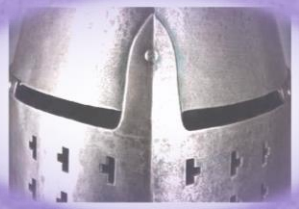


Chapter 14

Key Management and Distribution

Key Distribution Problem

- Problem: Deliver a key to two parties who wish to exchange data without allowing others to see the key
- Some techniques
  - If using symmetric encryption, the two parties must share the same key, and that key must be protected from access by others
  - If using public key system, it is easier, but key authentication is required
  - Frequent key changes are desirable to limit the amount of data compromised if an attacker learns the key

Symmetric Key Distribution

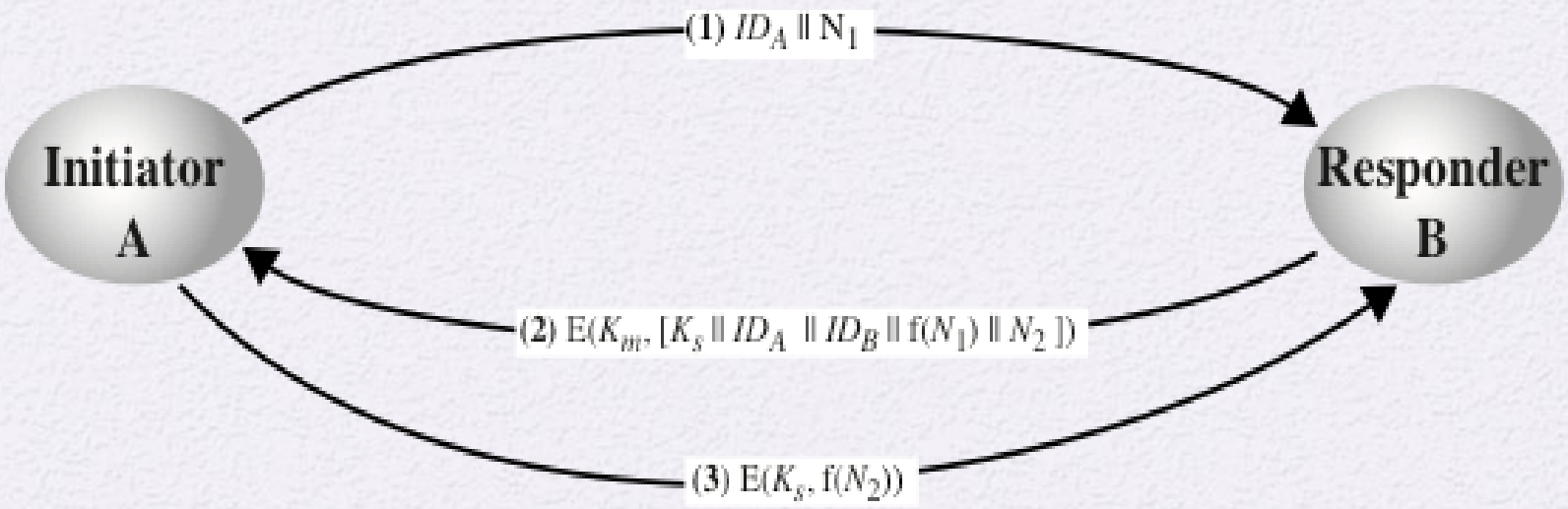
- A selects a key and physically deliver it to B
- A third party selects the key and physically deliver it to A and B
- If A and B have previously used a key, one party transmits the new key to the other by encrypting the new key with the old key
- If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B

Master and Session Keys

- It is hard for two parties to establish a shared key.
- Therefore, these keys are considered as “master” keys
- These master keys are used for establishing session keys for communication when needed.

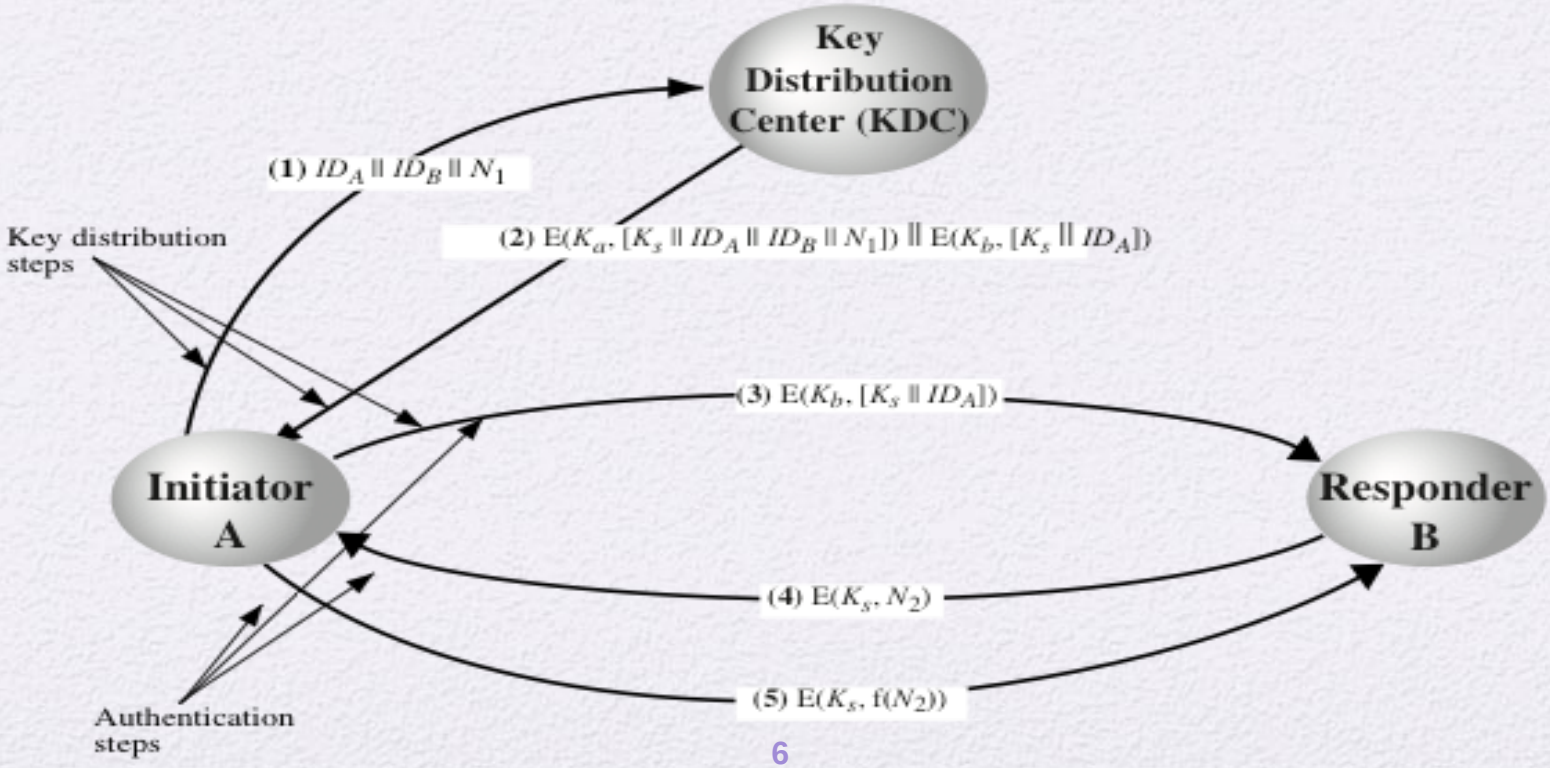
Session Key Distribution with Master Keys

- K_m: shared master key between A and B



Session Key Distribution with KDC

- Each use X shares with a master key K_X with the key distribution center (KDC)



Session Distribution with PK System

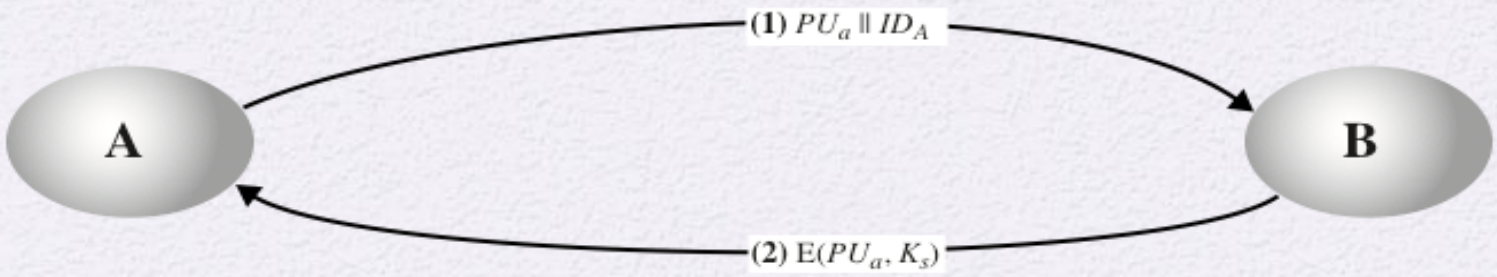


Figure 14.7 Simple Use of Public-Key Encryption to Establish a Session Key

Problem: How does B know that PU_a is A's public key?

➔ Need to authenticate PU_a

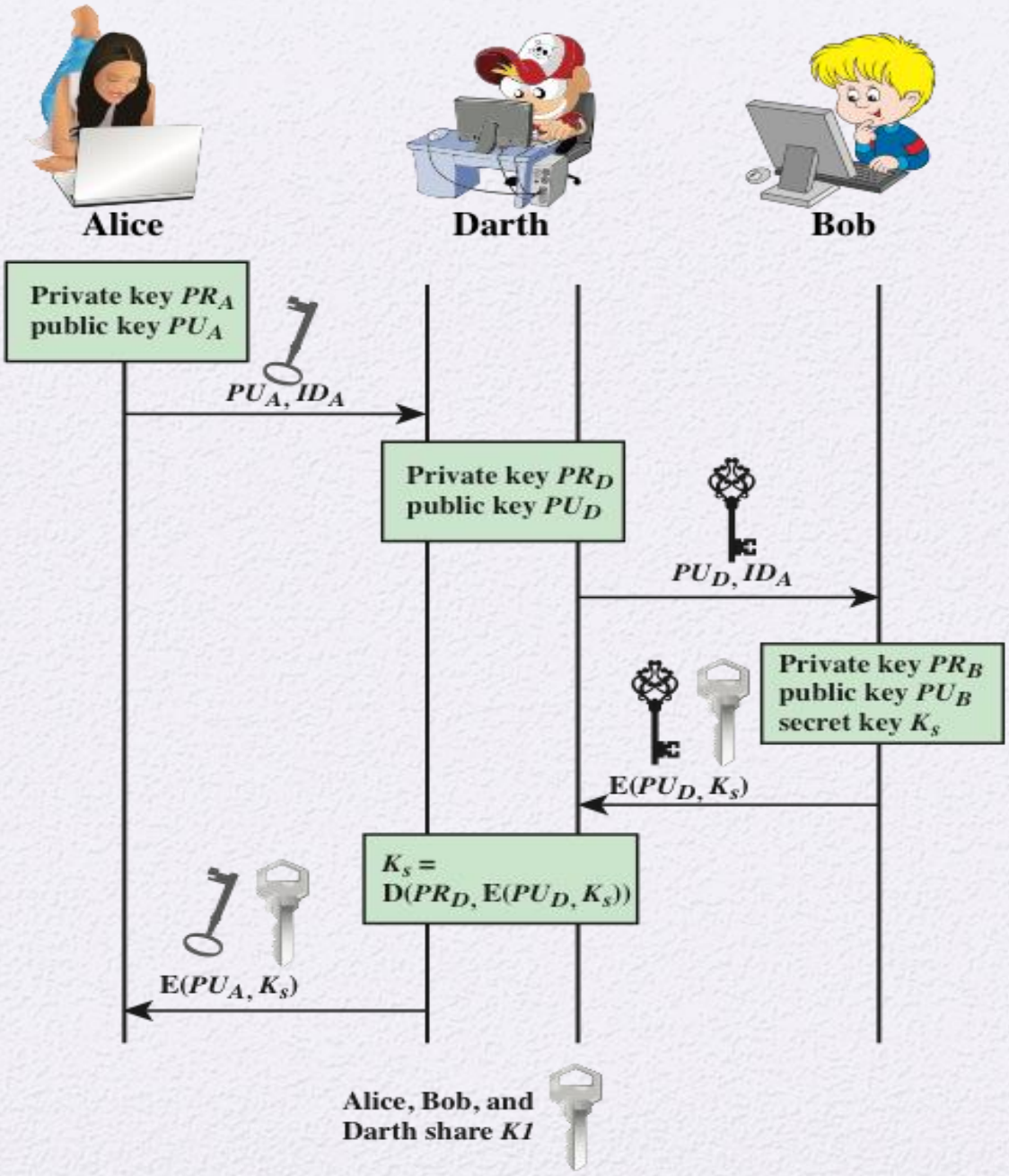
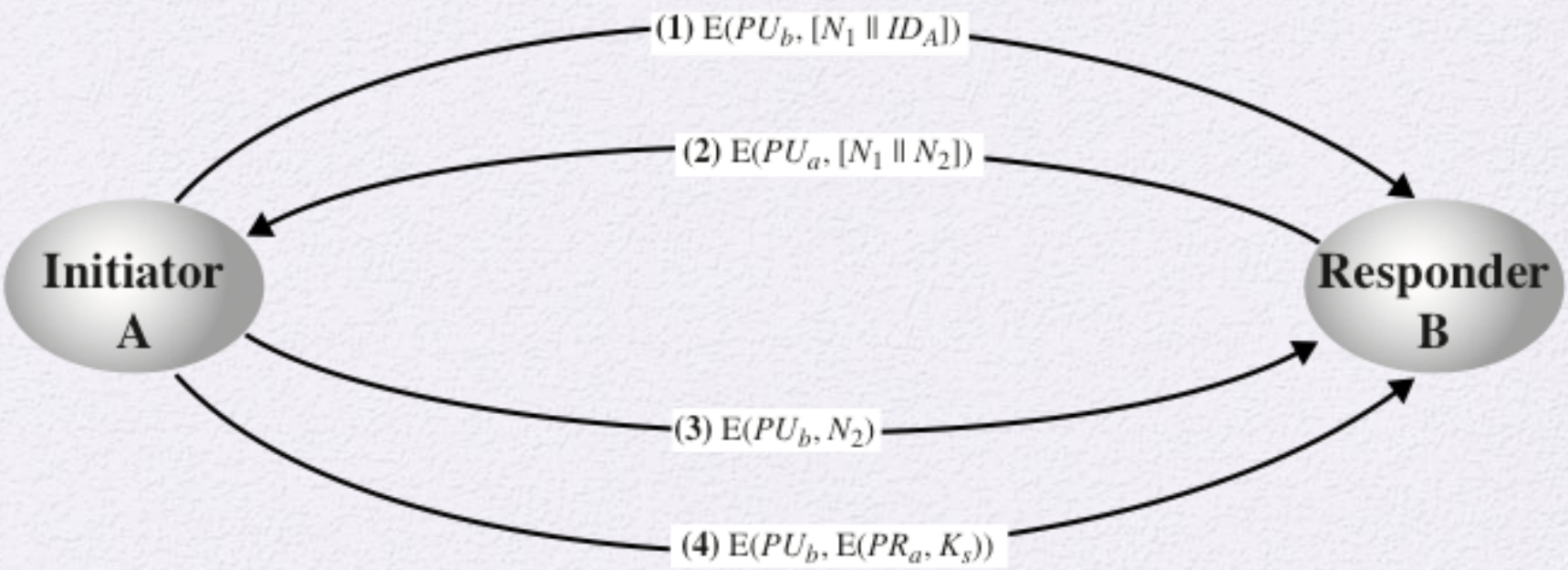


Figure 14.8 Another Man-in-the-Middle Attack

Another Key Distribution with Public Keys



Still have the problem of man-in-the-middle attack.

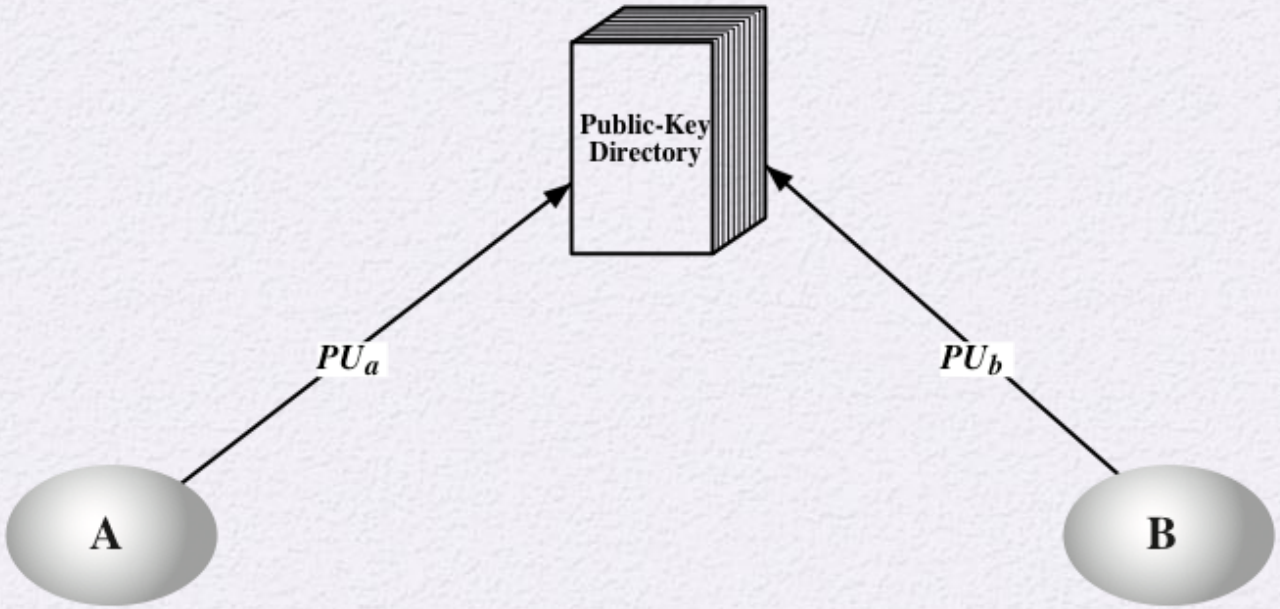
Distribution of Public Keys

- Some ways for the distribution of public keys
  - Public announcement
  - Publicly available directory
  - Public-key authority
  - Public-key certificate

Public announcement

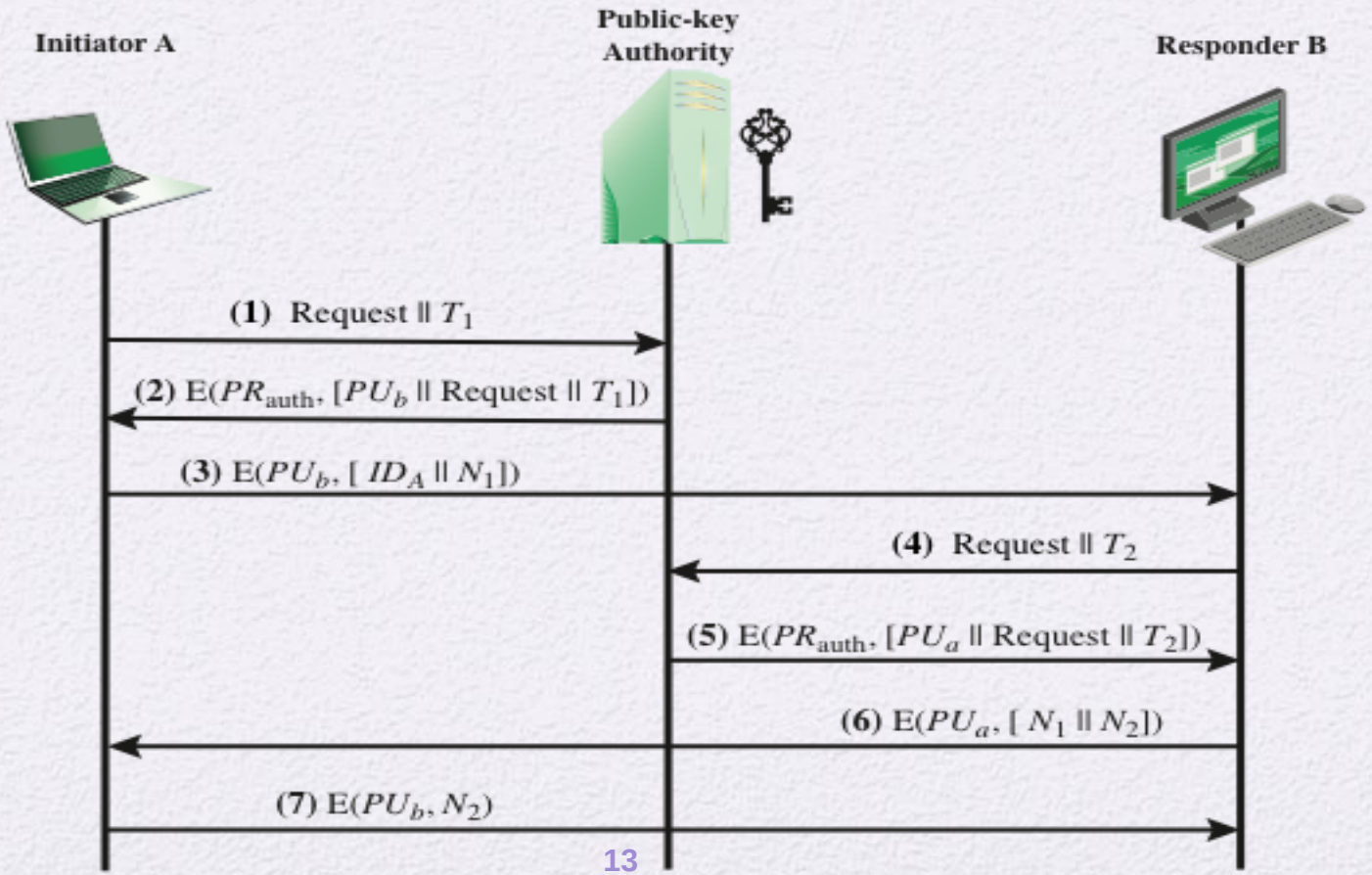
Figure 14.10 Uncontrolled Public Key Distribution

Public Directory



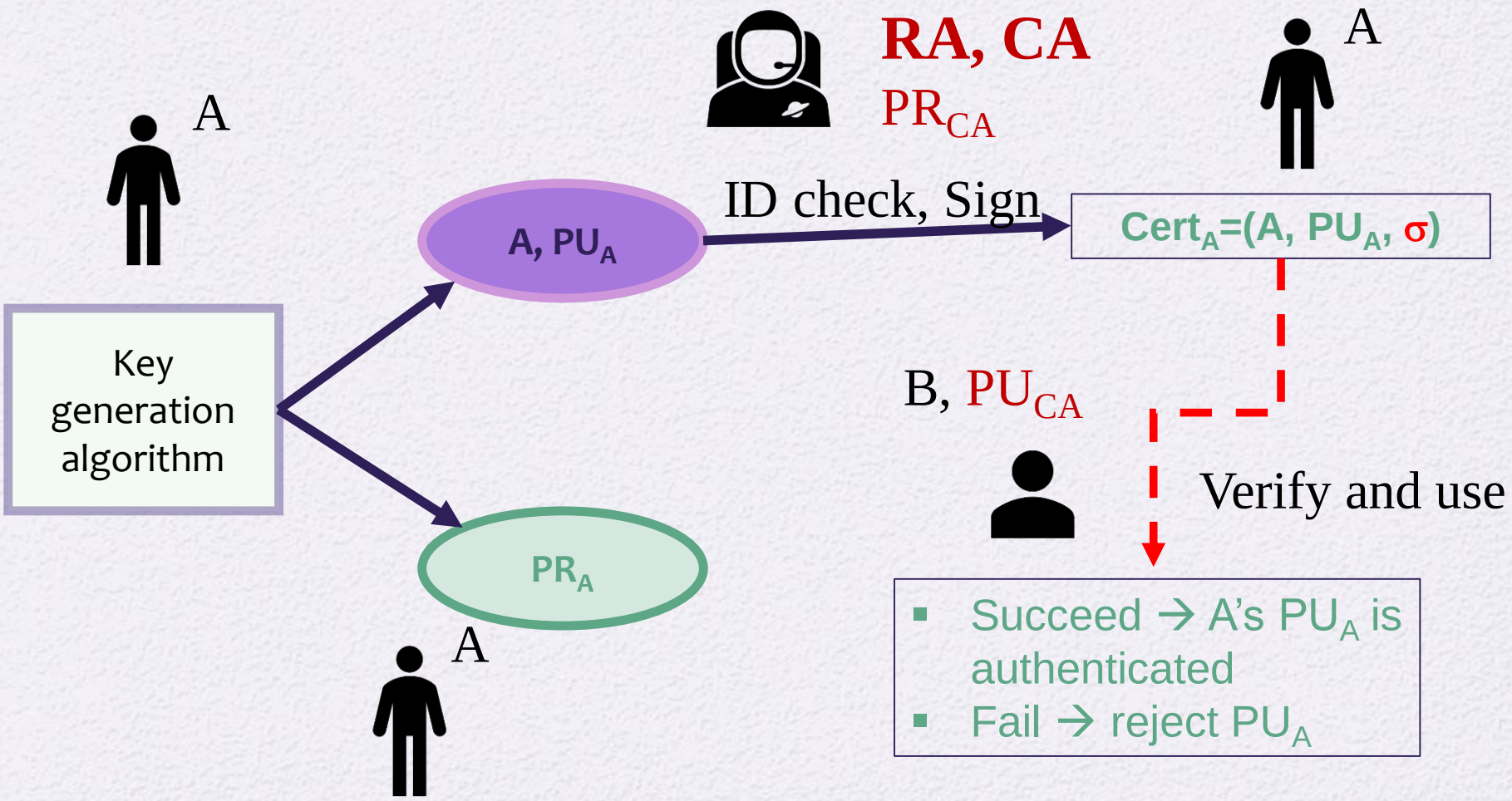
Public-Key Authority

- On-line authentication of public keys



Public-Key Certificate

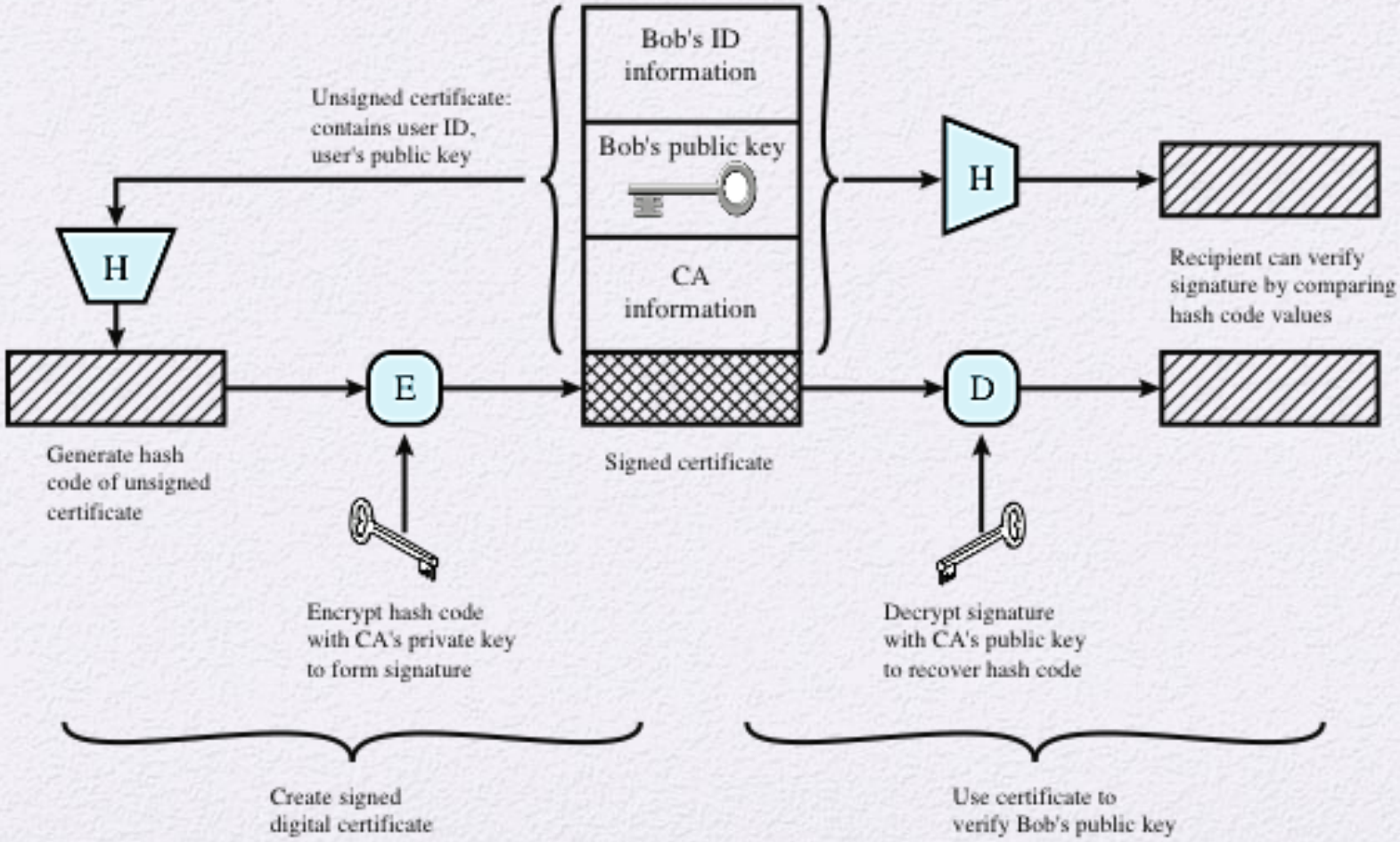
- **Off-line authentication of public keys**
- Trust starts from Certificate Authorities (CA)
  - Everyone trusts CA's, either direct or indirect
  - CA: authenticate A's public key PU_a with its private key
    - Signing the assertion of A's public key being PU_a
    - This assertion is called "certificate"
  - Another one with CA's public key PU_{CA} can verify the certificates issued by CA
  - The whole system is called Public-Key Infrastructure (PKI)


A
RA, CA
PR_CA
A
ID check, Sign
A, PU_A
Cert_A=(A, PU_A, σ)
Key generation algorithm
B, PU_CA
Verify and use
PR_A
A
Succeed → A's PU_A is authenticated
Fail → reject PU_A

X.509 Certificates

- Part of the X.500 series of a directory service
  - The directory is a server or distributed set of servers that maintains a database of information about users
- X.509 defines a framework for authentication services by the X.500 directory to its users
  - Use of public-key cryptography and digital signatures
- Each certificate contains the public key of a user and is signed with the private key of a trusted CA
- X.509 also defines authentication protocols by using public-key certificates

Use of Public-Key Certificates

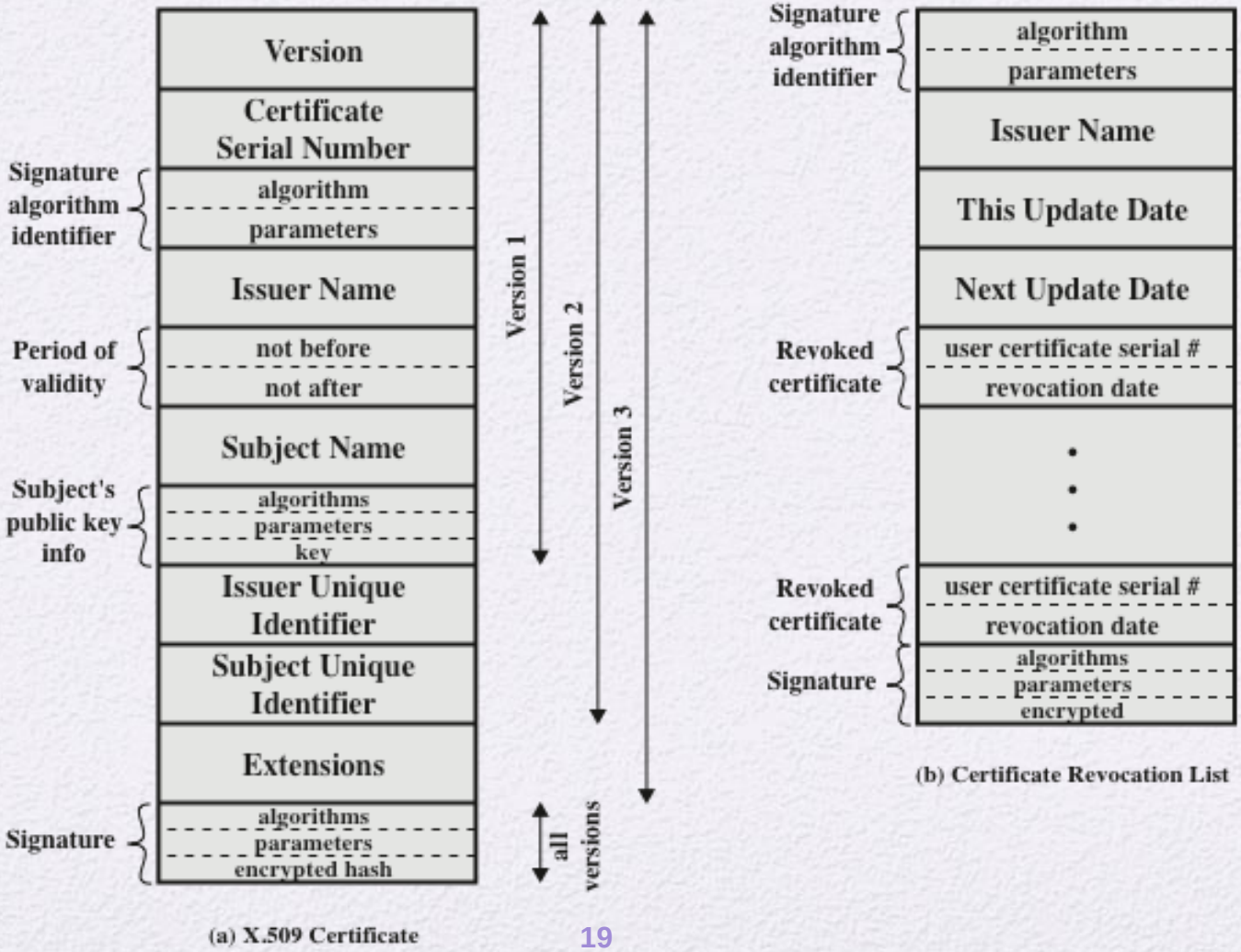


Certificates

Created by a trusted Certification Authority (CA) and have the following elements:

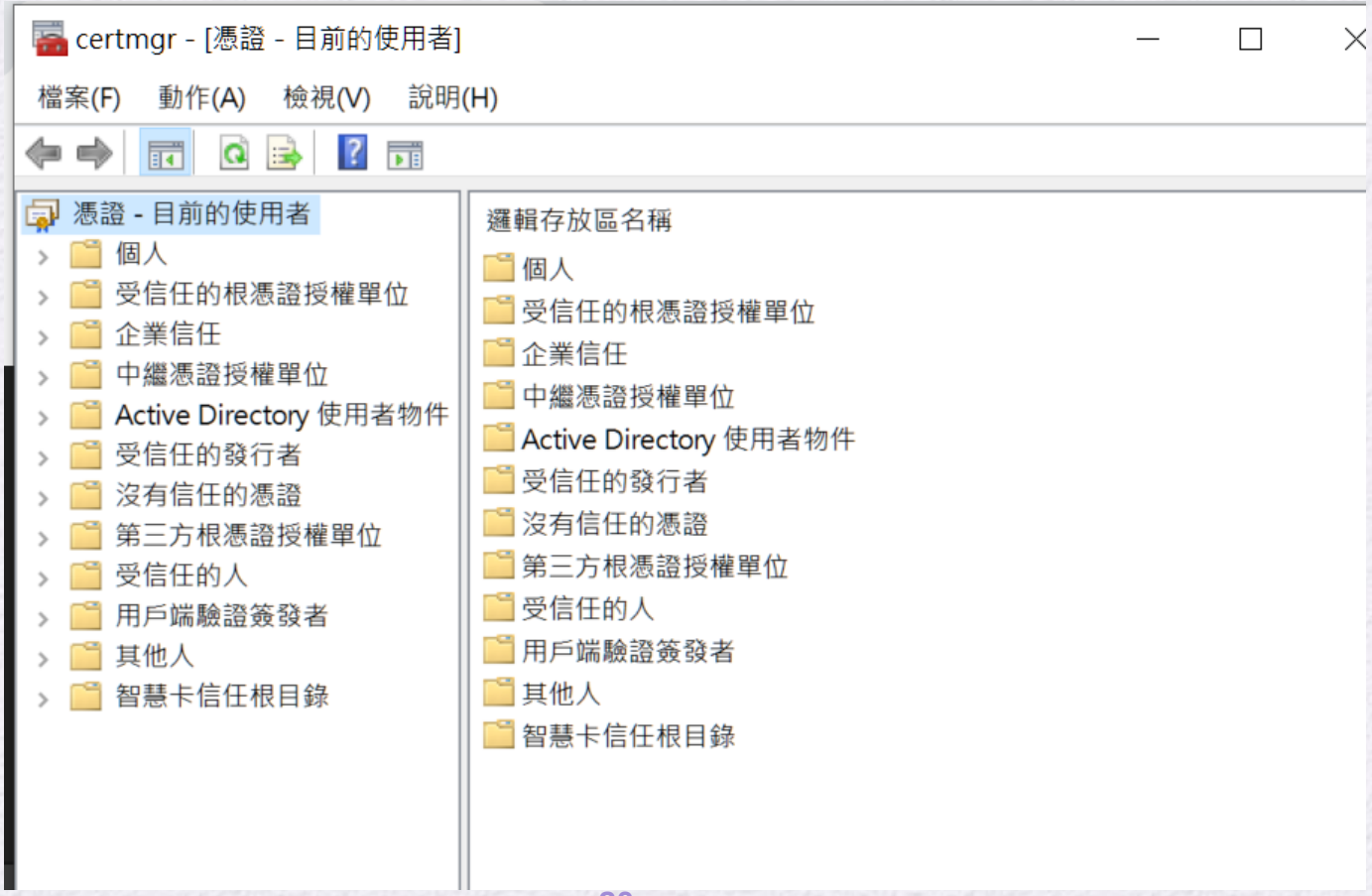
- Version
- Serial number
- Signature algorithm identifier
- Issuer name
- Period of validity
- Subject name
- Subject's public-key information
- Issuer unique identifier
- Subject unique identifier
- Extensions
- Signature

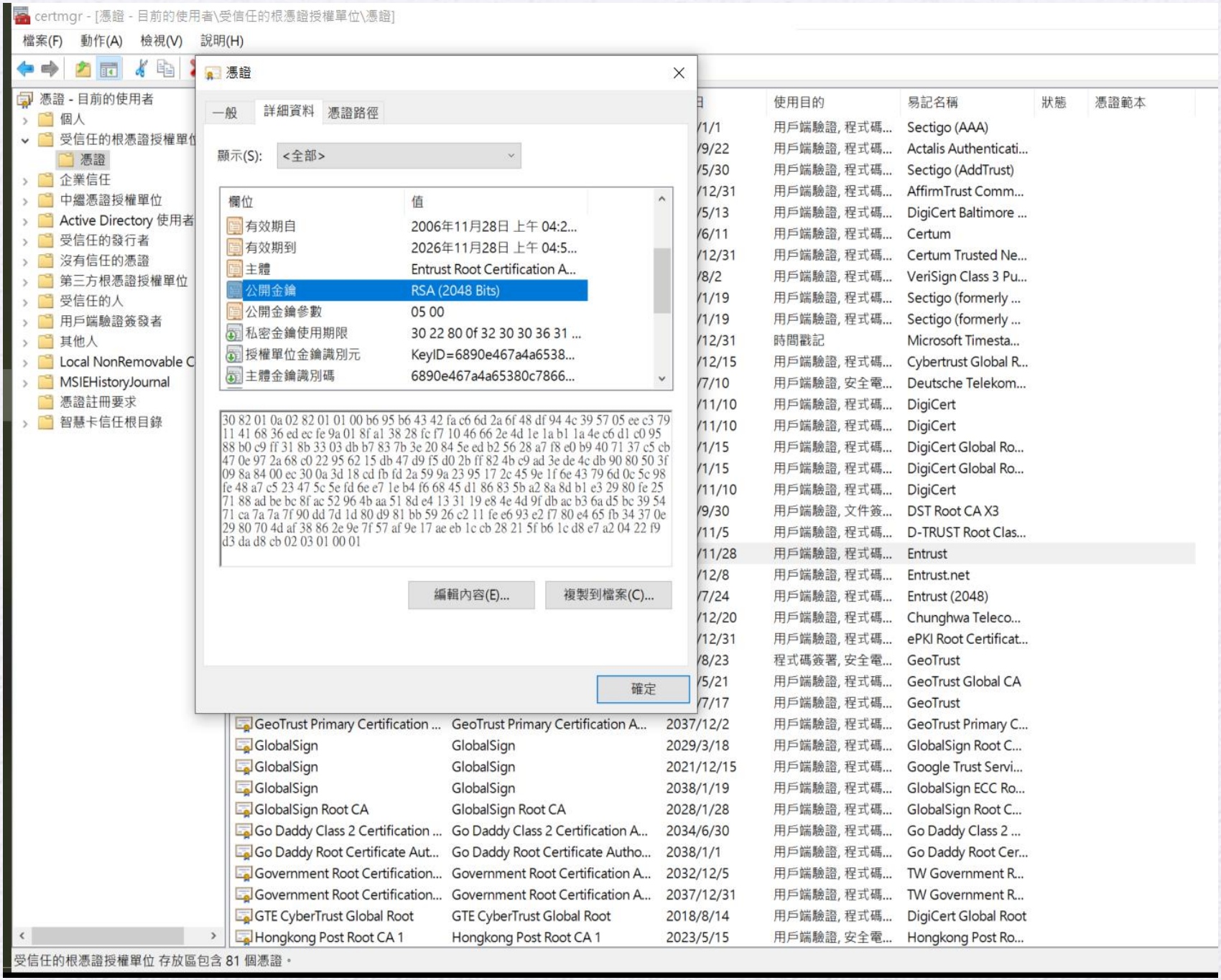
X.509 Certificate Format



Installed Certificates in Windows

- Run: certmgr.msc

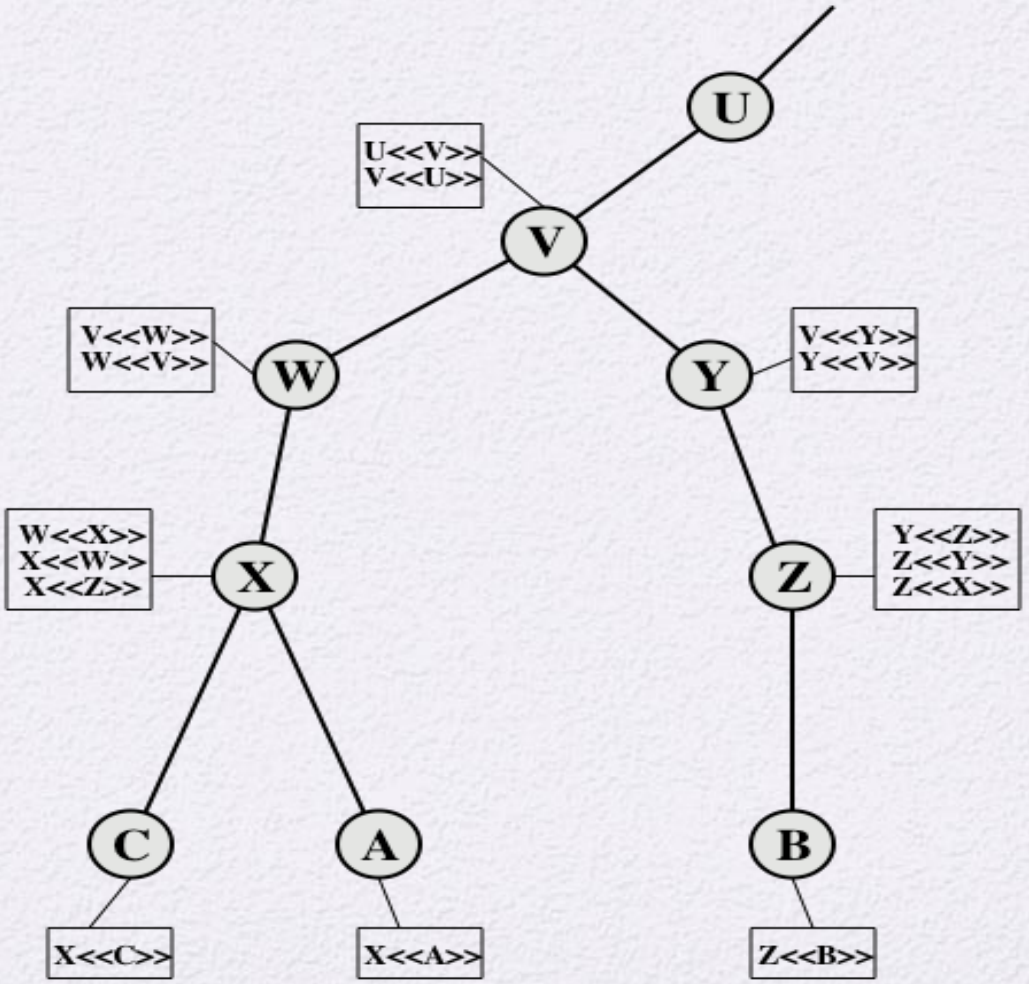



certmgr - [憑證 - 目前的使用者\受信任的根憑證授權單位\憑證]
檔案(F) 動作(A) 檢視(V) 說明(H)
憑證 - 目前的使用者
個人
受信任的根憑證授權單位
憑證
企業信任
中繼憑證授權單位
Active Directory 使用者
受信任的發行者
沒有信任的憑證
第三方根憑證授權單位
受信任的人
用戶端驗證簽發者
其他人
Local NonRemovable C
MSIEHistoryJournal
憑證註冊要求
智慧卡信任根目錄
憑證
一般
詳細資料
憑證路徑
顯示(S):
<全部>
欄位
值
有效期自
2006年11月28日 上午 04:2...
有效期到
2026年11月28日 上午 04:5...
主體
Entrust Root Certification A...
公開金鑰
RSA (2048 Bits)
公開金鑰參數
05 00
私密金鑰使用期限
30 22 80 0f 32 30 30 36 31 ...
授權單位金鑰識別元
KeyID=6890e467a4a6538...
主體金鑰識別碼
6890e467a4a65380c7866...
30 82 01 0a 02 82 01 01 00 b6 95 b6 43 42 fa c6 6d 2a 6f 48 df 94 4c 39 57 05 ee c3 79
11 41 68 36 ed ec fe 9a 01 8f a1 38 28 fc f7 10 46 66 2e 4d 1e 1a b1 1a 4e c6 d1 c0 95
88 b0 c9 ff 31 8b 33 03 db b7 83 7b 3e 20 84 5e ed b2 56 28 a7 f8 e0 b9 40 71 37 c5 cb
47 0e 97 2a 68 c0 22 95 62 15 db 47 d9 f5 d0 2b ff 82 4b c9 ad 3e de 4c db 90 80 50 3f
09 8a 84 00 ec 30 0a 3d 18 cd fb fd 2a 59 9a 23 95 17 2c 45 9e 1f 6e 43 79 6d 0c 5c 98
fe 48 a7 c5 23 47 5c 5e fd 6e e7 1e b4 f6 68 45 d1 86 83 5b a2 8a 8d b1 e3 29 80 fe 25
71 88 ad be bc 8f ac 52 96 4b aa 51 8d e4 13 31 19 e8 4e 4d 9f db ac b3 6a d5 bc 39 54
71 ca 7a 7a 7f 90 dd 7d 1d 80 d9 81 bb 59 26 c2 11 fe e6 93 e2 f7 80 e4 65 fb 34 37 0e
29 80 70 4d af 38 86 2e 9e 7f 57 af 9e 17 ae eb 1c cb 28 21 5f b6 1c d8 e7 a2 04 22 f9
d3 da d8 cb 02 03 01 00 01
編輯內容(E)...
複製到檔案(C)...
確定
使用目的
易記名稱
狀態
憑證範本
用戶端驗證, 程式碼... Sectigo (AAA)
用戶端驗證, 程式碼... Actalis Authenticati...
用戶端驗證, 程式碼... Sectigo (AddTrust)
用戶端驗證, 程式碼... AffirmTrust Comm...
用戶端驗證, 程式碼... DigiCert Baltimore ...
用戶端驗證, 程式碼... Certum
用戶端驗證, 程式碼... Certum Trusted Ne...
用戶端驗證, 程式碼... VeriSign Class 3 Pu...
用戶端驗證, 程式碼... Sectigo (formerly ...
用戶端驗證, 程式碼... Sectigo (formerly ...
時間戳記 Microsoft Timesta...
用戶端驗證, 程式碼... Cybertrust Global R...
用戶端驗證, 安全電... Deutsche Telekom...
用戶端驗證, 程式碼... DigiCert
用戶端驗證, 程式碼... DigiCert
用戶端驗證, 程式碼... DigiCert Global Ro...
用戶端驗證, 程式碼... DigiCert Global Ro...
用戶端驗證, 程式碼... DigiCert
用戶端驗證, 文件簽... DST Root CA X3
用戶端驗證, 程式碼... D-TRUST Root Clas...
用戶端驗證, 程式碼... Entrust
用戶端驗證, 程式碼... Entrust.net
用戶端驗證, 程式碼... Entrust (2048)
用戶端驗證, 程式碼... Chunghwa Teleco...
用戶端驗證, 程式碼... ePKI Root Certificat...
程式碼簽署, 安全電... GeoTrust
用戶端驗證, 程式碼... GeoTrust Global CA
用戶端驗證, 程式碼... GeoTrust
GeoTrust Primary Certification ... GeoTrust Primary Certification A... 2037/12/2 用戶端驗證, 程式碼... GeoTrust Primary C...
GlobalSign GlobalSign 2029/3/18 用戶端驗證, 程式碼... GlobalSign Root C...
GlobalSign GlobalSign 2021/12/15 用戶端驗證, 程式碼... Google Trust Servi...
GlobalSign GlobalSign 2038/1/19 用戶端驗證, 程式碼... GlobalSign ECC Ro...
GlobalSign Root CA GlobalSign Root CA 2028/1/28 用戶端驗證, 程式碼... GlobalSign Root C...
Go Daddy Class 2 Certification ... Go Daddy Class 2 Certification A... 2034/6/30 用戶端驗證, 程式碼... Go Daddy Class 2 ...
Go Daddy Root Certificate Aut... Go Daddy Root Certificate Autho... 2038/1/1 用戶端驗證, 程式碼... Go Daddy Root Cer...
Government Root Certification... Government Root Certification A... 2032/12/5 用戶端驗證, 程式碼... TW Government R...
Government Root Certification... Government Root Certification A... 2037/12/31 用戶端驗證, 程式碼... TW Government R...
GTE CyberTrust Global Root GTE CyberTrust Global Root 2018/8/14 用戶端驗證, 程式碼... DigiCert Global Root
Hongkong Post Root CA 1 Hongkong Post Root CA 1 2023/5/15 用戶端驗證, 安全電... Hongkong Post Ro...
受信任的根憑證授權單位 存放區包含 81 個憑證。

A Trust Hierarchy of CA's

The certificate of C issued by CA X:

X<<C>> = X{V, SN, AI, CA, UCA, A, UA, A_T, T^A}



Verify a Certificate

Certificate: $X\langle\langle C\rangle\rangle = X\{V, SN, AI, CA, UCA, A, UA, A_T, T^A\}$

- Obtain X's public key PU_X
  - Either pre-installed or obtained on-line
- Use's PU_X to verify $X\langle\langle C\rangle\rangle$
  - digital signature verification
- If CA X's public key PU_X is not trusted yet,
  - Go to find some X's certificate $W\langle\langle X\rangle\rangle$ issued by another CA W
  - Verify $W\langle\langle X\rangle\rangle$ by W's public key PU_w
- If CA W's public key PU_W is not trusted yet, …
  - Until you find a CA that can be trusted by you

Certificate Revocation

- Each certificate includes a period of validity
  - A new certificate is issued before expiration of the old one
- In some occasions, we need to revoke a certificate before it expires
  - The user's private key is assumed to be compromised
  - The user is no longer certified by this CA
  - The CA's certificate is assumed to be compromised
- Each CA maintains a list of all revoked but not expired certificates issued by the CA
  - These lists should be posted on the directory

Summary

- Symmetric key distribution using symmetric encryption
  - Key distribution scenario
  - Hierarchical key control
  - Session key lifetime
  - Transparent key control scheme
  - Decentralized key control
  - Controlling key usage
- Symmetric key distribution using asymmetric encryption
  - Simple secret key distribution
  - Secret key distribution with confidentiality and authentication
- Distribution of public keys
  - Public announcement of public keys
  - Publicly available directory
  - Public-key authority
  - Public-key certificates
- X.509 Certificates
  - X.509 Version 3