電子商務安全
Secure Electronic Commerce

數位憑證
(Digital Certificate)

992SEC10
TGMXM0A
Fri. 6,7,8 (13:10-16:00) L526

Min-Yuh Day
戴敏育
Assistant Professor
專任助理教授
Dept. of Information Management, Tamkang University
淡江大學 資訊管理學系

http://mail.im.tku.edu.tw/~myday/
2011-05-06

Syllabus

週次	月／日	內容（Subject/Topics
1	100/02/18	電子商務安全課程簡介 (Course Orientation for Secure Electronic Commerce)
2	100/02/25	電子商務概論 (Introduction to E-Commerce)
3	100/03/04	電子市集 (E-Marketplaces)
4	100/03/11	電子商務環境下之零售：產品與服務 (Retailing in Electronic Commerce: Products and Services)
5	100/03/18	網路消費者行為、市場研究與廣告 (Online Consumer Behavior, Market Research, and Advertisement)
6	100/03/25	電子商務 B2B、B2C、C2C (B2B, B2C, C2C E-Commerce)
7	100/04/01	Web 2.0, Social Network, Social Media
8	100/04/08	教學行政觀摩日
9	100/04/15	行動運算與行動商務 (Mobile Computing and Commerce)
10	100/04/22	期中考試週

Syllabus (cont.)

週次	月／日	內容（Subject/Topics
11	100/04/29	電子商務安全 (E-Commerce Security)
12	100/05/06	數位憑證 (Digital Certificate) [Module 4]
13	100/05/13	網路與網站安全 (Network and Website Security)
14	100/05/20	交易安全、系統安全、IC卡安全、電子付款 (Transaction Security, System Security, IC Card Security, Electronic Commerce Payment Systems)
15	100/05/27	行動商務安全 (Mobile Commerce Security)
16	100/06/03	電子金融安全控管機制 (E-Finance Security Control Mechanisms)
17	100/06/10	營運安全管理 (Operation Security Management)
18	100/06/17	期末考試週

教育部顧問室編輯 “電子商務安全”教材

委辦單位：教育部顧問室資通安全聯盟

執行單位：國立台灣科技大學管理學院

Module 4：數位憑證技術

本模組內容係引用台灣科技大學資訊管理所吳宗成教授
之公開金鑰基礎建設課程教材

學習目的

- 公開金鑰基礎建設（PKI）
- PKI技術概觀
- PKI相關安全技術規範與標準
- 憑證管理中心(CA)營運

Module 4: 數位憑證技術

- 4-1: 公開金鑰基礎建設（PKI）
- 4-2: PKI技術概觀
- 4-3: PKI相關安全技術規範與標準
- 4-4: 憑證管理中心(CA)營運
- 參考文獻

Module 4-1:
公開金鑰基礎建設（PKI）

什麼是PKI？(1/3)

- 雖然有數學理論或是長久的實務驗證說明公開金鑰密碼技術的各種演算法已達一定的安全性，然而如果無法確保“通訊雙方能夠正確地取得對方公開金鑰”，則縱使有完美的密碼演算法也是沒有用的

- 在實務上還需要建置一些管理機制、設施、或服務等，以確保可以達到“通訊雙方能夠正確地取得對方公開金鑰”的重要前提

什麼是PKI？(2/3)

- 所謂 “公開金鑰基礎建設”（Public Key Infrastructure，PKI）是一種支持公開金鑰密碼技術正常運作的基礎建設，所謂Infrastructure包含了設備、設施、服務、人員、法律、政策、和規範等

- PKI內含對稱及非對稱性密碼技術、軟體和網路服務的整合技術，主要是用來提供保障網路通訊和企業電子交易的安全

- PKI為一種支援憑證的軟體、標準和協定的安全性整合服務

什麼是PKI？(3/3)

- 狹義的公開金鑰基礎建設是指建置憑證機構提供憑證管理服務

- 廣義的公開金鑰基礎建設則涵蓋任何有助於公開金鑰密碼技術運作的機制或設施，甚至於相關管理措施或法規制度都可以算是公開金鑰基礎建設的一環

- 常見的PKI服務有憑證機構提供的憑證管理服務、憑證路徑建構服務（Certification Path Construction Service）、憑證路徑驗證服務（Certification Path Validation Service）、數位時戳服務（Digital Timestamp Service ）、資料驗證服務（Data Validation and Certification Service）等

什麼是憑證管理中心(CA)？

- 公開金鑰密碼技術的運作是建立在“通訊雙方能夠正確地取得對方公開金鑰”的前提下，否則極有可能使訊息洩漏或收到偽造的訊息而沒查覺

- 必須由通訊雙方都信任的公正第三者經一定的程序，鑑別個體之身分與金鑰對後簽發憑證，證明該個體確實擁有與其所宣稱的公開金鑰相對應之私有金鑰的根據

- 此種憑證稱為公開金鑰憑證（Public-Key Certificate），簡稱憑證（Certificate），而簽發憑證的機構稱為憑證管理中心（Certification Authority，CA）

PKI三大基本架構

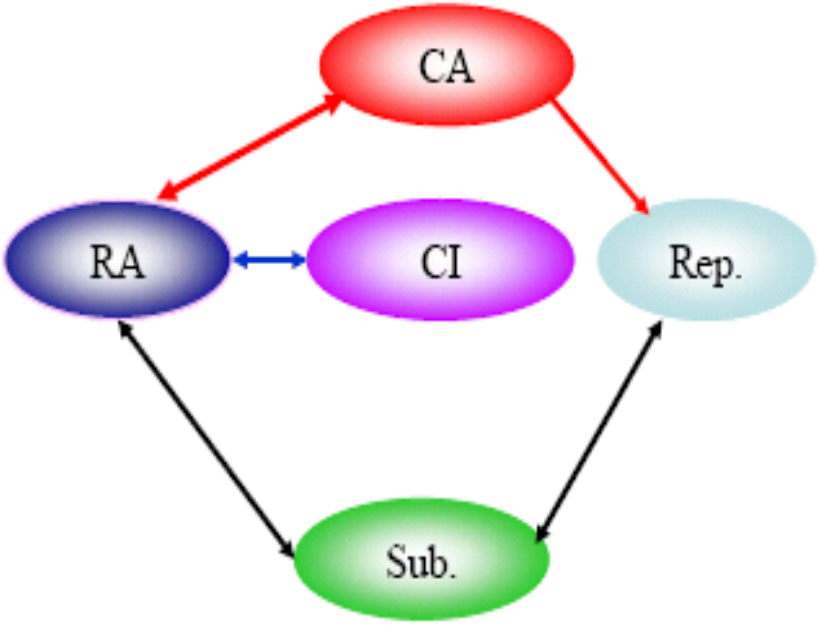
- 單獨集中式機構(single centralized authority)
  - 相當沒有彈性，也不具可劃分等級
- 階層式憑證管理機構(hierarchical structure of certificate management authorities)
  - 具可劃分等級、能夠執行一致的政策、保證PKI內之互通性、可以設立與非PKI使用者互通的政策
- 交互認證的憑證機構之結合(cross-certified CAs)
  - 具可劃分等級與彈性，但難管理，每一個CA皆須能執行與設立與其他CA使用者之互通性

PKI基本參與角色

- 註冊機構 (Organizational Registration Authority, ORA又簡稱RA)：執行使用者或CAs註冊程序的機構，實體及環境設施為安全考量之重點項目
- 憑證機構 (Certificate Authorities, CAs)：PKI架構最底層部分，負責產生及發行憑證，並提供憑證之交互驗證
- 政策認可機構 (Policy Approval Authority, PAA)：依循憑證架構進行CAs的管理
- 目錄服務 (Directory Service, DS)：負責維護憑證資料庫
- 電腦安全物件註冊機構(Computer Security Objects Register, CSOR)：指定物件識別符 (Object Identifiers, OIDs)(包含安全信任等級)，並經由主管單位授權之管理註冊機構分支

PKI的組成單位

觀念澄清：憑證管理中心 (CA)是公開金鑰基礎建設之核心，但**PKI≠CA**，而是**PKI ⊃CA.**



CA：憑證管理中心
RA：註冊中心
CI：憑證發給單位
Sub.：用戶
Rep.：儲存庫

PKI基本參與物件

- 憑證(certificate) -- 對CA的憑證與對使用者的憑證
- 交互憑證對(cross certificate pairs) -- 前向(forward)憑證與逆向(inverse)憑證
- 憑證註銷串列(Certificate Revocation Lists, CRLs) -- X.509 version 3
- 被破解金鑰串列(Compromised Key Lists, CKLs) -- X.509 version 2
- 安全政策(security policies) -- 管理政策(management policy)與技術政策(technical policy)

CA架構

- 階層式架構（Hierarchical）
  - 階層式架構就如同樹狀結構一般，其運作的方式是由一最高層級的Root CA對下一層的CA簽發憑證，再由這第二層CA對第三層CA或是其自身底下的使用者簽發憑證，一層一層的延續，以此類推。
- 網狀式架構（Web）
  - 網狀式架構則是由許多獨立的使用者互簽憑證所形成的一種架構，此架構下使用者一開始只相信自己，因此，若要驗證其他使用者的公開金鑰，則要自行尋找一條相對應的驗證路徑。

CA階層架構

- 最容易瞭解的CA架構，就是階層信任模型，簡單的說，就是下一層的CA須信任上一階層CA。
- CA之間必須信任其所簽署的使用者。
- 圖4-1更清楚地顯示這個模型。

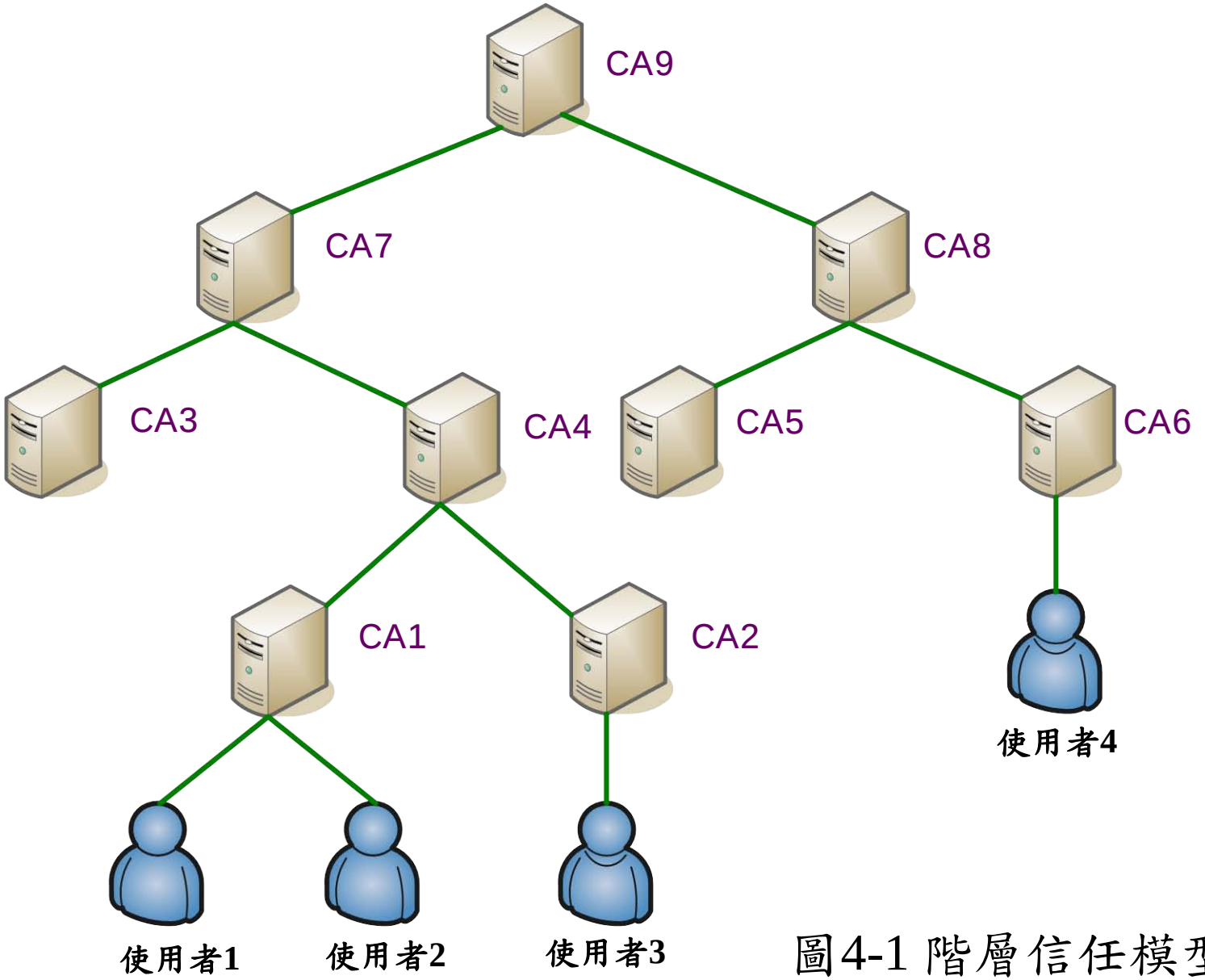


圖4-1 階層信任模型

資料來源:摘自Eric Maiwald：
Network Security: A Beginner's guide

CA階層架構

數位憑證驗證程序

- 如果『使用者1』希望驗證來自『使用者3』的資訊。
- CA1並不認識『使用者3』，因此『使用者2』也是一樣的情形。
- 『使用者1』並不是CA2的下層，所以也就不信任CA2。
- 只能信任上一層就是CA4。『使用者1』會透過CA4驗證來自『使用者3』的資訊，關係如下：

CA階層架構

1. 『使用者1』找尋由CA2發給『使用者3』的憑證。
2. 『使用者1』取得由CA4發給CA2的憑證。
3. 一旦『使用者1』信任CA4之後，就可以利用CA4的公眾金鑰來驗證CA2的憑證。
4. 在驗證CA2的憑證之後，『使用者1』即可驗證『使用者3』的憑證。
5. 在驗證『使用者3』的憑證之後，『使用者1』就可以使用『使用者3』的公眾金鑰來驗證資訊。

CA階層架構

- 階層架構的優點
  - 結構與一般組織單位中的信任關係結構雷同，因此，若組織單位要架設CA，則可輕易的依照原有的組織架構來架設各個層級的CA
  - 認證路徑的搜尋方式較直覺，可降低搜尋時間
- 階層架構的缺點
  - 依照此架構，全世界的CA必需要有一共同的Root CA，這在實際上是不可行的
  - 隨著系統的階層增加，階層的數位憑證驗證的架構也會越來越複雜

CA網狀架構

- 網狀架構模型是由Phil Zimmermann所提出的PGP（Pretty Good Privacy）首先利用這個概念。

- 這個概念所表達的是說，每個使用者驗證自己的憑證，並將這憑證告訴所有與自己相關的人員。

- 認識憑證擁有人的相關人員，則可以自行選擇是否信任這份憑證（詳見圖4-2）。

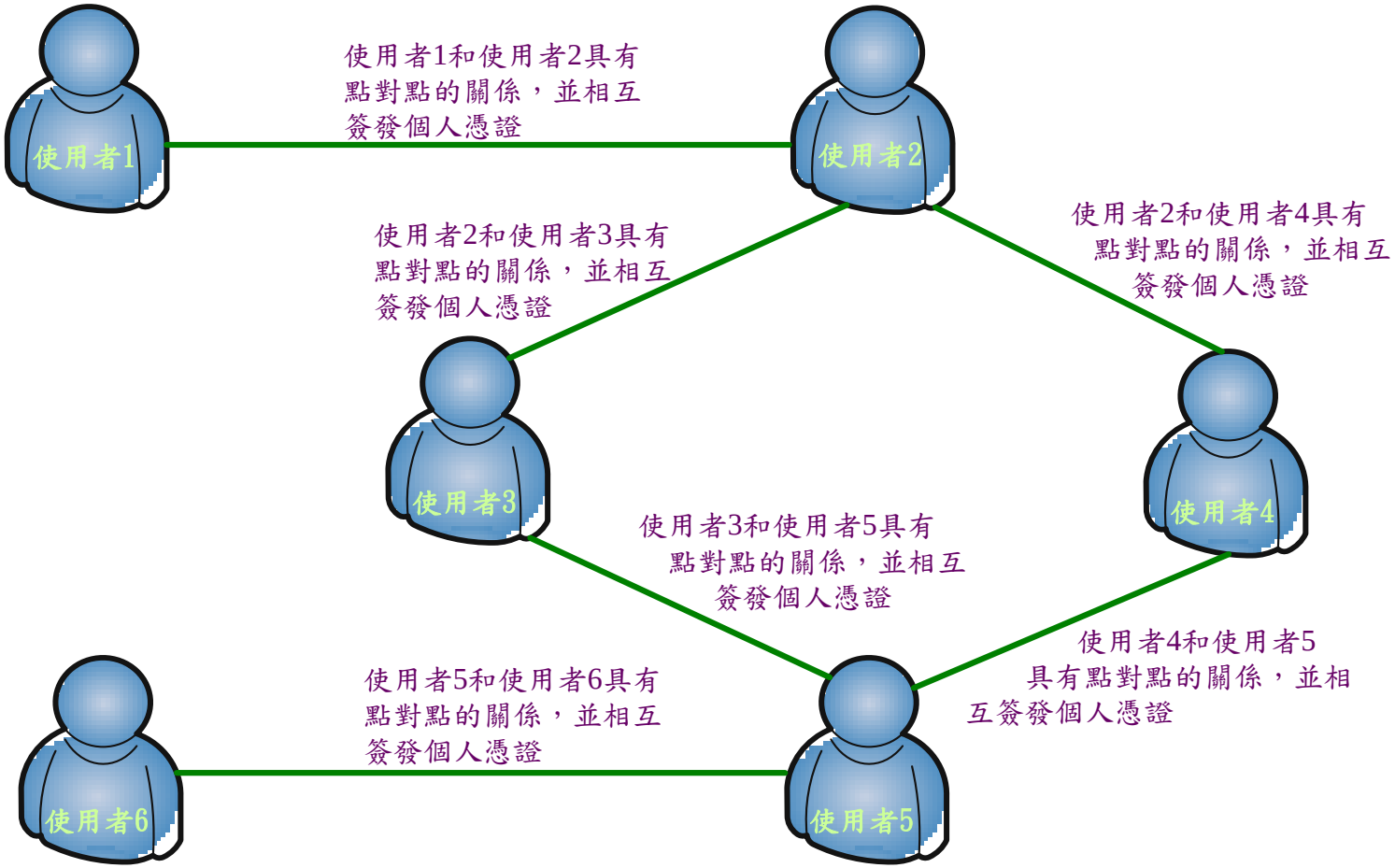


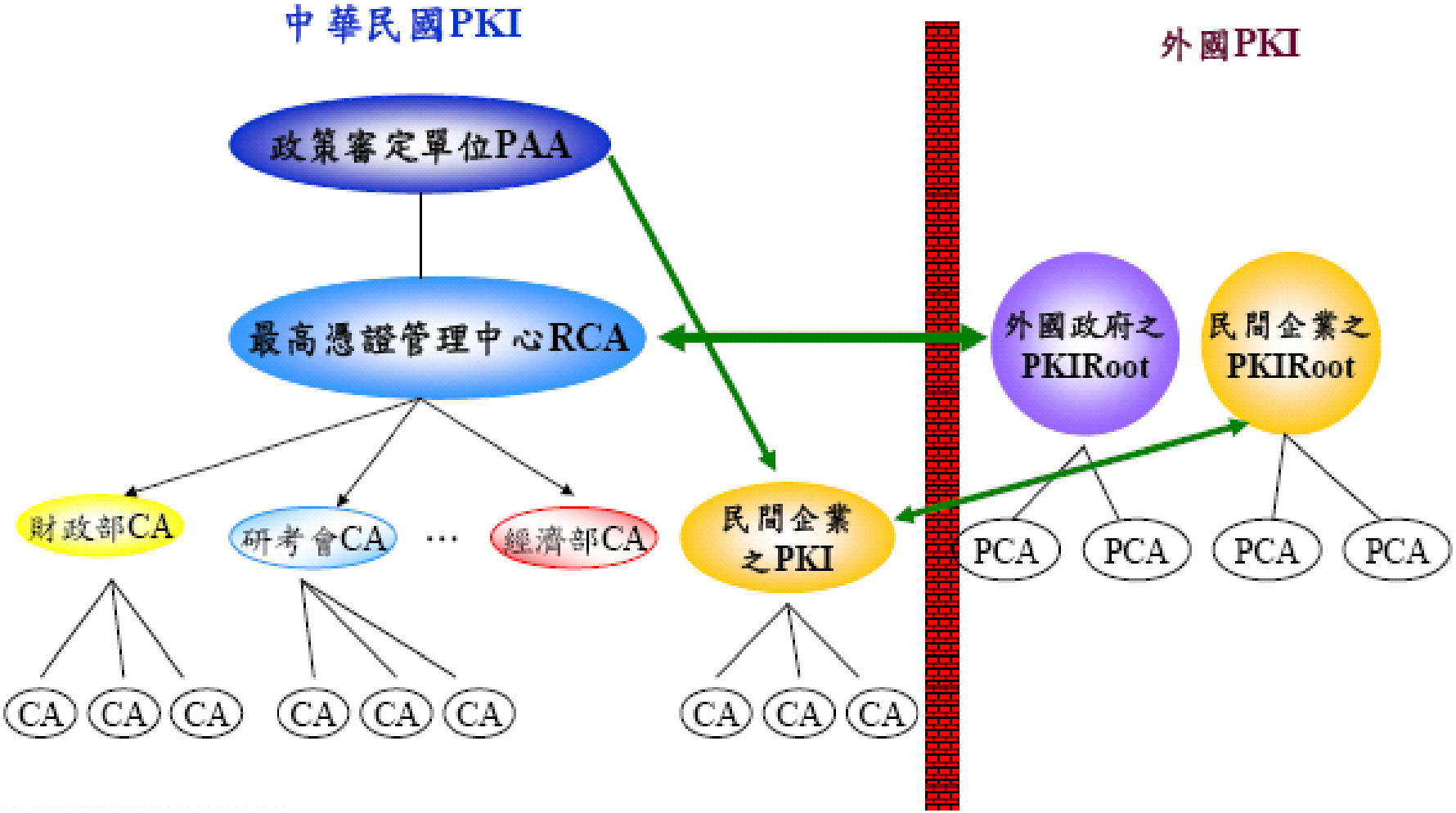
圖4-2 CA網狀架構

資料來源:摘自Eric Maiwald：Network Security: A Beginner's guide

CA網狀架構

- 網狀架構的優點
  - 這種信任模型無需建立憑證管理機構(CA)
  - 一般實務上使用者只和少部分的使用者通訊，以此架構已足以達成雙方通訊的目的
  - 每個使用者負責自己和他的連絡人的憑證，而組織可以自行決定是否提供憑證和註銷通知的集中儲存處
  - 不需要花費大量的建置經費、人力於基礎建設上
- 網狀架構的缺點
  - 規模太小是網狀架構的主要問題
  - 對於互不相識的兩位使用者在驗證路徑的搜尋會比階層式架構要複雜許多

我國政府公開金鑰基礎建設之架構

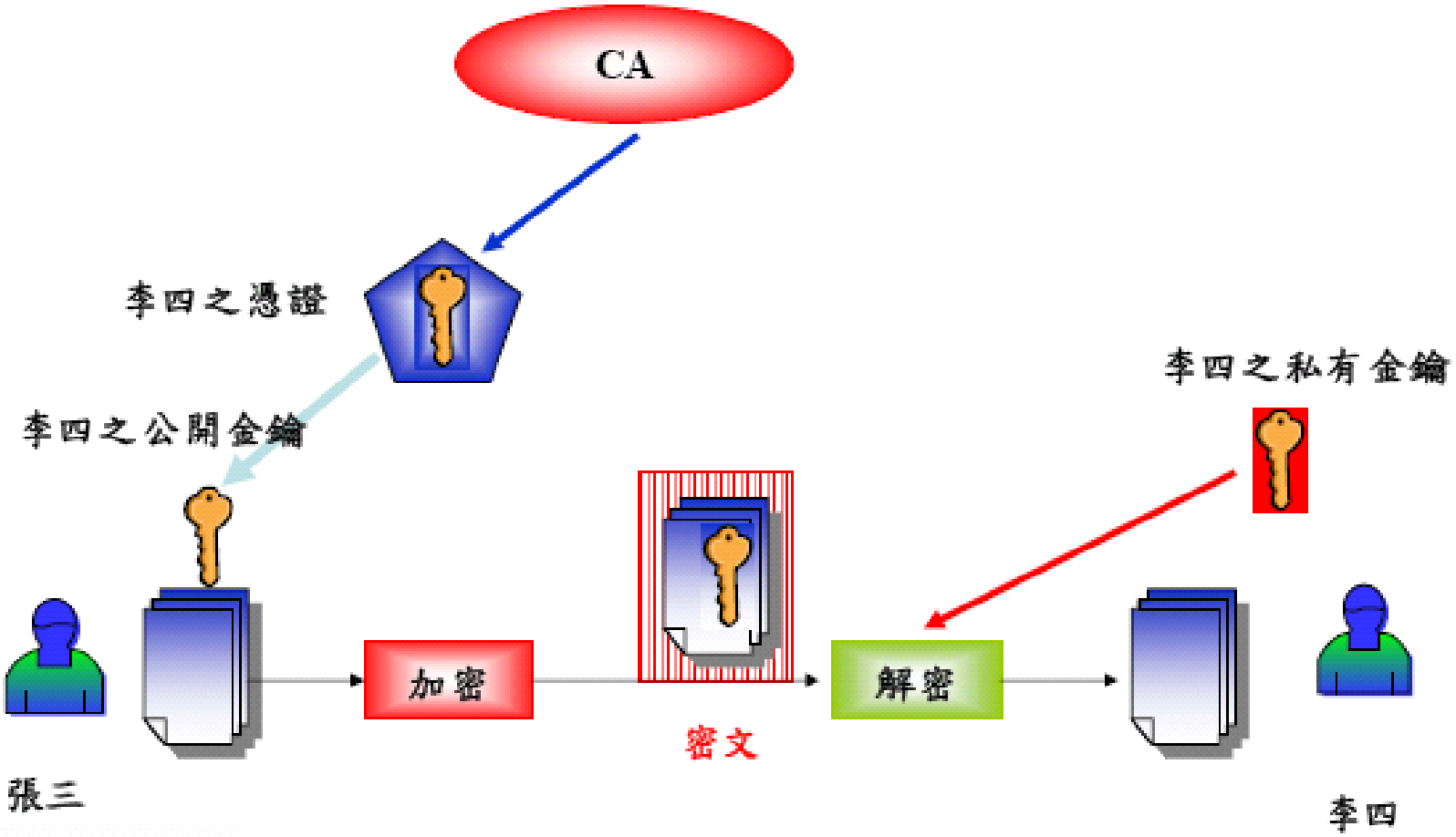


Module 4-2:
PKI技術概觀

PKI的內涵

- 配套法律系統（電子簽章法、個人資料保護法）→ 法律
- 釐定CA 架構、建置CA 與BCA (bridge CA) → 政策與建設
- 制訂憑證格式(X. 509)、密碼學技術標準 → 技術平台
- 制訂憑證政策(CP)與憑證實務作業基準(CPS) → 管理

憑證與加解密機制運作的關係



PKI技術概觀(I)

- PKI憑證管理(核心)
  - 憑證發行(issuing)、註銷(revocation)、封存(archiving)
  - 政策認可(approving)與金鑰託管(key escrowing)
- 安全技術(第一層)
  - 金鑰對之產生
  - 數位簽章之產生與驗證
  - 機密金鑰(含密鑰及私鑰)之交換
- 伺服器(servers)與代理機構(agents)(第二層)
  - 憑證遞送伺服器(delivery server)與公證伺服器(notary server)
  - 票證授與代理機構(ticket granting agent)
  - 金鑰託管代理機構(key escrow agent)

PKI技術概觀(II)

- 資訊與網路服務(第三層)
  - 資料封存(data archive)、目錄(directory)、命名(naming)與註冊(registration)
  - 存取控制(access control)服務(包含MAC與DAC)
  - 訊息機密性(message confidentiality)服務(包含加解密與數位簽章)
  - 完整性(integrity)服務(包含資料與系統完整性)
  - 鑑別(authentication)服務(包含個體鑑別與憑證鑑別)
  - 收方不可否認(destination non-repudiation)服務
  - 發方不可否認(source non-repudiation)服務
  - 交談機密性(session confidentiality)服務
  - 原文復原(plaintext recovery)服務
  - 時戳(time-date stamp)服務

鑑別技術協定

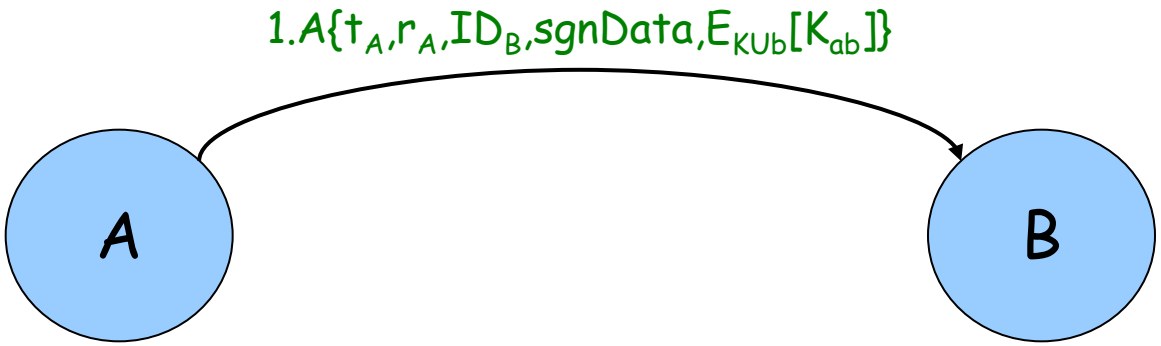
- 為應付不同的應用領域，X.509提供三種不同的鑑別的程序，這些程序均使用到公開簽章的簽章模式。
- 以型態歸類來看，X.509鑑別協定可能是單向或雙向相互認證，依架構可區分為下列三種鑑別型態

  - 單向認證 (One-way authentication)
  - 雙向認證 (Two-way authentication)
  - 三向確認(Three-way authentication)

鑑別技術協定

1.單向認證（One-way authentication）

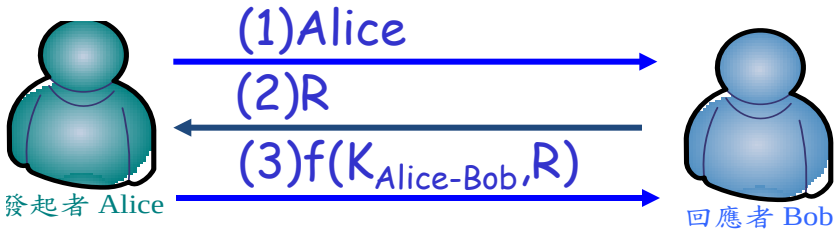
- 這是最簡單的認證方式，用戶端只需提供訊息給伺服端作存取確認，伺服端確認後就允許用戶端的登入。
- 訊息中包含時戳(t_A)、臨時亂數(r_A)、B的ID(ID_B)及以B的公開金鑰加密後的通訊金鑰(Kab)，除此之外，也可於這之中附加其他訊息(sgnData)，以上所有訊息都必須以A的私密金鑰加密後傳送。



鑑別技術協定

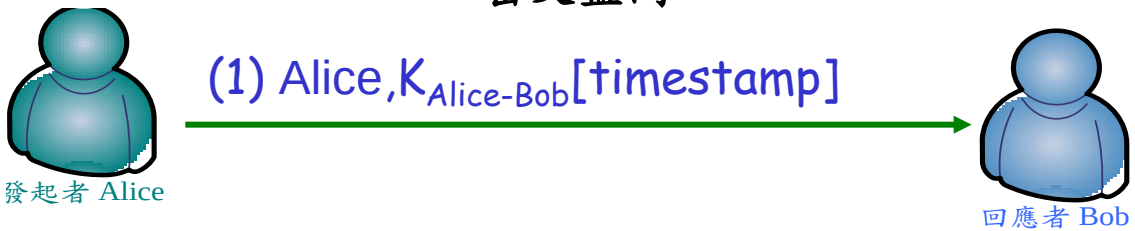
1.單向認證（One-way authentication）

- 伺服端認證大都採用盤問/回應(challenge/ response)方式
- 認證內容可區分明文盤問、密文盤問及時間戳記盤問三種方式，請詳見圖4-3



明文盤問

密文盤問



時間戳記盤問-(a)加密時間戳記盤問

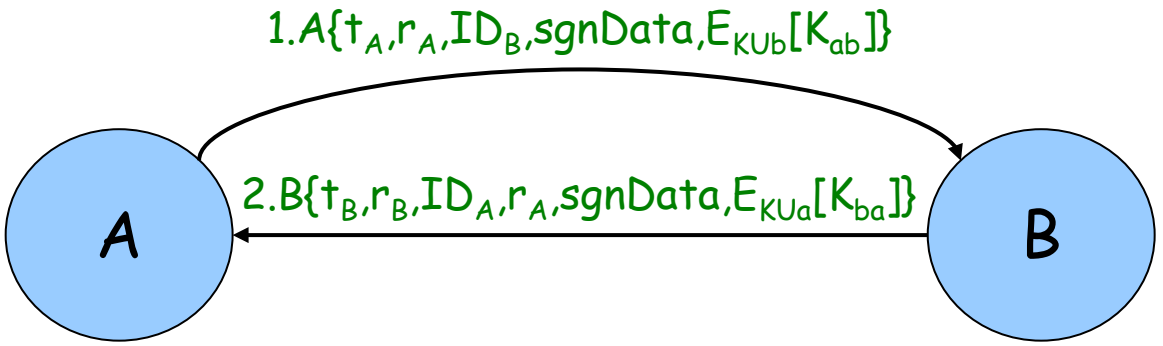
資料來源:摘自
黎添壽, 吳順裕, 資訊與網路安全技術 時間戳記盤問-(b)雜湊時間戳記盤問

圖 4-3 單向認證三種方式

鑑別技術協定

2.雙向認證（Two-way authentication）

- 需要兩個訊息 (A->B, B->A)，為一種雙方相互認證（mutual authentication）的方式，雙方都得提供認證資訊給對方，才能通過認證。
- B回應給A的訊息包括A原來的臨時亂數(r_A)、ID(ID_A)、時戳(t_B)、B的臨時亂數(r_B)及以A的公開金鑰加密的通訊金鑰(K_{ba})
- 雙向認證方式，必須維護對方所對應的認證資訊。



鑑別技術協定

2.雙向認證（Two-way authentication）

- 身份鑑別協定透過交換通訊金鑰(session key)用來確認雙方ID。
- 身份鑑別主要的安全考量是
  - 保密性(confidentiality)–保護通訊金鑰，防止外洩
  - 時效性(timeliness)–預防重送攻擊(replay attack)

鑑別技術協定

1.三向認證（Three-way authentication）

- 需要三個訊息 (A->B, B->A, A->B)，藉此達成上述確認性，並且過程中不需時脈同步即可完成
- 會多一個由A回傳給B的訊息，內容包含簽署過的B的臨時亂數(r_B)
- 因為雙方均傳回對方的亂數，故不需要依賴時戳，當雙方的時序無法同步時，此法就可派上用場

資料來源:摘自W. Stalling: Cryptography and Network Security

Module 4-3:
PKI相關安全技術規範與標準

FIPS 140-1 密碼模組安全需求(1/2)

- Level 1 (minimal security)
  - 最低安全等級，使用FIPS所核准的密碼演算法
  - 允許軟體密碼模組功能在一般的PC上執行
- Level 2 (role-based authentication)
  - 使用上鎖方式來防制破壞密碼模組
  - 使用塗層或密封來偵測已發生的破壞行為
  - 允許軟體密碼模組功能在C2以上等級的作業系統下執行

FIPS 140-1 密碼模組安全需求(2/2)

- Level 3 (identity-based authentication)
  - 若密碼模組被破壞或侵入，則安全參數會進行歸零(zeroization)
  - 允許軟體密碼模組功能在B1以上等級的作業系統下執行
- Level 4 (theoretical proofs)
  - 在超出正常電壓或溫度環境下，密碼模組會採取防制或歸零動作
  - 允許軟體密碼模組功能在B2以上等級的作業系統下執行

低保證等級CA之安全需求 (Low Assurance Level)

- 只能發行憑證及支援低風險的應用（例如E-mail），不能用於保護個人隱私資料及政府資料
- 需符合FIPS 140-1 Level 2的一般安全需求，但只能在單一的CA下運作，無法提供互通服務
- 金鑰必須儲存於受CA控管之硬體符記設備(hardware token)
  - 金鑰不能以明文或原文形式儲存
  - 金鑰品質檢測為 $< 10^{-6}$

中保證等級CA之安全需求 (Medium Assurance Level)

- FIPS 140-1 Level 2實體安全與作業系統安全，可允許互通性
- FIPS 140-1 Level 3金鑰管理需求
  - 金鑰不能以明文或原文形式儲存與傳遞
  - 金鑰品質檢測為 $< 10^{-9}$
- 安全權限必須加以分離，由多人共享

高保證等級CA之安全需求 (High Assurance Level)

- FIPS 140-1 Level 2實體安全與作業系統安全，可允許互通性
- FIPS 140-1 Level 3金鑰管理需求，金鑰品質檢測為 $< 10^{-12}$
- FIPS 140-1 Level 3角色與服務，提供角色及身分鑑別(role-based & identity-based authentication)
- 安全權限必須加以分離由多人共享
- 任何輸出金鑰必須要用DES或AES加密
  - 私鑰及公鑰都要加以保護
  - 公鑰儲存或傳遞時要使用數位簽章加以保護
- CA只接受經由兩個以上的ORA所簽署過的憑證

PKI相關安全技術規範與標準(1/2)
(以US Federal PKI為例)

- 加解密標準
  - DES, Triple DES (FIPS 46-2)
- 數位簽章標準
  - SHA-1 (FIPS 180-1), DSA (FIPS 186)
- 金鑰交換標準
  - X.509, ISO 9798-1, 9798-2, 9798-3, 9798-4, ANSI 9.17

PKI相關安全技術規範與標準(2/2)
(以US Federal PKI為例

- 金鑰託管標準
  - FIPS 185 (Escrowed Encryption Standard, EES)
- 憑證格式標準
  - X.500 directory, X.509 version 3 (CRL), X.509 version 2 (CKL)
- 其他相關技術及標準
  - IEEE 1363, Diffie-Hellman (KEA), RSA, ElGamal, IDEA, PGP
  - http://home.xcert.com/~marcnarc//PKI/thesis/bibliography.html

公開金鑰長度建議表

year	vs individual	vs corporation	vs government
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

內政部憑證管理中心採用的相關標準

- 公開金鑰管理：ISO/IEC 9594-8, RFC1422(PEM), ISO11166, X9.30-3, X9.63, FIPS PUB 171
- 憑證及CRL之格式：ISO/IEC 9594-8, X.509
- 認證協定標準：ISO/IEC 9594-8, ISO/IEC 11770-3, ISO 9798-3, FIPS196, X9.26
- 憑證及CRL存取協定：RFC 1777(LDAP)
- 資料編碼： ISO/IEC 8824, ISO/IEC 9834, ISO/IEC 9979

Module 4-4:
憑證管理中心(CA)營運

CA的設立

- 某些組織覺得建立內部CA ，最好和公開金鑰基礎建設結合，且必須先處理下列的問題
  - 必須建立CA公開金鑰組，金鑰必須大於安全的有效期限（一般是一年到二年）
  - 由自己的CA或更高層的CA來認證CA的公開金鑰，如果使用外部組織提供的CA時，必須額外付費
  - 在金鑰的有效期限內，必須自行保護CA的私密金鑰，如果曾經遭到侵害時，必須重新更新所有以此金鑰簽署的數位憑證

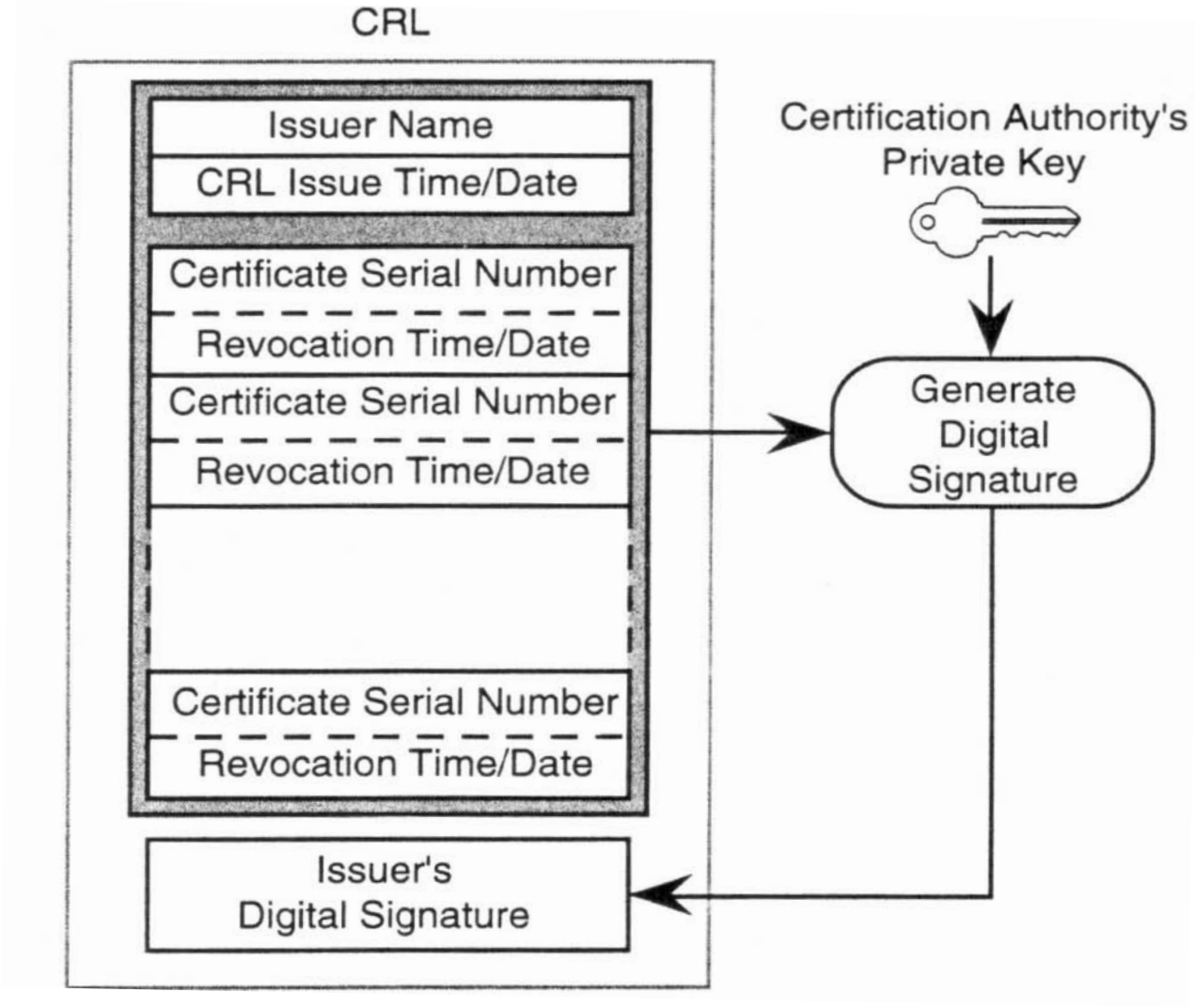
CA的功能職掌(1/2)

- 產生自己的公鑰/私鑰對
- 執行公鑰/私鑰對的品質測試(FIPS 186標準規範)
- 產生、遞送、註銷、及歸檔所屬CA或使用者的憑證
- 確保其所屬CA與使用者的命名並無碰撞(collision)
- 在發行憑證之前，驗證所屬CA或使用者所出示的公鑰是否唯一對應至其所持有的私鑰
- 簽署及驗證數位簽章

CA的功能職掌(2/2)

- 產生、維護、分派、及歸檔憑證被註銷的目錄(Certificate Revocation List，CRL)
- 維護已發行憑證的記錄
- 產生時戳(time-stamping)
- 在數位時代扮演可信任的仲裁者(提供憑證)
- 憑證之查詢及分送憑證管理之相關資料

Simple CRL


CRL
Issuer Name
CRL Issue Time/Date
Certificate Serial Number
Revocation Time/Date
Certificate Serial Number
Revocation Time/Date
Certificate Serial Number
Revocation Time/Date
Issuer's
Digital Signature
Certification Authority's
Private Key
Generate
Digital
Signature

CA服務準則

CA的驗證金鑰功能

- 只要透過憑證管理機構(CA)的公開金鑰，即可驗證金鑰組的擁有者

- CA以其私密金鑰對個人數位憑證簽章，以防止惡意的冒充行為

- 可利用CA的公開金鑰證明金鑰組擁有人的公開金鑰（詳見圖4-4）。

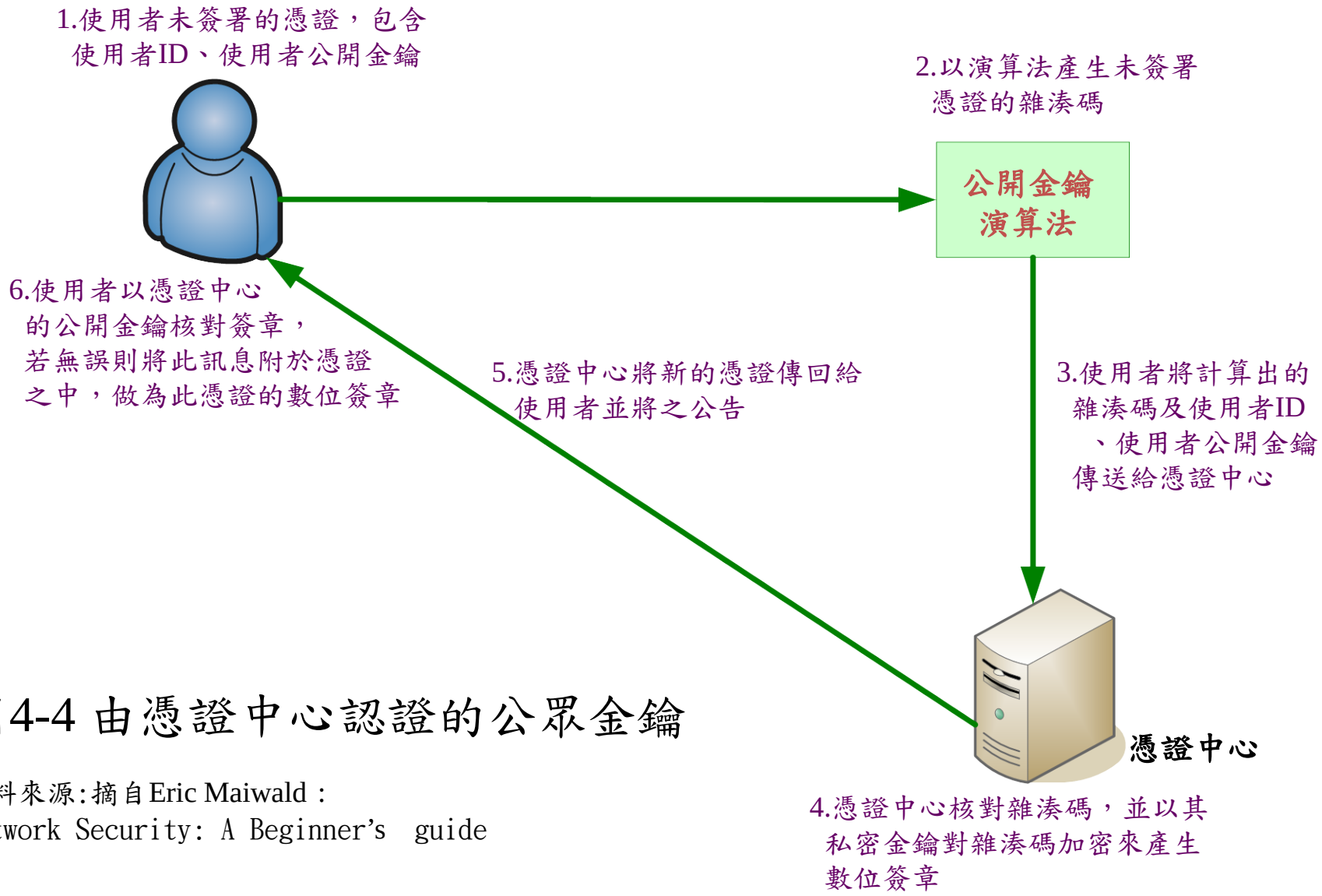


圖4-4 由憑證中心認證的公眾金鑰

資料來源:摘自Eric Maiwald：
Network Security: A Beginner's guide

CA服務準則

憑證的製作與簽發

- 製作憑證必須制訂相關的憑證政策和管理程序
- 在簽發新憑證之前，必須確實驗證每個個體的身份，憑證是否過期，而且還要註銷過期的憑證

憑證的儲存

- 運用一個目錄服務(X.500定義)儲存數位憑證以及使用者的公開金鑰

CA服務準則

憑證的驗證與註銷

- 為了讓每個底層之間能夠互驗彼此的憑證，因此CA必須建立一套驗證機制
  - 階層式架構
  - 網狀架構
- CA會在以下三種狀況於憑證到期前加以廢止
  - 使用者的金鑰被破解
  - 使用者不再由此CA來認證
  - CA的數位憑證遭到破解

憑證政策與憑證實務作業基準的定義

- ISO/ITU-T X.509 V3(1997)對憑證政策(Certificate Policy; CP)與憑證實務作業基準(Certification Practice Statement; CPS)都有分別定義。
- 我國的電子簽章法施行細則中的憑證實務作業基準應載明事項，根據X.509的定義：
  - CP定義：指為指明某一憑證所適用之對象或情況所列舉之一套規則，該對象或情況可為特定之社群或具共同安全需求之應用。
  - CPS定義：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。其中的憑證機構係指簽發憑證之機關、法人。

憑證政策（CP）與憑證實務作業基準（CPS）的關係（1/2）

- 撰寫者
  - 在大部分的PKI模式上，這兩份文件的作著出處通常是不同的。其中CP會是由該PKI的政策管理機構(Policy Management Authority, PMA)來制定及發行，CPS是由這個PKI內的CA(可能不只一個CA)的營運機構(Operational Authority)來制訂。也就是由負責監理的單位來制訂CP，而由實際負責營運執行的單位來制訂CPS。
- 撰寫目的
  - 一般來說，在憑證中所闡述的CP是著重於“政策所要做到的是什麼”(what to do)，CPS是著重於“如何達到所設定的政策”(how to do)，並且我們可以依照CPS中所記載的實務與程序，以進行憑證的簽發及管理工作。

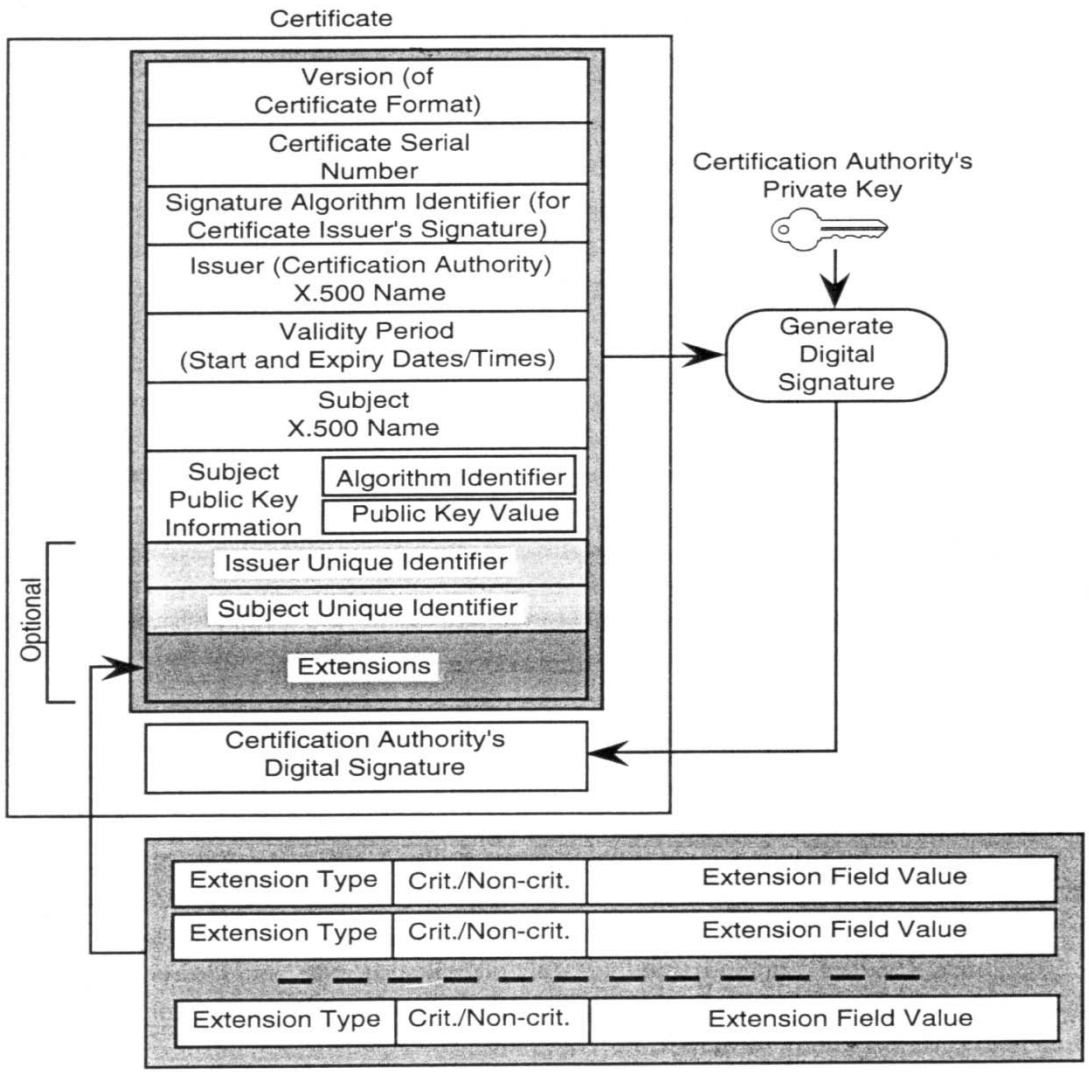
憑證政策（CP）與憑證實務作業基準（CPS）的關係（2/2）

- 針對工作的描寫層級
  - CP在同一件工作的描寫層級是比CPS還要高，因為一個是政策上的指導，一個是實務及程序的實作要領。所以有關一個CA在憑證的簽發及管理上，CPS會去詳細的描述CA的實作及營運實務，以便可以真的達成CP所設定及要求的保證等級(Assurance Level)。
- 描寫方式
  - 就CA在憑證的簽發及管理上，CP與CPS的描寫方式上是有著明顯的不同的。
- 公開性
  - 一般來說CP都較CPS對外公開，也就是常有一些CA都只有公佈其CP，而沒有對外公佈其CPS，例如美國聯邦政府的Bridge CA，及專用於大金額銀行交易轉帳的Identrus等，這是因為CPS常有一些營業的機密，而CP是PKI互通所必要的文件。

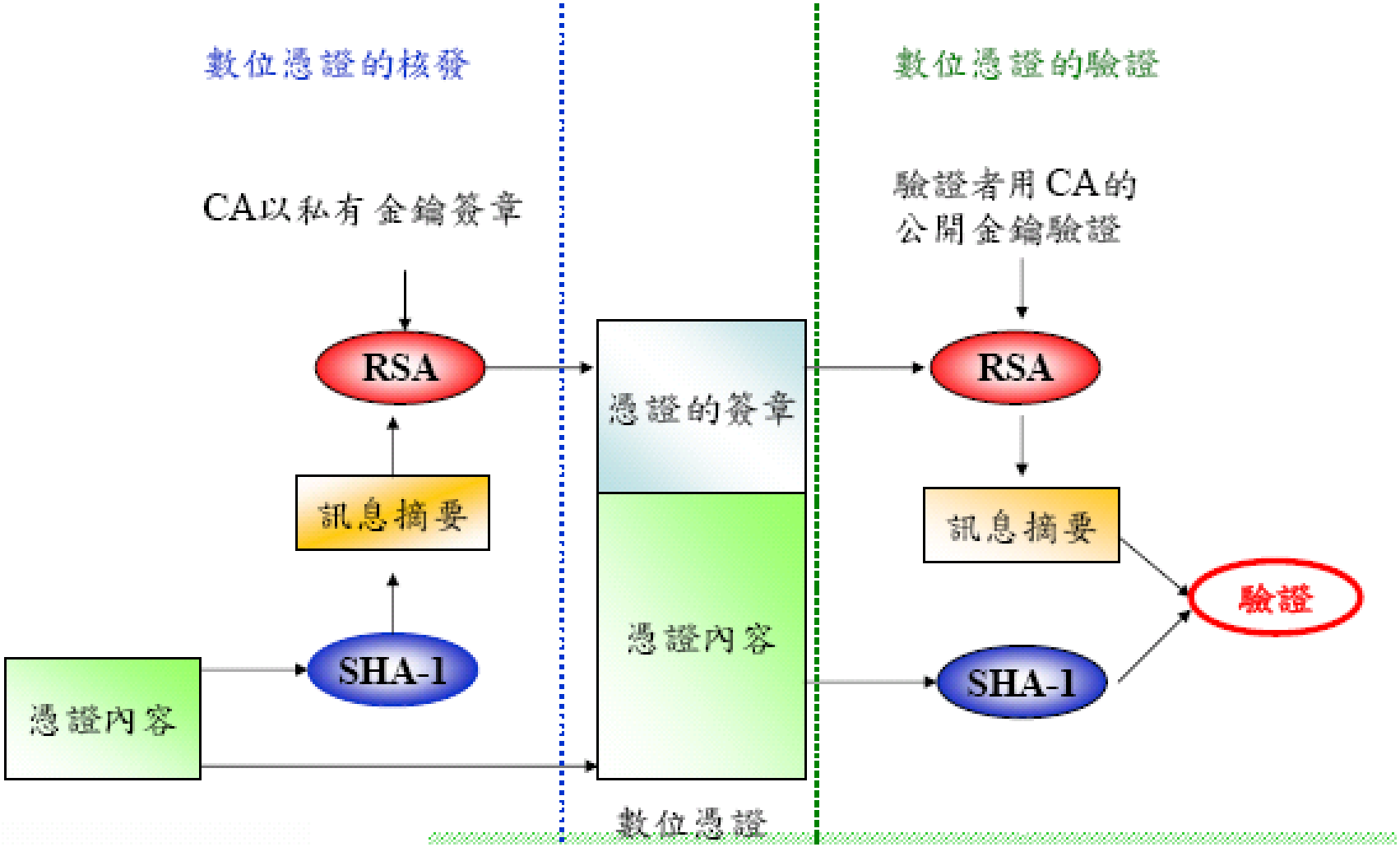
憑證標準格式(X.509)

1.版本	Version 3
2.序號	Serial Number
3.簽章演算法	Issuer Signature algorithm
4.憑證發行者	Issuer Distinguished Name
5.有效期限	Validate Period
6.憑證持有人	Subject Distinguished Name
7.持有人公開金鑰	Subject Public Key Information
8.發行者身分ID	Issuer Unique Identifier (option)
9.持有人身分ID	Subject Unique Identifier (option)
10.其他資訊	Extension (option)
11.上述各資料之簽章	Issuer's Signature on all the above fields

X.509 Version 3 憑證格式



數位憑證的核發與驗證過程



參考文獻

1. S. William, Cryptography and Network Security: Principles and Practice. Prentice Hall, Second Edition, 1999.
2. E. Maiwald, Fundamentals of Network Security, McGraw-Hill Technology Education, 2004, pp. 404 -411.
3. S. William, Network Security Essential ─ Applications and Standards by William Stallings，Pentice Hall , 2000.
4. 謝續平, 網路安全概要2005教材, 交通大學, 民國九十四年, http://dsns.csie.nctu.edu.tw/course/intro~securit/2005/。
5. 賴溪松、韓亮、張真誠,近代密碼學及其應用, 松崗, 民國八十五年。
6. 黃景彰, 樊國楨, 羅景原, “基於X.509之公文交換協定 ” ,國立交通大學資訊管理研究所, 碩士論文, 民85 。

參考文獻

7. William Stallings, Cryptography and network Security, Fourth Edition, Pearsion Prentice Hall
8. 黃明祥、林詠章著資訊與網路安全概論，美商麥格羅希爾
9. 林祝興、張真誠著電子商務安全技術與應用，旗標
10. 楊中皇著網路安全-理論與實務，金禾
11. 吳順裕、粘添壽著資訊與網路安全技術，旗標
12. 李順仁、葉乃菁著網路安全理論與實務，文魁
13. 李順仁著資訊安全，文魁

References

- 教育部顧問室編輯 “電子商務安全”教材
- Turban et al., Introduction to Electronic Commerce, Third Edition, 2010, Pearson