# Cryptography and Security

**Cunsheng DING**

**HKUST, Hong Kong**

**Version 3**

# Lecture 09: Public-Key Infrastructure

## Main Topics of this Lecture

1. Digital certificate
2. Certificate authority (CA)
3. Public key infrastructure (PKI)

# Part I: Digital Certificates

# What is a Digital Certificate?

**Definition:** A digital certificate is an electronic document issued and digitally signed by a "certification authority" that authenticates the identity of its holder.

- It can protect data exchanged online if a public-key is included.
- They cannot be forged.

**Real world example:** passport

## A Classification of Digital Certificates

- Server certificates, and
- personal certificates (e.g., containing a public key), also called client certificates.

**Question:** Any standard on the format of digital certificates?

# The X.509v3 Certificate

**Signature algorithm identifier:** The algorithm used to sign the certificate, together with any associated parameters. This information is repeated in the Signature field at the end of the certificate.

**Issuer and subject name:** X.500 Distinguished Name (DN)

- Comprised of multiple Relative DNs (RDNs)
- C = country, ST = state, L = locale, O = organiz.
- OU = organization unit, CN = common name

**Subject's public key information:** Public key of the subject, plus the identifier of the algorithm for which this key is to be used, together with any associated parameters.

# The X.509v3 Certificate

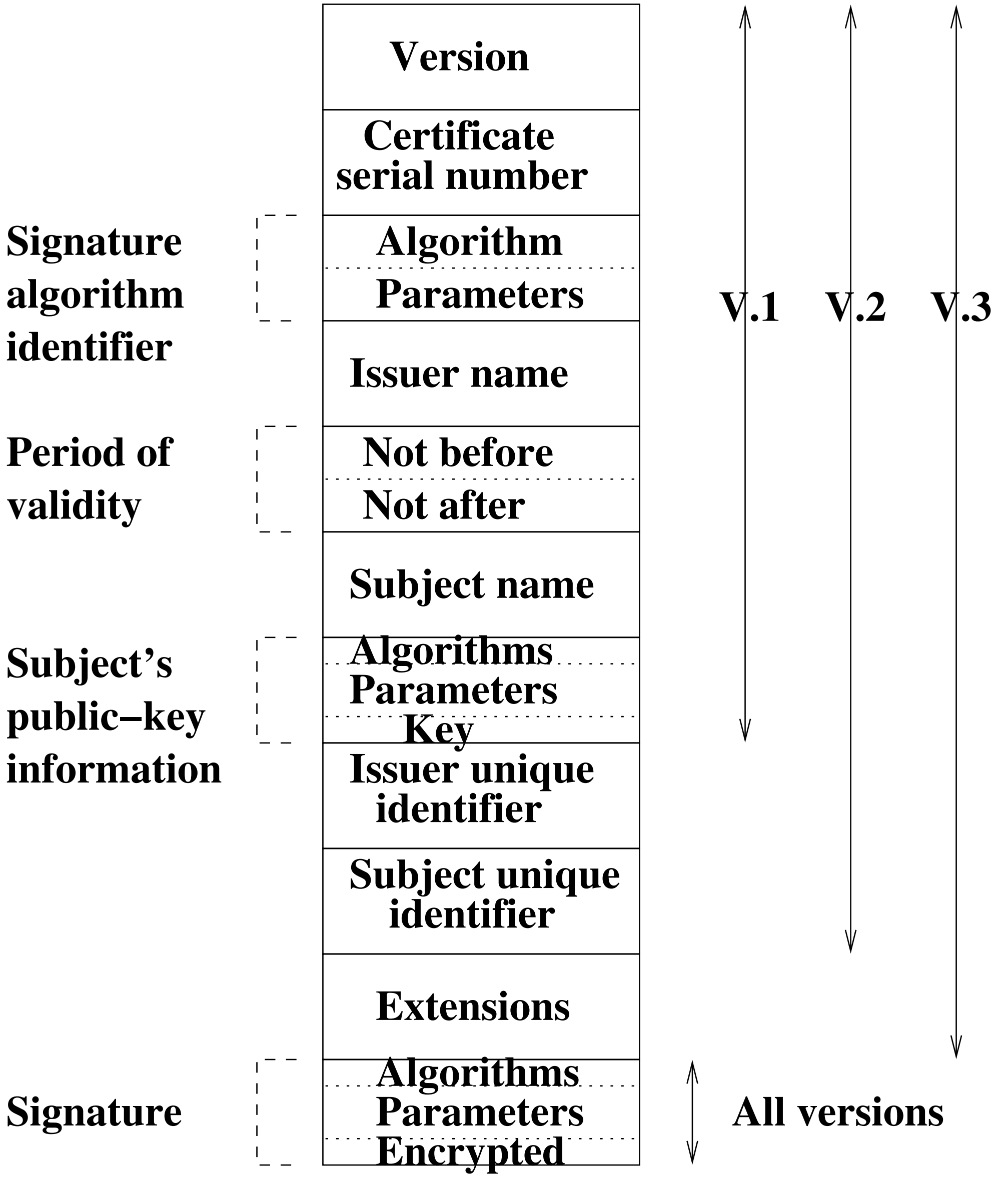
**Issuer unique identifier:** An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been used for different entities.

**Subject unique identifier:** An optional bit string field used to identify uniquely the subject in the event the X.500 name has been used for different entities.

**Extensions:** A key usage extension defines for which applications and under which policies a certificated public key can be used.

**Examples:** Digital signature, nonrepudiation, key encryption, data encryption, key agreement, CA signature verification on certificates, CA signature verification on CRL.

**Remark:** CRL: Certificate Revocation List (to be introduced later).

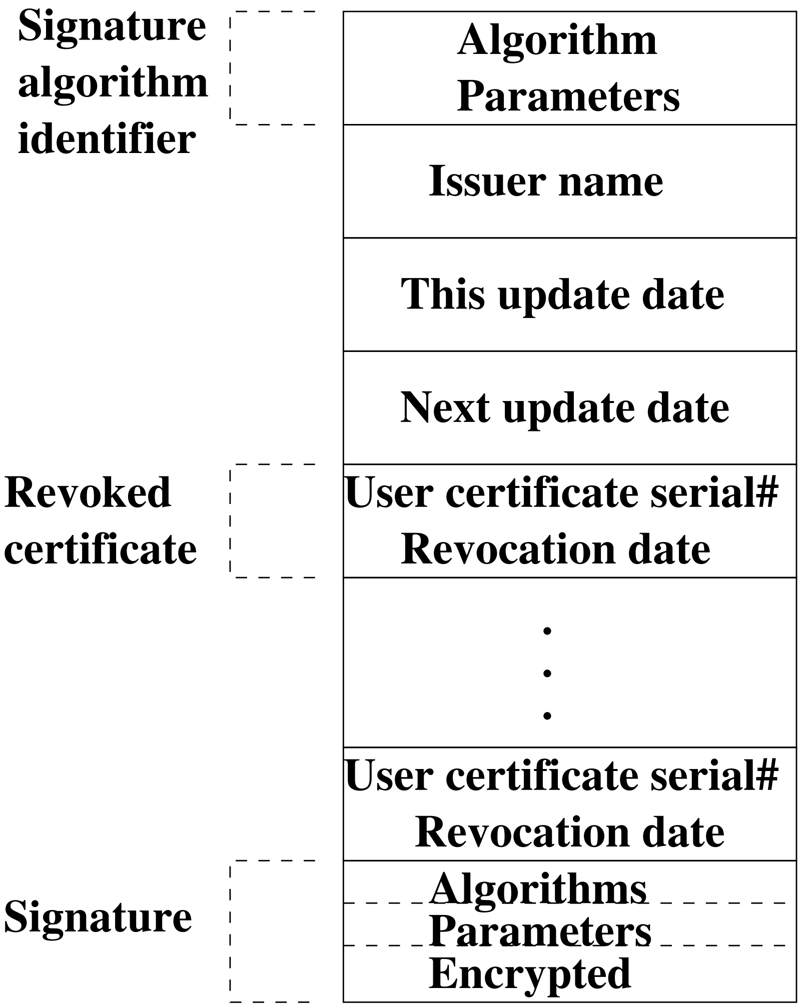

Version
Certificate serial number
Signature algorithm identifier
Algorithm
Parameters
Issuer name
Period of validity
Not before
Not after
Subject name
Subject's public–key information
Algorithms
Parameters
Key
Issuer unique identifier
Subject unique identifier
Extensions
Signature
Algorithms
Parameters
Encrypted
V.1
V.2
V.3
All versions

# Sample X.509 Certificates

```
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
        OU=Certification Services Division,
        CN=Thawte Server CA/emailAddress=server-certs@thawte.com
Validity
    Not Before: Aug  1 00:00:00 1996 GMT
    Not After : Dec 31 23:59:59 2020 GMT
Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
         OU=Certification Services Division,
         CN=Thawte Server CA/emailAddress=server-certs@thawte.com
Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public Key: (1024 bit)
     Modulus (1024 bit):
         00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
         68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
         85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
         6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
         6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
         29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
         6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
         5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
         3a:c2:b5:66:22:12:d6:87:0d
     Exponent: 65537 (0x10001)
X509v3 extensions:
     X509v3 Basic Constraints: critical
        CA:TRUE
```

```
Signature Algorithm: md5WithRSAEncryption
        07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
        a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
        3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
        4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
        8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
        e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
        b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
        70:47
```

This is an example of a self-signed certificate. There's no way to verify this certificate except by checking it against itself; instead, these top-level certificates are manually stored by web browsers. Thawte is one of the root certificate authorities recognized by both Microsoft and Netscape. This certificate comes with the web browser and is trusted by default.



Certificate Revocation List

# More Information on X.509 Digital Certificates

- Go to: https://en.wikipedia.org/wiki/X.509

# Part II: Certificate Authority

# Certificate Authority

**(1) It is a trusted third-party.**

It is responsible for verifying the identities of cryptographic key holders.

**(2) It issues digital certificates.**

Asserts that a public key is part of a key-pair held by an individual, organization, or other entity.

**(3) It publishes policy detailed in a Certification Practices Statement (CPS).**

# Part III: Public Key Infrastructure

# Definition of PKI

**Definition:** Standards and services that facilitate the use of public-key cryptography and X.509 version 3 certificates in a networked environment are collectively called Public-key Infrastructure (PKI).

**Remark:** There are slightly different definitions. This is similar to **education infrastructure**.

# Elements of Public Key Infrastructure

- Certificate Authority (CA): e.g., OpenSSL, Netscape, Verisign, Entrust, RSA Keon
- Public/Private Key Pairs - key management
- X.509 Certificates - certificate management
- LDAP servers (LDAP: Lightweight Directory Access Protocol)
- Certification Practice Statement (issued by a Certification Authority (CA) to specify the practices and standards that the Certification Authority (CA) employs in issuing certificates.)

## Issues

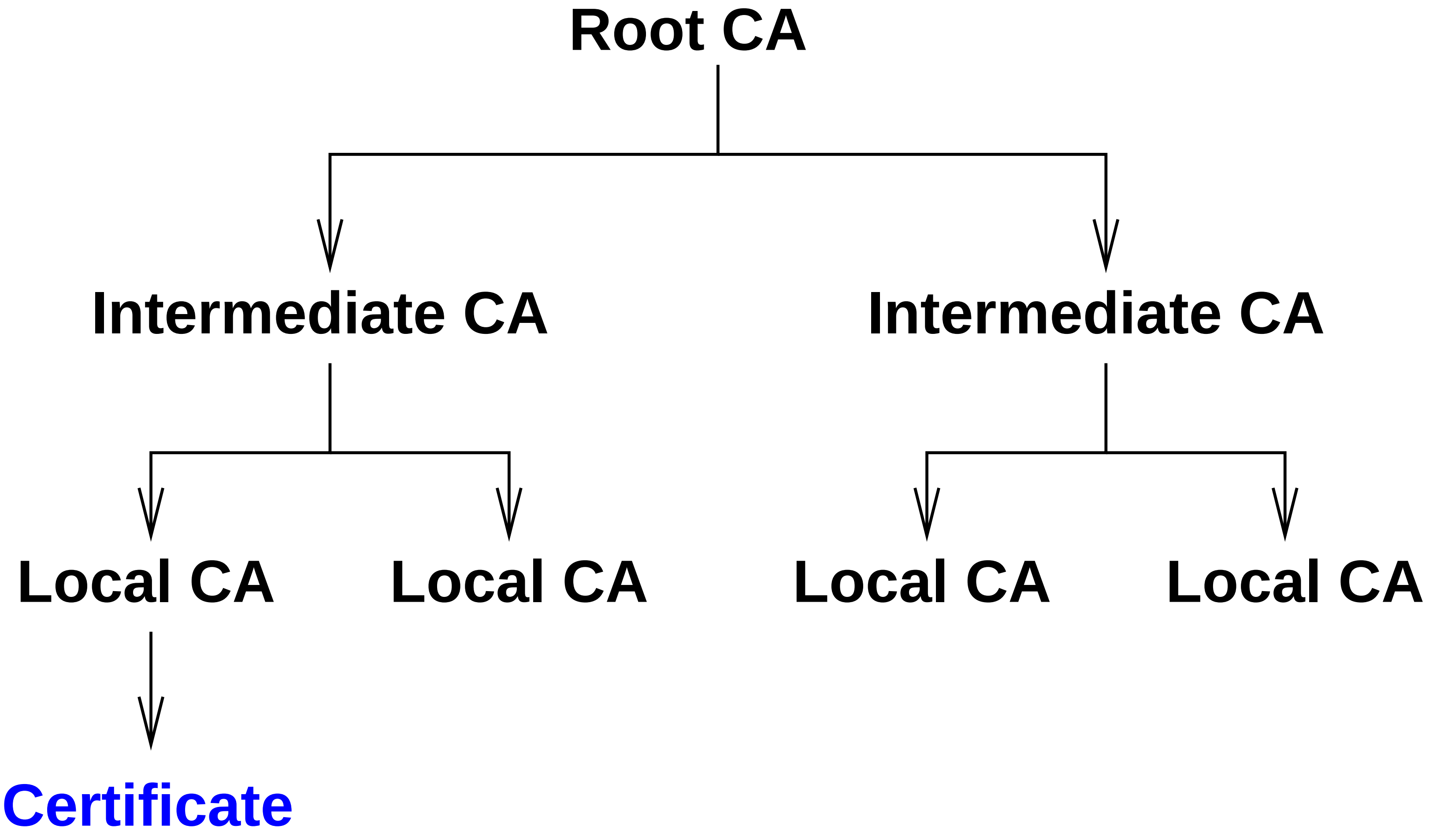
- Scalability: How many certificates can one CA manage?
- Administration: How to revoke already issued certificates?
- Trust:

  Why should I trust your CA?

# Issues: PKI Scalability

- A large PKI requires distributed CAs
  - Local, Reginal, National CAs
  - International CAs
- Certificate Hierarchy
  - Intermediate CA certificates are signed by the CA one-step up.
  - End-user certificates are part of a certificate chain.

# Certificate Hierarchy



Root CA

Intermediate CA

Intermediate CA

Local CA

Local CA

Local CA

Local CA

Certificate

# Verifying Certificate Chains

- Entity accepting certificates must be able to verify CA in the chain.
  - Should the entire chain be present during a handshake?
- Certificate types
  - CA certificates ("Basic Constraints" indicate whether the certificate belongs to a CA)
  - End-user certificates, which cannot be used to issue digital certificates.
- Must distinguish types of certificates. Otherwise, end-users could sign bogus certificates.
- X.509v3 extensions indicate usages of a certificate.

# Methods of Publishing Digital Certificates

**Without a 3rd party:** Own web page, via FTP file

**With a 3rd party:** Dedicated key server, directory

# Why Digital Certificates on Server?

- Encrypt data for someone without prior contact.
- You do not have to store all keys yourself.
- Easier distribution of new keys and updates.

# Directory as Key Server

- As a publishing medium for public keys and certificates.
- Users can put their public key certificate there.
- CAs may put their certificates there.
- The directory documents revocation of keys and/or certificates in the CRL.
- It documents status of a certificate at specific time.