回覆 327 份 佔總比率 63%

（表 1-1）非法侵入總數與內部、外部非法侵入的調查比率[1]

因此，不僅要強化對外部非法入侵的防堵能力外，對內部的網路安全維護的使用

性、稽查人員訓練、高層配合制定資訊安全的法則與確實執行、人員教育訓練與使用權限控管…等等都是需要值得注意的事項。

1.2 研究動機及目的

為了要讓身份辨識於網際網路的使用上能作有效的控管，需要有一套機制可以用來解決電腦網路作業環境安全使用上的安全性問題，目前最為廣泛使用的方法為公開金鑰基礎架構（Public Key Infrastructure，以下簡稱 PKI）。

PKI 在網際網路的使用上滿足使用者身份鑑別性（Authentication）、資料完整性（Integrity）、不可否認性（Non Repudiation）與隱密性（Private）等資訊安全四大需求功能。對於政府提供便民服務的 e 化作業或企業所提供的電子商務及內部企業的網域使用者的身份識別等都是 PKI 的應用範圍。

為了維護 PKI 架構下的憑證安全性，目前較常被使用的其中方法之一為憑證中心(Certificate Authority， 以下簡稱 CA)所發佈的資訊內容，稱為憑證註銷清單(Certificate Revocation List， 以下簡稱 CRL)提供使用憑證在驗證上依據。而在目前實際運用上，仍然有些問題值得去探討。

在國內 CRL 相關的資訊並不多見，而能夠廣泛的將 CRL 的發佈機制與使用上差異性能夠整理詳細的文件更缺乏。因此，希望本論文能為學術探討 CRL 在 PKI 應用領域中能有所貢獻，並提出個人的觀點提供往後研究的方向為撰寫本論文的動機與目的。

1.3 論文架構

本論文主要希望在PKI與其CRL的原理與相關機制介紹，並藉由所收集到的資料將CRL的發佈機制逐項探討並與比較其差異性。最後藉由所探討的研究方向之文件資料中，提出一些個人觀點與可行的方法提供往後研究參考。

另一方面，在實際PKI與CRL的憑證運用與驗證的架構，本論文的論文範例所使用的作業平台為微軟的伺服器2003企業版本，而其相關的介紹會詳載於本論文附錄中。

本論文共分六章：

第一章 緒論，描述前言、研究動機、目的與論文架構。

第二章 介紹PKI相關的背景，如憑證格式簡介、建置PKI的基本需求、憑證申請流程的介紹、建置PKI架構的優缺點與CRL相關的評估標準。

第三章 介紹CRL的相關資料，如CRL與PKI的關係、憑證註銷相關機制簡介、CRL格式簡介與運作的原理。

第四章 探討CRL的各種定期發行機制與各種機制特性之比較。

第五章 如何使用P2P實現CRL的發行機制的架構與實際設計時，運用JXTA為開發平台的運作方式。

第六章 結論與未來相關的研究方向。

第二章公開金鑰基礎架構的簡介

公開金鑰(Public Key)為一組電腦數字，經CA認證後，置於所發給的電子憑證內，可供使用者作為驗證私密金鑰的憑據。公開金鑰也可運作於多個異質應用系統，且很可以容易地使用單一簽入程序, 安全的取得存取權限與資源。如運用於企業，可對內部與外部使用者做到有效的安全控管與身分認證的安全性,減少企業受外部侵害的機會與避免安全出現漏洞的危機，這所有的運作基礎會是在PKI系統中。

PKI 包含了憑證伺服器所具備的憑證管理能力（發行、撤銷、儲存、收回、以及信任憑證的能力)，並提供憑證儲存備份的功能。 PKI 的主要特色在於 CA 是由一個人類實體 — 一個個人、團體、部門、公司、或任何協會 — 認可後發行使用者的電腦使用憑證，CA 所扮演的角色就如同國家政府機關的身分證管理最高機關。 CA 建立憑證後,使用 CA 的私鑰對其進行數位簽署。因為它們的角色是建立憑證,故 CA 也就成了 PKI 的核心組成元件。藉由使用者的公鑰，任何人想要驗證憑證授權其實就是在驗證 CA 發行的數位簽章、憑證持有者的公鑰和其身份與憑證內容的完整性。

PKI 的主要運作方式是以公鑰密碼學為基礎衍生出來的架構，其基本的四項功能建置元件包含 CA、憑證註冊中心（Register Authority, 以下簡稱 RA)、目錄服務（Directory Service , 以下簡稱 DS）伺服器與憑證主體。由 RA 統籌、審核用戶的憑證申請，將憑證申請送至 CA 處理後發出憑證，並將憑證公告至 DS 中。在使用憑證的過程中,除了對憑證的信任關係與憑證本身的正確性做檢查外，並透過 CRL 對憑證的狀態做確認檢查，了解憑證是否因某種原因而被註銷。憑證

就像是個人的身分證，其內容包括憑證序號、用戶名稱、公開金鑰、憑證有效期限等。相關的細節會在以下章節作說明。

目前 PKI 是由網際網路工程技術小組(Internet Engineering Task Force，以下簡稱 IETF)所制定的 X.509 標準，其主要的內容是定義出一套憑證的初期規格制定與作業模式使其依照 X.509 所產生的 PKI 機制適合在網際網路上運作。

2.1 公開金鑰基礎架構的的功能性

PKI 可提供符合維護資訊安全的四項目標：機密性、完整性、可用性與不可否認性。這些要點簡單敘述就是能確保使用者在使用電腦時，能為你保密、保存正確的資訊、隨時可為你提供服務與紀錄你在交易上的狀況。而對於 PKI 而言，是以公開金鑰密碼技術為基礎所衍生的架構，在電子訊息傳遞與交換過程中，提供訊息的身份識別（Authentication）、資料完整（Integrity）、不可否認性（Non Repudiation）與隱密性（Private）等資訊安全四大需求功能。以下以 PKI 應用面細節作說明：

1. 機密性：交易雙方可確認交易傳送方的身分，避免被冒名傳送假資料。
2. 完整性：交易雙方透過數位簽章之驗證可確保交易資料的完整性，避免被竄改。
3. 可用性：交易資料會使用金鑰予以加密，隨時提供資料保密安全功效。
4. 不可否認性：交易資料加蓋傳送方之數位簽章，具有法律效力，經接收方查驗確認後，即無法否認發送此交易的事實，可保障交易雙方，避免發生交易糾紛。

公開金鑰的功能定義說明：

- 註冊

一種流程，當憑證使用者將持有的憑證讓CA可以辨認。此部份如果CA具有RA的功能，可以經由RA執行或是直接由CA執行。憑證持有者的名稱與其他屬性需由CA作業程序中的憑證實作準則可作為認證之確認。

- 憑證

當CA為一個公開金鑰申請對象核發一個憑證並傳回憑證給憑證申請者或發佈憑證到資料庫內。

- 跨認證中心的認證

當一個憑證由一個CA所核發，憑證驗證也可以到另一個CA去認證其公有與私有金鑰組合只要原核發認證的CA與認證CA彼此建立信賴關係即可。

- 憑證註銷

CA負責維護憑證狀態的相關資訊，包含憑證的無效與過期使用時間的註銷。在X.509 V2的憑證註銷清單的功能中，已提供一種機制可以傳達憑證註銷狀態相關的訊息。當憑證被註銷後，只需將訊息加到下一次所發行的CRL中即可完成。另外，還有一種方式也可使用來作憑證註銷用途。CA可使用線上憑證公告機制，例如使用線上憑證狀態通訊協定去減少CA的憑證註銷與發行註銷公告給憑證持有者之間的時間上延遲因素。此機制並不像CRL發行機制，憑證持有者須使用線上方式與線上服務提供者見作為憑證確認。

- 憑證與註銷公告的分佈與發行

PKI提供發佈憑證與憑證註銷公告的工作。而當憑證持有者或使用者在完成註冊程序後，也可自行下載憑證。另外還有一種方式為資料庫服務方式。例如：簡易資料通訊協定可提供一般的目錄服務作為使用來提供憑證發行機制。憑證註銷資訊或者公告可分散發行一份憑證註銷清單到簡易資料通訊協定的目錄服務，然後發出一份聲明書給憑證使用者或提供線上存取服務讓憑證使用者去搜尋資料。憑證註銷清單也可以很彈性的定時發行或不定時發行到簡易資料通訊協定目錄中。

2.2 公開金鑰基礎架構的應用面

PKI 為了讓使用者存取權限控管機制，能提供安全的交易環境與保護重要的電子資料，防止交易雙方事後否認交易，所需的相關應用包含:

- 密碼系統 : 公開金鑰密碼系統、秘密金鑰密碼系統、雜湊法數值運算
- 安全機制 : 認證性、機密性、訊息完整性、不可否認性、存取管制
- 憑證的管理 : 核發、展期、終止、變更、查詢與驗證
- 標準的確立 : 憑證、簽章、保密, 如:ITU-T X.509, PKCS, LDAP 運作
- 可信賴體系的建立 : 階層式或網路式的認證架構
- 電子憑證 : 數位簽章、數位憑證

電子憑證又稱電子印鑑證明，全名為公開金鑰電子憑證，其內容包括：憑證序號、客戶代號或名稱、公開金鑰、憑證有效期限、認證機構單位名稱及認證機構之數位簽章等。認證機構驗證客戶之身分與其公開金鑰後，發給電子憑證作為其公開金鑰的有

效證明依據。電子憑證內容包含金鑰擁有者之基本資料及公開金鑰，並以 CA 之數位簽章保護、防止偽造及竄改資料，詳細部份會在下一章節作詳細說明。

數位簽章類似手寫簽名或蓋章，係以非對稱性之金鑰對演算法來達成，經由電腦程式將私密金鑰（電子印章）及將原網路交易訊息濃縮成訊息摘要予以運算，即可得出數位簽章，表示甲同意進行此網路交易。甲將數位簽章併同原交易訊息傳送給交易對方乙，乙可用以驗證該訊息確實由甲傳送，非由冒牌者傳送出。乙也可據此查驗交易訊息於傳輸過程是否遭竄改。若經乙查驗正確，則甲無法否認曾經傳送此訊息。換句話說，數位簽章賦予電子通訊之安全性，而提供如同書面文件簽名的法律效力。

2.3 公開金鑰憑證的相關標準簡介

PKI 可以想像成標準的書面憑證附加上一把公鑰，上面有你的名字和一些關於你的資訊，然後加上這份憑證發行者的簽署。

一 X.509 公開金鑰憑證

X.509 公開金鑰憑證目前為止總共定義了 3 個版本：

最初版本的公開金鑰憑證規格是在 1988 年建議制定的，但因為此版並無法擴充額外的屬性而導致內部運作的彈性化不足而反應不佳;而下一版本的公開金鑰憑證規格則修正了前版的缺失，最只要是在令人爭議的兩個非必須的部分。因為這些的需求性並非可以被忽略的而且也不如擴充欄所提供的支援來的好，因此公開金鑰憑證版本 2 還是沒有被外界所廣泛接受。

直到公開金鑰憑證版本 3 於 1997 年 X.509 建議書[X509-97]，解決了在前兩個版本所定義的缺乏部分。更特別的是，版本 3 比前兩個版本提供更顯著的改善於增加額外的擴充欄功能。

最近最新的版本為 2000 年版，大約是在 2000 年 6 月的時候發表版本建議書為[X509-00]。此版比前一版做了不少改變，包含了對第三版本的公開金鑰憑證多加了兩個額外的擴充欄。而對企業的使用而言可開始採用，因為此版本已接近實際應用面用途的規格，使用時可彈性化的運用以及提供了許多擴充欄，企業可以視實際需要判斷支援與否。

X.509 憑證完全是由 ITU-T X.509 國際標準而來的。所以，X.509 憑證可以適

用於任何相容 X.509 的程式。但實際上，不同的公司所創造了的 X.509 延伸欄位會造成憑證內容並無法相容，所以有時會因個別的因素而無法放在一起運作。

X.509 之公開金鑰基礎建設(Public Key Infrastructure X.509，以下簡稱 PKIX)也由 IETF 在安全領域方面，正進行標準訂定之工作，制定 PKIX 建議的 X.509 標準。其主要是以一個階層式的結構性公開金鑰基礎架構，由樹狀結構以根憑證授權的方式展開其憑證延伸的支點。在此結構下，信任的核心是以根為中心，然後透過 CA 依階層式的概念對使用者授權的方式，構築成形成一個樹狀網路。比較特殊的是根憑證授權的公開金鑰可以獲知所有在樹狀網路中的使用者，也可依樹狀網路的信賴路徑知道其他憑證公開金鑰的信賴關係。因此，可說是此份金鑰是可以被其他持有人知道它的存在。

－ 隱私權保護 (Pretty Good Privacy, PGP) 憑證

由於現今網路已經邁向商業上的應用，網路資訊的安全與維護是當前重要的課題，而 PGP 是可以讓電子郵件或檔案具有保密功能的程式，提供了強大的保護功能，即使是最先進的解碼分析技術也無法解讀，因此可以將檔案加密後再傳送給他人，加密後的訊息看起來是一堆無意義的亂碼，除了擁有解密金鑰的人看得到以外，沒有其它人可以解讀。隱私權保護憑證是利用所謂的公開金鑰密碼學為基礎，其原理是利用 PGP 憑證產生一對鑰匙而另一把是私人金鑰，一把是公開金鑰。當要傳送一封保密信或檔案給對方時，首先必須先取得對方的公開金鑰，並將加入自己的公開金鑰環中，接下來利用對方的公開金鑰將信件加密後再傳送給對方。當對方收到加密的信件後，

對方必須利用其相對的私人金鑰來解密。PGP 也有提供隱私權保護憑證專屬簽名，其目的通常是當要公開傳送訊息時，希望讓別人知道這訊息確實是由你所發出，一旦加入此專屬簽名後，任何人只要更改訊息本身或簽名的話，隱私權保護憑證都能偵測出此篇文章已被他人所更動，並非是原作者之文章。PGP 安全電子郵件採用就是一種 PGP 獨有的憑證。

一份 PGP 憑證大概可分為下列資訊：

- PGP 版本號碼：用來辨識與憑證相關的金鑰是由哪一個版本的 PGP 所產生的。
- 憑證持有者的公鑰：你的金鑰對公開部分以及這把金鑰所採用的演算法： RSA 、DH (Diffie-Hellman) 、或 DSA (Digital Signature Algorithm) 。
- 憑證持有者的資訊 — 由使用者相關的「身份」資訊組成，像是名字、使用者 ID 、照片等。
- 憑證持有者的數位簽章：這也被稱為自行簽發，也就是拿簽發憑證的金鑰對裡的私鑰直接對其公鑰加簽。
- 憑證有效期限：憑證的啟用日期／時間和到期日期／時間；用以指出這個憑證何時會過期。
- 這把金鑰偏好的非對稱性加密演算法：指出這個憑證持有者所偏好的資訊加密演算法。可用的演算法有 CAST 、 IDEA 、或 Triple-DES 。

PGP 可由個人或私人單位所發出的，並不像 X.509/PKIX 的憑證由專業的認證中心發出。任何人可以決定要信賴的對象。因此，應用一種機制稱為信賴網(Web of

Trust)可讓發行者並不需要指定保護措施與擁有專業技術，就可以使用 PGP 憑證達到對機密性的錯誤相容功能。在信賴網中許多金鑰持有人可核發內含公開金鑰的使用者鑑別碼的憑證，就可以證實其憑證之正當性。這種假設是針對各自獨立的不同金鑰持有者，假設其中有使用者做出錯誤的決定其他人也不會受到影響。驗證憑證的信賴程度需運用到 PGP 憑證的獨立簽章號碼。

一 簡易式公開金鑰基礎架構憑證(Simple Public Key Infrastructure certificates，以下簡稱 SPKI)

如同隱私權保護憑證一樣，SPKI 倡導廣泛簽發憑證而不需受制於核心為認證中心的架構。但它也有像 X.509 類似的憑證鏈結而不是像 PGP 憑證的信賴網。因為 SPKI 定義了一個 k-of-n 的物件可將包含金鑰與使用者名稱資料的 n 個物件清單結合在 k 與 n 的數值關係，如此驗證的工作就只需在此憑證與其最後結果之間的 k 個完整路徑就可完成，由憑證發行者依何種程度的錯誤容忍度來決定 k 與 n 的值。

在 X.509 憑證和 PGP 憑證間有許多差異，其中較顯著的項目列出如下：

- 一份驗證需要某人來使一把公鑰和金鑰主人的名字一起生效。在 PGP 憑證下，任何人都可以擔任驗證者的角色；而在 X.509 憑證下，驗證者永遠都是 CA 或由具信賴關係的 CA， PGP 憑證也同樣完全支援權力體系架構下的 CA 來驗證憑證。
- 你可以建立你自己的 PGP 憑證；但是 X.509 憑證卻只能經由申請的手續，由 CA
- 發行。
- X.509 憑證只能接受金鑰持有者使用單一名字。
- X.509 憑證只能接受單一的數位簽章來證明金鑰的有效性。

憑證的種類	憑證授權的特性	鑑別的種類
X.509	階層式授權 憑證交互簽發 憑證實作準則	全面性由初始時就定義好但內部使用則還在使用中[X.500 辨別名稱,由簽發憑證的認證中心所指定
PGP	信賴網 = 憑證可以有不同的來源，為了要有容錯機制來補強其非專業憑證簽發憑證的不足性	全面性 ［依賴電子郵件名稱，且是全是唯一性
SPKI	單獨用命名作授權 不需憑證實作準則	局部性 ［可隨意使用］
非命名方式 SPKI	層級式的委任授權 選擇性的 k-of-n 方式	全面性[公開金鑰或是以用雜湊法家密的公開金鑰 且金鑰完全是獨一無二的

(表 2-1)憑證類型的比較表[2]

2.4 建置公開金鑰基礎架構的基本需求

PKI是一種已獲國際所廣泛接受的資訊安全技術。這種技術在北美和歐洲的應用已經相當普及，但在亞洲地區則是近幾年才開始發展。而在企業內部要建置PKI，首先必需成立發行與管理憑證與金鑰的單位，同時也必須要制定相關的憑證和金鑰與CRL如何發行與管理的措施。下一步驟則是對內部人員提供教育訓練以及依現有組織架構發行員工憑證，然後依初步實施的成果作探討與改進後，制定出屬於自己企業內部公開金鑰的實施準則。而這些循序步驟需要有一些元件與服務來實現。

PKI提供的元件與服務必須要能夠符合使用者憑證特別的部署機制與系統作業要求。以下的幾項問題為PKI必須滿足：

- 產生合法金鑰的程序作業需無安全性問題
- 需對欲使用憑證之申請者身份作到身份完整確認的作業程序
- 需提供發給、更新與終止憑證服務的機制
- 對憑證合法性能提供驗證作業
- 憑證的分發需要結合使用者資訊一併處理
- 需提供金鑰保存的機密性與回覆的相關作業程序
- 數位簽章的產生機制與時戳服務
- 建立與管理信賴機制

對於憑證管理的政策需注意的事項如以下所列項目：

- 憑證發給、憑證更新與復原舊的憑證，而組成憑證的實質要素有應用程式，裝

置設備、系統與使用者所組成。

- 憑證分發可供使用者彼此利用數位簽章交換訊息
- 憑證註銷可取消先前所核發的憑證，原因可能為密碼被破解或是超過憑證使用期限。憑證註銷主要由 CRL 或是線上憑證狀態協定，或者類似的機制來完成的。
- 憑證暫時停用是將憑證暫時失效無法使用，可能是使用者遺失憑證所採取的暫時措施。
- 加密金鑰的託管與恢復提供加密金鑰因損毀、過期或遺失後仍然能取回或是復原。
- 不可否認性可藉由數位簽章所提供的技術讓參與的交易者行為有具高信賴的證據得以驗證其行為。
- 時間戳記提供一個官方所紀錄的所有交易時間，可證明事件發生的日期與時間。

2.5 憑證申請流程

PKI 包含公開金鑰與私密金鑰的密碼技術，建置一個具效率性、完整性與資料秘密傳輸的系統，可供信賴機構不需具備過多的技術與知識背景就可相互的進行資料交換。也就是說，此方式可讓信賴機構消除個別單位於處理公開金鑰與私密金鑰的密碼技術所可能帶來的缺失。

因此，PKI可以使用在各式繳費系統上，業者與消費者因為PKI提供的交易安全機制，可以獲得互信互利的交易環境。對於網路上的各式交易與電子商務(B2C或B2B)，PKI是不可或缺的重要環節。藉由PKI的機制，確保每一次交易的有效性。除了最基本的資料傳輸安全之外，利用電子數位簽章相關的功能（資料身份識別)，來確保交易雙方的「交易資料完整性」及「交易不可否認性」，對於交易雙方都是一項保障。除了電子商務的應用之外，公司內部的文件與流程，也可以利用PKI來達成分層負責的效用。有了PKI的安全機制，可提供更有保障的作法。利用電子數位簽章，保密性與資料的確認將更具公信力。

PKI可提供很重要的信賴性、機密性與完整性的需求；但必須在公開金鑰與私密金鑰並非被非授權使用的狀況下才有效。

在公開金鑰的架構下，有以下幾個基本元件：

- 認證中心(CA)：

負責確認公開金鑰與確認憑證持有使用者的符合性。CA 管理憑證產生的流程包括憑證的發給與註銷，扮演角色如同憑證的第三者信賴機構。CA 也有屬於它自己的憑證，

此憑證是由其所信賴上層 CA 所發給的數位簽章，使用此數位簽章憑證就可發給所有欲使用其服務之對象。然而，使用者對 CA 的信賴度是不需要任何證明文件的，就好比民眾對信賴政府機關的信賴一般。而這些少數的根 CA 是 PKI 所定義與形成的基本信賴階級制度。

- 憑證註冊中心(RA)：

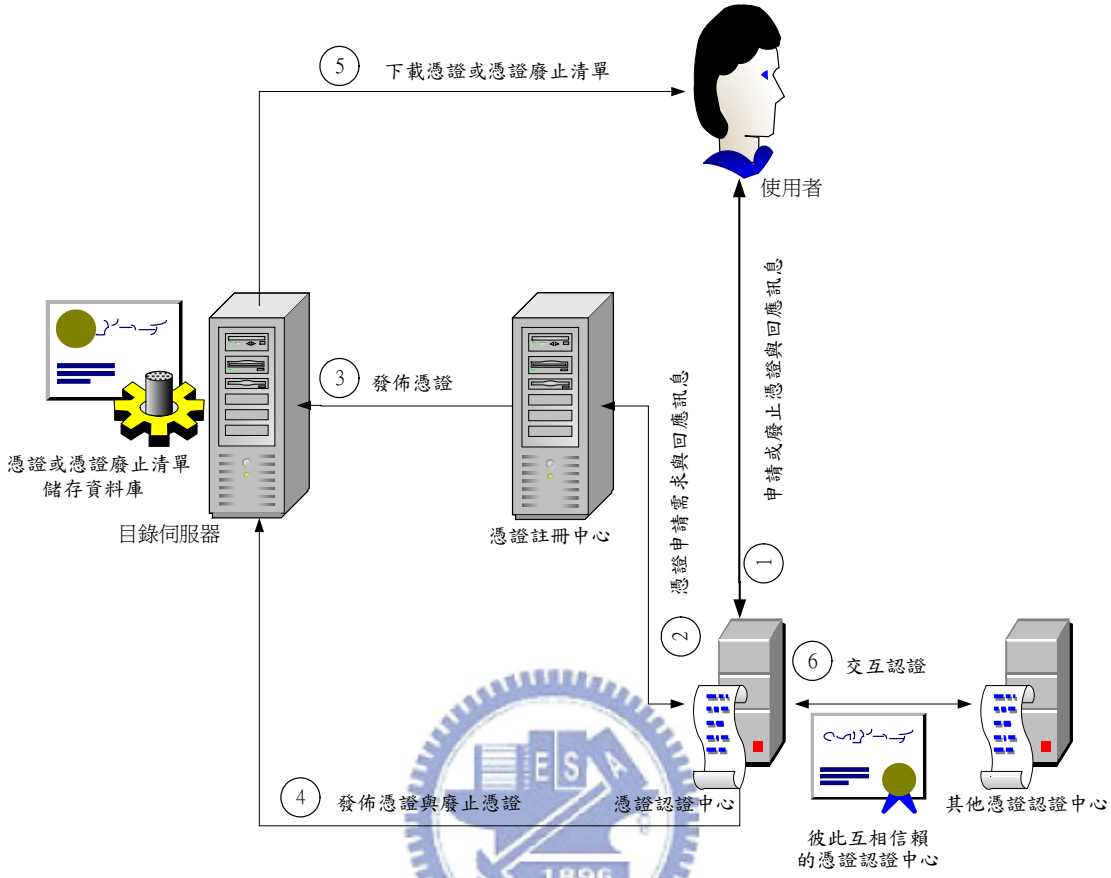
當使用者向CA提出申請數位簽章，CA需驗證此申請人真實身份的真確性，而RA則負責驗證工作。在真實世界中，有點像是公證人的角色當合法契約簽定時需要有人可以當見證人。由RA驗證過程的嚴謹度會影響此數位簽章的公信度。在將資料送CA之前，有些PKI還需要公證人扮演註冊授權的角色，而且也要在相關文件中共同簽名以聲明其見證人的有效性。而其他申請手續較不嚴謹之PKI服務提供者，則可能只需一份電子郵件位址與憑證能相互連結即可完成。簡言之，PKI提供了多層式的信賴性憑證，但最後始終還是依需求性來決定其使用方式。

- 使用者：使用公開金鑰的憑證使用者，或是系統及使用者擁有公開金鑰的憑證的實體。

- 目錄伺服器：負責儲存憑證與CRL的資料庫系統與提供憑證及CRL公佈機制給憑證使用者。

CA設立需求目的之一是為了要滿足PKI 所訂定的各種標準簽章演算法，產生並驗證PKI 所簽發的憑證資料，進而將認證資訊存於目錄伺服器供往後交易需求所使用。為能更清楚認識CA 在PKI 下的流程運作，我們以憑證交易與驗證流程(圖2-1) 描述

其運作方式。



(圖2-1)現行CA憑證之發佈及交易驗證流程[23]

流程概述如下：

1. 憑證申請或註銷：使用者向RA或直接向CA申請憑證，並等待回應，若使用者因故

2. 要註銷憑證，也可透過此管道進行。

3. 憑證審核及回應：RA受理交易端所提出的憑證申請後，將相關資料送至CA進行審

核，CA審核後再將結果回應給RA。

4. 憑證發佈：使用者申請憑證獲核准後，RA或CA會將憑證放置目錄伺服器上。

5. 註銷憑證發佈：CA定期向目錄伺服器發佈最新的CRL。

6. 下載憑證或CRL：使用者因交易需求等因素，需到目錄伺服器下載交易對象憑證或

CA定期發佈最新的CRL。

7. 交互認證：其他CA可向原發憑證的CA進行相互認證，只要CA之間能夠建立信賴關係即可。

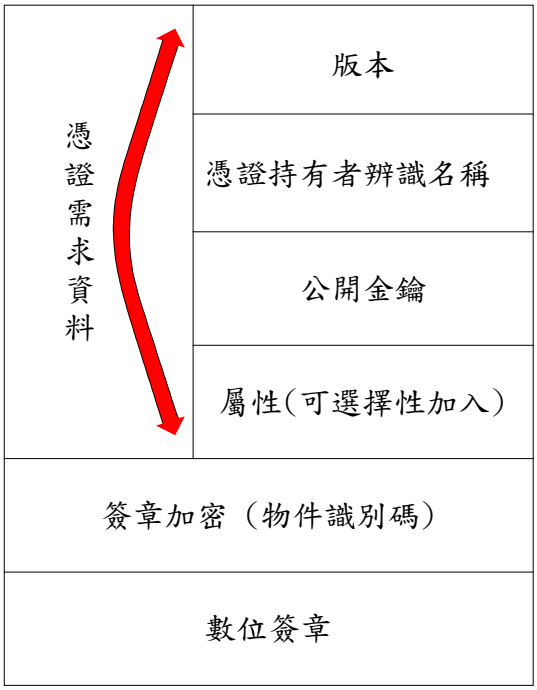
2.6 PKI通訊管理協定

PKI通訊管理協定主要是CAs要蒐集簽發憑證與CRLs的資訊時，需透過此協定建立具信賴性與安全性的資料傳輸協定。管理協定主要可分兩種基本型態分別為憑證需求與註銷需求。憑證需求指基本的憑證需求、初始憑證需求與CA憑證需求；註銷需求是基本的註銷需求與額外的憑證註銷需求。

談及PKI傳輸管理協定，首先需先介紹公開金鑰加密標準(Public Key Cryptography Standard，以下簡稱PKCS），PKCS是由提供機密安全解決方案著名的研究密碼學公司－ RSA Security[14]所提出的各種業界規格，而與本章節PKI相關的傳輸管理協定為PKCS #7訊息加密語法與PKCS#10憑證需求語法。以下除了介紹此兩種通訊協定，也對另外由此兩種所衍生的通訊協定作說明。

常使用的五種PKI傳輸管理協定：

1. PKCS#10基本上是由IETF的改善信件隱密性(Privacy-Enhanced Mail)的標準所演進而來的。主要是作為憑證需求標準語法，目前也是最常使用的PKI管理協定，使用上通常會與SSL或PKCS#7一併使用，成為訊息加密的主要訊息標準格式。



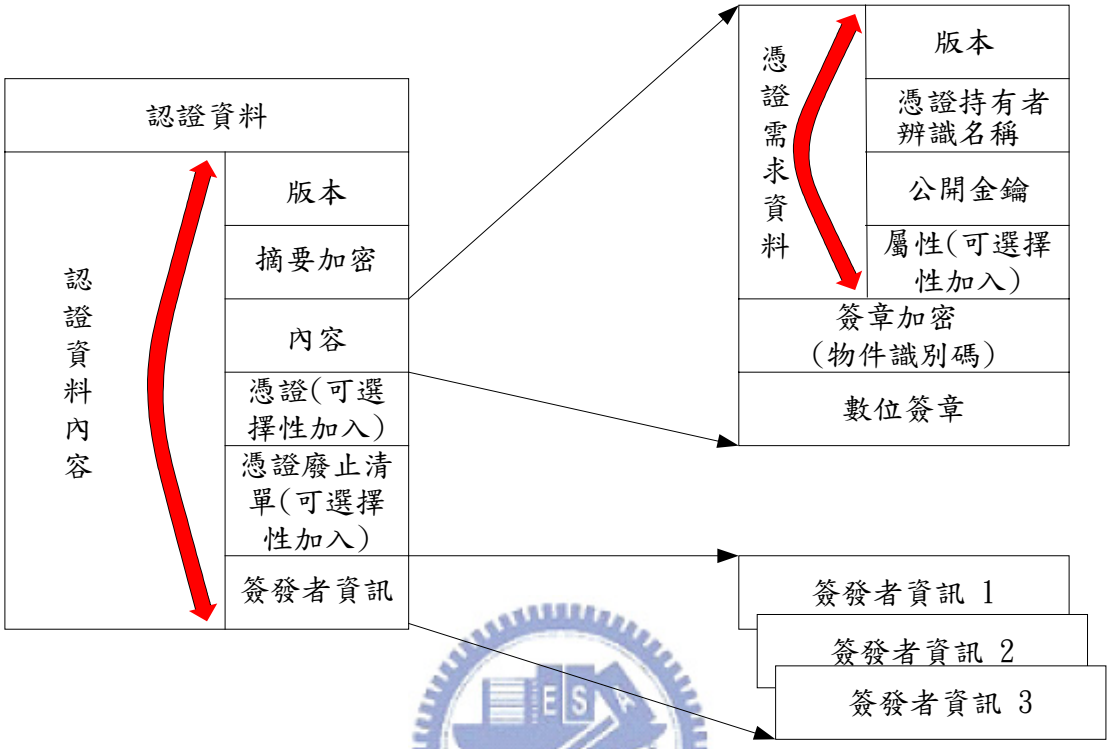
（圖2-2）PKCS#10訊息格式[8]

PKCS#10所定義的憑證需求訊息格式(圖2-2)，包含DN、公開金鑰、可選擇性加入的屬性欄、加密法物件識別碼與數位簽章。選擇性的屬性欄主要是為了提供給CA此憑證的額外訊息如電子信箱住址與建立驗證密碼給其後的憑證註銷需求使用。而此憑證需求是由憑證持有者使用相對應的私鑰產生。簽章則是為顯示私鑰所有者的身份。

2. PKCS#7是一種使用加密保護的訊息標準規格，同時也是許多通訊協定的建立基礎。標準的PKCS#7訊息格式有兩個部份：第一部份為內容型態；另一部份為內容主體。內容型態主要定義出PKCS#7不同的內容型態分別為資料、認證資料、附加資料、認證與附加資料、摘要資料與加密資料等六項內容型態。而此內容型態可以由物件識別碼來指定，並且也定義其內容的格式。

一般而言，PKI實際應用主要是使用認證資料訊息格式。內容如下圖所示，包含

了版本、使用來產生數位簽章的密法學、內容主體、憑證、CRLs與憑證簽發者資訊，而憑證與CRLs資料欄位是可以選擇性加入。



（圖 2-3）PKCS #7 簽發者資料內含一份PKCS #10的憑證需求[8]

憑證簽發者的資訊是由PKCS#7訊息格式(圖2-4)所描述，其包含版本、簽發者與憑證屬性序號做為公開金鑰數位簽帳驗證時使用、授權屬性、數位簽章加密的說明、數位簽章主體與未授權屬性，授權屬性與未授權屬性等資料欄位都是可以選擇性加入的。此數位簽章用來產生認證資料內容與簽發者資訊的授權屬性內容。而對每位簽發者提供的內容可以有不同的授權屬性。

版本
簽發者與序號
摘要加密
授權屬性(可選擇性加入)
加密摘要說明(數位簽章)
非授權屬性(可選擇性加入)

(圖2-4)PKCS #7 簽發者資訊結構[8]

一般而言，大多建議PKCS#7與PKCS#10同時使用，主要是因為兩者的結合可以得到以下四種優點：

— PKCS#7內含PKCS#10可以利用私鑰成為訊息加密的依據，這允許憑證使用者使用目前的簽章金鑰來簽發所提出之需求或是由RA使用其私鑰來簽發所提出之需求。

— CA可以使用PKCS#7做為鑑定憑證訊息將結果傳回給提出驗證需求的使用者，可使客戶端或是RA可以得知此憑證已經被簽發出去。

— PKCS#7也可以被使用作為CA回應訊息給提出需求者。當憑證被簽發後，CA可以使用認證資料訊息來回覆此新的憑證需求者，也可結合PKCS#10併用為一份完整的傳輸順序送出。

— CA可將原有的PKCS#7訊息驗證裡內含PKCS#10憑證需求做為檔案儲存用途，給使用者保留所簽發的PKCS#7回應訊息。每位使用者可擁有一份CA所簽發訊息保存作為往後的證明文件。

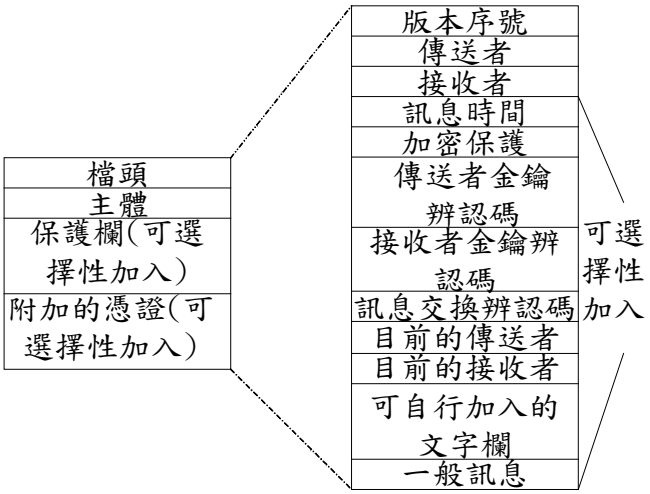
3. 憑證管理協定(Certificate Management Protocol，以下簡稱CMP)

當IETF PKIX工作小組準備開始開發給PKI管理使用的通訊協定時，就已經決定要保留PKCS#7與PKCS#10此兩種通訊協定，但由於此兩種在前面有提及是屬於RSA公司所開發的，故版權與相關文件的修定均是由RSA公司所負責，IETF並無權作任何修改。也因為如此，此工作小組就開發可以廣泛被使用作為RA的參與者與應用單一加密手續可供身份確認的通訊協定，來補強PKCS#7與PKCS#10的不足之處，因此就開發出CMP。

CMP初始是由RFC2510的憑證管理協定與RFC2511的憑證需求管理架構所結合產生的，而且兩者均同時在1999年獲得認定採用。CMP的訊息格式(圖2-5)可區分為檔頭、主體、保護與附加憑證等四部份，除了保護與附加憑證外，檔頭與主體是必須有資料存在。在保護的部份主要是用來維護檔頭與主體的資料完整性，避免遭受竄改。所傳送的部份包含一份數位簽章與訊息授權碼或是雜湊運算處理過後的訊息授權碼。

檔頭的部份如下圖所示，含有版本序號、傳送者、接收者而其他的部份如訊息時間與用來保護訊息的加密演算法…等等，都是可選擇性加入的資料欄位。

訊息主體部份是用來決定訊息型態，總共有24種可供選擇。常用的有憑證需求與回應訊息、跨CA憑證認證的需求與回應訊息、憑證註銷與回應訊息、金鑰回覆需求與回應訊息、金鑰擁所者驗證與回應訊息、憑證與CRL發放訊息與其他訊息確認與錯誤訊息回應訊息等。



（圖2-5）CMP訊息結構[8][25]

4. Certificate Management Using CMS(CMC)

隨著IETF PKIX工作小組的茁壯與廣泛被接受後，對之前的CMP通訊協定所定義的訊息交換有著多量訊息傳送與CMP需求端的訊息傳送不具效率性問題。另一方面又為了擺脫PKCS#7與PKCS#10遭RSA公司的束縛，故設計此CMC做為簡化其複雜處理過程的通訊協定。

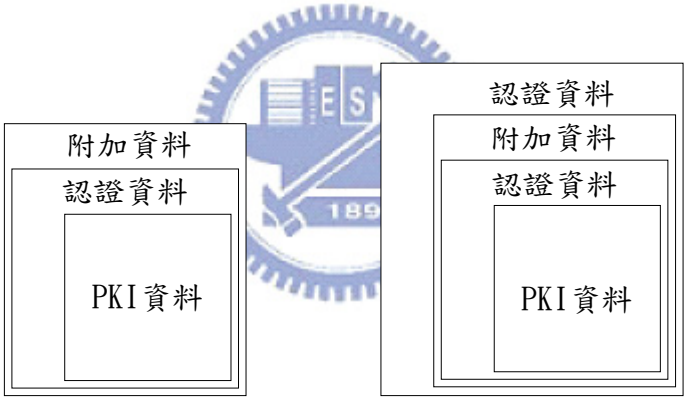
開發初期，運用RFC2797(Certificate Management Message Over CMS簡稱CMC)設計出與PKCS#10相同功能的基本憑證需求格式，然後運用RFC2511做為提供更多的可供使用的訊息交換格式使用於CMP中，加上RFC2630訊息加密語法作訊息加密與簽章加密用途同時也支援RFC2875由加密演算法大師Diffle-Hellman所提出的Proof-of-Possession演算法則，另外也可部份相容於舊有的PKCS#7與PKCS#10，使其成為匯集所有功能於一體的通訊協定。

CMC的規格定義兩種內容型態：PKI資料與PKI回應。PKI資料必須是一份需求訊息，PKI回應則是一份由CA回應的訊息。CMC運用CMS的認證資料與附加資料內容形態

提供保護。大部份的CMC訊息是不需要保密的，訊息是由PKI資料嵌入或是置於CMS認證資料內容由PKI回應訊息傳送，可參考圖2-6所示。

（圖2-6）CMC PKI資料保護的基本CMS資料內容形態[8]

實際運用上不僅上述的基本CMC訊息處理方式，CMC也可將訊息資料運用以下兩種方式將所要傳送的資料予以保護。因此，其靈活運用的方式比CMP好，而更重要的是比起CMP其處理方式似乎簡化不少。但是仍然比PKCS#7與PKCS#10複雜的多。



（圖2-7）其他CMC PKI資料保護的CMS資料內容形態[8][27]

5. 簡易憑證註冊通訊協定(Simple Certificate Enrollment Protocol，SCEP)

SCEP是由著名的思科網路通訊公司(Cisco Systems Inc.)所開發的，目的是為了運用現有的技術應用於網路設備中，可以安全無虞的傳送憑證。而其現有的技術包括RSA與DES密碼學、PKCS#7與PKCS#10訊息格式、HTTP與LDAP等。

SCEP是一種特殊的PKI管理協定，其運用範圍受限於網路設備與從憑證資料庫從事憑證回收與CRLs的工作。不同於之前描述的四種方式的是SCEP並不定義其資料格式

與內容形態，而是以實際需求面與商業考量為出發點，所設計的特殊PKI管理協定。目前SCEP支援四種不同的傳輸模式：CA的憑證發放與RA的公開金鑰傳送、憑證需求、憑證詢問與CRL的詢問。而憑證詢問與CRL的詢問主要是與憑證資料庫的功能相關，而SCEP將此兩者歸納於規格中。

2.7 PKI的原理

PKI的憑證格式與現有的相關標準主要是由IETF所制定的。而其現有的最新標準為X.509 版本的憑證定義格式。其原理主要在於數位憑證的設計與產生數位簽章之後，如何運用來達成身份鑑別的目的。

2.7.1 數位憑證的簡介

數位憑證又稱為電子憑證是由憑證授權單位發出，以向他人確認您的身分。憑證含有數位化的資訊，可用來保護個人資料或對其他電腦連線時提供建立安全保護機制。特別針對目前網路交易上的安全需求，提供完善的安全控管機制，使網路交易服務達到資料隱密性、提供身份確認性及不可否認性等安全需求。除增加網路交易之安全性及交易紀錄之完整性外，更確保委託單的訊息資料不會被篡改、及受到不法者冒名下單的危險，且在交易有紛爭時能有相關證據資料做為仲裁之依據。

關於一般使用上的應用，以下為實際生活使用的範例：使用網路下單時，券商必須確定此帳號擁有者。就類似現實生活中所使用的身分證，數位憑證提供券商辨識交易者身分的功能。當傳送重要的電子郵件時，電子郵件可以使用數位憑證針對電子郵件訊息作數位簽章。數位簽章主要用來幫助收件者確認該電子郵件確實由發信人所寄出，且確定電子郵件於傳送過程中並沒有遭到竄改。

關於數位憑證，概略上可分以下三種類型：

- 身份憑證：藉由公開金鑰與相對應身份相互結合，使他人能得知某特定人使用特

定的公開金鑰，藉以辨識身份。目前身份憑證的格式以國際電信聯盟電信標準化部門建議的X.509標準為主要準則，故有人將身份憑證稱之為「X. 509憑證」或「X.509公開金鑰憑證」。

- 授權憑證：藉由權限與公開金鑰的結合，使金鑰的持有者得以存取某資源的權限。
- 屬性憑證：屬性憑證僅是權限與身份的結合，並不以公開金鑰作為區別的要素，其運作與使用者存取權限控制清單較為類似。目前國際上關於數位憑證在權限管理上應用的討論，焦點仍集中在授權憑證與屬性憑證上，直接利用身份憑證作為權限管理則較為罕見。

2.7.2 X.509 的憑證格式

一份 X.509 憑證主要是由一組包含使用者或設備資訊的標準格式及所對應的公鑰所共同組成的。 X.509 標準定義了憑證裡應有的資訊，以及描述如何被組成其資料內容格式。所有的 X.509 憑證都具備下列資料欄：

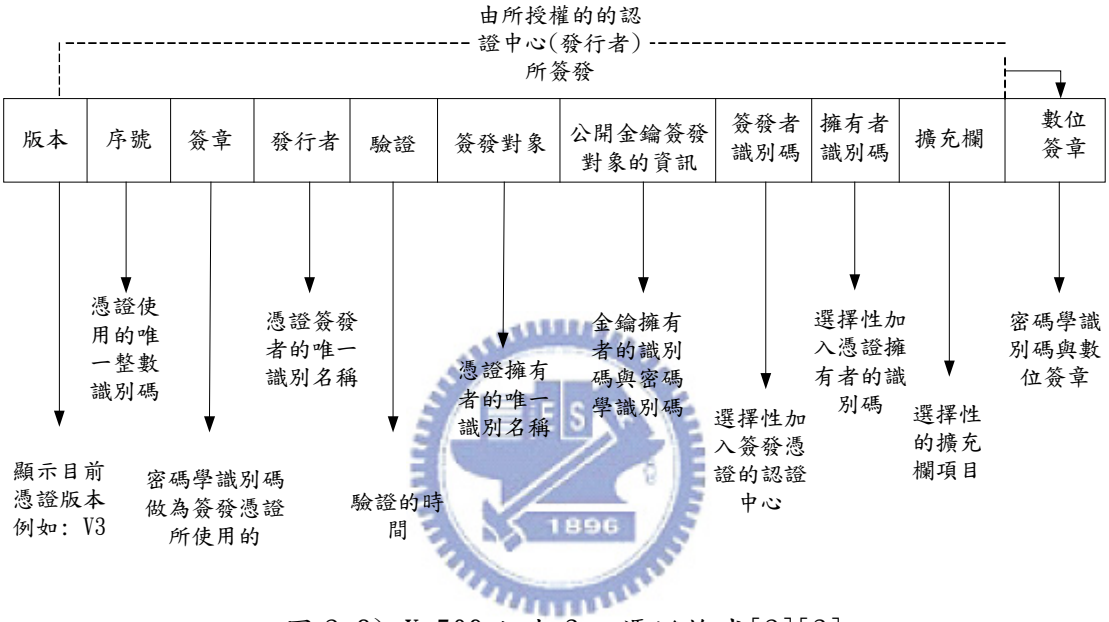


圖 2-8) X.509 版本 3 之憑證格式[2][3]

每個欄位相對應所代表的意義與其數值表示法是以 ASN.1 的語意做說明，ASN.1 是一種資料格式標準，目前被業界的許多應用程式或硬體設備所採用，可跨不同平台作資料交互的標準。使用 ASN.1 解釋定義如下：

版本編號欄代表 X.509 版本號碼，目的是為了顯示此份憑證是運用 X.509 的版本編號並會影響到資訊的相互相容性與內容格式標準的不同。其數值可分為 1、2 或是 3，

目前最新版本為第 3 版。

Version ::= INTEGER { v1(0), v2(1), v3(2) }

序號欄是此憑證對的唯一身份識別碼供憑證發給人辨認所使用，建立憑證的實體如程式或是個人需要提供一個可供辨識序號與其所發出的其他憑證區隔開來，以示負責，這項資訊可被多種方法所使用。例如當一個憑證被註銷時，它的序號就會被放進 CRL 裡。

VertificateNumber ::= INTEGER

憑證持有者辨識名稱（distinguished name，以下簡稱 DN）鑑定碼，這個名字應該是在網路上獨一無二的，就類似網址一樣，其格式定義是以 X.500 所定義的 DN 為標準。一份 DN 包括了多個子區段，其內容的表示法範例如下：

CN=LP TSAI， OU=NCTU，O=IIM， C=TW

（憑證擁有者的名字、組織單位、組織、以及國家。）

數位簽章欄為演算法的鑑定者，如同物件識別碼一般，加上演算法相關的參數作為計算憑證的數位簽章用途。例如：對 SHA-1 的物件識別碼使用 RSA 運算，代表的是一份數位簽章已經用 RSA 運算法加密。

UniqueIdentifier ::= BIT STRING

憑證發行者欄是認證中心的 DN 名稱，負責簽發憑證者必須永遠存在以便持續提供所需服務給憑證使用者。通常這會是一個 CA ，使用一份憑證依照信任關係，簽發這份憑證的實體。但在最高層級的 CA 憑證，其發行者則會行使自行簽發憑證的方式產生憑證。

UniqueIdentifier ::= BIT STRING

驗證欄指的是憑證有效期限 — 憑證生效日期／時間以及截止日期／時間，指出這份憑證的過期時間。其時間的使用格式有兩種表示方式 utcTime 與 General- Time 格式，在 RFC3280 中有定義出格式，其表示方式使用 ASN.1 的語法表示為：

```
Validity :: = SEQUENCE {

        NotBefore Time,

        NotAfter  Time }

Time ::= CHOICE  {
        UtcTime         UTCTime                 -- YYMMDDHHMMSSZ
        GeneralTime     GeneralizedTime         -- YYYYMMDDHHMMSSZ
}
```

簽發對象代表憑證擁有者的辨別名稱並且必須不得為空白，除非已有可取代的名稱形式被使用於擴充欄才可以。

公開金鑰簽發對象資訊指的是憑證持有者的公鑰，內容為憑證擁有者的資訊與公開金鑰結合及用來指定此金鑰使用何種密碼系統的演算法鑑定碼，還有其他此把金鑰的相關參數，實際使用時此欄位必需要強制性存在。

SubjectPublicKeyInfo ::= SEQUENCE {

Algorithm Algorithm AlgorithmIdentifier,

SubjectPublicKey BIT STRING }

憑證簽發者與擁有者的唯一識別碼此兩者都是可選擇性加入資料欄位，而憑證發行者的唯一識別碼也同時在版本 2 與 3 都有支援。此兩個欄位在實際應用上很少使用，一般是可以被忽略的，在 RFC3280 的報告書才開始被建議使用。

擴充欄是一個選擇性加入欄位，目前就只有版本 3 才有支援。如果此欄位被使用，則可以加入一筆到多筆憑證擴充資料。其每筆擴充資料需包含擴充識別碼、顯示旗標與一份擴充數值。

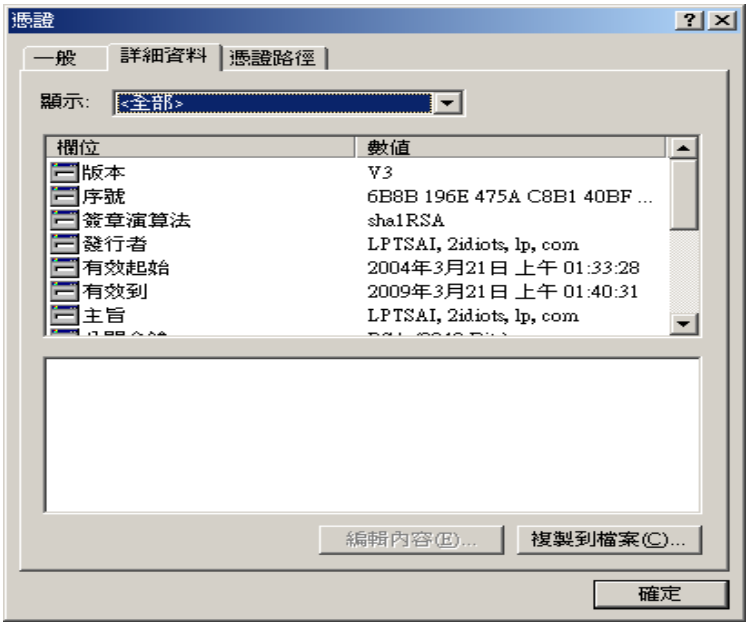
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

```
Entension ::= SEQUENCE {

        ExtnID    OBJECT IDENTIFIER,

        Critical BOOLEAN DEFAULT FALSE,

        ExtnValue OCTET STRING  }
```

數位簽章內含憑證發行者的數位簽章，也就是發行者使用憑證實體私鑰的簽章。另外，還有簽章演算法鑑定碼作為顯示 CA 當時簽發此份憑證時所使用的演算法。

一 憑證格式範例

微軟的 Windows Server 2003(以下簡稱 Server 2003)所提供的 PKI 機制中，可讓使用者自行架設部署屬於自己的 CA。以下資訊即由 Server 2003 所簽發的 CA 的相關資料。由於 Server 2003 支援 X.509 第 3 版，一般而言是可相容目前業界普遍支援的格式。



（圖 2-9）微軟憑證訊息格式

下載CA憑證的資料內容

[版本] V3

[序號] 6B8B 196E 475A C8B1 40BF 7378 C86F 0086

[簽章演算法] sha1RSA

[發行者] CN = LPTSAI

DC = 2idiots

DC = lp

DC = com

[有效起始] 2004年3月21日 上午 01:33:28

[有效到] 2009年3月21日 上午 01:40:31

[主旨] CN = LPTSAI

DC = 2idiots

DC = lp

DC = com

[公開金鑰]

3082 010A 0282 0101 00B7 78B3 A5AD 0BD3 8C79 1DD4 1C39 A1DD 9698 2284 2A7B

A8C4 EA83 27D5 ECA2 8B9F 4DC3 A30B 476D EA3D D952 2F59 27A1 9ED0 A1AB 8207

45B4 18F6 FA30 2A5A 40A9 446A A64A 5165 AED2 983D F180 118F 54EE 47EA 10AB

BF5D 0C84 DECC C769 34B2 EED4 4346 E284 F638 DC85 30D6 50BE 6D28 9501 7E4F

9CEC E6F5 21ED 53E3 D043 D81F CF73 8629 D6E7 C582 6512 83CB 4688 5ECF 81B0

EC5C 15B1 961F F2AE 5307 01C1 F3D9 E7CB CFDA 8031 A0D9 B105 C4CE 90EA 3037

531F 0D39 CF98 01AC 21BA 6831 35B9 77E7 A647 47B1 8211 589E B1F6 EDCD 2BC9

DA7C 7DA7 FCEB DBCD A4A3 2369 5150 CA3F 9AFC 4FE1 75ED B938 EBD9 522D 6B4B

8258 CC9D 4EAF 66C2 73DD 912F B524 8725 5D61 9B80 C205 36AA

[公鑰使用方式]

Digital Signature , Certificate Signing , Off-line CRL Signing , CRL

Signing(86)

[主體金鑰識別]

638D 3EEB BF3F D91A 2F5D E7E1 39B6 418F 0BA0 2D7A

[CRL發佈點]

[1]CRL Distribution Point

Distribution Point Name:

Full Name:

URL=ldap:///CN=LPTSAI,CN=server2003,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=2idiots,DC=lp,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint

URL=http://server2003.2idiots.lp.com/CertEnroll/LPTSAI.crl

[CA版本] V0.0

[基本限制] Subject Type=CA

Path Length Constraint=None

[拇指紋演算法] sha1

[拇指紋] AE24 9D1C B705 8E9E BFB0 850F 2FBD A538 2C6F 2362

2.8 PKI 的優缺點

PKI 的機制並非完全符合目前所有資訊安全應用面所需，本章節針對 PKI 的實際應用列舉出優點與缺點，以便了解其應用面上可以獲得的益處與可能會面臨的問題，減輕實際應用時所遭受的衝擊。

2.8.1 PKI 的優點

- 減少在資訊安全的管理成本，相對於多點服務的解決方案而言，PKI 算是最經濟實惠的解決方案。

- 達成多種應用使用單一憑証或密碼簽入的理想，可減少使用者簽入所需的步驟。現存的解決方案需要對異質的系統逐項作簽入系統才可以達到個別應用程式的身份認證功能，而PKI只需一次簽入即可。對企業而言，如果不考慮單項身份認證所帶來的風險問題，此單一簽入的功能可省去其他應用系統身份認證的架設成本與提高使用者的方便性。

- 電子簽核機制如無紙化、電子化及自動化的病歷流程之電子簽章及資料保密可利用CA所發憑證就可以減少文件作業流程與有效改善作業流程使商業處理更具自動化與安全性，不需太多文件申請作業流程，所有使用者權限都可完全自動化處理，相對也減少企業在文件審核與簡化複雜流程等問題，申請者也勿須等待過多時間。

- 主從架構應用系統的身份認証可讓資料得到保護，使用於企業內部網頁應用程式身份認証及資料保密，使用者就可以花更少時間在機密安全架構上，而使工作更具生產力。對資訊管理員而言，要同時去維護公司內各種不同系統的身份認證是頗為困擾

與耗費時間與成本的工作，而PKI就可讓資訊管理人員節省這類時間，使其更具時間效益。

- 以電子憑証結合組織階層架構，依照各層級人員職務權責作電子資料存取控制，達成以職務角色為基礎提供對電腦資源使用角色基礎存取控制的功能。利用金鑰分持(Key Shadow)的方式，對重要資訊系統例如憑証管理中心之金鑰，分別由多人或多個單位分別持有部分金鑰。在使用時，作業程序須要結合全部或部分金鑰持有者的金鑰，才能執行作業。

- 減少對使用者相關機密安全服務的教育訓練與設備花費，僅靠一套機密安全服務就可以取代以前多種機密安全服務。增加應用系統安全性，並簡化使用者實際操作的複雜性，利用一致化控管方式，易於維護、營運管理、存證與稽核作業。對於現存的各種系統，如要上線都需要有不同的硬體使用需求，例如：系統規格、資料庫的建置與機密安全所需使用的設備，如使用PKI就可節省此類重複性花費成本。

- 員工識別証與 IC 卡結合可機密地儲存個人資料，將個人金鑰與憑証置於 IC 卡內，並用 IC 卡與電腦資源作整合可提高資源存取之安全控管的安全性。如有特殊需求，可結合生物特徵例如指紋辨識，可對重要資訊系統或門禁作安全控管。

2.8.2 PKI的缺點：

- 如何驗證所使用的 CA 是一個值得被信賴的 CA

CA開宗明義就直接述說是”一個值得被信賴的CA”，倘若沒有CA沒有PKI。然而在密碼學的相關解釋上，代表的意義是CA本身可以做好在己身所擁有的私鑰保護。但

這並未告訴你可以使用CA所提供的服務就可以做到付費機制或是簽一份百萬訂單的契約都安全無虞。讓我們不禁懷疑是誰授權CA給予如此的權限？而誰又能讓CA做到讓人可以完全信賴的程度?

CA或許可以寫一份洋洋灑灑的憑證實作準則，昭告世人其憑證效力性與在何種狀況下憑證失效…等等，然而使用者就可依照憑證實作準則說明逐項閱讀後，就此完全可以高枕無憂使用嗎?“錯”，因為憑證實作準則並不保證你的應用程式上憑證是可以被信賴的。許多CA逃避了一個問題就是無法依照申請者的身份鑑別去發此憑證，因為任何人都可以給自己的憑證取個名字。這隱藏著風險在於驗證身分憑證時，當此份身分憑證有著其他控管方面的權限時，會有誤判而導致系統風險。

對CA而言，憑證發佈的順序是：

1. 你有一份身分憑證
2. 他會給你憑證使用者名稱
3. 此憑證使用者名稱讓你知道你是憑證持有者
4. 這就是你唯一知道的部份

若此身份憑證並非屬於你本人，或是你的資料與他人有相似之處(例如名字或相同身分證號碼…等等)，那又該如何處置呢?

- 如何證明使用此份憑證的就是使用者本人(不可否認性)

對個人而言，PKI的最重要部份就是我們所持有CA所簽發的私鑰。我們應該要如何保護此份私鑰呢?要如何才能避免被病毒或複製程式所侵害呢？即使你的私鑰放在

很安全的電腦，房間已鎖上也裝了保全系統，如果有密碼保護，則需要多久會被破解。如果是存在智慧卡內部，那有多少功能可以阻絕外部破壞呢？若一切都安全，當要使用時電腦具完整的安全性嗎？因此，無法認定一定沒有他人會使用此份私鑰。

簡言之，可用一個名詞”不可否認性”表示。當數位簽章演算法是牢不可破的，任何第三者都無法複製此份數位簽章時，提供PKI認證的廠商以此作為具法律效用，倘若第三者使用此數位簽章，你也無法否認被盜用者所使用數位簽章並非自己所擁有的。在美國猶他州與華盛頓州通過了數位簽章法條文指出，假設此簽章已經被批准為可以合法使用且經CA所認證過，則有責任要負起你應負責任。不管坐在電腦鍵盤前使用者是不是你或是電腦病毒使用了此份簽章，這都是屬於你的責任。這似乎比使用信用卡還可怕，因為至少還可以否認此信用卡帳單並非使用者所簽的，得由廠商舉證才有效。

- 憑證認證過程安全性是否可以被完全信賴

憑證認證過程中，並不需要另一份秘密金鑰，只需公開金鑰即可。因此，也就如同沒有任何秘密需要被保護，只需要有一份甚至多份需使用的公開金鑰就行。在此段期間，假設攻擊者將其擁有的公開金鑰加入清單中，就可以簽發屬於自己的簽章，而且完全跟合法簽章效力相同。只是此份簽章除了攻擊者修改部份的資料節段外，其他部份是跟合法使用者資料是一樣的。

對於持有主要簽章(Root Certificate)的主要金鑰(Root Keys)持有者而言，就如同自己簽發簽章然後自己認證，絲毫無機密安全可言。對此行為唯一的解釋是在電

腦系統作憑證認證過程中，對於入侵滲透行為如懷敵意的程式碼或實際竄改行為是不會輕易被破壞的。但這卻不能保證整體憑證認證過程的安全性是可以完全被信賴的。

- 是否為此份憑證的唯一合法使用者

先前提及CA發憑證順序是要有一份身份憑證，憑證依據只是使用者名稱。試想當收到此份憑證寫著”王小明”，只知道姓名為王小明是唯一合法署名為” 王小明”的憑證擁有者。但世界上總共有多少的CA知道呢? 又如何得知”王小明”的簽章使用哪個CA所發出的憑證呢?雖然可用附加的資訊，經由公開金鑰驗證此”王小明”的簽章，但確定這就是所指的憑證擁有者”王小明”嗎?由CA驗證的簽章或許會有一些可擴充的資料節段作簽章使用者的補充說明，但就可以知道這些資訊就是所意指的”王小明”個人資訊嗎?

當Diffie與Hellman提出簽章密碼學時，只是想在類似已經有處裡過的電話目錄中，找出公開金鑰罷了。取代舊有名字、住址、電話號碼方式；而採用名字、住址和公有金鑰為其組合內容。只要找出”王小明”的公開金鑰，就可以傳送給他任何訊息。在1976年時期，這或許可用在學校內已經處理過的此類電話目錄，但如果是其所居住的城市或國家會有多少名字叫”王小明”的人，更別提是運用在網際網路會有多少位”王小明”存在了。

這最主要是因為人類的行為主要是生活在小家庭裡，名字可以很容易就具有獨一無二的特性，但我們可能會為了配合PKI必須要改變我們的生活嗎?而在台灣假設我們使用身分證字號難道就具有唯一性?答案恐怕會令人失望。因戶政單位早期連線資訊

落後，在30年以前出生的台灣公民就曾有重複狀況的發生。

- 單一簽入

曾經有一家供應商員工宣稱他們已經在這幾年成功銷售出許多PKI的完整解決方案，但是他們的客戶卻不是很高興地使用。在CA安裝完後，使用單位會發給所有使用者一份憑證。但顧客開始問估應商：「我們該如何做到單一簽入呢？」而供應商卻回答：「你不需要，因為這需要修改整個系統軟體才能作到，現階段無法做到。」單一簽入或許是PKI的殺手應用程式，使用單一簽入的功能，早上只要用智慧卡簽入系統後，一整天直到下班都不需要重新再煩惱不斷的打帳號與密碼，甚至還有許多不同帳號與密碼分散於不同系統中。這樣是不是很吸引人呢？

對企業使用者而言，若無法使用單一簽入則使用憑證仍然是一種痛苦，能夠不使用盡量不使用，但認證機制的誘惑力已經完完全全將單一簽入的好處打敗了。認證機制是支援使用者提供身份確認來使用電腦，然而單一簽入卻是要在不同地點使用其帳號與密碼來使用目前所處地點的電腦，這是完全不同的設計。因此，未來可能會演變成每種系統有其所發的憑證。那為何還要對CA的認證流程如此著迷呢？為何它不能將架構做的彈性一點，最好就如同單一簽入那樣方便最好。

- 更新憑證註銷清單的頻繁性

憑證的註銷會在以下狀況發生：

1. 與公開金鑰相對應的私有金鑰被破解或遺失狀況之下。

2. 簽發認證的CA私有金鑰被破解，在此狀況所有的的私有金鑰都需要重新換發。

3. 認證契約被終止、認證持有者狀況改變（離職或單面終止使用權）或者是憑證使用範圍有所更改或取消的狀況下，憑證會被註銷。

當憑證被註銷時，理想性而言就需即時被註銷般，不容許有任何延遲。如果有心人士想破壞機密資料或用來簽發一些非法行為時，延遲時間是足夠去執行的。即使是用法律條文或其他方式約束，都無法補救已造成損失的事實。

第三章憑證註銷清單的說明

憑證註銷機制，其主要概念有一部份是來自信用卡的想法。例如信用卡的有效期間就如同當數位簽章所指定的使用期限已過，就需要被註銷。另外，還有其他因素數位簽章需要被註銷：

- 憑證的狀態改變
- 憑證持有人的姓名改變
- 憑證的持有人與組織的關係改變
- 憑證簽發的 CA 與使用其服務的機構的關係改變
- 授權核發憑證的作業停止相關服務作業
- 私鑰遭停止或暫停使用
- 經查出私鑰已遭破解或遺失
- 發現憑證有許多不符合實際運用或功能性錯誤的因素
- 憑證持有人不想使用

如上述狀況發生時，則憑證將不存在與CA之間的信賴關係。

3.1 憑證註銷清單

在憑證註銷機制中，CRL 是一種傳統的數位憑證確認方法，主要是用來列出已經終止與無效的數位憑證。這份文件是可供憑證使用者自行下載，由於是每間隔一段時間便會更新，用戶必須定期下載資料，才能取得最新資訊。CRL 會列出所有有效期限

未到，但已被 CA 註銷的數位憑證。而 CA 列出被吊銷的憑證外，還會在最新的 CRL 中說明本份 CRL 的有效期限，與何處可以取得最新版本的 CRL。

由於 CRL 本身更新模式會導致使用者必須時常去更新，因此可能會造成安全漏洞。例如：某位員工在正午 12 時離職，然而最新一份 CRL 在 11 時 50 分更新完畢，而 CRL 下次更新時間為下午 5 時，安全漏洞就出現在這段空檔時間內，存在著離職員工還是可以任意使用該憑證的問題。另外，不僅下載 CRL 的程序繁瑣而且若憑證機構一天更新幾次，就得下載幾次。通常 CRL 檔案容量龐大，還會增加網路傳輸的負擔，並需要很長的下載時間。

為解決這些問題，業界共同商議新的資料更新方式 — 線上認證狀態通訊協定(OCSP；Online Certificate Status Protocol)便因此而誕生，可提供給使用者一個或多個數位憑證的有效資料，同時定義可即時回應的機制，讓使用者可以即時確認每張憑證的有效性，解決CRL可能出現的安全漏洞問題。

3.1.1 憑證註銷清單的原理

一份公開金鑰憑證(Public Key Certificate，以下簡稱 PKC)是用來由金鑰持有者驗證其數位簽章的正確性。首先 CA 使用其公開金鑰簽發 PKC 給使用者，之後由目前的時間設定其 PKC 的有效期限，最後使用 CA 所發的 PKC 授權公開金鑰作為數位簽章的驗證依據。PKC 只是一份靜態資料而且內容也是已存在的舊資料，會在被破解或是使用者因某些因素而被註銷。而其註銷方法就是之前所述說的 CRL 機制，其內容基本上只是所有被註銷的 PKC 序號。

CRL 的運作模式主要是 PKC 使用者在收到 CRL 的資料後，透過下列步驟達到驗證 PCK 是否已經被註銷與否的目的。

1. PKC 使用者取得當初簽發憑證 CA 所發佈的 CRL

2. 確認 CRL 的數位簽章是否合法

3. 確認 PKC 序號是否在此份 CRL 的列表內。如果是，就代表已被註銷；反之，則為有效的 PKC。

CRL 是 PKI 顯示公開金鑰狀態憑證的基本工具，可讓使用者確認此憑證是否依然有效的機制。簡言之，只是一份數位簽章的序號列表儲存於特定目錄或 LDAP 目錄服務中，經由 CRL 也可得知額外資訊，例如憑證被註銷原因。假使數位簽章序號存在於表中，則代表此憑證已經被註銷了。因此，CRL 設計目的在於憑證擁有者因金鑰遺失、洩漏或遭破解等因素向 CA 要求將仍在有效期限的憑證註銷，或因憑證過了有效期限，CA 必須將這憑證相關資料定期向目錄伺服器發佈，供交易端驗證憑證有效性之用。而大量憑證使用者經常需向 CA 更新資料以取得註銷憑證資料，使用者必須依 CA 更新時間作資料下載作業，一般而言，CA 會一年更新一次或半年更新一次。

對 PKI 而言，CRL 是最令人爭議的領域。假若不檢查 CRL，則無法確認此憑證是否被註銷；但如要去檢查 CRL，則可能只是檢查此憑證在最後所發行的 CRL 版本中，沒有被註銷。CRL 是由當初核發憑證的 CA 負責去維護。但隨著整體電子商務的成長，所核發的憑證數量也呈倍數成長，不可避免地憑證註銷的數量也隨之增加。使用者要自行決定是否需每次去檢查 CRL 或是視情況需要而定。如在每次交易時就去檢查的

話，安全性可以得到較多保障。而在現實生活中，商業交易行為很多是不需要作身份確認。但若交易行為需經由電腦線上作業並需要身份確認的程序時，利用 CRL 作身份確認的過程還是有其必要性。

在憑證註銷的時間延遲定義是以當獲取此憑證必須被註銷的資訊到實際將憑證註銷資訊發佈之間所間隔的時間稱為憑證註銷的時間延遲。而憑證主要機制是與公開金鑰使用，而簽發的憑證也會因某種因素而導致無效相對地此公開金鑰功能也就不存在。而這種發生機率是跟隨著憑證註銷資訊何時被更新與公佈的時間而定，而這也會嚴重影響到所發的憑證安全性。

3.1.2 線上憑證狀態通訊協定 (OCSP)

線上憑證狀態通訊協定是由 IETF 所制定的標準在版本 1 規格制定是記載於技術文件號碼 RFC2560 名稱為"X.509 Internet Public Key Infrastructure Online Certificate Status Protocol CSP"。 線上憑證狀態通訊協定是一種相當簡便的需求與回應協定，提供傳輸工具作為一種由信任關係的線上憑證狀態通訊協定回應者提供維護線上憑證註銷資訊。

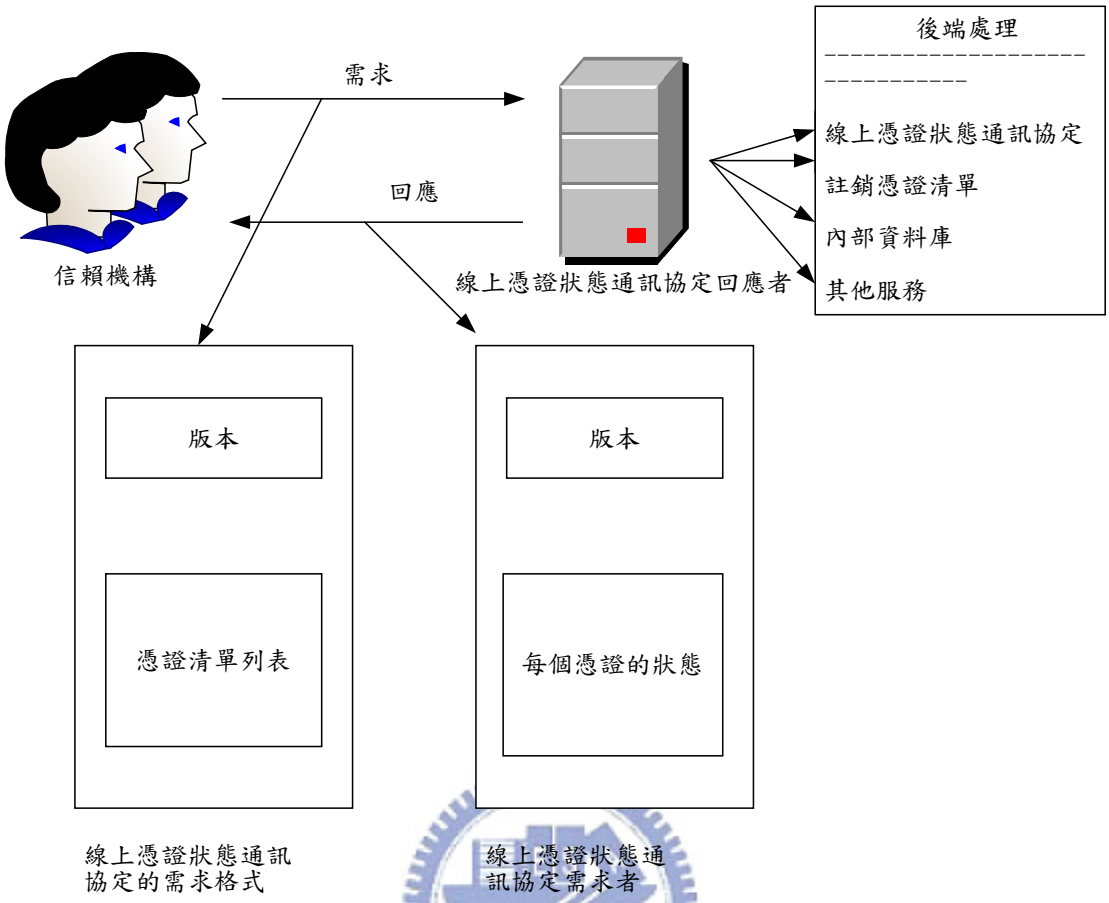
線上憑證狀態通訊協定的需求包含協定的版本編號(目前只定義到版本 1)，服務需求型態與一個或多個憑證鑑定資料。憑證鑑定資料包含憑證發行者的雜湊值，公開金鑰的雜湊值與憑證序號，額外的選擇性擴充欄則視實際需求而定。

回應部分則是比較直接，包含憑證的鑑別者，憑證狀態是正常、註銷或是未知、以及每個憑證鑑別者當初要求部分所驗證的回應間隔時間。假如當時核發憑證狀態被

註銷的，則回應的的顯示狀態也需符合。若憑證註銷的理由訊息有支援的話，也可再此時得到相對應的訊息。

而在驗證欄描述包含此次更新資訊與選擇性的下次更新資訊。而線上憑證狀態通訊協定的回應訊息，可以由此實際運作的政策決定是否可以在內部儲存其相關的資料。預期使用上是包含在與 CRL 同一區塊的位置。如同需求的部分一般，回應的部分也包含選擇性的擴充欄。

線上憑證狀態通訊協定也定義部份錯誤碼，主要是供給錯誤的事件發生時提供相對應的錯誤狀態顯示。線上憑證狀態通訊協定元件之間的相互關係(圖 3.1)可依信賴機構與一個線上憑證狀態通訊協定的回應者方式做說明。在許多不同憑證註銷策略可以應用於線上憑證狀態通訊協定的回應者方，也就如圖中所標記的後端處理。



(圖 3-1)線上憑證狀態通訊協定元件之件的互動關係

線上憑證狀態通訊協定的回應訊息必須要經由數位簽發保證，證明回應訊息是來自信賴方所傳遞，且未經任何修改的訊息。簽發的金鑰可能來自同樣簽發金鑰的 CA、另一個信賴機構或由原簽發憑證的 CA 簽發憑證給另一 CA 提供彼此信賴的認證機制。在任何情況下，信賴機構必須要能夠信賴回應信息，也就是說信賴機構必須信賴簽名者的回應信息。信賴機構也需持有一份線上憑證狀態通訊協定回應者之公開金鑰憑證，而這憑證是由信賴的來源所核發的。

線上憑證狀態通訊協定的主要功能是要驗證目前的憑證是否被註銷，不會去驗證其他憑證擴充欄所提供資料，例如憑證的有效期限範圍與金鑰的適用性…等等。但信

賴機構也是可以與其他方式合併使用來補強其不足之處。

3.1.3 CRL與OCSP 之比較

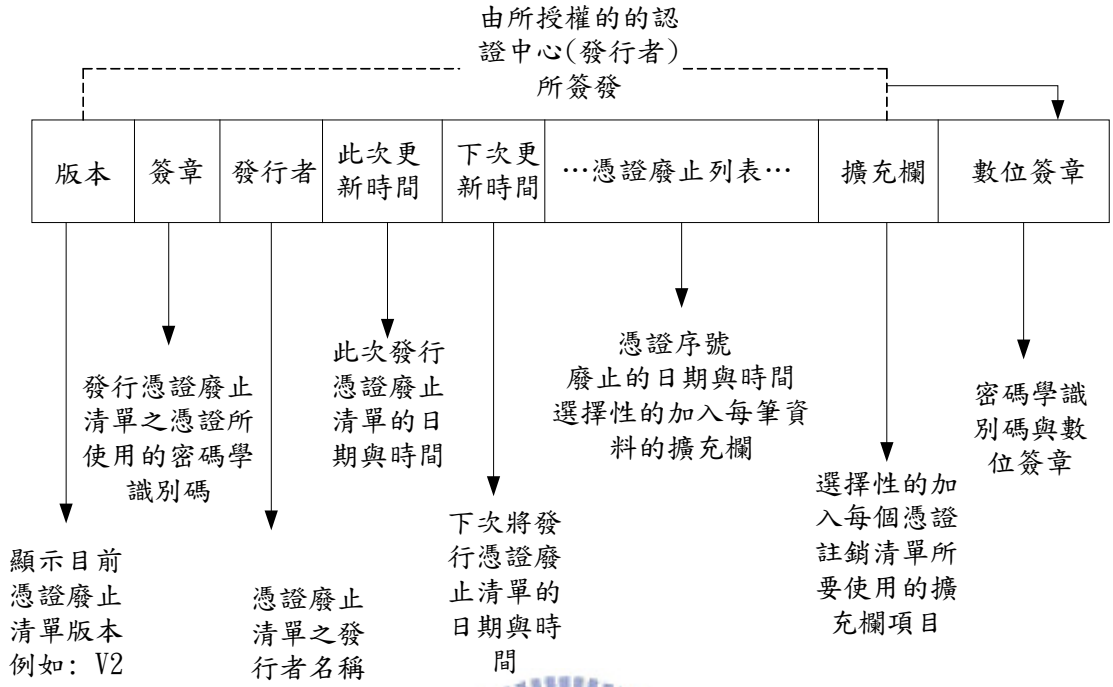
在實際應用面，CRL傳輸資料量過大且，網路頻寬過窄。若CRL更新頻率過高，使用者在每次使用憑證時，都必須從CA下載最新CRL資料。明顯地，對大多數使用者而言，是較不便利的。對於需長期且大量使用憑證資料驗證的使用者而言，有可能會為了方便而冒險使用舊的CRL版本，然而如此方式難保能每次皆順利查驗出憑證的正確身份；相對OCSP而言，可直接查詢利用線上提供憑證狀態功能，使用者可立即知道憑證是否有效，雖然沒有CRL 機制所造成的安全問題，但由於線上查詢之資料量過大，對於查詢的效能而言，影響頗大。使用者在使用OCSP 時，並不希望在每一次檢查時，OCSP利用網路進行大量且低價值的資料傳輸，由於所有的憑證及資料均集中在OCSP伺服器上，不僅維護工作會變得複雜，對於系統的運作效能而言，更是雪上加霜。

在台灣的內政部憑證管理中心，是我國電子簽章法的「憑證機構」，負責簽發我國滿18歲以上國民IC卡與公開金鑰憑證，提供自然人憑證與電子化政府應用服務網路通訊的主要機構。在內政部憑證管理中心在92年11月26日所出版的憑證事務作業基準1.2版[10]內文中所建議的使用方式為兩者並存，主要以OCSP為主要的方式，而CRL為輔助的方式。而公佈的CRL內容頻率則是一天一次公佈於資料庫。

3.2 CRL的標準

目前在IETF所制定的CRL版本為第2版，台灣內政部憑證管理中心所簽發的X.509憑證之CRL版本也為第2版。CRL的第1版與第2版的最大不同是在CRL版本1的部份，其實用性是非常欠缺應用性考量且無法彈性使用其擴充欄與效率太差。在CRL版本2標準中，除了改善先前的問題之外還訂定兩種解決方案加強其效率性的問題：差異式CRL(以下簡稱Delta-CRL)與CRL發佈點。Delta-CRL的內容只將先前所發佈的CRL與最新版本的CRL之間資料的差異處列出；而CRL發佈點則是使用憑證註銷資訊的各種原因如未使用、金鑰遭破解與暫時停止使用金鑰的種類區分後再加以分類，並且載明其分類後的CRL的儲存位置。如此就可藉憑證註銷的原因分類減低集中處理的負荷，幫助CRL分散其網路儲存的負擔。

3.2.1 CRL版本二格式說明



(圖3-2)第二版CRL的格式[2]

一 版本欄代表 CRL 的版本，其值為版本 2 或是此欄沒有出現則表示這是版本 1 的 CRL，因為此部份在版本 1 並沒有定義其語法。

一 簽章欄代表運算法則的物件碼，可使用來計算在 CRL 數位簽章的數值。例如一般是在物件碼中使用訊息摘要 5 裡含有 RSA 運算法則，簡單的說就是一 數位簽章是一個訊息摘要 5 的雜湊值，而其運算編碼是使用 RSA 的方式。

發行者欄是 CRL 發行者的識別名稱，其值必須提供而且必須是唯一的不得重複的值。

一 此次更新時間欄是此次 CRL 發行的時間，使用的是 UTC 時間或 Generalized 時間。在 RFC3280 報告書中有記載這些時間使用的相關規則。

一 下次更新時間欄為一個選擇欄位，代表下次 CRL 要發行的時間。

一份新的 CRL 可能在下次更新時間所指定時間之前發行，這完全端賴實際需求而定而

非強制性的。

— 憑證註銷列表欄是一份清單記載憑證註銷的資料，裡面內容為每筆註銷憑證的唯一識別碼，也就是說清單中含有註銷憑證的唯一序號而不是整份實際的憑證。每個項目包含了所註銷的憑證在何時不再生效。另外，還可選擇性的加入預先擴充欄。而憑證並不會記錄在 CRL 裡，僅是將一個參考值寫到註銷憑證欄位置，例如憑證的唯一序號。

當註銷憑證已經過期，也就是說使用的日期與時間超過時，就不再需要去保有此序號存在於之後所發行的 CRL 內容。但事實並非如此，假設憑證已經被註銷仍然必須有一份 CRL 存有其資料，即使此憑證的有效使用期限即將過期在首次憑證註銷時間與下次 CRL 發行的時間，還是要有所紀錄。這是要確定所發給的憑證是已經被註銷而且被紀錄下來適當地保存下來。此訊息會與憑證相結合，而且需機密性的保存作往後參考用途。

在憑證註銷列表欄描述一份憑證被註銷資訊包含被註銷的憑證序號、憑證註銷日期與憑證資料擴充欄。而憑證資料擴充欄可以用來描述憑證被註銷的原因與其他輔助資訊。

— 擴充欄是可以自行擴充的資料欄位，可配合CRL的政策或資訊作擴充使用。

— 數位簽章欄是憑證簽章演算法的辨識碼，可使用簽章演算法如MD5、SHA的演算法算出其簽章數值。數位簽章指的是發行者的數位簽章，使用發行這份憑證的實體的私鑰的簽章。另外，還有簽章演算法鑑定碼作為 CA 簽署這份CRL時所使用的演算法。

以ASN.1表示法描述CRL的格式[8]結構：

```
CertificateList ::= SEQUENCE {
    tbsCertList           TBSCertList,
    signatureAlgorithm    AlgorithmIdentifier,
    signatureValue        BIT STRING  }
TBSCertList ::= SEQUENCE {
    version               Version OPTIONAL,(版本2才支援)
    signature             AlgorithmIdentifier,
    issuer                Name,
    thisUpdate            Time,
    nextUpdate            Time OPTIONAL,
    revokedCertificates   SEQUENCE OF SEQUENCE {
        userCertificate    CertificateSerialNumber,
        revocationDate     Time,
        crlEntryExtensions Extensions OPTIONAL } OPTIONAL,(版本2才支援)
    crlExtensions         [0] EXPLICIT Extensions OPTIONAL }(版本2才支援)
```

- 使用微軟伺服器 2003 版本實作憑證註銷清單資訊如下：

[版本]　V2

[發行者]　CN = LPTSAI

DC = 2idiots

DC = lp

DC = com

[有效日期] 2004 年 3 月 21 日 上午 01:34:06

[下次更新] 2004 年 3 月 28 日 下午 01:54:06

[簽章演算法] sha1RSA

[授權金鑰識別碼] KeyID=638D 3EEB BF3F D91A 2F5D E7E1 39B6 418F 0BA0 2D7A

[CA 版本] V0.0

[2.5.29.20] 02 01 01 ...

[1.3.6.1.4.1.311.21.4] 17 0D 30 34 30 33 32 37 ..040327

31 37 34 34 30 36 5A 174406Z

[2.5.29.46]

30 81 F5 30 81 F2 A0 81 0..0....

EF A0 81 EC 86 81 B0 6C l

64 61 70 3A 2F 2F 2F 43 dap:///C

4E 3D 4C 50 54 53 41 49 N=LPTSAI

2C 43 4E 3D 73 65 72 76 ,CN=serv

65 72 32 30 30 33 2C 43 er2003,C

4E 3D 43 44 50 2C 43 4E N=CDP,CN

```
3D 50 75 62 6C 69 63 25   =Public%
32 30 4B 65 79 25 32 30   20Key%20
53 65 72 76 69 63 65 73   Services
2C 43 4E 3D 53 65 72 76   ,CN=Serv
69 63 65 73 2C 43 4E 3D   ices,CN=
43 6F 6E 66 69 67 75 72   Configur
61 74 69 6F 6E 2C 44 43   ation,DC
3D 32 69 64 69 6F 74 73   =2idiots
2C 44 43 3D 6C 70 2C 44   ,DC=lp,D
43 3D 63 6F 6D 3F 64 65   C=com?de
6C 74 61 52 65 76 6F 63   ltaRevoc
61 74 69 6F 6E 4C 69 73   ationLis
74 3F 62 61 73 65 3F 6F   t?base?o
62 6A 65 63 74 43 6C 61   bjectCla
73 73 3D 63 52 4C 44 69   ss=cRLDi
73 74 72 69 62 75 74 69   stributi
6F 6E 50 6F 69 6E 74 86   onPoint.
37 68 74 74 70 3A 2F 2F   7http://
73 65 72 76 65 72 32 30   server20
```

```
30 33 2E 32 69 64 69 6F   03.2idio
74 73 2E 6C 70 2E 63 6F   ts.lp.co
6D 2F 43 65 72 74 45 6E   m/CertEn
72 6F 6C 6C 2F 4C 50 54   roll/LPT
53 41 49 2B 2E 63 72 6C   SAI+.crl
[1.3.6.1.4.1.311.21.14]
30 81 C2 30 81 BF A0 81   0..0....
BC A0 81 B9 86 81 B6 6C   .......l
64 61 70 3A 2F 2F 2F 43   dap:///C
4E 3D 4C 50 54 53 41 49   N=LPTSAI
2C 43 4E 3D 73 65 72 76   ,CN=serv
65 72 32 30 30 33 2C 43   er2003,C
4E 3D 43 44 50 2C 43 4E   N=CDP,CN
3D 50 75 62 6C 69 63 25   =Public%
32 30 4B 65 79 25 32 30   20Key%20
53 65 72 76 69 63 65 73   Services
2C 43 4E 3D 53 65 72 76   ,CN=Serv
69 63 65 73 2C 43 4E 3D   ices,CN=
43 6F 6E 66 69 67 75 72   Configur
```

```
61 74 69 6F 6E 2C 44 43   ation,DC
3D 32 69 64 69 6F 74 73   =2idiots
2C 44 43 3D 6C 70 2C 44   ,DC=lp,D
43 3D 63 6F 6D 3F 63 65   C=com?ce
72 74 69 66 69 63 61 74   rtificat
65 52 65 76 6F 63 61 74   eRevocat
69 6F 6E 4C 69 73 74 3F   ionList?
62 61 73 65 3F 6F 62 6A   base?obj
65 63 74 43 6C 61 73 73   ectClass
3D 63 52 4C 44 69 73 74   =cRLDist
72 69 62 75 74 69 6F 6E   ribution
50 6F 69 6E 74            Point
```

OID	代表的意義
2.5.29.20	CRL 序號
1.3.6.1.4.1.311.21.4	下次 CRL 發佈的時間
2.5.29.46	Freshest CRL
1.3.6.1.4.1.311.21.14	自行簽發的 CRL

（表 3-1）微軟 CRL 範例之 OID 對照表

3.3 如何評估CRL的效率

評估一份CRL的效率，首先必需滿足資料傳輸的四項要點：

唯一性：CRL資料傳輸必須要能夠完整的確認完成處理過程。若CRL傳輸資料在一半網路斷線時，則必須將此資料交易中斷，已確定資料交易傳輸的唯一性。

資料一致性：當各憑證用戶端提出CRL資料需求時，若沒更新任何資料時，其同時間所有的資料交易需一致，以避免CRL有被竄改之疑。

獨立性：每份CRL資料傳輸必須能獨立完成。若CRL資料在傳輸時遭修改，導致此份CRL資料部份不是原始CRL版本，而是兩份不同版本所結合資料，則會影響其驗證資料的正確性。

持續性：目錄伺服器提供CRL資料傳輸必須要有足夠的能力提供各憑證用戶端下載使用。若因某些原因無法提供服務時，必須要尋求其他資源取代，而不能因軟硬體異常而終止服務。

除了要滿足其資料傳輸要點外，最重要還是對其功能性提出評估標準。目前在學術界中，所提到的要點都相當類似。以下將列出幾項要點主要是根據所蒐集到的資料整理歸納後，提出CRL標準評估要點。

機密性：憑證註銷機制作業過程與相關資料在產生、傳送、儲存或內部溝通的通訊機制都需加以保護，已確定其安全性的完整。

即時性：當憑證狀態已被合法CA所改變，並且憑證註銷的資訊已被加入到憑證註銷內容，提供憑證用戶端下載其間隔的時間延遲需減少到近似於零，也就是趨近於完全無

時差的水準。

更新頻率：指上次發佈憑證註銷資訊與資料需求所間隔時間。一般而言，更新頻率越頻繁代表效率越佳，但相對地所付出的成本也相對越大。

頻寬：指的是網路頻寬，資料由通訊管道傳到目的地的最大資料量。在此則是指CA與目錄伺服器及憑證驗證端與目錄伺服器之間的資料通訊管道品質。

延展性：描述一份憑證註銷結構能力是否可以足夠容納額外的需求與回應訊息，而又不會影響其效率、即時性與增加系統複雜度。如果可以的話，未來可以擴充能力就可以提供更多種類的用途。例如：增加越多的擴充欄位，讓未來應用上可以更具彈性化。

資料集結性：指資訊所呈現的階層分割能力，可以便利憑證註銷機制的憑證狀態發佈。因為一旦資料被系統化的分割，就可依據其分割方式快速地應用其正確驗證法則，順利找出其所需的驗證資訊。

效率：指的是由憑證狀態資訊提供者發出回應給需求者的處理過程。

運算能力需求：指硬體設備是否足夠負荷及憑證驗證運算時的需求，而在此所謂的硬體設備為電腦及其他的特殊硬體需求。

網路基礎架構需求：指所需使用的網路架構需要程度需求為何等級，才能有效的發揮其應用所需。

標準相容性：在所使用CRL資料結構是使用標準的、私人的或是研究型的模式與如何與現存的應用程式整合，將會是影響其相容性與未來整合能力的重要因素。

專業審核：由具公正性的專家與研究學者執行專業審核、反覆測試與文件資訊化的管

理，此項會成為其運作成功與否的重要關鍵之一。

管理需求：如何去簡化CRL結構的複雜性、維護與儲存都需要專業管理能力，而最佳方式是採用自動化管理。目前所常用機制為組態管理，可以依不同規則與政策制定，完成所有作業。當然必要時，手動的操作還是有其需要性。

線上或離線更新：依據實際需求與技術面判斷，決定憑證用戶端應使用線上或離線方式更新CRL資料。

3.4 使用CRL的應用瓶頸

目前實際應用上，使用CRL憑證註銷發佈訊息，有三個目前待解決問題：首先是無法有效發佈最新憑證註銷發佈訊息；其次是大量CRL資料內容與缺乏不可否認性機制。

- 無法有效發佈最新憑證註銷發佈訊息

針對 CRL 無法有效發佈最新憑證註銷發佈訊息，主要是因為 CRL 並無法經常都保持最新 PKC 的狀況，因為 PKC 是定期被發佈的，PKC 使用者也需知道下一次 CRL 被發佈時間執行下載動作。而這時間延遲就會成為問題。解決這問題最簡單方法就是經常性的發佈 CRL；另外，使用者也需每次驗證一份數位簽章時，就去取得最新的 CRL 資料。但是，這種解決方式並不具備可行性，主要原因是即時性與頻寬考量。

- 大量 CRL 資料內容

CRL 因為要保存大量 PKC 的有效期間內憑證註銷序號資料內容，其資料內容會不

斷膨脹到很難掌控與預測，因為憑證使用者數量與 CA 交互認證等因素而變得很複雜。因此，憑證用戶端要經由網路取得 CRL 與將此資料在本機作備份行為，其高成本與機密性是問題所在。而這問題的嚴重性會導致 CA 架構的使用性遭受質疑。

目前而言，由 CA 所簽發的 PKC 被註銷的主要原因為憑證擁有者的個人身份或組織改變。對一個大組織架構員工數以千或萬計的企業而言，經常性的改變人事、部門與組織架構重整或是憑證擁有者姓名更改等等，這些原因會導致註銷的 PCK 數量龐大，相對地 CRL 資料量也會增加。例如，有一間企業有 1 萬人其 10%的員工因為組織重整需要調動，則此時就要將 CRL 的資料量增加約 20K 位元，可見這將會對每次要花時間取得資料作驗證工作影響可見一般。

在 CRL 的第 2 版已經改善了處理龐大資料量的部份問題，使 CA 可以經常性更新與發佈 CRL 資料，因為 CA 利用 Delta-CRL 方式發佈，可使其所需傳輸的資料比先前版本還要少很多。但對使用者主機而言，並不能將儲存 CRL 憑證註銷資料量減少，仍然要處理原始 CRL 與 Delta-CRL 才能夠完成確認動作，這對使用者主機的負荷依然存在。因此，嚴格來說 CRL 第 2 版是不能完整解決 CRL 資料量龐大的問題。

- CRL 缺乏不可否認性機制

當更新 PKC 憑證註銷資訊後，使用者就可以藉由下載後的資料作數位簽章確認動作。這樣的方法需要確認網路連接來源的合法性與提出資料庫需求來確認使用者是否有此權限來執行更新 CRL 下載動作，但這還是無法確認提供訊息服務的來源者。因為使用者收到 PKC 內含來源者公開金鑰，卻無法得知是否真為其人所產生的訊息。有可能

別人冒用訊息來源者送出後讓所有使用者使用。因為訊息是可以被攔截與複製的，唯有將資料傳輸加密加上數位簽核文件與如同商業機密傳輸資料保護才可阻絕與確認其訊息來源的真確性。除此以外，針對訊息傳輸的保密性還可加上時間戳記方法，可保證所接收的資料同步性無誤。

第四章 CRL 的定期發行機制

4.1 CRL 的定期發行機制簡介

目前現存已被採用標準中，CRL 是廣為被接受的模式之一。而對其基本架構而言，又分為許多不同的運作方式。CRL 需要定期發佈其含有 CRL 資料結構，而對憑證發佈者而言，也需具備時戳服務與數位簽章的需求。另一方面，其他信賴第三方也需提供憑證註銷服務來發佈與簽發 CRL。一般而言，一份 CRL 會依照 X.500 目錄服務標準發佈，並且儲存憑證於特定 CA 網域中。

定期發佈機制必須取決於信賴方實際營運需求，並與憑證政策結合。發佈的通訊協定需顧及 CRL 本身維護的完整性，只要取得憑證註銷資訊，而不需引用憑證簽發與傳輸機制。

目前在 1998 年 X.509 標準中已經定義出兩種 CRL 版本標準。而在 RFC2459 的文件中，也記載數種已經被開發出來，可供特殊用途需求的方式來提供使用者實作使用。而本論文章節中，探討的不同定期發佈機制並不侷限於 RFC2459，主要是將目前所收集到的各種方式作探討與比較。

4.2 不同 CRL 的定期發行機制簡介

目前所使用的 CRL 定期發行機制，主要為了能有效率與正確地讓使用者驗證憑證的合法性。其實際應用方式也十分彈性化，主要原因是在於應用擴充欄內容可多樣化混合使用，而不同定期發行機制可以加以改善原本處理上不敷使用之處，即可達到因

時因地不同需求的定期發行機制用途。

為了能更具系統性的介紹各種不同 CRL 定期發行機制，將所有 CRL 定期發行機制依照其原理與特性概分為以下四類：

減少資料量：將 CRL 所需傳送的資料量利用其新舊版本的差異特性，僅傳送使用者所需的 CRL 更新資料部份。屬於此類的定期發行機制有差異式憑證註銷清單與更新憑證註銷清單。

改善階層架構：透過 CA 分層傳輸模式減少在網路傳輸的負荷。屬於此類的定期發行機制為憑證授權註銷清單。

資料叢集特性：將 CRL 儲存資料庫以叢集或資料切割方式，達到資源與網路負載分散目的。屬於此類定期發行機制為憑證註銷清單分配點、導向式證註銷清單、間接式憑證註銷清單。

搜尋法則：利用特殊運算法則，將 CRL 資料可以到特定儲存點迅速找到所需資料。一般而言，此類需先將資料事先經樹狀分類後才可使用。屬於此類的為憑證註銷樹。

基本而言，每種 CRL 定期發行機制並非互斥，大部份在實際應用時是可以交互使用。使用狀況端賴當時環境而定。

4.2.1 完整的憑證註銷清單(Complete Certificate Revocation Lists，CRLs)

此方式為最初始 CRL 發佈方式，其完整憑證註銷清單需將其所涵蓋領域的註銷憑證完整列出才能使用。此方式在未來延展性問題會有疑慮，因為其資料量會不斷增加，對其不斷新增的憑證註銷清單資料量會導致執行效率降低，造成無法被接受的後

果。另外，在發佈憑證註銷資訊的即時性也會影響憑證檢驗的正確性。

以現有技術而言，完整憑證註銷清單定期發行機制，將所有憑證註銷資訊結合一個特定的 CA 管轄領域發佈一份憑證註銷清單，其在技術的可行性是沒問題的。然而對完整憑證註銷清單定期發行機制，有兩個主要的評量重點值得去深思其實際使用的問題：

延展性問題使得憑證註銷資訊必須與一份已發給憑證的使用期限共同存在，可想而知完整憑證註銷清單的發行會在一些領域使用上，其資訊量會超乎想像的繁多。雖然對憑證使用者與資料通訊量少的使用範圍是不會造成影響，但如果是憑證使用者多與資料通訊量大則會形成很大負擔。

註銷憑證資訊發佈的即時性會隨著憑證註銷清單資料量不斷增加，導致驗證憑證註銷情單所需時間也會加長。因此，每次持續性下載最新版本資料量大的憑證註銷清單來驗證一份憑證是否有效的方式，將會帶來無法承受的網路資源下降後果。

儘管此方式很難去評估一個 CA 使用範圍內，完整憑證註銷清單發佈的資料量會是多少臨界值的實際數據，但藉由已知的主要可能影響因素儘可能去做的此臨界值的可能落點還是可行的。特別是有多少憑證終端用戶、憑證可能被註銷的數量、發給憑證的有效期限與憑證序號大小也會影響到所發出的憑證註銷清單的使用資料量。

合理性的臨界值若在某種環境中，在當初評估時被低估了。則完整憑證註銷清單發佈是否會因系統無法負荷而作一些選擇上的妥協呢？為了要補救此缺失，引用相關論文所介紹的憑證註銷清單定期發行機制可對完整憑證註銷清單發佈之不足提出更

有效的解決方法。

4.2.2 憑證授權註銷清單(Certification Authority Revocation Lists，CARL)

CARL 也屬於 CRL 的一種，主要是限制使用於 CA 彼此將憑證註銷資訊互傳。使用 CARL 時，是將 CARL 資訊置於發給憑證的資料處理擴充欄位，用來做為 CA 憑證註銷公開金鑰機制的資訊參考依據。

因 CARL 主要是專職於各個 CA 的 CRL 註銷憑證資訊工作，所以 CARL 單並不會針對使用者去控制憑證註銷的工作。換言之，CARL 會依賴憑證發給的分佈點與 CRL 擴充欄的範圍，一起使用完成驗證憑證正確性工作。

實際運作上，目前普遍是被用於上層的 CA 而非底層的 CA 或跨 CA 認證機制，主要架構使用於各 CA 公開金鑰憑證註銷機制。而一份 CARL 發行者為上層的 CA，負責去通知下層的各 CA 憑證註銷的相關資訊；或由憑證核發 CA 透過跨 CA 認證的機制發佈憑證註銷的相關資訊。

另外一種可能的使用方式為非直接 CARL。當驗證一份憑證路徑時，一份有效 CARL 必須能讓在此憑證路徑中的每個 CA 所發出憑證都能得到，但如果是由 CA 自身所簽發的憑證就無法適用。一般而言，如果是 CA 自身所簽發的憑證其註銷機制往往是無法使用一些規定去執行。因此，在 CARL 中所列憑證註銷資訊，基本上只是會少數存在而已，這樣才能將 CARL 所需接收訊息成本降到很低。

對於 CA 憑證的註銷是很少見的。一般而言，一份 CA 憑證會被註銷會是在 CA 已經不再使用、私鑰被破解或是停止使用時才需要用到。並且從樹狀架構來看，任何已

知上層 CA 也會影響到在其下屬所有 CA 的運作。假設在樹狀結構愈上層的 CA 被註銷憑證後，所影響的涵蓋範圍也就越大。如果有跨 CA 認證行為的話，就可透過此機制避免上述的問題。

4.2.3 憑證註銷清單分配點(CRL Distribution Points)

CRL 分配點(又稱為分割式 CRL)可允許一個單獨 CA 發佈其註銷資訊置於多份 CRL 內容中，而此大量 CRL 內容可被分割為數個易於管理小區塊，當需要驗證憑證時，會被指向 CRL 儲存位置區塊即可取得。因此，不需知道目前所使用 CRL 存在於何處就可自動去找尋其所在位置。

在 CRL 擴充欄中，憑證註銷清單分配點是由 id-ce-cRLDistributionPoints[8] 的物件標號碼顯示其支援與否。以下依 ASN.1 的表示法表示其語法：

```
id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::= {id-ce 31}

cRLDistributionPoints ::= CRLDistributionPointsSyntax

CRLDistPointsSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
    distributionPoint   [0] DistributionPointName OPTIONAL,
    reasons             [1] ReasonFlags OPTIONAL,
    cRLIssuer           [2] GeneralName OPTIONAL  }

DistributionPointName ::= CHOICE  {
    fullName                [0] GeneralNames,
```

```
    nameRelativeToCRLIssuer [1] RelativeDistingguishedName  }

ReasonFlags ::= BIT STRING  {
    Unused                  (0),
    KeyCompromise           (1),
    cACompromise            (2),
    affiliationChanged      (3),
    superseded              (4),
    cessationOfOperation    (5),
    certificateHold         (6)  }
```

CRL 分配點允許一個 CA 所管轄區域發佈憑證註銷資訊於多份 CRL 內容。CRL 分配點比完整性憑證註銷清單多了兩個顯著優點：

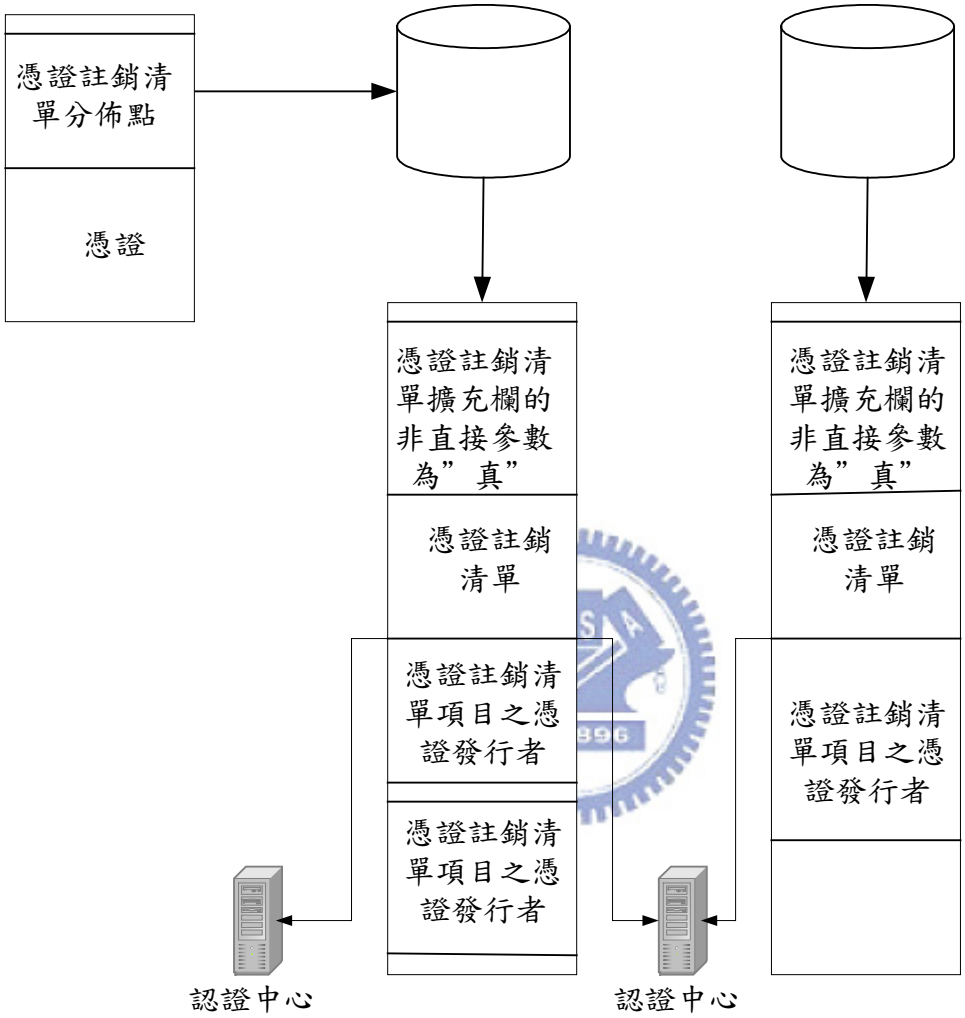
■ 憑證註銷資訊可以在被細分或是分割區塊行程易於管理的小部份，避免產生資料量過大的憑證註銷清單情形。

■ 憑證可指到 CRL 分配點所在處，故信賴團體並不需知道先前特定憑證的憑證註銷資訊置放於何處。

CRL 分配點擴充欄語法反映出驗證憑證所需的相對應 CRL 分割區所在。例如一個 CRL 分配點可藉由網域網路名稱或是網路位置，可鑑別一個特定伺服器的存在與否，然後藉由目錄服務去找尋此伺服器存取憑證註銷清單分割區的位置(見圖 4.1)。

簡單說明，CRL 分配點提供一個比完整性 CRL 更具延展性的架構。當結合適當的

分割機制與快取資料空間就可以減輕效率負荷過重的問題。當使用 CRL 分配點需注意的問題，只是憑證註銷清單分割區需是靜態或是固定的模式。



（圖 4-1）憑證註銷清單分佈點[3]

4.2.4 導向式證註銷清單(Redirect CRLs)

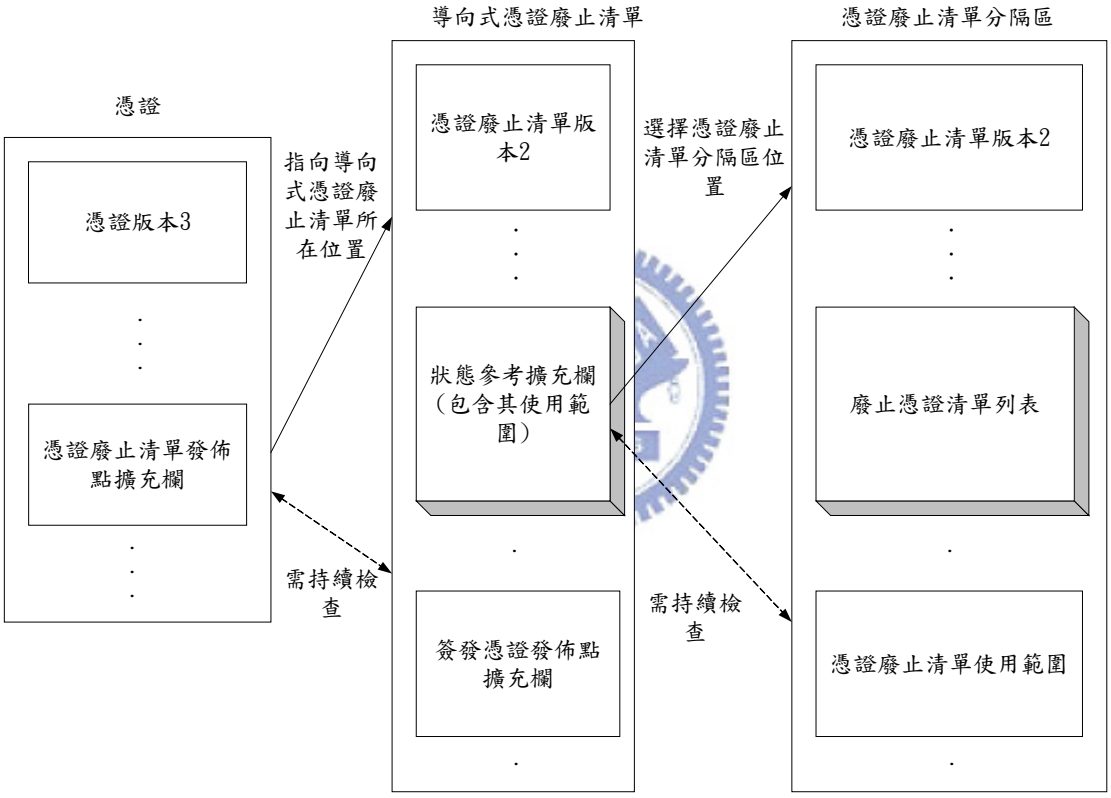
CRL 分割在資料方面是屬於靜態處理,CA 具有事先獲取資訊了解 CRL 要如何被分割與分割的次數，但是不具經常性改變的能力。分割方式可以依照憑證序號的區間、當初被註銷的理由、憑證的類型…等等。對實際運作則，具有較大的彈性化分割能力則越佳，此即為 CRL 分配點運作的基礎所在。

對 CRL 分配點使用性而言，有一項缺點就是一旦互相關聯的憑證被發給，CRL 分配點就會指向 CRL 分割點同時憑證的生命週期也因此被固定了。相對地，CA 需具有事先獲取資訊與了解 CRL 是如何分割與分割的次數的方式，也不能經常性的去改變。但為了要使其更具彈性化，CRL 分割大小與儲存空間區域需常常被改變。例如：為了要符合公開金鑰社群的規格改變，使系統效率更佳的時候，就需調整分割大小與改變架構的實際需求性。

另一方面，分割策略可依憑證序號的區間、當初被註銷理由、憑證類型、節點子數名稱或任何其他 CRL 資訊中可運用來行程區間差異的標準都可拿來使用。所以，定義一份新的 CRL 擴充欄資訊就可以很彈性的達成自動分割區間能力。

因此，為了改良憑證註銷清單分配點的缺點，目前最新 2000 年版 X.509 標準中，IETF 的 PKIX 會員已開始著手制定自動化且具分割能力的標準，而這些概念也會成為未來 CRL 新增功能並加入到狀態參考擴充欄內。狀態參考擴充欄也提供導向能力連結到合適信賴機構的 CRL 位置。換言之，狀態參考擴充欄是可以被指到另一個存有地點含有 CRL 資訊的位置。此中介的 CRL 也被稱為導向式憑證註銷清單。

導向式 CRL 可依現存的標準語協定，將每份 CRL 分割區指到的所在位置。一份導向式 CRL 可使用於指定到多份 CRL 所存放的位置，其概念就如同一個指標陣列一般。當 CRL 資料處理擴充欄的憑證連結到導向式 CRL 時，會依其提供範圍敘述擴充欄內容將其位置指向 CRL 分割區所在位置，找出其憑證註銷的清單內容。CRL 範圍擴充欄語法類於現存的憑證發佈分配點擴充欄語法，只是加入 CA 的名稱、序號的範圍、樹狀架構子署名成限制…等等。



（圖 4-2）導向式憑證註銷憑單[2]

如上圖所示，CRL 分配點憑證擴充欄指到導向式 CRL 所在位置，而導向式 CRL 包含了狀態參考擴充欄並指向含有 CRL 的合適位置。持續性的檢查主要是為了避免有心人士將憑證註銷清單內容修改或者替換等攻擊問題。因此，導向式 CRL 並不會持有註銷憑證的清單內容，只是提供一個中介資訊告知 CRL 存放位置。這樣就可以任意的隨

時修改分割組態也不會影響到現存憑證運作，特別是 CRL 分割設計已經改變了，而憑證的 CRL 分配點並不需改變。

另外，其導向過程也可以反覆的作業。但會帶來導向資訊回覆過多問題，導致添重負荷與降低效率的不良效果。一般而言，最好是間接一層就足夠滿足需求了 CRL 範圍擴充欄的語法與現存的憑證發給分佈點擴充欄語法很類似，只是增加了許多新屬性。其增加屬性如：CA 名稱，不同憑證發給者就需要此資訊提供參考；特殊的區間，例如憑證序號的區間、公開金鑰的鑑定者區間、樹狀架構的子樹名稱…等等。

因此，憑證發給分佈點擴充與 CRL 範圍擴充欄會有使用上重疊問題。例如：兩者都有憑證驗證分佈點名稱、使用者憑證、授權憑證者名稱與代表一些特殊理由的旗標等，可能會導致兩個擴充欄的互相影響。在此情形下，有兩個擴充欄並不會同時一併使用。然而，這是明確的被禁止，因為還需要更多的實際運作模擬才能確認在兩者共同使用下所造成的一致性問題。

4.2.5 更新憑證註銷清單(Freshest CRL)

Freshest CRL 又可稱為 Delta-CRL 的分配點擴充欄，因為它是做為描述 Delta-CRL 如何被取得。為了滿足信賴團體憑證註銷資訊的即時性與經常性更新需求，基於成本與架構上具效率性做法使得 Freshest CRL 可達成上述需求。在信賴團體需要有更具時效性的憑證註銷資訊時，會需要使用最新版本 CRL 內容，但通常是用 Delta-CRL 機制來滿足其最短時間延遲的需求，經由 Freshest CRL 擴充欄位的使用即可完成。在 1999 年 4 月的最終憑證擴充欄報告書中，已經明確加入 Freshest CRL 成為標準之

一。

基礎 CRL 與 Freshest CRL 的不同主要是在於信賴團體在憑證資訊發佈所使用的網路負荷差異程度，針對商業用途上往往需要服務其使用者，若因效率上不佳的狀況，會導致客戶無法即時執行憑證驗證作業，而導致整個系統不具備可用性的後果。CRL 擴充欄中，Freshest CRL 是由 id-ce-freshestCRL[8]的物件標號碼顯示其支援與否。以下依 ASN.1 的表示法表示其語法：

id-ce-freshestCRL OBJECT IDENTIFIER ::= { id-ec 46 }

FreshestCRL ::= CRLDistributionPoints

4.2.6 差異式憑證註銷清單 (Delta-CRL)

Delta-CRL 僅改變憑證註銷清單內容，就可改善即時性問題，而且不因與日漸增的憑證註銷清單資訊導致嚴重影響系統效率，也不需要每次更新就需要產生完整憑證註銷清單資料。實際運作上，Delta-CRL 並不會忽略完整憑證註銷清單的發佈，主要是以先前發佈的一些憑證註銷資訊為基礎，然後將新增憑證註銷部份為其主要內容。

對於 Delta-CRL 而言，資料量小是很容易發佈與處理所內含的資訊，並不會因發佈多份差異式憑證註銷清單而去影響原本現存的基礎憑證註銷清單，其會去檢查憑證註銷資訊並只更新最新差異式憑證註銷清單即可。

CRL 擴充欄中，判斷 Delta-CRL 是否使用是由 id-ce-deltaCRLIndicator OBJECT IDENTIFIER[8]的物件標號碼顯示其支援與否。以下依 ASN.1 的表示法表示其語法：

id-ce-deltaCRLIndicator OBJECT IDENTIFIER ::= { id-ec 27 }

BaseCRLNumber ::= CRLNumber

差異式與間接差異式憑證註銷清單(Delta and Indirect Delta CRLs)

Delta-CRL 的方法是允許漸增式發佈憑證註銷資訊。而 CRL 資訊就可以只針對特定資料位置的 CRL 或者是相對的特定時間點。如果此 Delta-CRL 是參考到基本的 CRL 內容，則會將此兩者資料結合為另一份完整 CRL 資訊後，依照顯示的範圍將目前最新 Delta-CRL 發佈出去。在這種特殊的狀況，Delta-CRL 顯示擴充欄是作為指到基本的 CRL 號碼。另一種作法是將 CRL 範圍擴充欄基本憑證註銷資訊元件使用作為這次 Delta-CRL 的辨別依據。在此種條件下，基本的憑證註銷資訊會參考 Delta-CRL 的一個特殊時間點作更新。這樣就可以選擇要參考或不參考到原來的 CRL 完整範圍，而且也可能參考到另一個 Delta-CRL 內容，如此就可以較彈性運用。但不論是 Delta-CRL 擴充欄或是 CRL 範圍擴充欄基本憑證註銷資訊元件的兩種做法就只有其中一種可以允許使用。

Delta-CRL 剛開始是在 X.509 的 1997 年版本才納入標準，但早期還無法將實作的細節了解清楚。例如：應該要每次將完整 CRL 發佈，然後才將 Delta-CRL 發佈的問題。這就很清楚違背原有 Delta-CRL 目的。較完整版本是在 X.509 的 2000 年版本，將間接 Delta-CRL 加入，而主要目的是將讓這些 CRL 能夠改善其即時性問題不會造成系統效率的減低。

為了描述 Delta-CRL 影響性，先探討一個特殊應用下 Delta-CRL 與完整 CRL 之間的差異。Delta-CRL 基本上是依照先前發佈的憑證註銷資訊，而這些又是參考基本的

CRL 為基礎，故如果沒有基本的 CRL 就沒有 Delta-CRL 的存在。相對地，發佈少量的 Delta-CRL 就比基本式 CRL 更容易作到經常性發佈，因為這不會去影響系統效率，不論是最佳化其完整性與即時性都可以容易達成。

對於產生與發佈多份的 Delta-CRL 相對於基本的 CRL 而言，每個發給 Delta-CRL 會依照先前發佈的 Delta-CRL 內容資訊，找出其憑證註銷資訊的清單，再加上最新被註銷的憑證資料。因此，只需接收最新版本的 Delta-CRL，並不需要去將之前所發的 Delta-CRL 也一併接收。

舉個例子，一家企業因為改善效率的原因，想要每個禮拜去限制其使用完整的 CRL 發佈次數。然而，在內部機密政策考量下，憑證註銷資訊需在八個小時內就將一份憑證的註銷資訊發佈完成，也就是說憑證註銷機制作業不得超過八小時。很顯然地，在效率問題與即時性需求是會與註銷憑證發佈的機制有所衝突。如何在每八小時將基本的 CRL 與 Delta-CRL 的發佈在每個禮拜都能完成呢？方法就是將大量資訊的 CRL 應用在只需去下載並每個禮拜儲存一次，然後相對資料量較小的 Delta-CRL 只需需要時去下載就可以了。

Delta-CRL 可以被儲存直到其使用有效期限已過才不能使用。所以，儲存機制是可以被禁止的，只要 Delta-CRL 在每次使用時，都去更新來確認此憑證的有效性就可以做到，這樣就可以應用於想要即時性取得憑證註銷資訊的零延遲政策狀況下。

假使 Delta-CRL 提供多種方式使用，則一個彼此信賴的團體就可以決定使用不同的方式來滿足實際需求。例如：可由一份發行政策說明中決定，在發佈憑證內容裡面

記載特定的政策識別碼(OID)就可以知道其使用方式。另外，也可經由檢查目前 Freshest CRL 的憑證擴充欄得知。此憑證擴充欄可被使用作為直接指到 Delta-CRL 所在位置，此方式與 CRL 分配點擴充欄指向特定憑證註銷清單的分割區做法類似。

在 X.509 內容裡提及，當 Delta-CRL 是經由目錄服務發佈的時候，傳統上是將此 Delta-CRL 的屬性與 CA 目錄所在位置放在一起。但 Freshest CRL 擴充欄則只會使用於指向 Delta-CRL 清單的所在位置用途。

X.509 的 2000 年版本也有介紹間接式 Delta-CRL 的概念。如同差異式憑證註銷清單，間接式 Delta-CRL 是根據先前發佈的版本資訊作漸進式發佈。主要差異在於間接式 Delta-CRL 可由發行者一次就將數份 CRL 資訊發佈出去。例如：一份間接式 Delta-CRL 可由已知 CA 發佈給所有的 CRL 分配點。另外，也可以一次更新多份 CRL 給很多的發行者。

4.2.7 憑證註銷樹(Certificate Revocation Tree,CRT)

CRT 是由一間公司名稱為 Valicert Essentially 的美國公司所開發的憑證註銷技術，主要是以 Merkle 雜湊樹概念，將現存憑證註銷資訊用樹狀結構的點表示，相關資料可在公開金鑰社群中找到。雖然 CRL 是用來產生 CRT 的主要依據，但 CRT 僅提供定期發佈機制而且並不使用 CRL 的結構。

為了產生雜湊數，每個參與的 CA 必須依照循序方式列出。每個順序表代表著一個使用範圍，對 CA 而言此範圍的較低節點代表憑證註銷的序號，例如下列表示式[2]:

"$CA_1 = CA_n$ and 1138　　X < 2001,"

X 代表由 CA1 所發給的憑證的序號，正在處理進行中

這表示式含有以下幾個意義：

由 CA1 的發給憑證序號 1138 已經被註銷

由 CA1 的發給憑證序號 1139 到 2000 並未被註銷

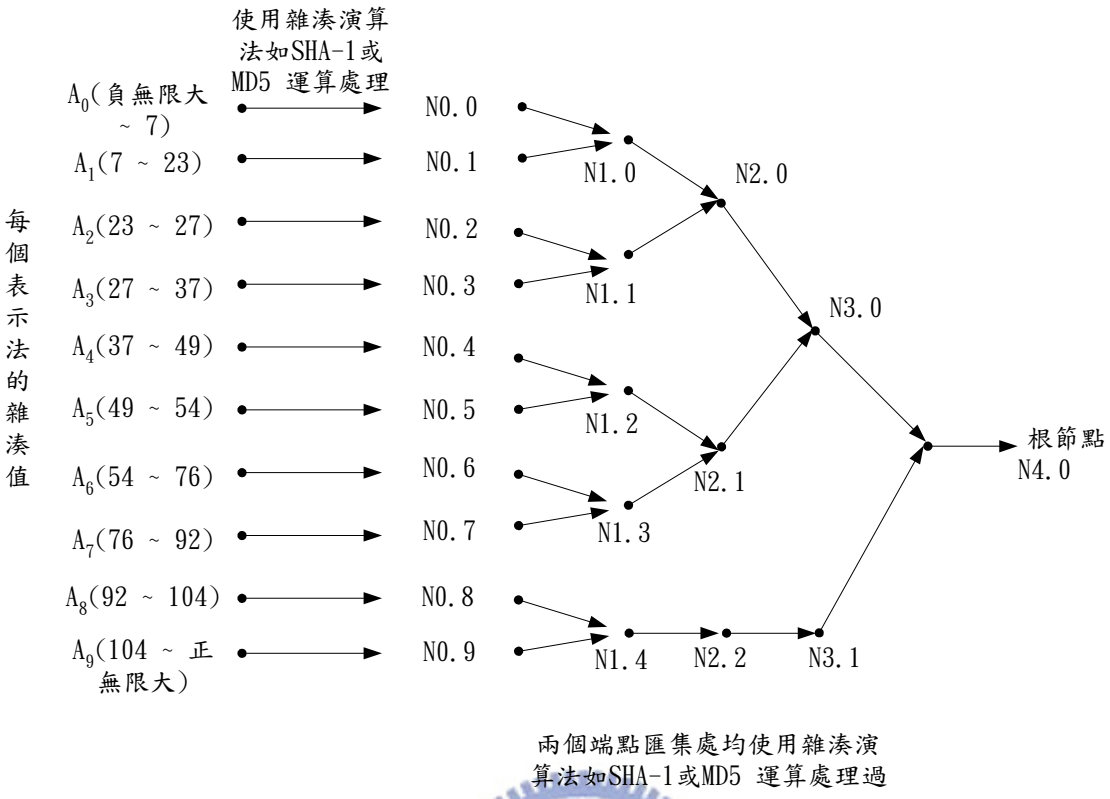
對已知的 CA 而言，此表示式是循序相關的資訊。此數學表示式也代表著所有獨立 CA 都可藉由此雜湊樹得到此認證已經被註銷的資訊。

一個 CRT 範例(圖 4-3)，在最左邊節點代表著已知項目經由一個數學表示式形成雜湊值，然後將這些資料組成樹狀結構圖。在圖中箭頭與每個成對的連接節點組合形成樹狀關係圖，而每個樹狀層的端點經由雜湊法運算後，產生下一個樹狀層的節點，此步驟不斷重複直到最後產生根節點，而此根節點是用來代表樹狀結構的完整性與用來提供驗證憑證用途。

為了決定此憑證是否已經被註銷，信賴團體只需依現有 CA 所發佈的憑證序號經由樹狀架構圖運算，判斷此憑證是否在樹狀圖各節點的定義範圍內。假使有則表示憑證已經被註銷了，反之則憑證未被註銷。這個決策過程是根據比較憑證序號與最接近其序號值數學式計算而得。

此過程的完整性需提供驗證服務才能使用，故信賴團體須重組根節點與比較所核發的根節點值來提供驗證，這需要產生後的樹狀結構提供最接近的憑證序號數值範圍、所有必須支援的節點、所簽發根節點與其時戳資料才能達成此功能。而此資訊是由當時產生樹狀結構的實體，此可能由一個第三方信賴團體的服務或是企業所管理的網域提供服務。此必要資訊可以提供給信賴團體，作為評估自己本身所得資訊或是依賴一個信賴伺服器提供驗證服務。

結合 CRT 最主要是優點可依賴其有效方法去處裡大量憑證註銷資訊。事實上，憑證註銷樹的大小是樹階值 $\log_2 N$，而 N 的值代表註銷憑證數目。



（圖 4-3）CRT 範例圖

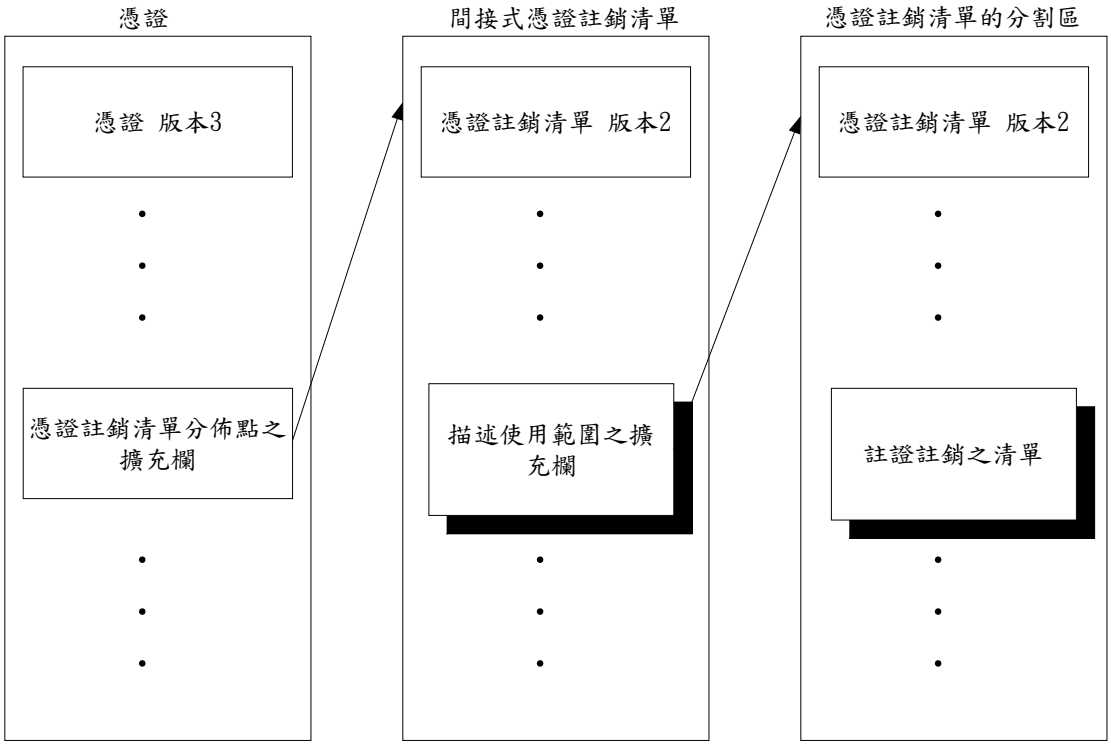
4.2.8 間接式憑證註銷清單(Indirect CRLs)

間接式 CRL 使用於多個 CA 環境，用來提供憑證註銷資訊。不需要去取得很多份 CRL，一份間接式 CRL 就可以滿足需求。一般使用上，會與其他應用程式一起使用。

間接式 CRL 可由許多 CA 中的某個 CA 發佈一份 CRL 來提供憑證註銷資訊即可。間接式 CRL 可用來減低 CA 數量，只需藉由信賴團體得來的憑證驗證流程即可。例如：一個 PKI 所管轄的區域會有數個 CA，且必須要讓信賴團體收取多份從每個 CA 所發佈的 CRL，而此區域為了要改善效率問題，將所管轄區域的憑證註銷資訊都整合到一份間接式 CRL 即可完成。同時對內部管轄區域中，也可運用此機制來降低網路流量與成本。而三方信賴團體也可就由此服務收取費用。在所有的案例中，信賴團體必須信賴間接式 CRL 發行者，同時也要相信所任賴的 CA 所發行之憑證。

對於間接式 CRL 辨認問題，有一種方式可提供確定 CRL 是一個間接式 CRL，只需檢查間接式 CRL 的元件是否存在於 CRL 分配發點擴充欄即可得知。假設其值為真，則 CRL 就含有來自多個來源點的 CRL，而憑證發佈者的元件結合著每個憑證註銷項目來作為判斷發佈者相關訊息。

在實際應用上，間接式 CRL 已被納入 X.509 的 2000 年版本中。間接式 CRL 也支援目前在多個授權範圍內，有不同的 CA 名稱指定在授權名稱元件欄位。標準的 X.509 並不會指出 CRL 是如何在個別的 CA 與核發間接式 CRL 的 CA 傳送的。但對於間接式 CRL 發行者而言，要去對照各個 CA 的不同 CRL 是近乎合理的。這雖對現存標準機制是項問題，但對每個信賴團體都必須下載的對象而言，可以減少 CRL 數量就是一項很好的誘因。合理假設，信賴團體數量往往會超過間接式 CRL 的發行者。而已知優點是考量的一項因素，包含了保證間接式 CRL 並不會變得很大到降低效率，可藉由多個來源點來整合憑證註銷資訊解決。



（圖 4-4）間接式憑證註銷清單[2]

4.3 不同憑證註銷的機制之比較

經由前面章節描述，可以清楚了解憑證註銷可區分為連線與離線模式。連線模式機制為 OCSP 架構，透過即時連線得到憑證驗證的結果；而其他的方式均屬於離線模式，也就是 CRL 定期發行機制的方法。

為了能更清楚了解各個憑證註銷機制差異，可參考以下資料。

憑證註銷機制	一般描述	特性
完整式憑證註銷清單	核發憑證的資料結構已含註銷憑證的清單 定義於 X.509	在系統效率、延展性與即時性方面不是很好。但 X.509 的標準已存在此機制，也是著在系統效率、延展性與即時性尋求改善。
憑證授權註銷清單	一種憑證註銷清單型式僅單獨提供給多個認證中心憑證註銷資訊 定義於 X.509	分離終端使用者認證中心在憑證註銷清單上的處理，可藉由實作準則中發掘相關資訊
改良式憑證註銷清單分配點	一種憑證註銷清單型式僅單獨提供給終端使用者 定義於 X.509	分離終端使用者與認證中心憑證註銷資訊可同時被發現於應用準則
憑證註銷清單分配點	用來指定憑證註銷清單資訊所在點 定義於 X.509	允許憑證註銷資訊被分割為已可易於管理的幾個部分，但一旦被建立後就從此固定
差異式憑證註銷清單與間接式憑證註銷清單	使用於發佈少量憑證註銷資訊與漸進式發佈 定義於 X.509	可用於改善系統效率與支援即時性更新需求。主要用於連接其他形式的憑證註銷清單。例如：憑證註銷清單分配點。
間接式憑證註銷清單	憑證註銷資訊是由多個認證中心只需發佈一份憑證註銷資訊 定義於 X.509	從不同的來源中，收集憑證註銷資訊並予以整合，其效率優於從個別的來源接收資訊的機制，在此狀況下可改善系統效率。
OCSP	提供線上功能用來回應一個或多個憑證的註銷狀態	雖然是設計用來提供即時回覆所需資訊，但最新資訊需依照最後的來源提

	定義於 RFC2560.	供的資訊來源為主。
導向式憑證註銷清單	用於支援自動分割憑證註銷資訊 定義於 X.509	相對其他項目，此概念較新也改善原來憑證註銷清單分配點技術的缺點
憑證註銷樹	允許憑證註銷資訊存在僅用少量資料表示的二元雜湊樹，屬於私人技術由 Valicert 公司所開發	可成為多種選擇的一項不可或缺的技術應用，設計方法是可讓第三方提供憑證註銷服務
非以上所述	既非憑證註銷資訊所需也非此論文所寫的機制，其有可能是由後端的資料庫提供	可經由適當的共同資料來源傳輸驗證憑證所需之授權資料。例如：當銀行的交易行為需仰賴信賴團體提供驗證機制。

表 4-1 憑證註銷設計總結說明[2]

4.4 技術探討改善憑證註銷清單定期發行機制

到底要如何做到真正即時更新憑證註銷清單服務，同時又具備安全性與效率性，這是目前所要追求目標。事實上，這需要考量當時使用環境差異而定，譬如憑證使用者數量、CA 網路架構等都會是考慮的因素，並無法使用一種方式就可以完全滿足。因此必須依使用環境而定。基本上，針對一般企業或具廣大使用者的環境而言，主要方向不外乎是以下幾個重點：

1. 減少資料傳輸量，以便提高網路傳輸效率。
2. 建立有效資料連結，以便提高搜尋效率，減少更新的資料結構時間。
3. 利用分散式系統架構，提高網路傳輸效率。
4. 建立許多資料映射伺服器與高效率壓縮資料程式，減少資料更新時間。
5. 將CA服務的範圍縮小與建立多點CA達到多層式架構,減少集權式CA架構的應用。

第五章 運用 P2P 實現 CRL 定期發行機制

所謂 P2P (Peer-To-Peer，以下簡稱 P2P)其名稱為點對點對等連接技術，與現存的客戶端與伺服端(Client-Server)技術架構最大不同處為 P2P 並不具主控者或是系統管理者的集中權限控管機制，完全屬於分散式網路系統架構，同時擁有網路使用時可扮演客戶端和伺服端的雙重能力，在兩個點與點之間相互依客戶端對伺服端或伺服端對客戶端連線關係做溝通。實際應用上，可在電腦對電腦之間擁有資源相互分享功能，這些資源包括硬碟儲存空間、運算處理能力及網路頻寬等。

5.1 P2P 的特性

P2P 並不代表著一個新技術的誕生也不屬於一種特定技術，而是一種網際網路技術上的特別應用。其原本精神是在於利用使用者相互分享資源的方式，將資源藉著分享而擴大使用範圍與層面。一般的企業體，如善加運用 P2P 技術，就可達成資源分散與共享、協同運作的功能。如果技術供應商應用 P2P 概念在產品上，就可強化其產品的競爭力，並提高顧客價值。

在分散內容管理部份，P2P的角色具備多元性，理想上必須允許以下行為才可維持其分享的精神：

- 如屬於伺服器集中管理型態，分散資源必須提供搜尋的功能。
- 資源管理者藉由分散資源中取得所欲提供的內容索引資訊給各個使用者，則資源擁有者可掌控自身資源，並可以即時改變或更新分享資訊內容。

◆ 使用者身份確認，以便提供相對應的服務機制。

◆ 網路即時內容傳遞必須無法被複製，以免遭受攻擊癱瘓服務。

◆ 可使用資源管理者帳號簽入系統，藉由任意的服務點進入管理模式，修改整個網路服務內容。

◆ 經由使用者個人專屬設定達成客製化介面顯示與服務。

◆ 可自動產生分享資料的描述欄位內容，以便提供搜尋服務。

◆ 對分享資源內容必須要維護其原有的資料內容，不允許有修改情況。

在現實應用面，由於 P2P 服務模式會有所不同，故會有個別不同的差異性產生，但主要的營運模式可由下一章節作分類說明，介紹個別特性之不同與應用領域的差異性。

5.2 五種 P2P 的營運模式

根據 Gerthing Consulting 顧問公司針對 P2P 研究文件[15]提出五種 P2P 營運模式，分別為個人主義、使用者集中、資料集中、Web Mk 2、運算集中與分散處理。以下就簡略以此五種模式分別作說明：

■ 個人主義模式(Atomistic)

個人主義模式的 P2P 方式是最為簡略的技術架構，只需使用者彼此利用已知的網路位置或是使用網路廣播方式就可以找到彼此相互溝通機制。因此，並不需有任何伺服器存在，只要網路頻寬足夠與彼此確認身份與找尋所在位置的機制，就不至於會有任何技術性的問題。

其運作方式是以使用者先送出訊息讓其他使用者得知所在位置，然後彼此間相互確認彼此身份與服務後就可以開始進行資料傳輸。此類的應用最廣為人知的軟體服務是微軟的 Net Meeting 應用程式。

由於個人主義模式是最早期且最為簡單的模式，對使用者而言又沒有任何束縛。因此，可稱得上是完全的 P2P 應用也就是 Client-to-Client 的服務機制，少去中間任何的伺服器負擔。

■ 使用者集中模式(User Centered)

使用者利用第三者單獨或是分散伺服器的目錄管理，進行P2P應用程式集結的網路群。此模式需要使用者先在某一個資料庫中進行目錄登錄後，使用者就可以直接進行與其他使用者的連線動作，進行即時性訊息傳遞。目前此類型應用程式很多，例如ICQ、AOL、MSN Messenger均屬於這種技術。未來此機制真正發揮效用的領域將會是在行動通訊領域。根據Gartner Consulting資料顯示，未來將會以口袋型電腦、PDA與手機為此類服務模式主軸，屆時這類 P2P 機制將會發揮無比威力，也會衝擊現有電信服務業。

■ 資料集中模式 (Data Centered)

此模式的運作模式是將使用者目前資料動態製作成索引資料庫並可自動更新資料，而且也能夠讓其他人可以使用此資料庫索引資料，找到資料所在位置。讓使用者能在連接上網路後可以掃瞄其特定服務或資訊，並將所建立資料索引傳送至某特定主機上，提供他人分享。當使用者離線時，此主機會負責將這些服務或資訊移除掉，以

免造成資料提供點停滯而影響系統效率。

資料集中模式主要是以分享檔案與內容應用為主，此類服務目前頗受使用者青睞，台灣廠商所提供的Ezpeer、Kuro與國外的Donkey、EMule與之前讓智慧財產權成為一個重要的議題的Napster均是運用這種技術。在資料集中模式下，每個使用者皆可以分享自己擁有的資料，但由於目前對資料本身缺乏一套集中管理的機制，因此在某些法律議題仍值得相關單位探討。

■ Web Mk 2

Web Mk 2目標是朝向一個整合所有目前網頁相關技術與架構的應用平台，其中技術部份包含訊息與資料內容傳遞及運算處理等方面。資料瀏覽會加入使用者自行設定的工作管理資料，然後Web Mk 2模式將引領使用者可以應用前述的三種形式的P2P互動架構進入其工作環境中。這當中有許多目錄服務將會整合為一，使用者一次就可以使用所有提供的服務。在目前此類的使用環境，有許多資料索引資料可以被轉換為不同形式資料，不論是在伺服器端的Web、 FTP、應用伺服器或是客戶端系統均可被轉換為共同格式，以便管理工作。

因此，可以想像未來Web Mk 2架構將成為一種需要大量智慧型軟體代理人服務的應用環境，幫助使用者進行資料蒐集與分類整合工作。如果此架構使用於企業界，就可以輔助企業在資訊管理與應用方面擴大其服務層面與品質。例如：應用在客戶關係管理、供應鏈管理、企業內部應用程式整合與產品開發管理等方面都可透過智慧型軟

體代理人的資訊處理能力。不僅如此，使用者對資料權限也可仰賴智慧型軟體代理人作控管工作，達到資料分享與權限控管功能，如此就可將使用層面與範圍擴大。

■ 運算集中與分散處理 (Compute Centered—Distributed Processing)

分散運算處理是屬於P2P在運算處理服務領域的一項服務，主要是為了改善舊式使用單顆大型工作站處理器環境，讓應用程式可以將某個需大量運算處理的任務分配給數個使用者端同時處理。伺服器則負責協調被切割的各個使用者端部份，將各使用者端的運算結果做整合工作。此模式與傳統平行處理運算的主要區別在於每個運算服務端點，在分配網際網路上可以成為一種可彈性與隨機選擇運算服務的端點。

簡略而言，運算集中與分散處理模式皆可透過網際網路連接，利用運算服務端點來降低成本進行分配及執行複雜、非連續性的運算工作，並將運算結果由伺服器整合成為有意義資訊。這類的技術可運用在高科技需要大量運算的領域，IC設計的系統模擬與複雜的密碼學處理均是極佳的應用範例。

在本論文所提出的 PKI 架構運用 P2P 實現 CRL 定期發行機制，主要是探討在資料集中模式與使用者集中模式的結合下，又參雜著部份個人主義模式運作。因此，將此研究的模式稱之為 Web Mk 2 模式。透過前幾章內容包含 PKI、CRL 與 CRL 定期發行機制及本章所介紹的 P2P 機制，經由整體的研究探討之後，提出個人對此主題的技術架構分析與實際運用的做法。在所蒐集到的學術論文中，並無類似與相關的做法。因此，可算是個人的獨創性研究。

5.3 應用 P2P 於 CRL 的定期發行機制

近幾年網路風潮中，繼分散式運算架構的概念推演至資料分散網路架構，主要是在頻寬問題隨著基礎建設更新而推昇整個網路應用的多元化。而 CRL 資訊如果應用於 P2P 機制下，就可以形成許多資料儲存的群聚效應，藉由彼此之間信賴機制與數位簽章驗證之下，就可築構一個可滿足大量憑證註銷資訊傳輸所使用的驗證機制管理平台。

相對於 PKI 原有系統架構而言，P2P 架構具有以下幾種特性：

- 簡化連線手續

簡化網路連線過程。可直接利用網址連線，使用者不需記住連線對方網域名稱，簡化網路設定的繁雜問題。

- 擴散使用範圍

使用者可以與各 CA 直接進行連線。藉由身份確認而相互知道對方在做什麼，不同於只登入一個 CA，只透過網域而導致地域有所限制。

- 立即性更新

因為採直接連線，使用者可以相互進行立即溝通，增加時效性。

- 資料相互分享

透過各 CA 間相互資料分享，減少與 CRL 資料庫伺服器負荷。另一方面，使用者資料下載時可以利用各 CA 提供的下載點選擇可提供下載 CAs 執行更新服務。

- CRL 資料分割

針對下載 CRL 資料檔而言，PKI 架構一般以一份完整的基礎 CRL 或是 Delta-CRL 檔案傳輸處理方式。在 P2P 架構，可藉由檔案分割與重組方式，透過雜湊函數確認檔案的符合性與可用性。

本論文中所提出的方式是以單點對多點的方式做探討，以 CAs 為提供服務點讓使用者可以做下載服務。為何不以多點對多點方式讓 CAs 與各使用者均可相互分享 CRL 更新資料，最主要原因有以下幾點：

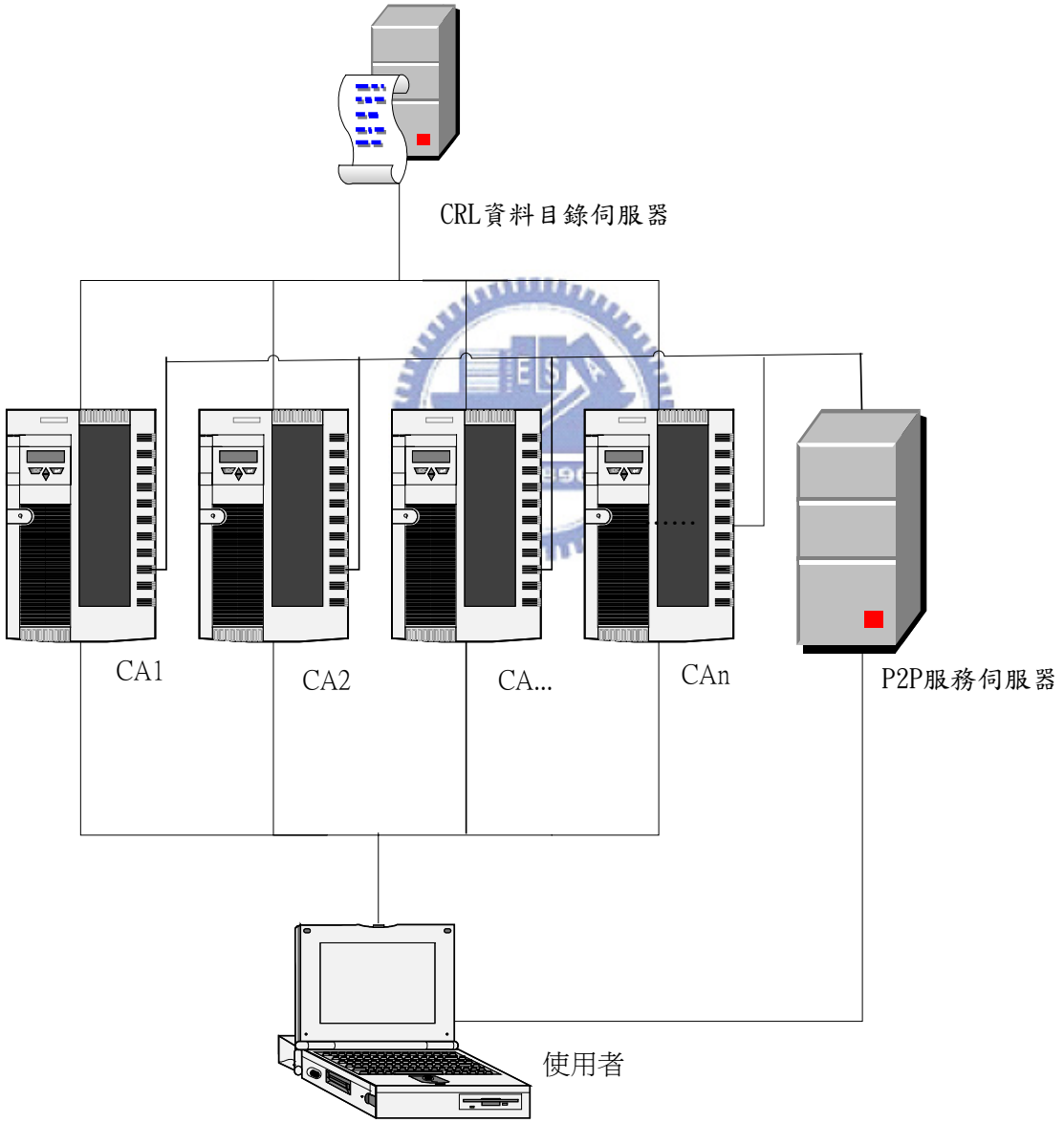
◆ 身份認證問題：使用者對使用者缺乏彼此的身份認證機制。

◆ 網路安全性:無法有效防堵使用者被植入木馬或病毒感染而危害整個網路的使用安全性，藉由 CAs 對簽入系統的使用者身份確認提供下載的服務使主要的系統身份確認的基礎。

◆ 資料的竄改：防止使用者可能意圖修改 CRL 資料與重建雜湊函數，使系統無法完整運作。

5.4 系統架構

上一章節中所提出的各種 CRL 定期發佈機制，每種機制都有其優缺點與適用領域。相對於 P2P 的機制也是相同，首先最大問題會是在於 CRL 資料保存點的互信機制，資料內容是否能一致也需注意。但藉由 PKI 基本元件的輔助與信賴資料傳輸的建立是可以減低其風險性。



（圖 5-1）CRL 定期發行機制結合 P2P 的網路架構示意圖

論文所提出的架構(圖 5-1)屬於結合集中與分散式而成的混合模式。最上層的

CRL 資料庫與各 CA 之間為集中式架構,連接關係為單點對多點方式,此部份類似 CARL 的架構(詳見 4.2.2)。在各 CA 之間與使用者端的關係屬於分散式架構，利用多重連接關係可讓彼此資料傳輸擴散到多點對多點與多點對單點連接,但為了減低系統複雜度與效率、資料一致與儲存風險問題，本論文不探討 CAs 與 CAs 之間資料相互分享功能。

對 P2P 運用而言,可將其架構想像成 CRL 由一些 CAs 形成的一種類似資料快取伺服器(Proxy Server)經由資訊判斷，可以選擇出最接近使用者的服務點或是網路速度較快的 CA，以便提供 CRL 或是 Delta-CRL 下載服務。而這些資料快取伺服器服務的功能均相同，可作到類似 CRL 分配點類似的架構，但卻用有極大的擴充性與可用性的特性。

在最新的 P2P 技術其實際運用技術是將每筆資料均經由編碼後,其編碼數值均具有唯一性，而為了防止資料有下載不完整或是遭竄改之虞，都會提供 CRC 檢驗機制，一旦資料曾經被修改過都會經由驗正之後得知與原來的 CRC 編碼數值不符,而達到資料完整性的功能。

另一方面，資料下載也需經由切割機制而形成類似資料叢集的功能。當一份 CRL 資料被切割成數個小區塊，使用者可以從數個 CA 中詢問哪些是可以提供服務的點後，記錄於本機的資料庫中，待一個或多個 CA 可以提供服務時就可以與其建立下載 CRL 連線,依切割區塊可分成數個部份下載,待下載完成後再整合為一份完整的 CRL，並且將其 CRC 數值與資料作運算確認其完整性即可完成。因此，對大量 CRL 資料運作

上，可以藉由此機制提供更多的下載點與資料分割的多點傳輸解決網路單點瓶頸。詳細說明請參閱 5.4.2 內容說明。

使用 P2P 平台其彈性的選擇性比上一章節所介紹的相關機制更具彈性化。如果是將 CA 的機制轉換成在網域中所有使用者，當獲知有新版 CRL 或 Delta- CRL 已經被發佈後，藉由某些已從 CA 下載完後的使用者點轉而變成可提供憑證註銷資訊下載的服務點，則其他使用者除可使用先前的下載點之外，也可從新的使用者提供的點來下載，就可滿足大量使用者的實際環境需求。但由於管理面的問題，並不建議提供此應用範圍。

實際運作模式中，P2P 有兩項需被提供的服務。首先是需具備管理通訊協定，因為一旦有最新的 CRL 或 Delta-CRL 被發佈後，使用者端需能由此通訊協定獲得告知，然後才開始同步執行最新版本資料下載的工作；另一項是應用程式的開發工作，在論文的 P2P 架構需有的基本元件至少需具備檔案切割與組合的功能外，還必須能夠確認檔案完整性。另外，藉由服務點的最佳化判斷服務可以使整個系統的整體效率提昇，而不會因為某些服務點的網路下載速度或硬體能力不佳而導致系統服務下降的問題。

5.4.1 系統整體架構說明

本論文的系統架構主要是採用智慧型代理人為基礎完成所有的功能服務。所謂智慧型代理人指的就是軟體代理人，主要是為了達成某種功能而設計的一種程式模組或是應用程式，以目前的多層式(Multi-Tier)系統架構或是利用在網際網路的多點式應用大多會利用此類概念，提供給特定的系統服務使用。

智慧型代理人主要可分為兩種：資料型服務模組與常駐型服務模組。在 P2P 網路的程式架構兩者執行的結果是相同的，唯一最大差別是在於其程式碼模組執行的額外負擔與效能而已。

資料型服務模組是指某特殊的程式功能模組與其資料結合，執行電腦與電腦間相互傳遞訊息資料。此類的服務就如同在網路購物商店，例如：使用者在註冊購物網站時必須輸入個人相關資料，包含年齡、性別、工作、喜好運動、閱讀書籍等資料，在下次登入時就會依照使用者行為特性與資料將使用者會感興趣的物品搜尋與分類後，呈現給使用者。

常駐型服務模組是一項存在於使用者本機的一項常駐服務應用程式，使用者會依據當時的需求自行決定服務的項目做為達成某種特殊應用功能需求。例如：使用者可以在此常駐應用程式輸入想要購買的物品或是想要搜尋檔案的名稱，則此常駐服務程式就自行依據這些條件，透過特殊群組網路搜尋，將符合條件的結果呈現給使用者，類似於分散式運算架構的應用。此類的應用有點類似商店銷售員，使用者只需負責提供資料，商店負責提供銷售員。

系統的整體架構(圖 5-2)主要網路資料傳輸與訊息溝通、資料分割與演算法服務均由智慧型代理人程式的概念作構想。此智慧型代理人會在系統啟動時常駐執行各元件所擁有的功能，而此類應用方面的結合在 P2P 的環境是極為契合。由於各元件的智慧型代理人程式其基本功能的相似性頗高，可以利用相同模組的使用節省設計耗損的時間，並簡化不少流程設計。

智慧型代理人在網路的通訊與下載服務通訊協定有以下三類：PKCS#7、PKCS#10 與 SSL。其使用範圍會因所傳送資料而有所區分，但彼此之間可以交互或共同使用。例如：由 CRL 資料目錄伺服器與 CA 的傳遞就可選擇 PKCS#7 與 PKCS#10、PKCS#10 與 SSL 共用均可。

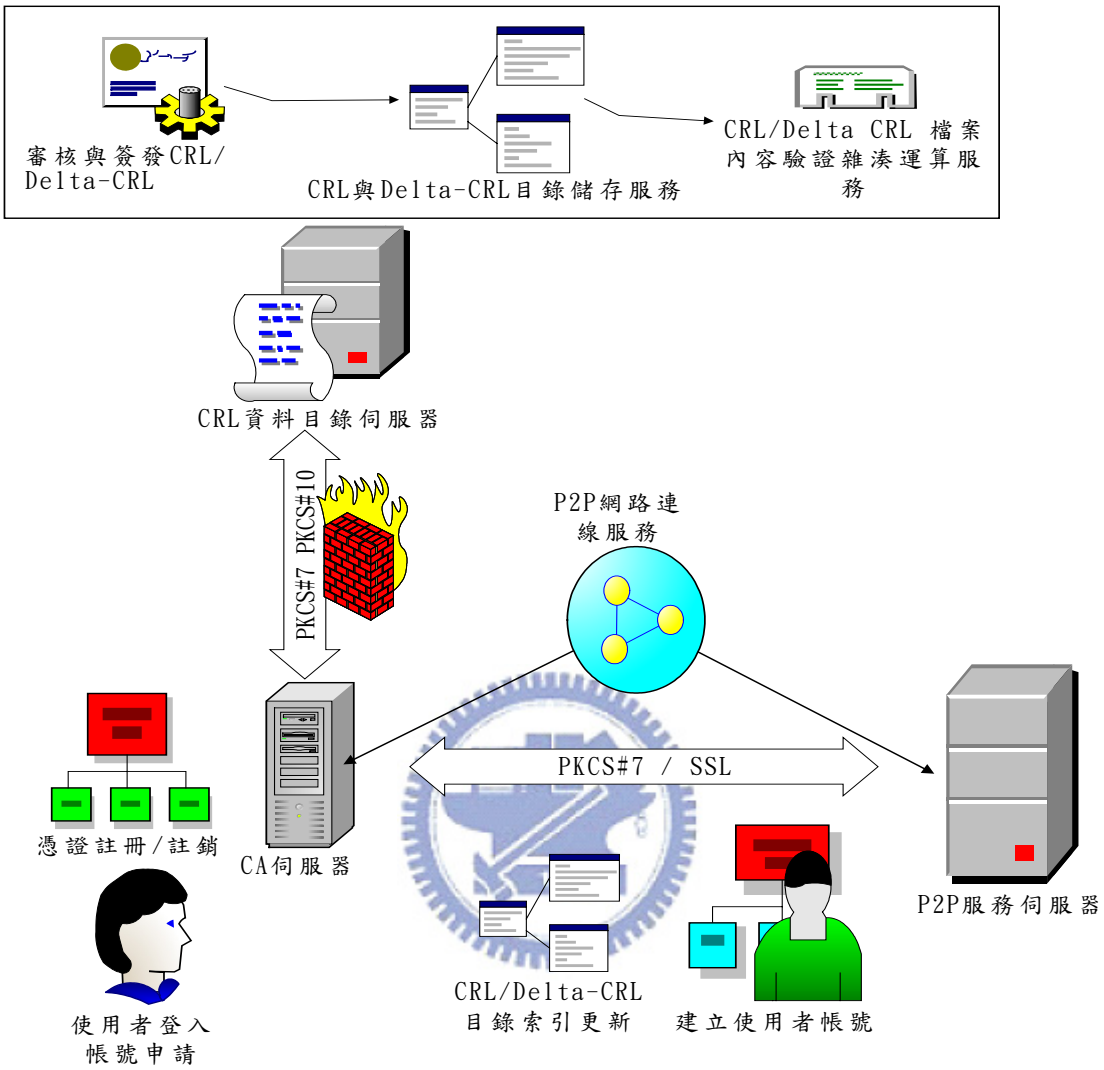
主要元件功能說明：

- CRL 資料目錄伺服器
  - 接收由各下層的 CAs 所傳送之憑證註銷資訊
  - 負責審核與簽發 CRL/Delta-CRL 資料
  - CRL/Delta-CRL 資料經由智慧型代理人程式的雜湊法運算產生雜湊值
  - 將各 CRL/Delta-CRL 資料與雜湊編碼製作 OID 編碼
  - 將所簽發之 CRL/Delta-CRL 資料置於內部的目錄儲存伺服器
  - 提供下層 CAs 下載 CRL/Delta-CRL 與其相對應之雜湊編碼值資料服務
- CA 伺服器
  - 上載所簽發憑證使用者的憑證註銷更新資訊。

- 將CRL資料目錄伺服器下載的CRL/Delta-CRL與其相對應之雜湊編碼值資料的OID作成索引傳送給P2P服務伺服器。
- 系統啟動服務時，P2P服務伺服器與CA的智慧型代理人程式需執行連線服務，並確認其CA的身份與可提供的服務類型。
- 檔案的切割及使用者端的連線服務。
- 將使用者申請的簽入帳號與密碼傳送給P2P服務伺服器。

- P2P服務伺服器
  - 確認使用者身份與其使用權限。
  - 提供使用者檔案資料搜尋與資料更新通知服務。
  - 將目前可提供服務的CAs與其資料連結的資訊傳送給使用者。
  - 建立資料流量過濾器計算CAs的資料流量，以維護網路下載服務品質與系統效率。
  - 建立使用者簽入檔(Log)，以便追蹤系統異常與使用者行為分析。
  - 定時維護與各CA的連結狀況與更新資料。
- 使用者端
  - 使用CA約定的帳號與密碼簽入P2P服務伺服器，也可利用私鑰加密的方式做使用者身份確認。
  - 接收從P2P服務伺服器傳送的更新訊息與資料搜尋結果。
  - 下載各CAs提供的CRL/Delta-CRL與其相對應之雜湊編碼值資料，並將所接

收的資料結合為一個檔案並透過雜湊演算法計算其檔案的正確性。



（圖 5-2）系統網路架構

為了能更清楚了解整個系統架構，以下提供了各元件交互關係的說明。在整體各元件之間的關係架構可概分為三個部份討論，其劃分主要是依照資料管理、安全控管、系統效率影響與資源分享等考量項目為原則，主要概分為 CRL 資料目錄伺服器與 CAs、CAs 與 P2P 服務伺服器及 CAs 與使用者端三個部份，以下就依照這些部份作說明。

- CRL 資料目錄伺服器與 CAs 之間

CRL 資料目錄伺服器儲存 CRL 與 Delta-CRL 的資料，是資料的集散中心。負責與各 CAs 使用 PKCS #7 或 SSL 訊息加密互傳訊息，以便更新憑證註銷的資訊，並透過智慧型代理人將資料同樣以 PKCS #7 或 SSL 加密的方式更新所有的 CAs。

CAs 需負責將所簽發的使用者的最新憑證狀況透過 PKCS #7 傳送訊息與透過智慧型代理人將資料以 SSL 加密的方式傳給 CRL 資料目錄伺服器。

- CAs 與 P2P 服務伺服器之間

CAs 需負責所簽發的使用者憑證狀況更新外，還需提供 CRL 或 Delta-CRL 的下載與資料加密的功能給 P2P 服務伺服器。而此 P2P 下載服務的智慧型代理人必需要滿足以下的需求：

- 將目前所儲存的 CRL 或 Delta-CRL 依據 CRL 資料目錄伺服器所訂的檔案 OID 編碼製作成資料庫索引目錄，傳送給 P2P 服務伺服器。
- 需將所簽發的使用者當初申請所擁有帳號與密碼透過 PKCS #7 傳送給 P2P 服務伺服器，以便未來使用者登入使用。
- 維護與 P2P 服務伺服器之間的通訊連接的工作。

在此部份 P2P 服務伺服器所扮演角色就如同資料集中模式的伺服器一般，需要將目前可提供下載服務的 CAs 連線狀況與掌握所提供的 CRL 或 Delta-CRL 的檔案目錄，以便使用者作搜尋與下載的服務提供。另外，還需依照 CAs 所傳遞的使用者帳號申請決定提供服務與否。

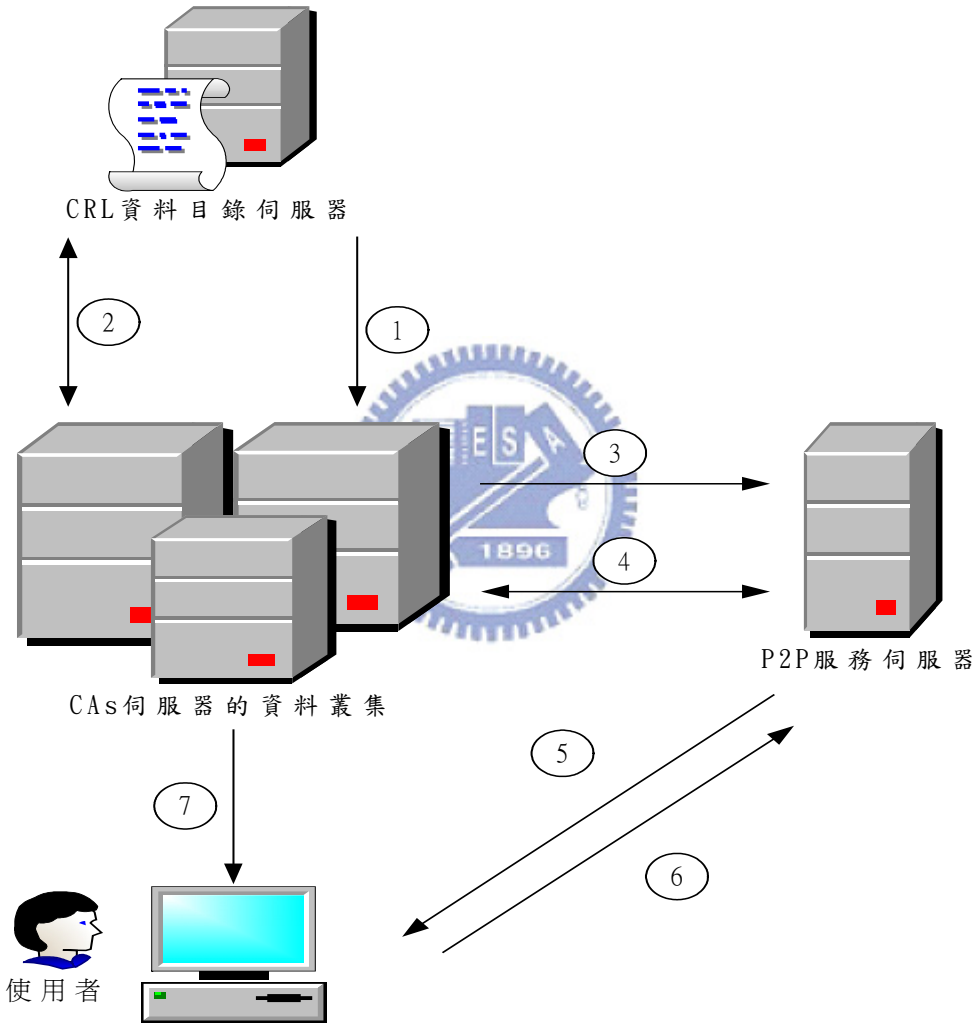
- CAs 與使用者之間

CAs 必需提供使用者下載 CRL 或 Delta-CRL 的資料，透過智慧型代理人加密後傳遞使用者所需的檔案區段給使用者。而在此所指的檔案區段意謂著一份相同的使用者所需的 CRL 或 Delta-CRL 檔案之 OID，透過各 CAs 共同的智慧型代理人切割後，然後由可提供服務的 CAs 提供使用者所需之檔案的某個區段，達成資料分散下載減輕集中方式的負荷狀況。

使用者必須依當初所約定的帳號與密碼透過智慧型代理人連接到 P2P 服務伺服器以確定身份後，使用者本機的智慧型代理人會去依照 CRL 或 Delta-CRL 的 OID 的演算法與規則模式去下載所需的最新 CRL 或 Delta-CRL 的資料。而所接收的資料是屬於區段性的，當檔案下載完成後，智慧型代理人需將檔名與各區段予以整合為一完整檔案。

5.4.2 訊息與傳輸管理機制

在本系統所提供的使用者登入 P2P 服務伺服器的帳號，並不是由使用者自行與 P2P 服務伺服器申請而是以 CAs 所提供的當初約定帳號，主要目的是減少手續的問題之外還有一項更重要的是要與 CAs 所簽發的憑證為訊息加密的依據相結合，增加系統安全性。



（圖 5-3）訊息傳遞與下載服務使用情節說明

為了充分了解整體的訊息傳遞與下載服務的架構，以下依(圖 5-3) 訊息傳遞與下載服務使用情節說明圖利用一份資料從發佈到使用者下載完成的動作依途中所顯示的數字部份說明：

[1]：當 CRL 資料目錄伺服器有更新的資料行為時，需傳遞訊息告知所有的 CAs。

[2]：各 CAs 連結到 CRL 資料目錄伺服器執作訊息溝通與下載動作。

[3]：CA 傳送訊息告知 P2P 服務伺服器資料更新需求。

[4]：P2P 服務伺服器下載目前所指定 CA 提供下載服務的資料索引 v

[5]：P2P 服務伺服器傳送 e-mail 或訊息通知使用者下載。

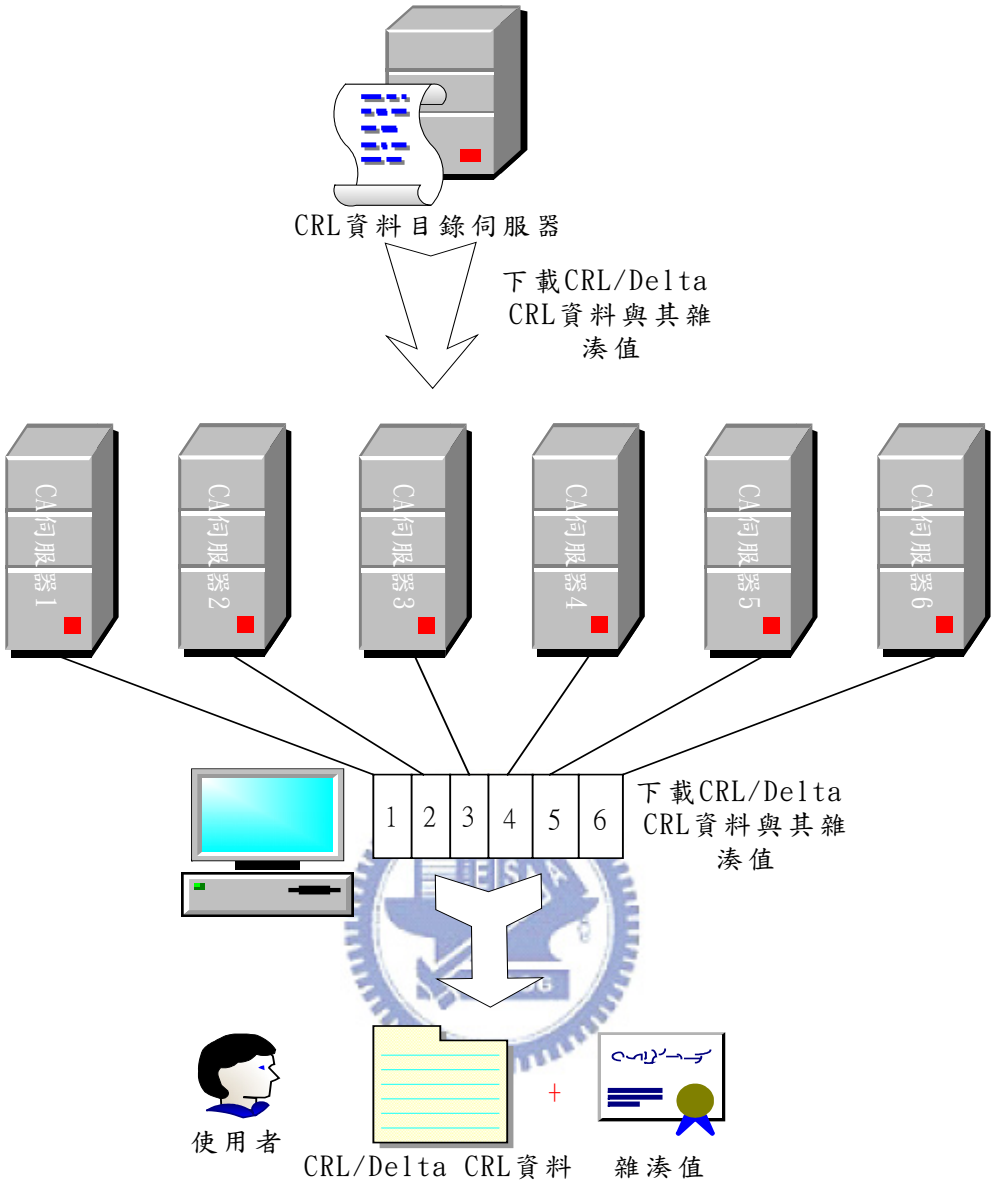
[6]：使用者簽入 P2P 服務伺服器尋找可提供服務的 CAs 下載點。

[7]：執行下載服務的動作。

5.4.3 資料處理流程說明

對資料下載而言，P2P 的傳輸可以將下載資料透過資料連結網路演算法將資料切割成很多小單位後，即可將下載點的資料流量的負荷減低，解決點對點傳輸時的傳輸不對稱的問題。

在本論文架構中，CRL 資料目錄伺服器並不牽涉到資料分割下載的問題。主要是因為要維護資料的機密性、一致性與完整性問題，但因為其所服務點並不是大量的使用者而是 CA 伺服器，並不會有很大的負載與不確定因素。



（圖 5-4）CRL/Delta CRL 資料下載與處理流程

CA 伺服器與使用者端會有資料分割下載處理問題。以下就用 CRL/Delta CRL 資料下載與處理流程圖(圖 5-4)作說明。假設在六個可提供服務的 CA 伺服器與一個使用者使用狀況時，在此時間點有六個資料分割區由上述 CA 伺服器提供下載後即可完成整個資料下載的動作。

當使用者完成每個下載節點的分割資料後，會在其本機的資料暫存位置將資料移至使用者儲存的位置，並與 OID 所對映的檔名作結合，成為完整的檔案。接下的步驟

就是與 CRL 目錄伺服器所產生的檔案雜湊值作運算後，確認檔案是否有經過竄改或破壞。經由以上的行為，使用者即可使用此資料作憑證驗證使用。

5.4.4 使用者權限與資料維護的管理機制

使用者權限的管理是以各 CAs 主導；但真正執行面則由 P2P 服務伺服器負責維護。這樣的好處在於 P2P 服務伺服器可以有更大彈性，不會被整個系統所約束，隨時都可移轉。唯一要做的處理是將 P2P 服務伺服器所提供的智慧型代理人程式移轉到另一台主機；另一方面，向所有 CAs 提出使用者帳號重建的工作就可輕易轉移或增加另一台 P2P 服務伺服器提供給另一族群的其他使用者以為減輕系統負荷。

資料維護管理的工作是由 CRL 資料目錄伺服器主導，負責維護資料的建立與依賴雜湊運算的機制以便建立其資料完整性。當所有使用者或 CAs 收到下載 CRL 或 Delta-CRL 資料時，智慧型代理人需一併將附加的雜湊碼與下載資料內容作確認是否有遭受竄改。另一方面，CAs 需扮演資料更新的角色。當有使用者憑證狀況資料需更新時，需立即將資料傳送給 CRL 資料目錄伺服器。

在資料下載維護如同使用者權限管理一般，若系統負荷過重則可增加下載的 CAs 服務點，只需複製 CAs 的智慧型代理人程式就可完成。實際上，此下載服務的 CAs 並不牽涉到任何憑證的事務與使用者登入帳號，因此以類似 FTP 伺服器看待之。

5.4.5 功能比較

在本 P2P 運用於 CRL 定期發行機制上，不論是彈性度與資料更新能力都遠超過原有的架構，僅是改變技術上的不同與調整系統架構，就可讓整體效能提昇。但更重要的是所有的機制均是使用目前現有的技術即可整合此系統。例如：昇華所提出 P2P 服務的 JXTA[30]技術，其為使用 Java 語言利用其跨平台的特性，可讓 P2P 架構輕易實現於任何系統。而且 JXTA 也是開放軟體，使用者可以輕易的附加所需的功能就可解決基本元件與執行平台等問題。

但並非此應用為完全達到零缺點。與之前提及的問題一樣，使用者仍需儲存所有的 CRL 與 Delta-CRL 的資料於本機硬體中，以便執行憑證確認的工作。還有使用者的資料保護的問題也是風險之一，但本系統藉由智慧型代理人的角色將系統危害降低到僅使用者資料的風險，若下次更新則智慧型代理人會檢查本機資料更新受危害的資料。

5.5 應用 JXTA 平台於系統架構

JXTA[29]是由昇陽微系統(Sun MicroSystem)公司所提出的一種開放原始碼系統架構，主要是應用於 P2P 的相關環境為主。在其實際應用方面，目前已經有許多以其為開發平台所架構的應用案例公佈於 JXTA 開放性原始碼社群的相關網站。

JXTA 是希望在集中處理與分散處理間取得最佳平衡點，因為 JXTA 體認到 P2P 網路裡的某些服務，最好還是由某些特定點來執行。而在 P2P 程式應用特性是需要有相對稱的頻寬與相連網路的端點需可動態不連續，主要是在於執行效率與特殊網路連接應用，以便提供點跟點之間溝通管道為考量因素。在這方面 JXTA 提供極佳的彈性，可讓 P2P 的相關應用可依設計者做不同的程式設計與應用。因為 JXTA 可滿足以下三要項：作業系統獨立性、語言獨立性、提供 P2P 應用程式可用的服務和基礎架構，主要的因素就在於 JAVA 可跨平台的特性、XML 的訊息格式與 JXTA 的核心服務平台。

由於大部份 JXTA 程式架構都是分散式的,因此在智慧型代理人的分類通常都會被視為常駐型服務模組(請參閱 5.4.1)。但 JXTA 在系統架構應用方式，也可輕易建立資料型服務模組與常駐型服務模組此兩類智慧型代理人。JXTA 擁有常駐在電腦裡的代理人，彼此溝通需要的所有工具程式，智慧型代理人也可將程式模組和資料移到另一台電腦以操作該電腦上特殊資訊。另一特性是降低頻寬使用率,節省程式碼不需要在網路上傳輸，只有最終運算結果產生後才回傳給原始的運算需求點。

為了讓系統設計者可運用 JXTA 快速的開發相關運用，JXTA 所應用的智慧型代理人可支援以下系統開發優點:

●可應用於完全集中化與分散式的 P2P 應用程式

●在訊息的接收與傳遞即使用者身份認證都需要符合高度安全性的應用

●可支援任何網路協定之間的轉換

●不同研發人員開發的元件可透過 XML 相互溝通不需受平台限制

●程式碼的移植性高可將任意的應用程式在不同機器執行功能複製或取代作用

5.5.1 JXTA 系統架構

JXTA 是屬於多層式系統架構，軟體架構(圖 5-5)可分為以下三層：

- JXTA 應用層

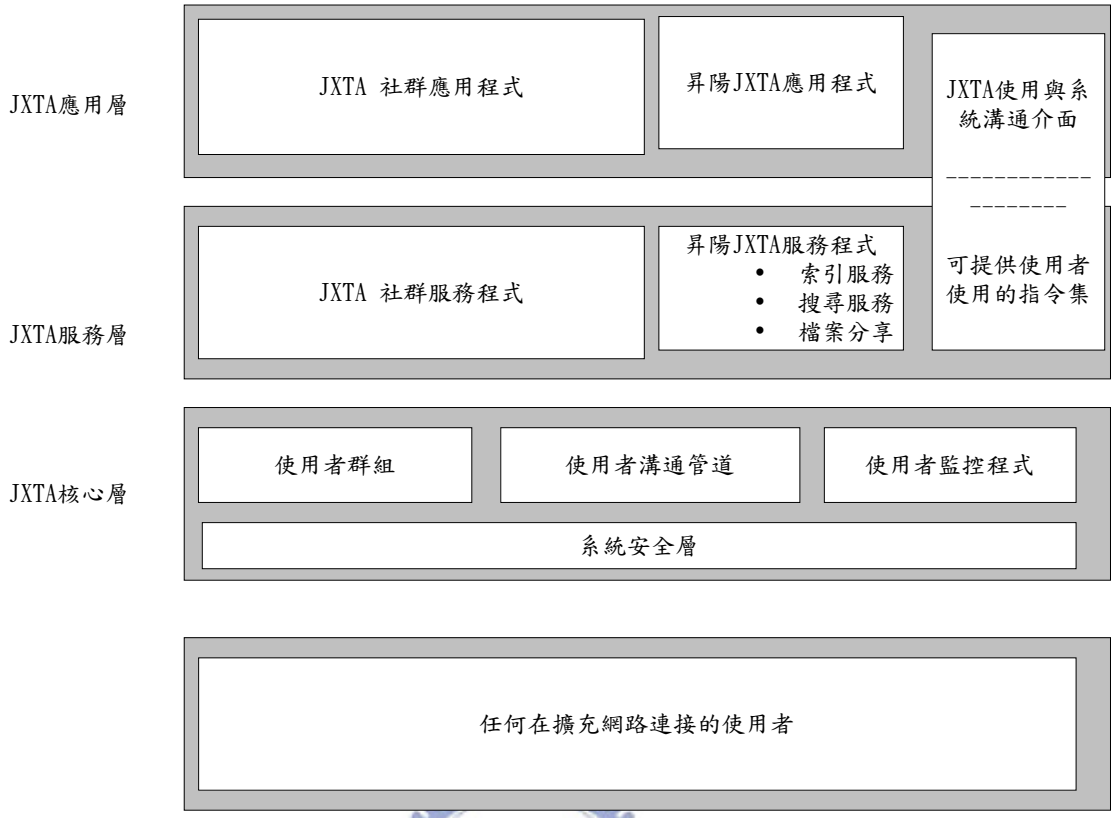
可提供給使用者應用的 JXTA 網路與各種工具程式。例如：立即訊息的傳遞與接收、文件與資源的分享、媒體內容的管理與傳遞、P2P 電子信件系統、分散式拍賣系統…等等。

- JXTA 服務層

提供應用在 JXTA 協定服務的溝通介面。JXTA 本身已提供在 P2P 應用上許多服務如索引、搜尋與檔案分享…等等。其他的服務包含 JXTA 通訊協定轉換、身份確認與 PKI 應用服務元件。另外，還提供給應用層使用與系統溝通介面使用的指令集，可在特殊應用開發時執行一些基本監控功能。

- JXTA 核心層

此核心功能提供最小與必須性的 P2P 網路應用的功能，主要負責提供上層基本服務的基礎。整體而言，核心層包含系統安全、網路連線與流量監控及建立點對點連線等元



件。

（圖 5-5）JXTA 專案軟體架構［30］

JXTA 的網路連結與訊息傳遞的特殊技術:

●某些種類的訊息只會被傳遞有限次數，如此可以避免此訊息傳到所有的點上，大部份的 P2P 應用程式都不需要所有點同時參與。

●點找出的資料會先行暫存在本機端，以排除每次需要資料時都得重查一次的困擾。

●依照資料型別的不同，有些有存活時間屬性以避免網路上累積過多過時的資料，當某個訊息超過它的存活時間，就會被丟棄掉。

●會用具有高度運算能力的點，來減輕低頻寬或運算能力點的工作量，避免這些點的頻寬被佔滿。

●訊息路由採用最聰明的做法進行，以確保以最佳的路徑將資料傳至目的地。

●會根據網路的使用現狀採用最佳的通訊協定，當要在區域網路內傳送訊息時，會以 IP 廣播的方式將訊息傳給每一個點。如跨網域傳送時，則會採用 TCP 或 HTTP 協定[1]來直接通訊。

JXTA 提供一些概念性的目標[29]應用於 P2P 網路連線機制:

●使用群組來組織點，作為服務和應用程式的執行背景。

●群組內使用認證和證書，以提供群組等級的存取權和安全性控管。

●將所有有關點和網路資源的資訊分散到整個網路上。

●將查詢分散到整個系統上。

●提供點和點之間路由和通訊的基礎架構，此目標的關鍵處是要讓位於防火牆或其它障礙物之後的點，也可以正常通訊。

●提供可讓點能監控其它點或資源的機制。

以上的特殊應用就如同 CRL 的網路連線機制中，智慧型代理人所要滿足的使用者權限控管、網路監控與稽核、群組間建立安全連線與 CRL 資料發佈與下載、搜尋 CRL 檔案資料等功能。因此，在 JXTA 所提供的架構來實際應用於本論文的 P2P 實現 CRL 定期發行機制是非常適合的，因為所有需要開發的系統服務、訊息連結部份再加上使用者權限與資源管理…等等，都可以仰賴 JXTA 平台所提供的功能達到快速開發且易

[1]註：HTTP 隧穿(HTTP Tuneling)的技術，能增加程式穿透防火牆的能力，因為一般的防火牆可能會擋住任何其他協定，但很少會擋 HTTP 協定，而且這種技術同時也解決了代理(Proxy)伺服器和 NAT 裝置可能造成的問題。

於維護的目的。

但 JXTA 並非完全滿足本論文架構所需，尚需增加與修改的部分有以下四個項目：

1. 通訊協定

JXTA 的通訊協定主要是以服務為導向，也意謂著需要何種服務就使用 JXTA 的特殊通訊協定。而當特殊服務並不包含於 JXTA 基礎所提供的服務時，設計者就可以自行增加所需服務與相對應的 JXTA 通訊協定。

2. 內容管理與服務

在 CRL 的檔案公佈是採取分層式的架構與 JXTA 原有架構有些略不同，必須將整個流程與服務的客戶端，也就是 JXTA 所稱的會員，都需套用在本論文架構，故修改此項以符合 CRL 內容下載與服務管理所需。

3. 平台安全性

論文架構採用 JXTA 與大部份的應用於 P2P 的環境有所不同，為了點與點網路連線的機密性及與各主要元件相互溝通、CRL 下載、及使用者的不法使用的安全性，需藉由 JXTA 的特殊設計來完成。

另外一項重點是在訊息通訊加密部份，至少訊息加密在架構中所需要能夠支援 PKCS#7、PKCS#10 與 SSL 此三項通訊協定，因此在訊息加密的實作上需要有支援這些通訊協定。

4. 檔案切割、重組與驗證

此部份是 JXTA 尚未提供的部份。但藉由 JXTA 內容管理所提供的檔案處理機制，

加入檔案切割後的多點傳輸與重組檔案的功能後，就可以使用 JXTA 內容管理的驗證機制完成。而這些不含於 JXTA 平台的基本功能，可以使用 JAVA 的其他相關物件。

5.5.2 JXTA 通訊協定

JXTA 所提供的基本通訊協定有七項，這對於本論文架構的應用可直接採用目前所提供通訊協定，達成以下的功能：

●點探索協定(Peer Discovry Protocol, PDP)

當使用者要對 CRL 的檔案作資源搜尋時，必須先探索有那些 CA 服務點目前可以提供下載服務。

●點解決點協定(Peer Resolver Protocol, PRP)

當使用者要對 CRL 檔案作一般的查詢服務時，可以將所需搜尋的條件輸入後，就可以將 P2P 服務伺服器所建立的索引資料依搜尋的條件輸入，提供給使用者端顯示於應用程式。

●點資訊協定(Peer Information Protocol, PIP)

當系統管理者需要去監控目前的伺服器使用狀況時，可透過此協定將目前的網路流量與線上使用者狀況…等等，呈現於所使用的管理者介面。

●點成員資格協定(Peer Membership Protocol, PMP)

當使用者欲簽入 P2P 服務伺服器時，其所需的使用者安全認證機制與其所扮演角色的權限均可透過此協定完成。不論是使用憑證加密或是最基本的使用者帳號與密碼的確認身份在 JXTA 平台均可支援。

●管道繫結協定(Pipe Binding Protocol, PBP)

本論文架構中的主要元件包含 CRL 資料目錄伺服器、CAs、P2P 服務伺服器與使用者之間要做訊息傳送時，此協定可做兩端定址的訊息傳送服務。簡言之，此協定會建立通訊所需的連線與訊息傳輸的機制。

●集結點協定(Rendezous Protocol, RVP)

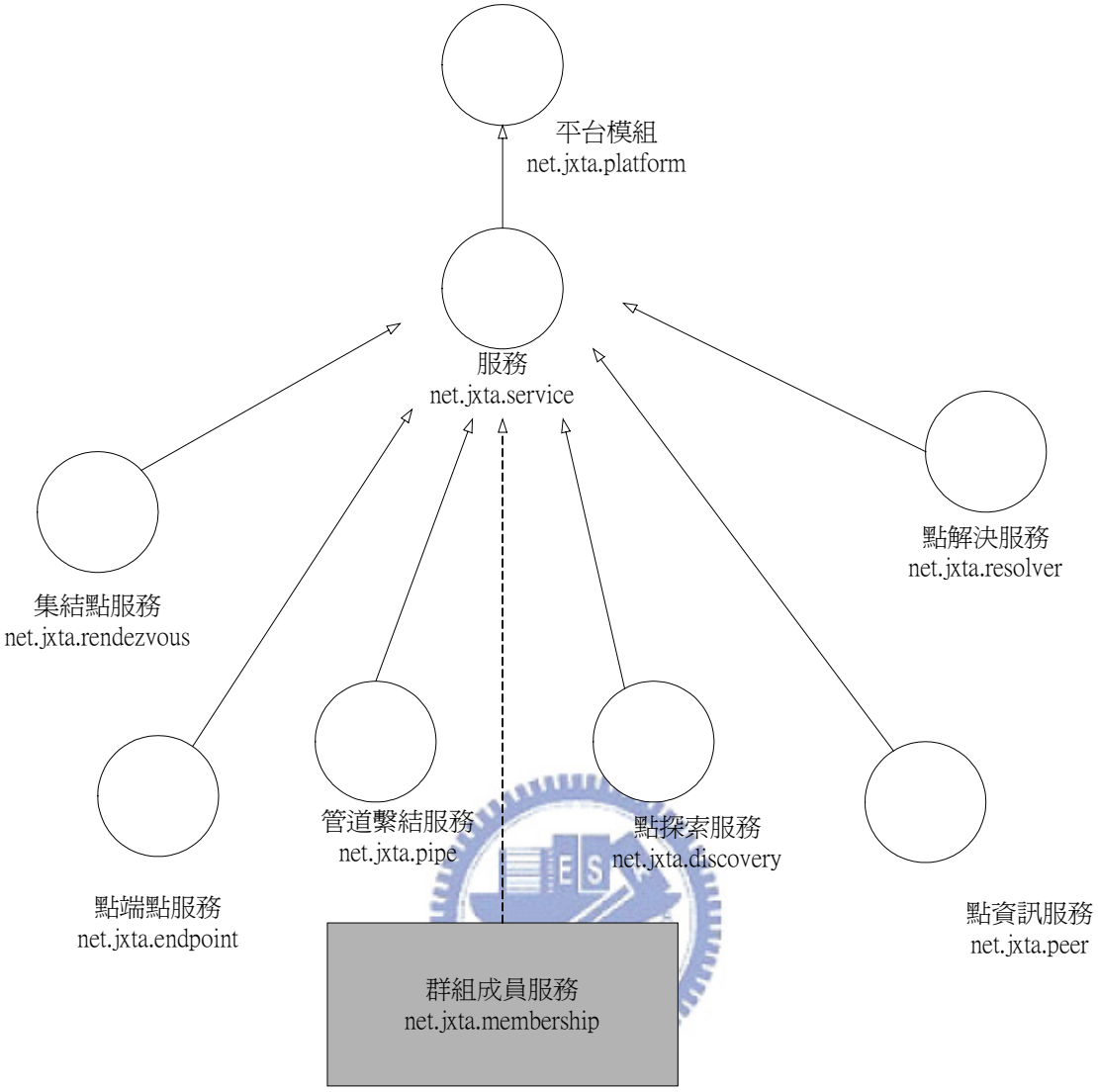
當某一個 CA 的服務啟動或停止時，可透過此協定利用傳播式方式將訊息傳送給所有的元件，通知此 CA 的服務狀態已有更動

●點端點協定(Peer Endpoint Protocol, PEP)

當各元件的網路通訊協定有不同時，此協定將會扮演類似路由器的角色，可轉換不同的 protocol 讓元件間的通訊絲毫不受影響。

上述七項基本通訊協定會形成個別所相對應的物件，並與使用群組成員服務的物件共同匯集於服務物件，而服務物件則向平台模組直接溝通(圖 5-6)。如此的運作是作為分層式連接所需服務的管理作業，而當設計者的應用程式需使要提供何種服務的功能，僅需使用所相應的服務模組並透過其個別服務的通訊協定，即可達成所要的功能。

而若是要將某個檔案的區段作不同的 CAs 的批次傳遞服務時，必須要新增一組服務作此類檔案傳輸的特殊功能。



（圖 5-6）JXTA 服務軟體模組［29］

5.5.3 JXTA 內容管理服務

在 JXTA 的內容管理是以 JXTA CMS(Content Management Service)為功能物件，主要負責提供 JXTA 的點與點之間相互分享與內容交換的基礎架構。使用 CMS 服務可以在多個點之間分享內容,唯一的條件是這些點必須在同一個點群組內。換言之，就是必須透過 JXTA 會員管理物件了解此使用者的角色與權限後，提供其使用的範圍與相對應的服務內容。

JXTA 的資料識別是採用資料真實內容的 128bit MD5 總合檢查碼作為每個內容的

識別字，同時也是獨一無二的內容識別字。對於 CRL 資料目錄伺服器所產生的 CRL 資料內容識別碼 OID 的實際作法是不謀而合，唯一差別的部份會是在對資料的描述與搜尋部份。

內容公告(Content advertisement)在 JXTA 平台主要是使用在提供該資料內容相關的中介資料(metadata)，此中介資料主要是用來描述資料的形態與其相關細節，除可包含文件的識別碼之外，還有以下幾個資料描述欄位:

內容名稱：任何使用者為分享內容所指定的名稱。

內容長度：內容的長度(以位元組為單位)。

Mine 格式：內容的資料格式。

描述：對此資料內容的簡單文字描述。

除以上幾項資料描述欄位，在論文架構還需加入的資料描述欄位如下：

CRL 版本：提供索引與搜尋 CRL 資料使用。

文件切割點：當 CRL 被切割成數個區段時，所需對應資料區段的資料儲存位址。

資料加密識別碼：除 JXTA 所提供的 128bit MD5，如有其他擴充的密碼技術需透過此識別碼作區分。

5.5.4 JXTA 平台安全

JXTA 在平台安全性模組提供以下三項功能：

1. 傳輸層安全協定(Transport Layer Secure, TLS 或稱 SSL V3.1)

主要是以 PKI 技術為其協定基礎，讓 JXTA 有安全通訊的傳輸媒介。在應用程式

中，只要使用安全管道溝通就可以擁有在傳輸層中高安全性傳輸的優點，也因為安全管道是透過傳輸層安全協定做防堵被動式攻擊的侵害，因此可以防止資訊竊聽與流量分析的駭客行為。

2. 點憑證

TLS 層需使用憑證才能啟動功能，故每個點都要扮演 CA 的角色發行各自的 Root CA 憑證，自行執行各自所屬點的支援服務做進行簽章動作，故 Root CA 憑證會隨著所在的點公告散佈出去。因此，每個點都能驗證某個公告其是否正確是由原公告點所發行的。

3. 個人化安全環境

每個點都由一組 ID 和相對應的密碼所保護著，就如同個人化安全的私有金鑰一般，驗證成功後才能進入環境，這是防護本機攻擊的第一道防線。

而對 JXTA 的安全套件是以 JavaCard 2.1 安全物件模型為基礎所設計符合 JXTA 的機密安全相關的物件模型開發工具集，主要會將資料加上數位簽章，其實際做法首先要將要簽章資料計算其雜湊值，然後使用私有金鑰加密此雜湊值最後再將加密過後的資料即數位簽章，做為將來使用於附加文件內供加密用途。

JXTA 相對於論文架構的安全通訊所需，僅提供 SSL 的機制而這只相當於訊息的加密用途。實際上，使用 PKCS#7 與 PKCS#10 除了可提供類似的訊息的加密動作外，運用 PKCS#7 與 PKCS#10 的通訊協定還可做與憑證的整合與標準化的訊息格式。

5.5.5 檔案切割、重組與驗證

JXTA 本身並沒有相當應的檔案切割、重組與驗證功能，但檔案切割的方式是可以使用 JAVA 所提供的相關物件也可完成其功能。例如：java.io 是屬於 JAVA 語言中負責檔案處理或是硬體裝置相關，接近底層服務的物件模組，繼承其物件的 java.io.file 就可以運用於切割與重組的功能。

至於 CRL 的驗證服務，在 JXTA 有提供許多的安全套件可以使用，也包含 JAVA 所提供的 JCE(Java Cryptographic Extension)模組，並還有許多公開原始碼可使用於憑證與訊息傳遞的加解密用途，這對於要實作論文架構有具彈性化的選擇性。

5.6 應用領域

此系統實際的運作方式，基本上是要擁有使用者數眾多與大量 CRL 下載需求為執行平台，若是針對封閉與小型的 PKI 架構則不太適合。因為在 P2P 的環境中，主要是以支援點的數目多寡為考慮的要素，使用者數少或下載的頻率需求不高皆無法呈現其高效率的下載能力，但最主要還是在效率與經濟規模為考量重點。

將 JAVA 的開放原始碼 JXTA 加入於實際的論文系統架構開發平台，其所獲的益處是非常多，包含跨平台特性、原始碼可依實際需求進行修改以符合需求及可進行偵錯的深度更高、完全物件化開發與訊息使用 XML 傳遞可跨平台溝通…等等，都是可以縮短開發時間與簡易維護程式的優點。而對於延展性與移動性而言，也都具有高度支援性，對於未來的效率的調整或系統的變動都具有完整的評估與支援能力。

但此架構並非完全解決 CRL 定期發行機制的所有問題，只是可以應用於解決 CRL 定期發行機制的即時性與資料量大的下載問題，但還無法解決使用者本機儲存資料會與日俱增的問題。另一方面，在不可否認性的問題並不在此架構中有改善的機制，主要因為 P2P 架構特性並不是使用在此的應用。簡言之，藉由 P2P 可提昇整體資料下載的流量問題，而加入智慧型代理人機制則會改善 CRL 定期發行機制的即時性問題，提供類似 OCSP 的憑證驗證機制，並且也改善 OCSP 的部份缺點，譬如相容性與網路頻寬等問題。

相對而言，這些不足之處均可作為未來改善的空間。

第六章 結論與未來發展

6.1 結論

P2P 的應用架構似乎是影響了整個世界的資訊平台。在本論文探討中，似乎體會得到一些未來的發展與應用領域。在憑證驗證處理機制，不論是線上處理的 OCSP 或是離線處理的 CRL 都有系統性的負擔過重的問題產生，而 P2P 即是最佳的解決方式之一。而 OCSP 的即時查詢能力而言，也會被 P2P 加上智慧型代理人的即時處理能力所跟進。因此，可以預想到本論文所提出的方法是可以讓一些目前的系統問題得以改善不少。

另外，在本論文提出的架構隸屬於改良式的 P2P。主要原因有兩點：系統的安全性問題，為了讓系統能夠藉由流量分析與控制使用者的權限達到系統穩定性要求；資料的一致性考量，避免因資料竄改與連結錯誤而導致整體效率下降，更重要的是驗證憑證的資料需顧及安全性。

6.2 未來發展

透過本論文的探討，未來在相關的研究方向是非常寬廣的。因為這是屬於一個新的架構而非針對一項問題所提出的論點述說，所以不論是相關的 P2P 在 PKI 相關的應用系統或是相關智慧型代理人的探討與開發皆是很值得去探討。

再者，如能從簡化系統的通訊協定與比較應用 P2P 的效率提昇則可以更加強化系統的效率與可用性與可行性。目前有許多的開放原始碼的架構已具有此方面的基礎架

構，而且在作業系統方面也提供需許多的 PKI 應用技術於網際網路或企業內部的使用者管理，藉由整合這些功能就可將整體 P2P 應用架構的效率與管理的功能更加強化，就可以擴展此架構的使用領域與應用範圍。

參考文獻

[1] Computer Security Institute, “CSI/FBI COMPUTER CRIME AND SECURITY SURVEY(2003)”, EIGHT ANNUAL http://www.gocsi.com

[2] Carlisle Adams & Steve Lloyd，” Understanding Public-Key Infrastructure Concept, Standards, and Deployment Consideration Second Edition”. Addison Wesley, November 06, 2002

[3] Nash, A., Duane, W., Joseph, C., & Brink, D. (2001). “PKI: Implementing and Management E-Security”, California: Mc-Graw Hill.

[4] W.Rankl & W.Effing.(1999),” Smart Card Handbook Second Edition.” Wiley.

[5] Carl Ellison & Bruce Schneier, “Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure”,2000

[6] Ellison, et al.，(September 1999).” SPKI Certificate Theory” http://www.isi.edu/in-notes/rfc2693.txt

[7] “SPKI/SDSI and the Web of Trust” http://world.std.com/%7Ecme/html/web.html

[8] Russ Housley & Tim Polk, “Planning for PKI”, Wiley

[9] Patrick McDaniel, Sugih Jamin,”Windowed Key Revocation in Public Key Infrastructures”, Electrical Engineering and Computer Science Department University of Michigan, October 12, 1998

[10] 內政部憑證管理中心網站 http://moica.nat.gov.tw/

[11] 微軟資訊網站 http://www.microsoft.com

[12] William Boswell, “Inside Windows® Server 2003”， Addison Wesley

[13] NIST web site，http://csrc.nist.gov

[14] RSA Security Inc. http://www.rsasecurity.com/

[15] Gartner Consulting，” The Emergence of Distributed Content Management and Peer-to-Peer Content Networks Engagement #010022501”，January 2001

[16] Hassan M. Fattah. (2002). “P2P How Peer-to-Peer Technology Is Revolutionizing the Way We Do Business”.

[17] Yoshiki SAMESHIMA and Toshiyuki TSUTSUMI，” Reducing Certificate Revocation and Non-repudiation Service in Public Key Infrastrucatue”， IEC TRANS. FUNCAMENTALS, VOL. E83-A, NO. 7 JULY 2000

[18] Scott Fairbrother，” Certificate Revocation in Public Key Infrastructure”，SAN Inistitute 2001-2002

[19] Andre Arnes and Svin J. Knapskog,” Selecting Revocation Solution for PKI”

[20] D.Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang, “Introducation to Public Key Technology and the Federal PKI Infrastructure”,National Institute of Standards and Technology, 26

Feburary 2001

[21] Japan Network Security Association, “Implementation Problems on PKI”, Information Technology Promotion Agency Japan, Feburary 13,2003

[22] Asa Hagstrom, Christopher J. Michelsen, David Rowe, “Cryptographic Support for Certificate Revocation”, Secure Telecommunication Systems, April 2001

[23] R. Housley, W. Polk, W. Ford, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC3280, Network Working Group, April 2002

[24] W. Polk, R. Housley, L. Bassham, “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC3279, Network Working Group , April 2002

[25] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, RFC3647, Network Working Group, November 2003

[26] M. Myers, C. Adams, D. Solo, D. Kemp, “Internet X.509 Certificate Request Message Format”, RFC2511, Network Working Group, March 1999

[27] M. Myers, X. Liu, J. Schaad, J. Weinstein, “Certificate Management

Messages over CMS”, RFC2797, Network Working Group, April 2000

[28] S. Boeyen, T. Howes, P. Richard, “Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2”, RFC2559, Network Working Group, April 1999

[29] Daniel Brookshier, Darren Govoni, Navaneeth Krishnan, Juan Carlos Soto, “JXTA: JAVA™ P2P Programming”, SAMS Publishing, 2002

[30] “Project JXTA: Java™ Programmer’s Guide”, Sun Microsystems, Inc. ,2001

附 錄

使用Microsoft Server 2003架構PKI應用環境

運用微軟伺服器2003版本(以下簡稱Server 2003)所提供的服務也可作為PKI的開發實作平台，除了可以縮短開發時間與輕鬆部署PKI環境，相關技術的說明文件也較完整。

在網路安全內容的保護而言，Server 2003強化企業系統與網路安全管理。例如：可透過IPSEC加強網路傳輸安全性、網路安全傳輸(SSL)、E-Mail安全傳輸及數位簽章…等等。但這些技術都需憑證才可完成，目前取得憑證的方法比較常見的有兩種：由具公信力的CA所簽發或是企業自己可以建置CA自行管理。若使用前者，可以向網際威信或臺灣網路認證公司類似的公司申請，一般而言需繳交小額的年費；在本論文附錄是以介紹後者為主，藉由熟悉Server 2003的運用建置屬於自己的PKI環境。

現有技術架構簡介

Server 2003提供了對目前PKI現有的標準支援架構。不論是對使用者、電腦主機或是服務程式均可作加密與簽章能力的支援。

根據微軟網站(http://www.microsoft.com)公佈的資訊所描述，其細部的功能特色如以下所列出的要項：

- 可使用智慧卡作機密性登入
- 建立高信賴度與機密性的電子郵件收送功能

- 可將程式碼加以保護

- 互信機制的建立，可使用隨選遠端存取網路資源方式藉著使用者登入與建立互信關係以便利未來使用，此網路機性機制包含遠端網路存取、虛擬私有網路(VPN)與無線網路的認證授權等方式。

- 在可攜式電腦中檔案遭竊取或遺失或是其他的儲存媒體均可提供檔案保護

- 跨網路或應用伺服器的使用者或電腦的存取控制與身份認證

- 提供數位簽章可免於資料遭竄改的保護與附加在資料傳輸保密功能

- 延展性技術可讓數以百萬計的使用者與高儲存量的數位簽章傳輸無虞

憑證服務可透過憑證服務的工具元件和認證管理工具，可用來部署自己的 PKI。透過 PKI，可實作遵循標準的技術，例如智慧卡登入功能、用戶端驗證(透過 Secure Sockets Layer 和 Transport Layer Security)、安全的電子郵件、數位簽章和安全的連線(使用 Internet Protocol 安全性(IPSec))。透過憑證服務即可建立與管理發出與取消 X.509 V3 認證的認證授權。這意味著不需倚賴商業的用戶端驗證服務，但若想使用這些服務的話，可將商業用戶端驗證整合到 PKI 內。

其他功能在 Server 2003 改進的部份包括：

— 註冊增強功能：此功能可讓應用程式預期認證存在，而不需開發另一個註冊處理序。這是為了讓使用者更輕鬆地處理認證而設計的。此功能包括了使用者自動註冊、使用者自動更新、委派註冊和手動認證要求。

— 認證對應：此功能可根據認證鏈結中的任何下層憑證授權，利用目錄服務發行者

可作多對一客戶端憑證的對應於 Secure Sockets Layer/Transport Layer Security (SSL/TLS)加密訊息中。而在之前的 Windows 版本中，只能根據終端認證的直接發行者進行多對一的對應。

— 可編輯的認證範本：此功能可編輯認證範本，也做了一些符合 X.509 標準的變更，以包含部署的相關資訊到認證和認證範本內。

微軟對PKI所提供的技術服務架構

微軟為了讓伺服器能更便利的去處理憑證事務，在Server 2003版本提供了自動註冊的功能，其功能是針對PKI可以用較快速與簡便的方式發佈使用者憑證與帶來應用方面的便利性。藉由此功能可以讓使用者自動註冊相對地就減低PKI在發佈的成本。因此，使用自動註冊的功能，組織機構可以藉由使用者範本版本2的結構去管理憑證的生命週期。這包含：

- 憑證的更新
- 暫停使用憑證
- 一次發佈給許多人憑證的需求

在此，範本指的是憑證的建立計劃。而一個範本可將憑證需求透過CA使用其私密金鑰簽發憑證。例如：一個範本定義了憑證有效時間與憑證持有人姓名。而對微軟的使用者範本版本2則是在Server 2003才提供，主要是比使用者範本版本1更具彈性化與更多的註冊功能提供給企業CA使用。

自動註冊功能主要是結合群組政策設定與使用者範本版本2的基礎發展而來。在

使用自動註冊功能時,憑證需求者也須註冊並且經由認證是否使用者或電腦為Active Directory的一員及是否具有此權限可執行此服務。

如同第3章內容所介紹的，當新的CRL需要被下載時，使用Delta CRL可減少網路流量。而微軟在此版本也提供此CRL定期發佈機制。但使用上有兩項限制須注意：

1. Delta CRL只能由Server 2003單獨發佈而且是企業的CA之一才行。

2. 在客戶端的系統虛限制在Windows XP專業版或較晚發行的版本才能使用Delta CRL確認憑證的有效性。

其他相關憑證技術：

- 認證自動註冊和自動更新
- 支援Windows Installer 數位簽章
- 支援Delta CRL
- 金鑰保存與復原

— 認證自動註冊和自動更新

這些重要的新功能可大幅減少管理 X.509 認證所需的資源數量。

Server 2003 可讓您自動地註冊和部署使用者的認證— 並且當認證過期時，自動更新它們。認證的自動註冊和自動更新可讓您更輕鬆快速地部署智慧卡，並透過自動過期和更新認證，改善無線(IEEE 802.1X) 連線的安全性。

— 支援微軟安裝應用程式的數位簽章功能

數位簽章支援可讓微軟安裝應用程式封裝和外部封包進行數位簽章。如此 IT 管

理員將可提供更安全的微軟安裝應用程式封裝，這對於封裝傳送於網際網路時更為重要。此功能也可讓微軟安裝應用程式封裝採納新的軟體使用限制原則設定，以指定該使用哪些應用程式。

－ 支援 Delta CRL

改善功能使內含的認證伺服器可支援 Delta CRL 與 CRL 可更有效率地發行取消 X.509 認證，並讓使用者更輕鬆地擷取新的認證。因為您現在可指定 CRL 的存放位置，因此可更輕鬆地移動它，以滿足特定的企業和安全性需求。

－ 金鑰保存與復原

金鑰的保存與復原可提供私用金鑰的管理，並在發生終端實體遺失時加以復原。金鑰的保存與復原包含了下列功能：

- 金鑰的保存與復原只需要一個復原代理人員來復原私用金鑰。
- C 語言的應用程式介面和一個 Common Object Model (COM) 物件介面，以供外部開發人員使用。
- 金鑰保存僅適用於企業 CA，並且伺服器執行的是 Server 2003 系列產品。
- 金鑰保存對於使用者、電腦和應用程式都是相同的。執行認證註冊的流程並不需要使用者或管理員介入。
- 金鑰復原則需要由指定的復原代理人員介入，如同檔案系統加密需要一個復原代理人員復原檔案加密金鑰一樣。
- 支援轉換 Exchange 2000 KMS 和 OutlookR *.epf 金鑰儲存格式。
- 支援來自協力廠商的 CA 的外部金鑰契約。

在微軟的 Server 2003 版本提供支援 PKI 相關機制，並且結合了智慧卡的功能使用者將可以更容易管理與發佈及操作。

- 交互認證支援

交互認證只允許附屬的 CA 在其 CA 所簽發的憑證作認證的行為，並且也允許在不同的 CA 階層作信賴關係的建立。交互認證可讓 PKI 的管理作業應具效率性。

- Delta CRL

在微軟的 Server 2003 的憑證伺服器服務支援 Delta CRL，可讓 X.509 憑證的註銷作業更方便。一份 Delta CRL 內容只是憑證的列表清單，代表自上次完整的 CRL 發佈後至今憑證狀態有改變的憑證清冊。這比完整的 CRL 資料小很多並且可以經常更新也不會影響系統與網路效率，細部說明請參考前章節所述。

- 金鑰恢復

有些時後金鑰回復功能是可能需要的。例如：要將資料恢復，就需藉由恢復的金鑰將資料的權限打開。在 Server 2003，CA 可使用私鑰將單獨的憑證取得或是恢復其憑證功能。因此，企業對員工的帳號控管才能作到完整的資源掌握，不會因員工離職或請長假而延宕工作。

- 自動註冊

在Server 2003支援憑證自動註冊與自動更新，可以明顯減少去管理X.509加密憑證的資源浪費。特別是使用智慧卡與無線上網的設備而言，憑證自動無效與自動更新就不需要經常性的人工設定帳號與網路資源。

Server 2003所提供的支援

在微軟伺服器 2000 版本是第一個緊密整合密碼運算工具的首項產品，而本論文附錄所介紹的 Server 2003 則改善這些工具並針對企業使用上的考量作修正。 而新加入的功能包含以下項目：

金鑰的恢復：提供儲存與重新簽發的功能，可防止當使用者的金鑰已經遺失或失效時的補救措施。

提供自動註冊功能：此功能允許使用者由作業環境 Windows XP 或 Server 2003 網域簽入就可簽發使用者憑證。而使用者可使用於此簽證於 EFS、S/MINE 與 IPSec 的用途。如此，就可顯著的改善這些應用方面的複雜程度。

3DES 與 AES 的支援：在 Server 2003 提供的加密功能新加入的有 3DES (Triple-DES) 與進階加密標準(Advanced Encryption Standard，AES)，使系統得以相容於美國政府在個人電腦的密碼學標準規格 FIPS-140。

FIPS 180-2 的支援：在 2002 年 8 月 26 日，國際數標準機構(National Institute of Standard and Technology, 以下簡稱 NIST)所發表的 FIPS 180-2 是一種機密性的雜湊法標準，包含機密性的雜湊運算法的規格 SHA-1，SHA-256，SHA-384 與 SHA-256。而在 2004 年 2 月 25 日新增了另一項雜湊運算法 SHA-224 目的是將雜湊法功能的輸出分開以增進內部運作的能力[13]。

Delta CRLs： 為了避免憑證資料過長與不易管理的 CRL，在最新的標準規格提出定期將以 CRL 格式為基礎的資料發佈出去，稱為 Delta CRLs。發佈 Delta CRLs 時，只

要每次完整的 CRL 內容被修改時，就只需使用較少的網路與客乎端系統的資源即可完成。詳細部分已在第三章有詳盡的說明。

可管理性的憑證範本：Server 2003提供了一種新的範本版本可支援更新憑證的擴充欄，可選擇性的設定其支援的方式。

智慧卡支援的改善：可使用智慧卡經由伺服器支援的遠端簽入的方式，達到使用者身份確認的目的。

CA 根憑證的更新：當驗證一份憑證是由外部的 CA 所簽發的情況時，XP 與 Server 2003 的客戶端將需能自動更新網頁方式取得一份根 CA 的憑證做為檢查用途。這樣即可簡化第三方 PKI 的發佈驗證的問題。

合格的附屬 CA 認證

傳統的 PKI 在應用方面難去擴充，因為組織與組織之間自然會不加以限制去交互認證，而產生問題一些管理問題。Server 2003 利用規格的相容性使其限制交互認證的範圍與憑證型態在外部階層架構信任關係建立的使用。

如何建置PKI系統

在建置PKI系統之前，首先必須要完整的定義一份計劃方案。如果沒有此方案，則很容易在短時間內就會在執行時，發現整個團體缺乏共識與衝突產生，最後參與的人員會感覺所參與的計劃毫無價值，而導致失敗。

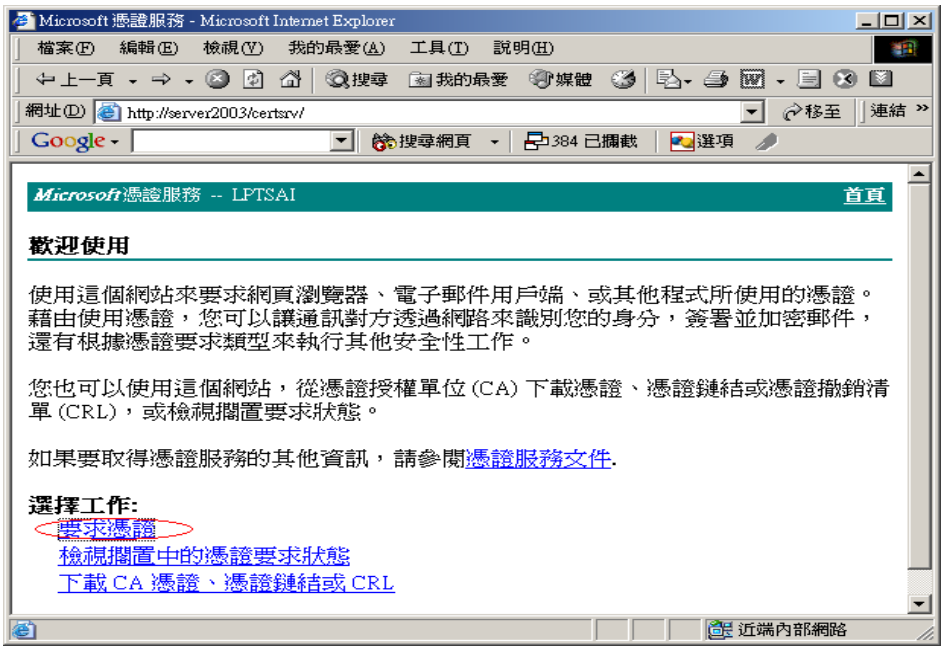
在PKI部署計劃需考量的重點有很多，而且是會因時因地而有所不同。以下舉一個企業的範例提供參考：

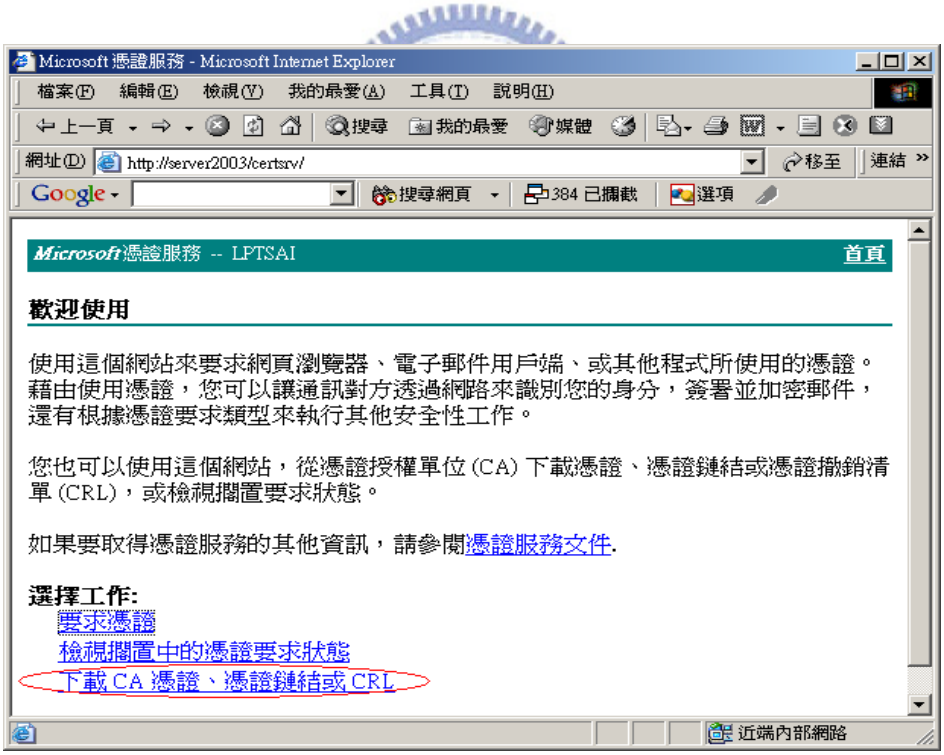
規劃範圍	需考慮的因素
企業需求面	定義應命的需求面 定義完整解決方案的目標 選擇合適的技術 需上層資訊安全的最高主管全力支持
CA需求面	CA 內部的需求面 CA 外部的需求面 內部應用面的互動關係 PKI信賴模式的建立
註冊的政策	建立憑證實作準則 使用者與電腦的註冊分類 憑證使用者的範本 服務層次的需求分析
憑證註銷政策	CRLs，Delta CRL與OCSP 回應的時間延遲容許度 遭受危害的回覆程序的建立

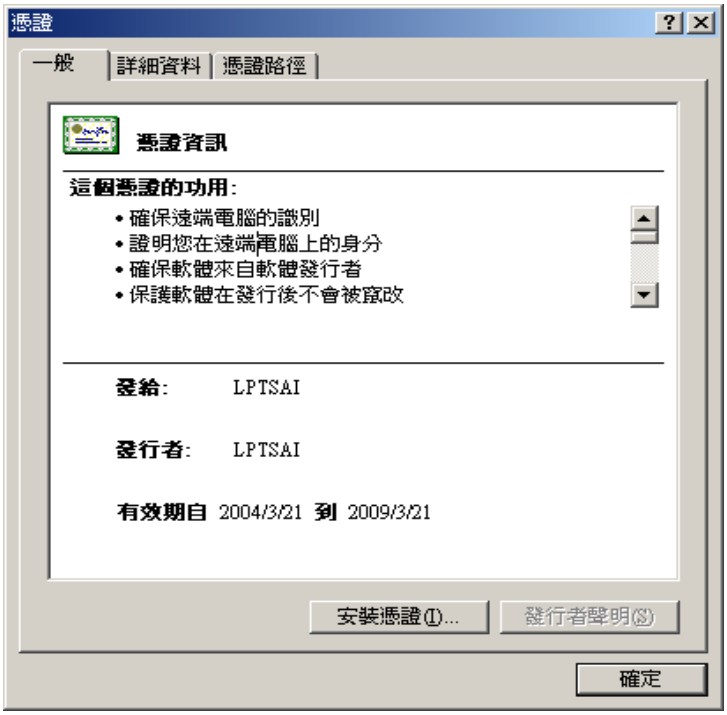
CA的需求面判斷需依據以下幾項要素：

1. 憑證所發佈的數量與分佈的地理環境
2. 在CA與憑證持有者的信任關係建立的需求考量
3. 依不同的憑證實作準則的需求而定
4. 依應用面的技術需求而定
5. 夥伴關係與信賴模式的需求
6. 機密需求、可用性與服務層次來代表其階層架構與CA的位置為何處

應用Server 2003建置PKI系統的實作部份：



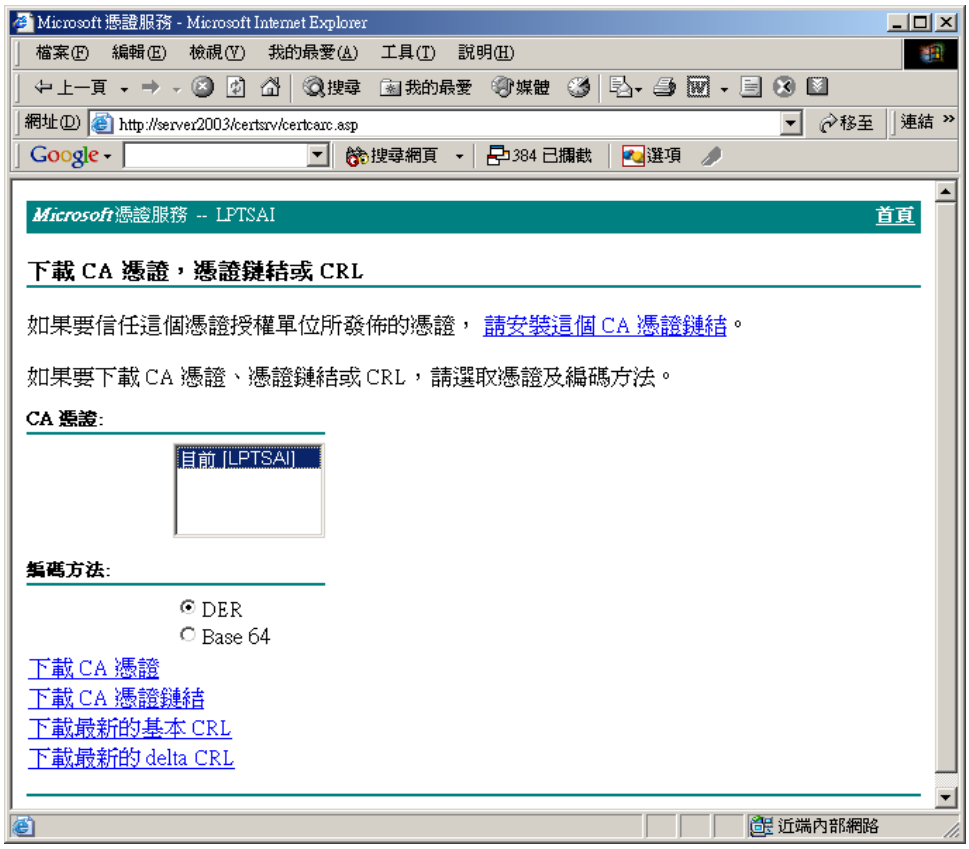




在安裝完CA所發出的憑證後，憑證資訊所定義的憑證的功用為：

- 確保遠端電腦的識別
- 證明您在遠端電腦上的身分
- 確保軟體來自軟體發行者
- 保護軟體在發行後不會被竄改
- 保護電子郵件訊息
- 允許資料以目前的時間來簽署
- 允許您以數位方式簽署憑證信任清單
- 允許在 Internet 上進行安全通訊
- 允許加密磁碟上的資料
- Windows 硬體驅動程式驗證
- Windows 系統元件驗證

- OEM Windows 系統元件驗證
- 內嵌 Windows 系統元件驗證
- Key Pack 授權
- 授權伺服器驗證
- 智慧卡登入
- 數位權利
- 檔案修復



編碼方法分為兩種：DER與BASE64其憑證的內容使用微軟的憑證檢視工具是相同的，但如用其他的工具由於其編碼的格式不相同故所看的資料當然不同。因此，可確定微軟的憑證檢視工具具有支援此兩種編碼格式的解碼功能。

- 下載 CA 憑證鏈結

儲存CA的一份資料再使用者個人目錄，可便利未來對不同的憑證來源共同管理。

- 下載最新的基本 CRL

憑證註銷清單資訊

[版本]　V2

[發行者]　CN = LPTSAI

DC = 2idiots

DC = lp

DC = com

[有效日期] 2004 年 3 月 21 日 上午 01:34:06

[下次更新] 2004 年 3 月 28 日 下午 01:54:06

[簽章演算法] sha1RSA

[授權金鑰識別碼] KeyID=638D 3EEB BF3F D91A 2F5D E7E1 39B6 418F 0BA0 2D7A

[CA 版本] V0.0

[2.5.29.20] 02 01 01　　...

[1.3.6.1.4.1.311.21.4]　17 0D 30 34 30 33 32 37　..040327

31 37 34 34 30 36 5A　　174406Z

[2.5.29.46]

30 81 F5 30 81 F2 A0 81　0..0....

```
EF A0 81 EC 86 81 B0 6C   .......l
64 61 70 3A 2F 2F 2F 43   dap:///C
4E 3D 4C 50 54 53 41 49   N=LPTSAI
2C 43 4E 3D 73 65 72 76   ,CN=serv
65 72 32 30 30 33 2C 43   er2003,C
4E 3D 43 44 50 2C 43 4E   N=CDP,CN
3D 50 75 62 6C 69 63 25   =Public%
32 30 4B 65 79 25 32 30   20Key%20
53 65 72 76 69 63 65 73   Services
2C 43 4E 3D 53 65 72 76   ,CN=Serv
69 63 65 73 2C 43 4E 3D   ices,CN=
43 6F 6E 66 69 67 75 72   Configur
61 74 69 6F 6E 2C 44 43   ation,DC
3D 32 69 64 69 6F 74 73   =2idiots
2C 44 43 3D 6C 70 2C 44   ,DC=lp,D
43 3D 63 6F 6D 3F 64 65   C=com?de
6C 74 61 52 65 76 6F 63   ltaRevoc
61 74 69 6F 6E 4C 69 73   ationLis
74 3F 62 61 73 65 3F 6F   t?base?o
```

```
62 6A 65 63 74 43 6C 61   bjectCla
73 73 3D 63 52 4C 44 69   ss=cRLDi
73 74 72 69 62 75 74 69   stributi
6F 6E 50 6F 69 6E 74 86   onPoint.
37 68 74 74 70 3A 2F 2F   7http://
73 65 72 76 65 72 32 30   server20
30 33 2E 32 69 64 69 6F   03.2idio
74 73 2E 6C 70 2E 63 6F   ts.lp.co
6D 2F 43 65 72 74 45 6E   m/CertEn
72 6F 6C 6C 2F 4C 50 54   roll/LPT
53 41 49 2B 2E 63 72 6C   SAI+.crl
[1.3.6.1.4.1.311.21.14]
30 81 C2 30 81 BF A0 81   0..0....
BC A0 81 B9 86 81 B6 6C   .......l
64 61 70 3A 2F 2F 2F 43   dap:///C
4E 3D 4C 50 54 53 41 49   N=LPTSAI
2C 43 4E 3D 73 65 72 76   ,CN=serv
65 72 32 30 30 33 2C 43   er2003,C
4E 3D 43 44 50 2C 43 4E   N=CDP,CN
```

```
3D 50 75 62 6C 69 63 25   =Public%
32 30 4B 65 79 25 32 30   20Key%20
53 65 72 76 69 63 65 73   Services
2C 43 4E 3D 53 65 72 76   ,CN=Serv
69 63 65 73 2C 43 4E 3D   ices,CN=
43 6F 6E 66 69 67 75 72   Configur
61 74 69 6F 6E 2C 44 43   ation,DC
3D 32 69 64 69 6F 74 73   =2idiots
2C 44 43 3D 6C 70 2C 44   ,DC=lp,D
43 3D 63 6F 6D 3F 63 65   C=com?ce
72 74 69 66 69 63 61 74   rtificat
65 52 65 76 6F 63 61 74   eRevocat
69 6F 6E 4C 69 73 74 3F   ionList?
62 61 73 65 3F 6F 62 6A   base?obj
65 63 74 43 6C 61 73 73   ectClass
3D 63 52 4C 44 69 73 74   =cRLDist
72 69 62 75 74 69 6F 6E   ribution
50 6F 69 6E 74            Point
```

- 下載最新的 Delta CRL

憑證註銷清單資訊

[版本]　V2

[發行者] CN = LPTSAI

DC = 2idiots

DC = lp

DC = com

[有效日期] 2004 年 3 月 26 日 下午 10:51:06

[下次更新]　2004 年 3 月 28 日 上午 11:11:06

[簽章演算法]　sha1RSA

[授權金鑰識別碼] KeyID=638D 3EEB BF3F D91A 2F5D E7E1 39B6 418F 0BA0 2D7A

[CA 版本]　V0.0

[2.5.29.20]　02 01 04　...

[1.3.6.1.4.1.311.21.4]

17 0D 30 34 30 33 32 37　..040327

31 35 30 31 30 36 5A　150106Z

[1.3.6.1.4.1.311.21.14]

30 81 BC 30 81 B9 A0 81　0..0....

B6 A0 81 B3 86 81 B0 6C　.......l

```
64 61 70 3A 2F 2F 2F 43   dap:///C
4E 3D 4C 50 54 53 41 49   N=LPTSAI
2C 43 4E 3D 73 65 72 76   ,CN=serv
65 72 32 30 30 33 2C 43   er2003,C
4E 3D 43 44 50 2C 43 4E   N=CDP,CN
3D 50 75 62 6C 69 63 25   =Public%
32 30 4B 65 79 25 32 30   20Key%20
53 65 72 76 69 63 65 73   Services
2C 43 4E 3D 53 65 72 76   ,CN=Serv
69 63 65 73 2C 43 4E 3D   ices,CN=
43 6F 6E 66 69 67 75 72   Configur
61 74 69 6F 6E 2C 44 43   ation,DC
3D 32 69 64 69 6F 74 73   =2idiots
2C 44 43 3D 6C 70 2C 44   ,DC=lp,D
43 3D 63 6F 6D 3F 64 65   C=com?de
6C 74 61 52 65 76 6F 63   ltaRevoc
61 74 69 6F 6E 4C 69 73   ationLis
74 3F 62 61 73 65 3F 6F   t?base?o
62 6A 65 63 74 43 6C 61   bjectCla
```

```
73 73 3D 63 52 4C 44 69    ss=cRLDi

73 74 72 69 62 75 74 69    stributi

6F 6E 50 6F 69 6E 74       onPoint

[2.5.29.27]

02 01 01                   ...
```