Module4: X.509

Module 4:大綱

4-1 數位憑證概念(*)

4-2 鑑別程序(*)

4-3 X.509 V3 格式(**)

4-4 CA服務(*)

ul

* 初級(basic):基礎性教材內容
**中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容
***高級(advanced):適用於深入研究的內容

u1

* 初級(basic):基礎性教材

**中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容

***高級(moderate):適用於深入研究的內容

user, 2007/2/14

Module 4-1: 數位憑證概念

4-1數位憑證概念

數位憑證的用途

- 數位憑證(certificate)就像是一張在網路環境中使用的護照，利用公開金鑰密碼技術來提供身份識別的能力，以保護網路上資料傳輸的正確性、保密性等。
- 它不僅僅可以代表使用者，也可以代表機器、組織機構甚至是程式的身份，所以才有所謂的個人數位憑證、伺服器數位憑證、物件數位憑證。
- 它是由憑證管理機構應用數位簽章技術所簽發的一組資訊，內容包含個體（entity）的公開金鑰、憑證擁有者、簽發單位以及其他一些訊息。

4-1 數位憑證概念

- 數位憑證是由一個具公信力的憑證授權中心(Certificate Authority, CA)所核發的資料，第三者除非取得憑證管理機構的私有金鑰，否則無法假造出由該憑證管理中心簽發的憑證。
- 數位憑證常應用在網路環境中，證明某個體的身份(identity)。
- 數位憑證可以應用到電子商務、電子郵件、金融匯款等方面。例如進行線上電子交易(e-commerce)時，使用者就可利用伺服器所提供的數位憑證來驗證伺服器的真實性。

4-1 數位憑證概念

X.509鑑別性服務

- X.509是一套由國際電信聯盟之遠程通信標準組織(ITU-T)所建議的一種跨網路間的身份確認架構，提供使用於ITU-T的 X.500 郵件系統。
- 此架構是基於公開金鑰密碼學及數位簽章而建立的。
- X.509在1988年首次發表，經過幾年公開討論後，在1993年重新修定，改正了一些安全性的問題。第三版草稿於1995年發表，於2000年修訂。
- 雖然X.509沒有制定出特定的演算法，不過此協定推薦使用RSA演算法。

4-1 數位憑證概念

- **數位憑證的儲存**
  - 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
  - 數位憑證是由憑證管理機構(CA)運用其私密金鑰簽署，以做為此憑證的數位簽章
- X.509鑑別性服務是X.500標準中的一部份，而 X.500定義了目錄服務(Directory service)，有關使用者身份的定義與識別則是沿用了X.500系列標準中的相關規定。

4-1 數位憑證概念

數位憑證的應用

- X.509是一個重要的標準，定義了數位憑證的結構，並運用數位憑證在多種應用程式上，如X.509的憑證格式被運用在
  - 電子郵件S/MIME中
  - IPSec（IP Security）
  - SSL（Secure Socket Layer）Protocol
  - SET（Secure Electronic Transaction）
  - PEM（Privacy Enhancement for Internet Electronic Mail）
  - RSA公司所制定的公開金鑰密碼系統標準（Public Key Cryptosystem）也採用了X.509的資料格式 [PKCS]。

4-1 數位憑證概念

數位憑證的格式—X.509 憑證格式

- 自1988年開始X.509中總共定義了三個X.509憑證版本。在剛開始的版本一（X.509 v1）的規範中，因為這版本擴充能力不佳，所以已經逐漸被版本三(X.509 v3)所取代。
- 而版本二(X.509 v2) 主要是引進憑證主旨(subject)及簽發人唯一的概念，但是這版本不常被使用。
- 在 1993 年發表的版本三中，則加入了擴充(extension)欄位，如Key Usage，可限制憑證的使用。目前廣為使用的即為此版本。
- 以下圖 4-1 為X.509系列憑證的一般欄位內容，我們將一一介紹這些欄位的功能。

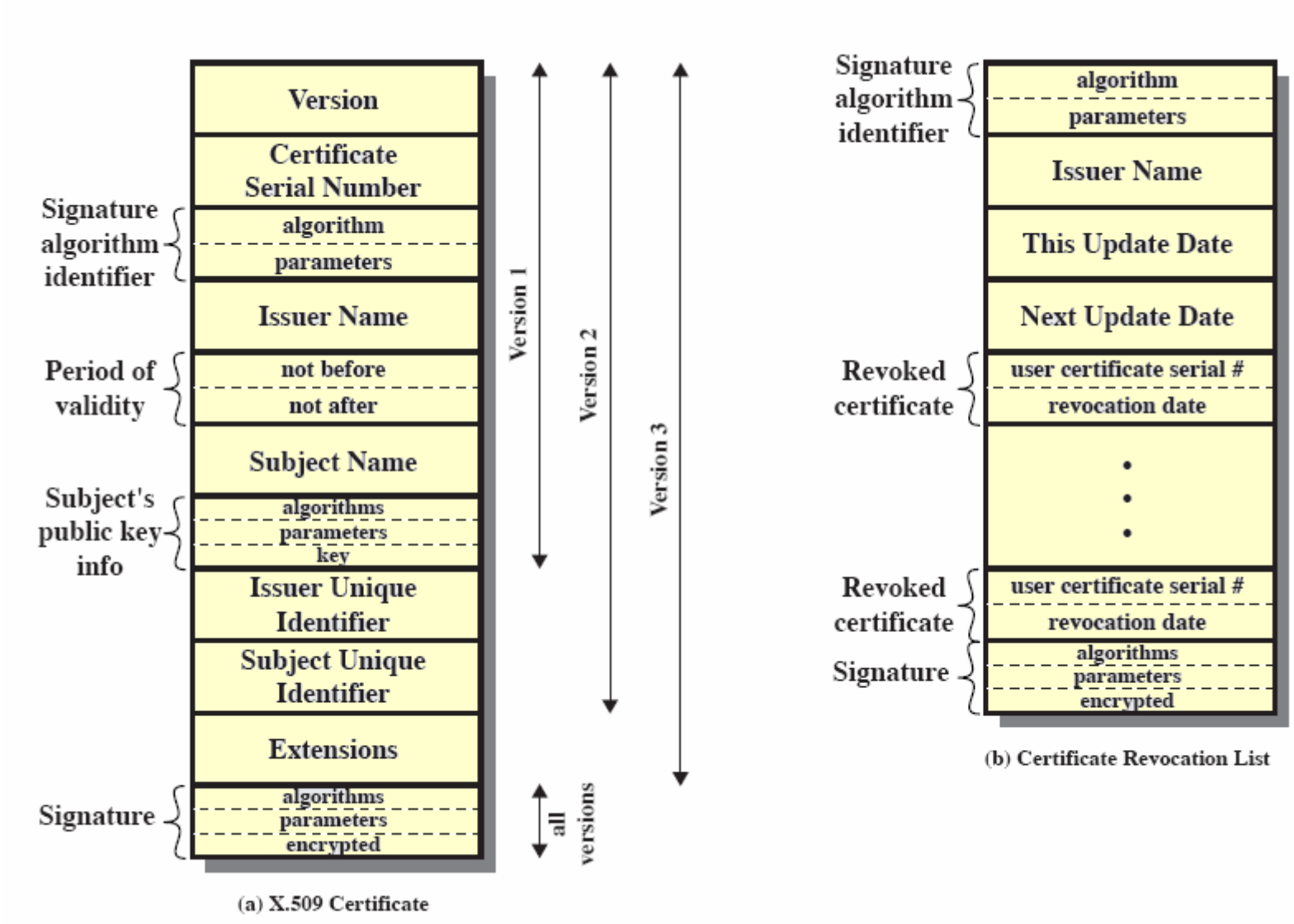


圖4-1 X.509 數位憑證內容

4-1 數位憑證概念

- X.509 憑證是由憑證管理機構(CA) 核發，一般格式如下:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (from - to dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (或是憑證中所有欄位的雜湊值)
- X.509以下列定義數位憑證：
  CA<<B>> 表示由 CA 所簽署使用者B 的憑證

4-1 數位憑證概念

數位憑證的取得

- 由憑證管理機構(CA) 核發的數位憑證具有下列特性：
  - 若可存取CA的公開金鑰 ，任何人均可取得經過驗證過的使用者公開金鑰
  - 除認證管理機構外，任何人無法在不被偵測發現的情況下，變更數位憑證的內容
- 因為數位憑證不易偽造，一般可放在公開目錄中，讓所有使用者存取。
- 若所有使用者均採用同一憑證授權中心(Certificate Authority, CA) ，使用者可以相互信任
  - 對方使用公開金鑰加密的訊息，可達成安全且不易被竊取的目的
  - 對方使用私密金鑰簽署的訊息，是不易被偽造

4-1 數位憑證概念

- 若使用者很多時，須使用多個CA才符合實際，此時每個CA只提供部份使用者的公開金鑰 ，因此須解決由不同CA所核發數位憑證的信任問題。解決方式如圖4-2互連的階層式架構。
- 解決不同CA所核發數位憑證的信任問題
  - 假設有兩個不同憑證管理機構，CA1及CA2，分別對A及B簽發憑證
  - 若使用者A收到經由CA2所簽署的B的數位憑證，則其驗證流程為

4-1 數位憑證概念

1. 使用者A先取得CA1的公開金鑰，以取得CA2的公開金鑰。
2. 使用者A運用 CA2的公開金鑰，取得使用者B的公開金鑰。
3. 利用B的公開金鑰解密可取得並比對B的數位憑證內的公開金鑰，及以CA2公開金鑰對數位憑證進行驗章(CA2發出B數位憑證時已使用CA2的私密金鑰進行簽章)，以鑑別此數位憑證的完整性與可鑑別性。

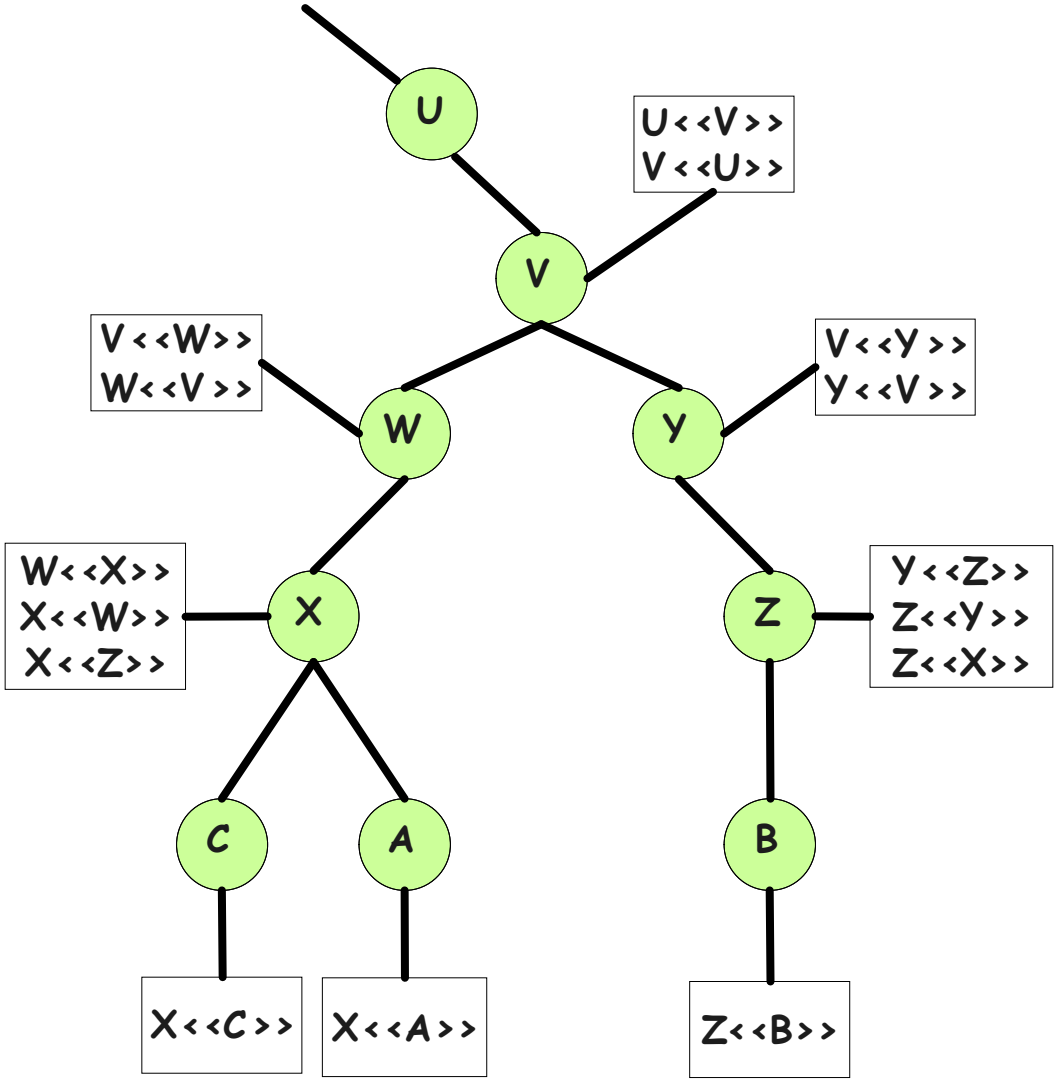


圖4-2 X.509 CA互連的階層式架構

4-1 數位憑證概念

- 如果兩個使用者採用不同一個CA，則我們假設其知道各別CA的公開金鑰，否則CA之間必須形成層級架構。
- CA利用憑證來連結層級間的成員，藉此確認其他CA
  - 每個CA具有正向憑證(Forward certification)、反向憑證(Reverse certification)
- 每個子端(下層)信任父端(上層)所發出的憑證。
- 確保某個CA的發出的憑證，可以由其他CA的使用者來驗證。

4-1 數位憑證概念

- 由圖4-2可知，CA(X)內包含兩種數位憑證：
  - 正向憑證(Forward certification)
    - 由其他CA對CA(X)產生的憑證，例如 W<<X>>
  - 反向憑證(Reverse certification)
    - 由CA(X)對其他CA產生的憑證，例如 X<<W>>、X<<Z>>
- 一個CA(X)的使用者A可從目錄中，取出下列數位憑證，找出CA(B)中使用者B的憑證

  X<<W>>W<<V>>V<<Y>>Y<<Z>>Z<<B>>

4-1 數位憑證概念

數位憑證的廢止

- 由前述X.509 數位憑證內容可知，每一個憑證均有一個有效期限，當發生下列情況，憑證就會在到期前加以廢止
  - 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

4-1 數位憑證概念

數位憑證的廢止

- 憑證授權中心(Certificate Authority, CA)會維護一個憑證廢止清單(certificate revocation list, CRL)，記錄已廢止的數位憑證，資訊包括
  - 核發人姓名
  - 清單產生日期
  - 下一張CRL預定產生的日期
  - 所有廢止的數位憑證序號及其日期

- 因此使用者運用數位憑證前，必須先檢查CA的CRL，以確保其憑證是有效的。

Module 4-2: 鑑別程序

鑑別協定

- 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(K_{ab})，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。

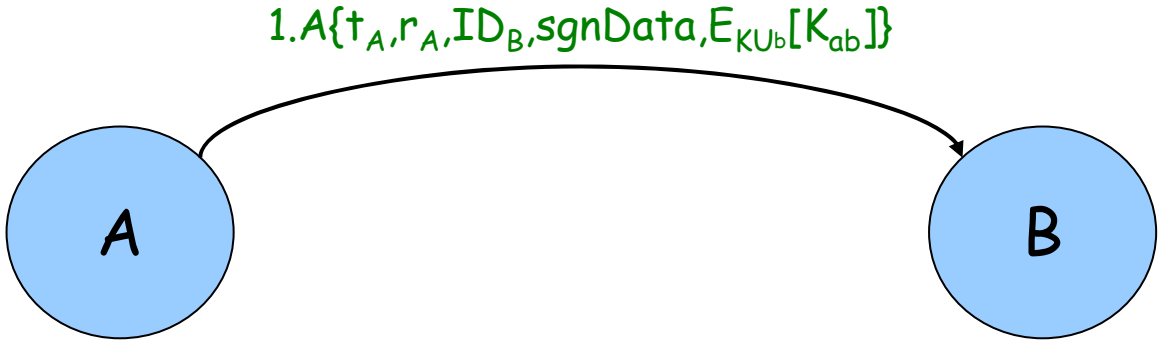
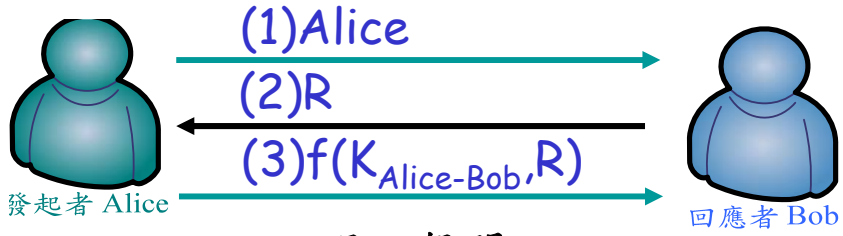


圖 4-3 單向認證

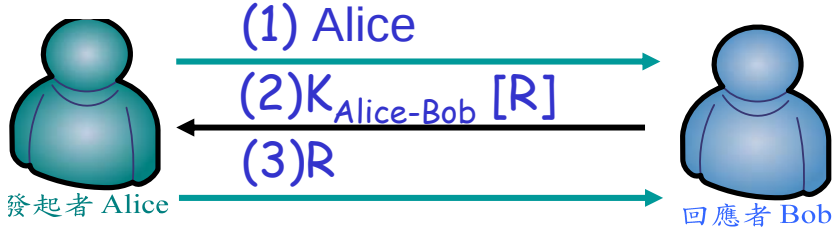
鑑別技術協定

1.單向認證（One-way authentication）

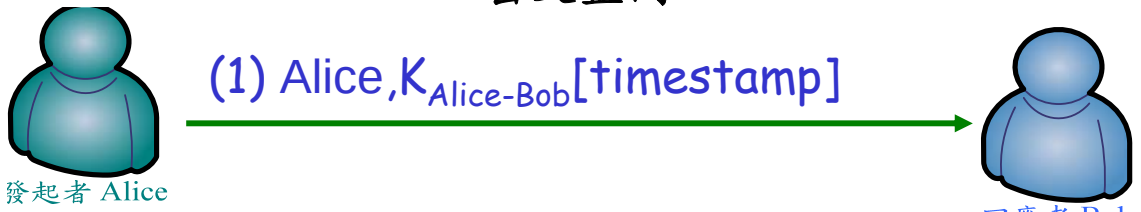
- 伺服端認證大都採用盤問/回應(challenge/response)方式
- 認證內容可區分明文盤問、密文盤問及時間戳記盤問三種方式，請詳見圖4-4。



明文盤問



密文盤問



時間戳記盤問-(a)加密時間戳記盤問

時間戳記盤問-(b)雜湊時間戳記盤問

資料來源:摘自
黎添壽, 吳順裕, 資訊與網路安全技術

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。

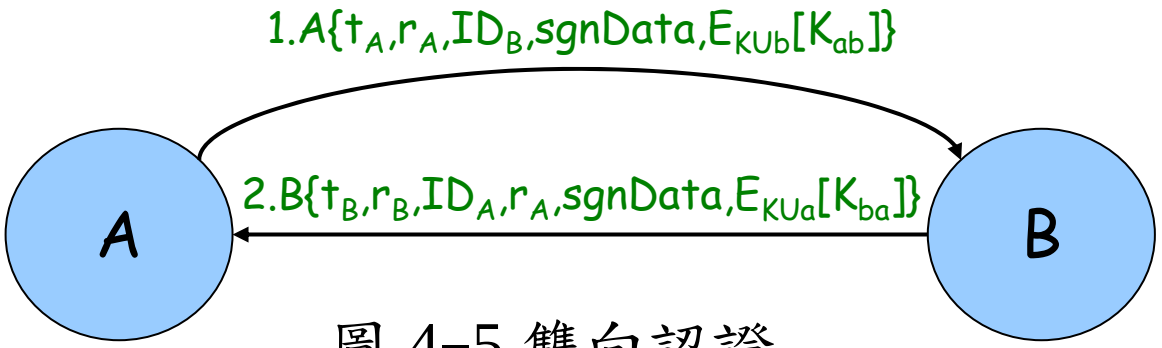


圖 4-5 雙向認證

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

3.三向認證（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

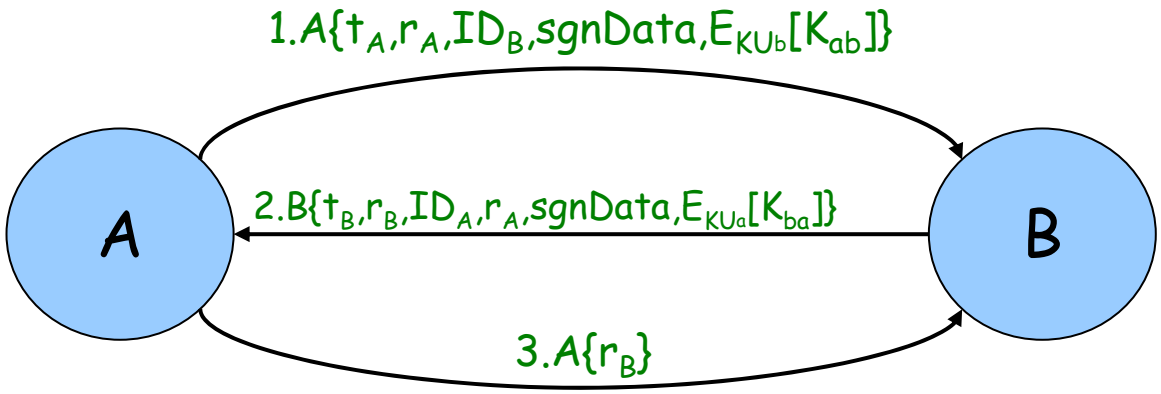


圖 4-6 三向認證

Module 4-3: X.509 V3 格式(**)

u2

u2

user 2007/1/24
user 2007/1/24
* 選擇性(optional)介紹的章節:教師依據學生的吸收情況，選擇性介紹本節的內容

** 先進(advanced)的章節:適用於深入研究的內容
user, 2007/1/24

X.509 v 3 (**)

- X.509 v 2，無法傳送所有需要的資訊，必須在憑證中加入額外訊息，包括以下擴充需求
  - **Subject欄位的改進**：原subject不適用在email/URL表示擁有者的身份
  - **策略的細節**：需指出所採用的安全措施，讓與安全性有關的應用程式可將X.509的憑證與安全措施整合在一起
  - **安全的措施**：必需限制某些憑證的使用範圍，以確保將錯誤或是假的CA所造成的損失降到最小
  - **使用的限制**：必須能夠辨識同一個使用者於不同時間內使用的不同金鑰，此特性可利我們管理金鑰的生命週期

X.509 v 3 (**)

- X.509 v 3避免一直增加固定格式的欄位， 故採用彈性的作法—不需明確地替新欄位命名，設計為可擴充項目，每一擴充項目包括：
  - 擴充 ID：ID的編號
  - 關鍵指標：指出此擴充項目於系統無法辨識時是否可安全地略過
  - 擴充值：數值

4-3 X.509 v3 格式(**)

- X.509 V3 格式內含:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (from - to dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (或是憑證中所有欄位的雜湊值)

X.509 V 3擴充項目(**)

憑證中擴充項目(extension fields)可被區分成三大類:

1.金鑰與策略資訊

- ✓ 包含憑證擁有者與核發者的金鑰，加上憑證策略的指標，欄位包括
  - ➢ Authority key identifier
    - 用來檢查憑證或是CRL簽章時所用的公開金鑰，因可以分辨出同一個CA所擁有的不同金鑰，所以又可做為更新CA金鑰組的功能
  - ➢ Subject key identifier
    - 用來表示被審核過的公開金鑰，對於更新憑證擁有者的金鑰組合時很有用
  - ➢ Key usage
    - 指出針對此已認證過的公開金鑰使用方法做限制

X.509 V 3擴充項目(**)

- Private- Key usage period
  - 用來表示與公開金鑰相對應的私密金鑰其所能使用的期限，一般來說公開金鑰與私密金鑰其二者所能使用的期限將有所不同
- Certificate policies
  - 因憑證所處的環境可能採用多種不同的確認策略，因此此欄位列出此憑證所採用的策略，及一些相關的選擇性資訊
- Policy mapping
  - 此欄位只有由其他CA發給CA來使用的憑證時才會使用到，這當中可以指定一個或多個此核發者的策略，以對應到接收端CA的策略，使之視為相同。

X.509 V 3擴充項目(**)

2.憑證擁有者與核發者的屬性

- ✓ 支援別名，憑證擁有者與核發者的另一個格式，欄位包括
  - ➢ Subject alternative name
    - 包含一個或多個別名，可選訂任意格式
  - ➢ Issuer alternative name
    - 包含一個或多個別名，可選訂任意格式
  - ➢ Subject directory attributes
    - 表示出任何有關此憑證接收者的X.500目錄屬性

X.509 V 3擴充項目(**)

3.憑證路徑的限制

- ✓ 可以限制其他 CA 使用憑證的方式，欄位包括
  - ➢ Basic Constraints
    - 指出這個接收者是否為CA角色，若是的話須指定認證路徑的長度
  - ➢ Name Constraints
    - 指定認證路經當中，所有憑證擁有者的命名範圍
  - ➢ Policy Constraints
    - 此欄位通常用在於設置剩餘認證路徑上明確的策略名稱，或是限制某些策略的對應方式

Module 4-4: CA架構與服務

CA架構

- 憑證授權中心(Certificate Authority, CA)架構的目標就是如何建立和維護可相互信任的數位憑證系統。
- 目前可做為信任公眾金鑰環境的兩種主要模型分別是：
  - 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，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4-6更清楚地顯示這個模型。

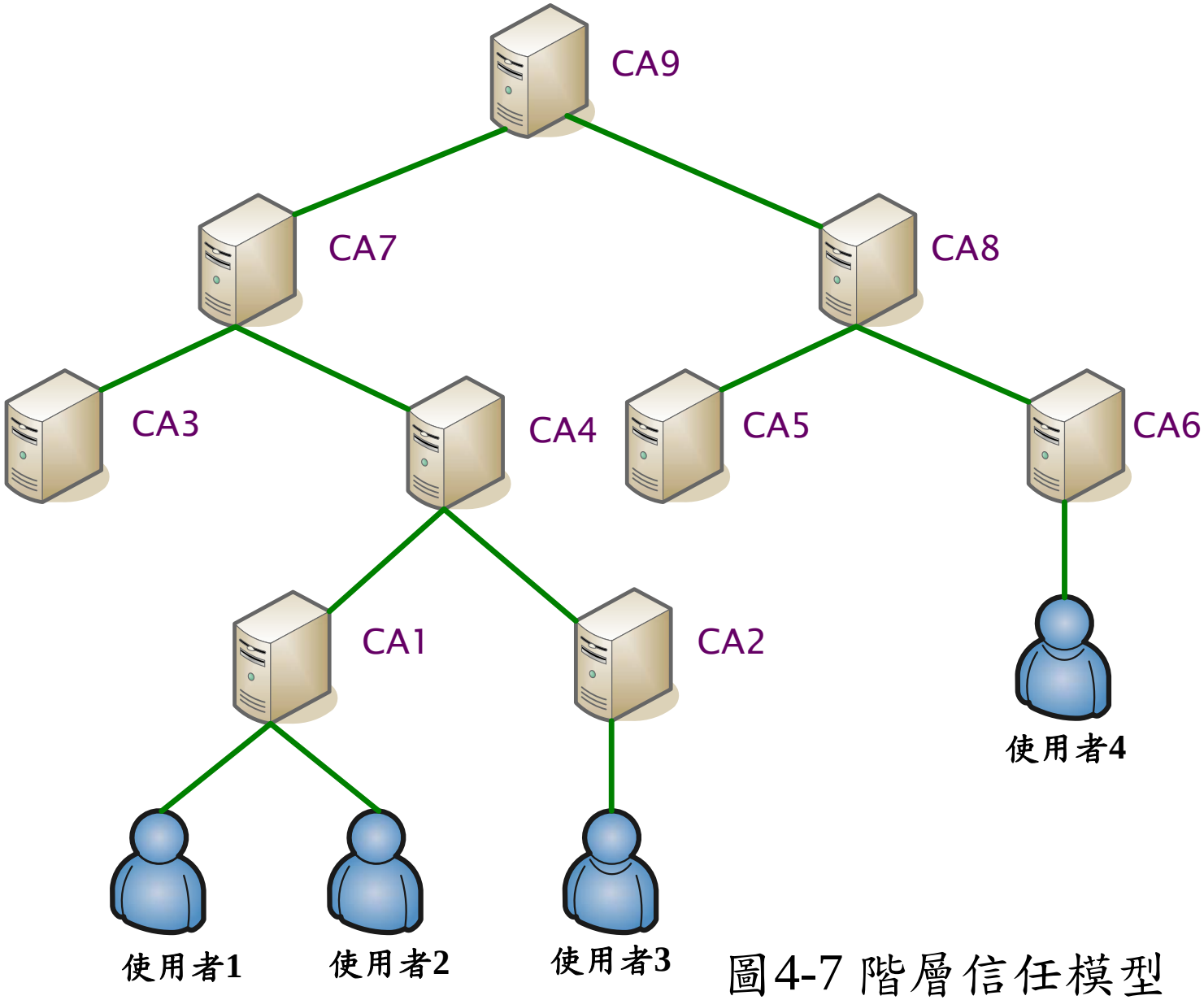


圖4-7 階層信任模型

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

數位憑證驗證程序

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4-8）。

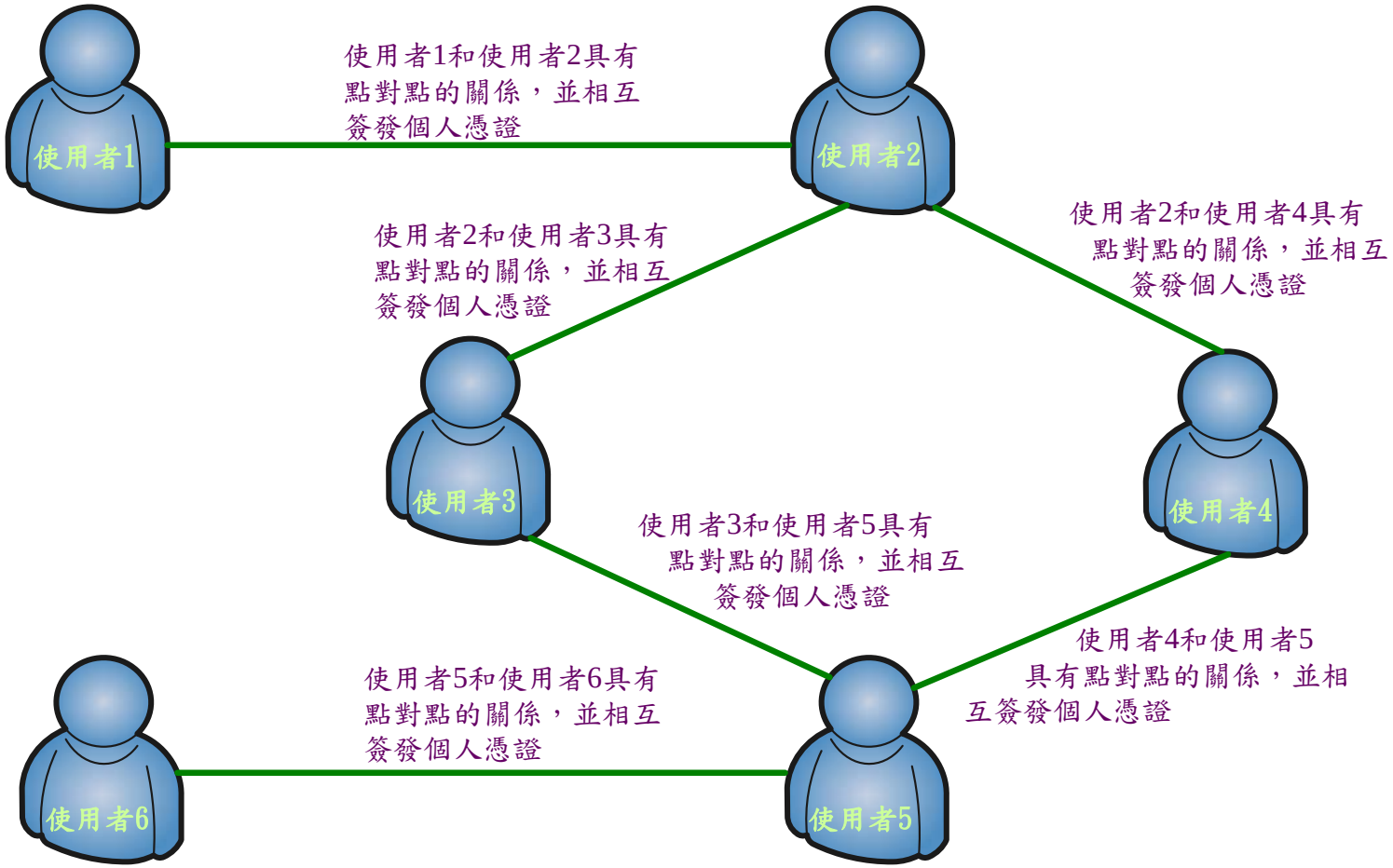

使用者1
使用者1和使用者2具有
點對點的關係，並相互
簽發個人憑證
使用者2
使用者2和使用者3具有
點對點的關係，並相互
簽發個人憑證
使用者2和使用者4具有
點對點的關係，並相互
簽發個人憑證
使用者3
使用者4
使用者3和使用者5具有
點對點的關係，並相互
簽發個人憑證
使用者4和使用者5
具有點對點的關係，並相
互簽發個人憑證
使用者5和使用者6具有
點對點的關係，並相互
簽發個人憑證
使用者6
使用者5

圖4-8 CA網狀架構

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

CA服務準則

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4-9）。

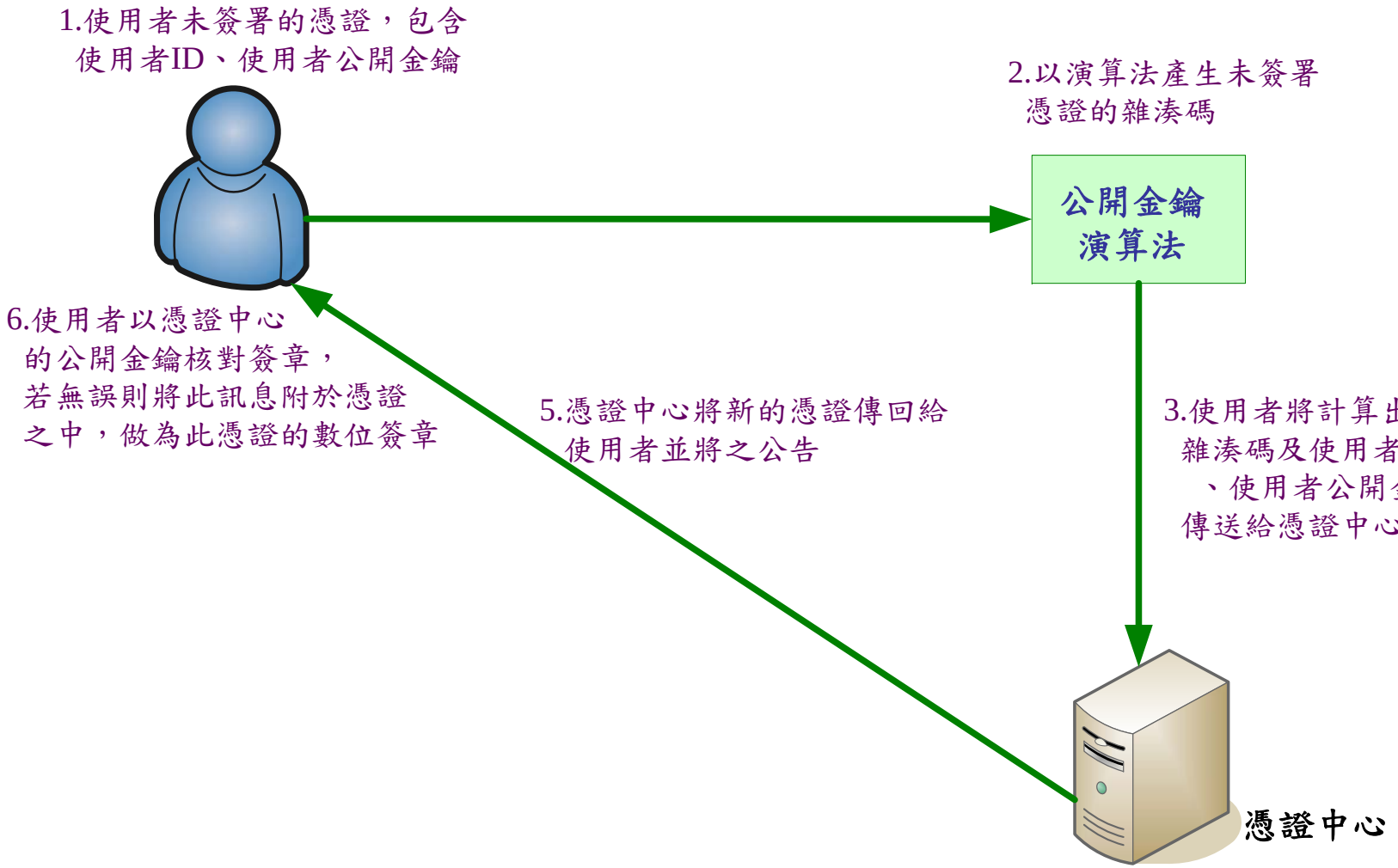


圖4-9 由憑證中心認證的公眾金鑰

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

結語

我們已學到內容:

(1) 數位憑證的用途、種類與格式

(2) 單向及相互鑑別程序

(3) X.509 v3 數位憑證

(4) 對數位憑證的製作、儲存、認證及憑證授權中心架構與服務作詳細的說明

透過原理解說，提供同學對數位憑證運作完整的概念。

※相關應用趨勢與研發議題

- 政府機關公開金鑰基礎建設（Government Public Key Infrastructure,GPKI），藉由自然人憑證提供線上電子化政府服務機制。
- 電子商務應用可信賴的憑證管理中心（Certification Authority）做為買方與賣方的互信基礎，確保電子交易的安全。