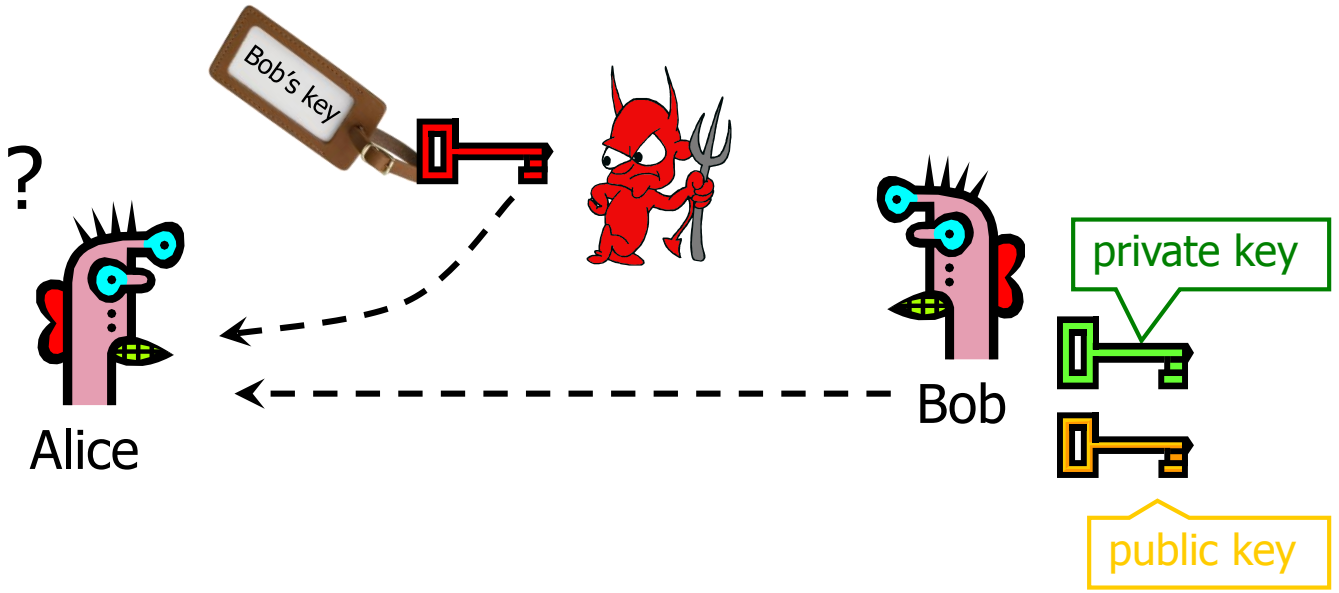
Fundamentals of Information & Network Security
ECE 471/571

Lecture #28: Public Key Infrastructure

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Authenticity of Public Keys



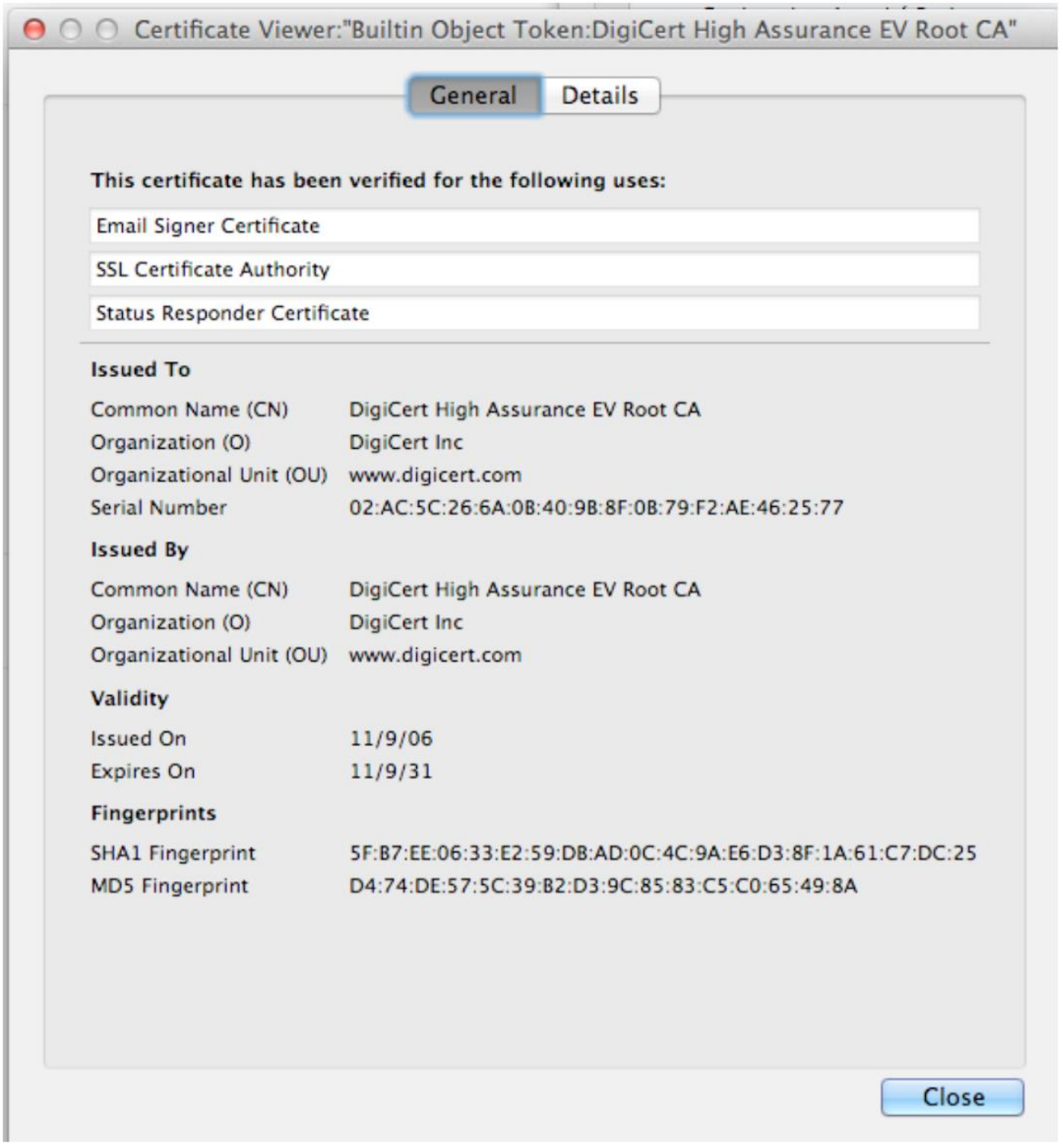
Problem: How does Alice know that the public key she received is really Bob's public key?

Certificate and CA

- Certificate: signed public key
- Solution: Certification Authority (CA), a trusted node
  - Public key equivalent of KDC
  - Register (by phone or by …) the public key with CA
  - CA signs each node's public key with its private key; the result is called a certificate, which can be stored anywhere.
  - Everyone is required to be pre-configured with CA's public key (trust anchor), so he can verify the authenticity of someone else' certificate.

Advantages of CAs

- The CA does not need to be on-line
- It can be a simpler device
- The failure of the CA would not disable the whole network
- Certificates are not security-sensitive.
- A compromised CA cannot decrypt conversations between two parties.


Certificate Viewer:"Builtin Object Token:DigiCert High Assurance EV Root CA"
General
Details
This certificate has been verified for the following uses:
Email Signer Certificate
SSL Certificate Authority
Status Responder Certificate
Issued To
Common Name (CN) DigiCert High Assurance EV Root CA
Organization (O) DigiCert Inc
Organizational Unit (OU) www.digicert.com
Serial Number 02:AC:5C:26:6A:0B:40:9B:8F:0B:79:F2:AE:46:25:77
Issued By
Common Name (CN) DigiCert High Assurance EV Root CA
Organization (O) DigiCert Inc
Organizational Unit (OU) www.digicert.com
Validity
Issued On 11/9/06
Expires On 11/9/31
Fingerprints
SHA1 Fingerprint 5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25
MD5 Fingerprint D4:74:DE:57:5C:39:B2:D3:9C:85:83:C5:C0:65:49:8A
Close

Advantages of CAs

- The CA does not need to be on-line
- It can be a simpler device
- The failure of the CA would not disable the whole network
- Certificates are not security-sensitive.
- A compromised CA cannot decrypt conversations between two parties.

Certificate Revocation

- Certificate for A:
  - CA.privateKey{A.name, A.publicKey, expiration time, serial number, …}
  - Every one in the group has a trust relationship with CA, with CA's public key pre-configured.
  - CA can extend this trust relationship by issuing certificates.

- When A leaves the group, this trust extension should be terminated, but if A's certificate is not expired, this extension still exists.

- Certificate Revocation List (CRL) is published periodically to revoke certificate.

- B accepts A's certificate only when it has a valid CA signature, has not expired, and is not in the CA's most recent CRL.

Public Key Infrastructure

- The task of PKI is to securely distribute public keys.
- A PKI enables communication parties to authenticate each other and establish confidentiality and integrity *without prior contact or having to exchange any secret information in advance.*

- PKI consists of
  - Certificate issuance
  - a repository for retrieving certificates
  - a method of revoking certificates
  - a method of evaluating a chain of certificates from a trust anchor to the target name

Hierarchical Approach

- Single CA certifying every public key is impractical
- Instead, use a trusted root authority
  - For example, Verisign
  - Everybody must know the public key for verifying root authority's signatures

- Root authority signs certificates for lower-level authorities, lower-level authorities sign certificates for individual networks, and so on
  - Instead of a single certificate, use a certificate chain
    - $sig_{Verisign}(\text{“UA”}, PK_{UA})$, $sig_{UA}(\text{“Alice”}, PK_{Alice})$

Question: What happens if root authority is ever compromised?

Authencity of Web pages comes under attack

By Byron Acohido, USA TODAY

Updated 2h 1m ago

Comment 95 Recommend 95 Tweet 167

Reprints & Permissions

The keepers of the Internet have become acutely concerned about the Web's core trustworthiness.

USA TODAY

Hackers cracked three companies that work with the most popular Web browsers to ensure the authenticity of Web pages where consumers type in sensitive information, such as account log-ons, credit card numbers and personal data.

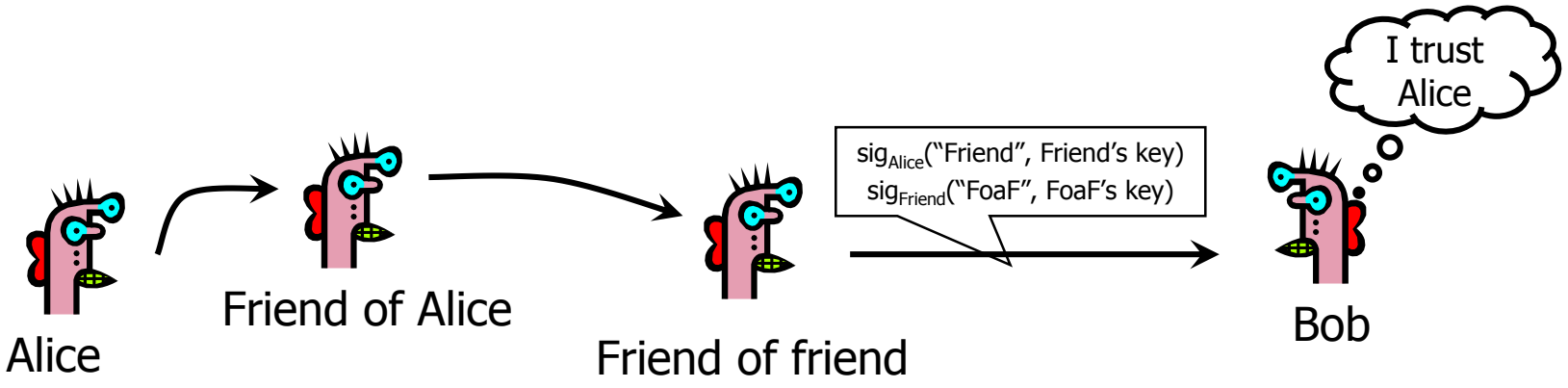
The hacked firms are among more than 650 digital certificate authorities, or CAs, worldwide that ensure that Web pages are the real deal when served up by Microsoft's Internet Explorer, Firefox, Opera, Apple's Safari and Google's Chrome.

But a hacker gained access to digital certificate supplier DigiNotar this summer and began issuing forged digital certificates for hundreds of Web pages published by dozens of marquee companies.

http://www.usatoday.com/tech/news/story/2011-09-27/webpage-hackers/50575024/1

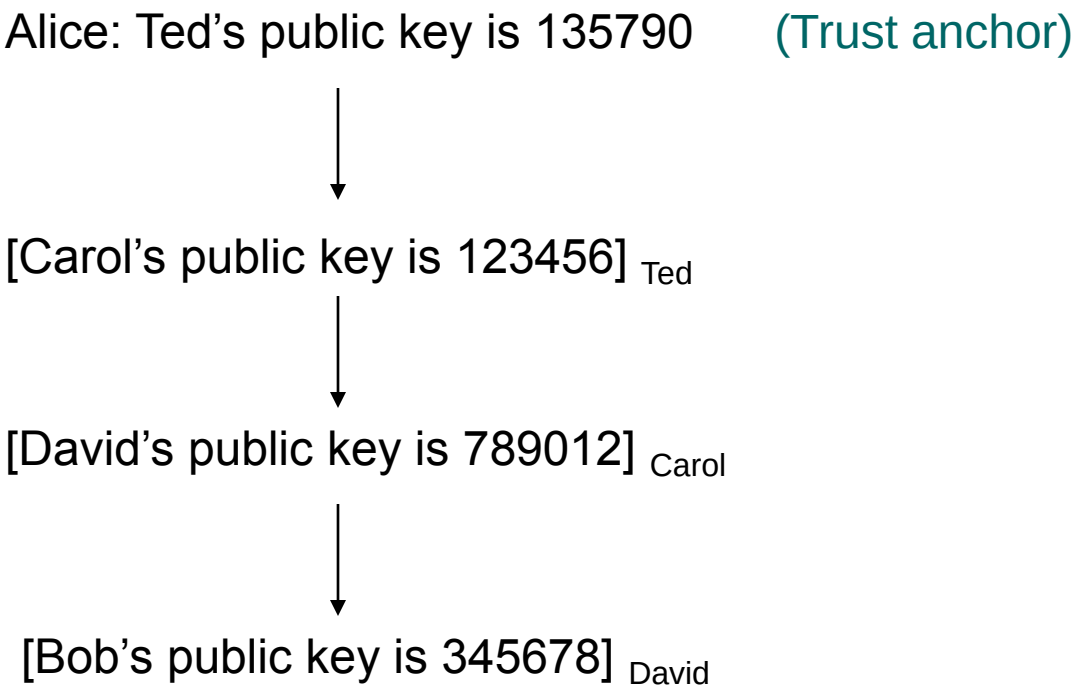
Alternative: “Web of Trust”

- Used in PGP (Pretty Good Privacy)
- Instead of a single root certificate authority, each person has a set of keys they “trust”
  - If public-key certificate is signed by one of the “trusted” keys, the public key contained in it will be deemed valid
- Trust can be transitive
  - Can use certified keys for further certification



Chain of Trust

- Small World: Any two people in this world can be connected via “six degrees of separation”



PKI Trust Model

- Answering the following questions.
  - Where to get trust anchors?
  - Which chain of trust to follow?

- Various models
  - Monopoly Model
  - Monopoly plus Registration Authorities
  - Delegated CAs
  - Oligarchy
  - Anarchy Model
  - Top-Down with Name Constraints
  - Bottom-UP with Name Constraints

Monopoly Model

- Monopoly Model
  - There is a single CA, which is the trust anchor of all principles.

- Monopoly Plus Registration Authorities (RAs)
  - CA issues certificates, but delegates the verification of keys to RAs.

Delegated CAs

- The trust anchor CA generates certificates for delegated CAs, which in turn generates certificates for principles.
- More than one certificate is needed in the process of verification of a public key.

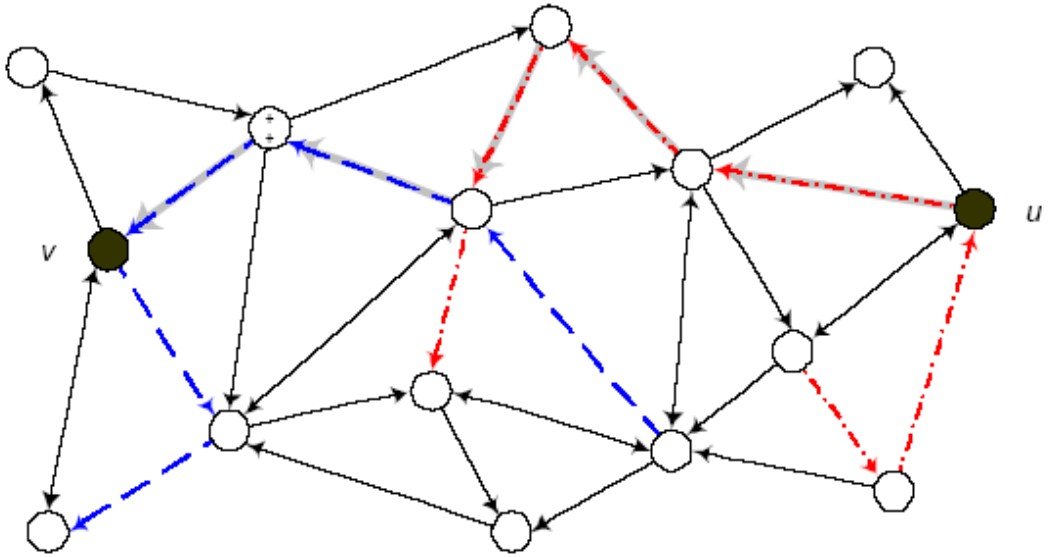
Oligarchy Model

- Multiple trust anchor CAs are pre-configured in all principles
- User has an option to modify the list of trust anchor CAs
- Commonly used in browsers (SSL/TLS)

- Adv./Disadv?

Anarchy Model

- Each principal selects a set of peers as trust anchors.
- Principles sign each others' certificates.
- A principal may store a database of known certificates; Some organization may offer public repository of certificates.
- If a chain of trust (certificates) can be found from a trust anchor to a target name, then the public key of the target is verified.
- Used by PGP.



Top-Down with Name Constraints

- Name constraints: each CA only trusted for signing a subset of users.
- Similar to DNS hierarchy, each domain may have a CA server. The CA of the parent domain (usu.edu) generates certificates for the CAs responsible of the sub-domains (cs.usu.edu).
- Each principle is pre-configured with the public key of the root.
- The only trust path is from the root to the target.

Bottom-Up with Name Constraints

- A parent CA and a child CA generate certificates for each other.
- Two CAs without parent-child relationship may generate a certificate, known as a cross-certificate.
- The trust paths start from a trust anchor, follow up-links to an ancestor, possibly follow a cross-link, then follow down-links to the target.

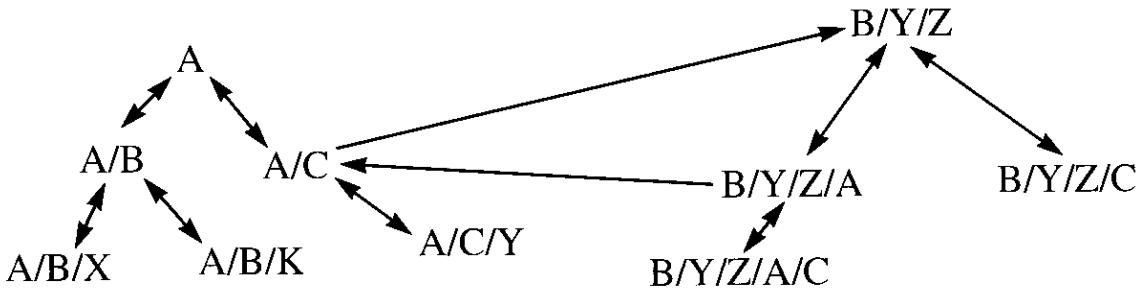


Figure 15-1. Bottom-Up PKI Model

Directories

- A directory is a distributed hierarchical database indexed by a hierarchical name, where associated with each name is a repository of information for that name.
- E.g., DNS, X.500

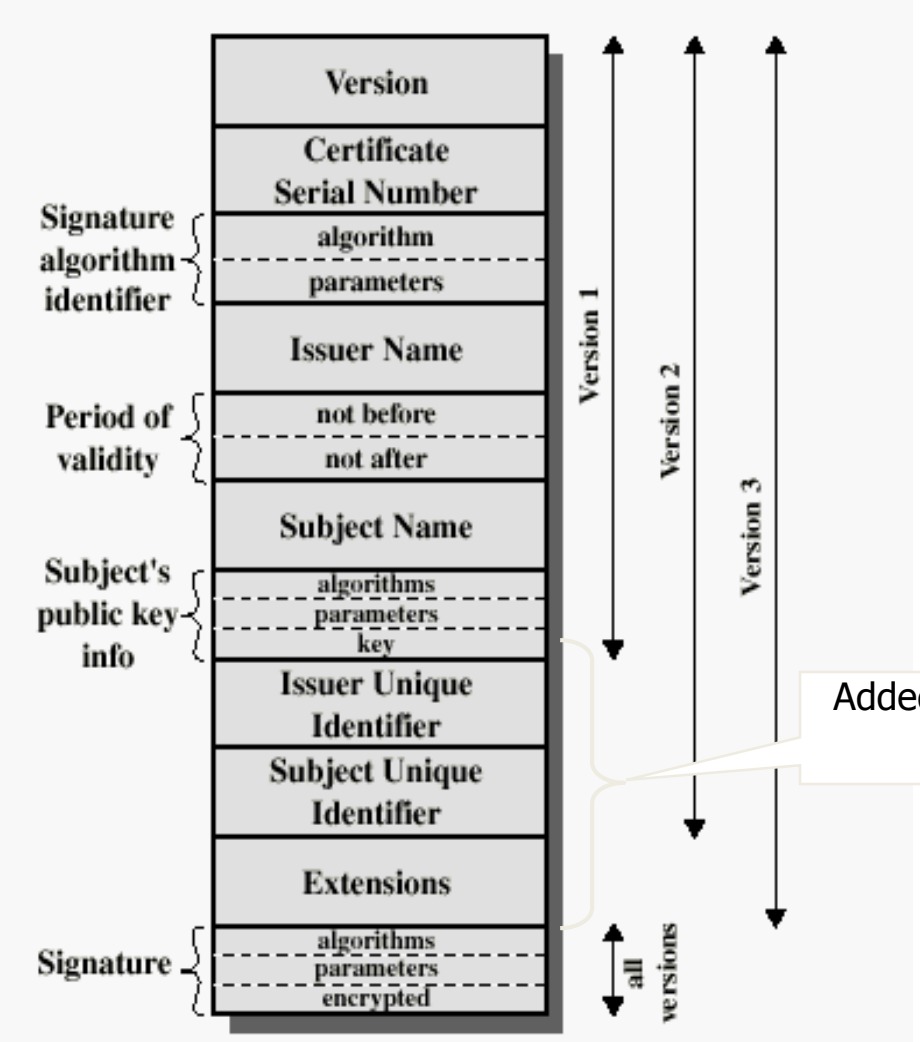
PKIX and X.509

- X.500 defines a hierarchical naming scheme.
- X.509 defines the format of certificates, using X.500.
- PKIX defines the trust model, and specifies which X.509 options should be supported.

X.509 Authentication Service

- Internet standard (1988-2000)
- Specifies certificate format
  - X.509 certificates are used in IPSec and SSL/TLS
- Specifies certificate directory service
  - For retrieving other users' CA-certified public keys
- Specifies a set of authentication protocols
  - For proving identity using public-key signatures
- Does not specify crypto algorithms
  - Can use it with any digital signature scheme and hash function, but hashing is required before signing

X.509 Certificate



Added in X.509 versions 2 and 3 to address usability and security problems

Certificate Revocation

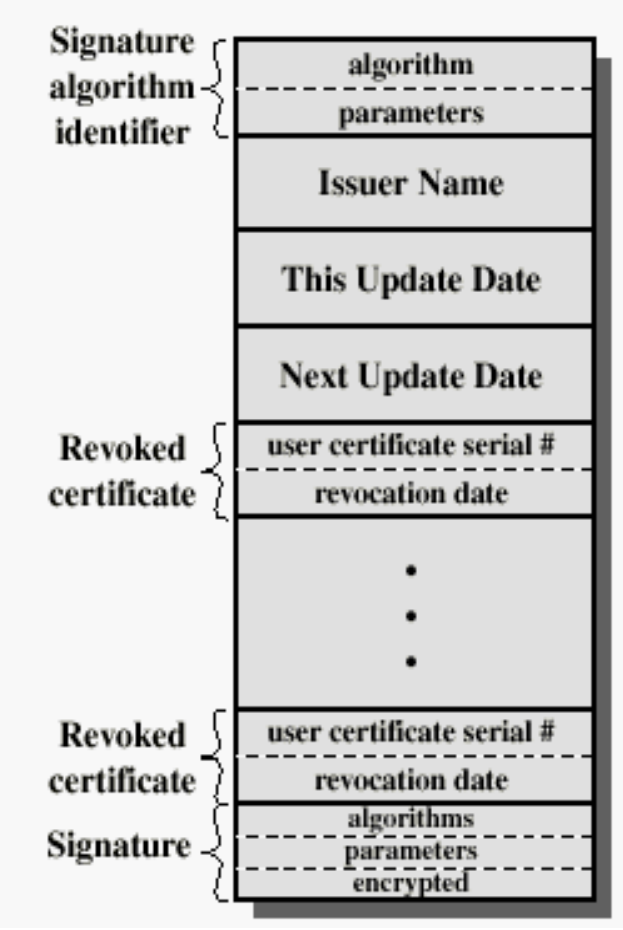
- Revocation is very important
- Many valid reasons to revoke a certificate
  - Private key corresponding to the certified public key has been compromised
  - User stopped paying his certification fee to this CA and CA no longer wishes to certify him
  - CA's certificate has been compromised!
- Expiration is a form of revocation, too
  - Many deployed systems don't bother with revocation
  - Re-issuance of certificates is a big revenue source for certificate authorities

Certificate Revocation Mechanisms

- Online revocation service (OLRS)
  - When a certificate is presented, recipient goes to a special online service to verify whether it is still valid
    - Like a merchant dialing up the credit card processor
  - OLRS may generate a certificate for the validity of another certificate.
- Certificate revocation list (CRL)
  - CA periodically issues a signed list of revoked certificates
    - Credit card companies used to issue thick books of canceled credit card numbers
  - Can issue a "delta CRL" containing only updates

- *Question*: does revocation protect against forged certificates?

X.509 Certificate Revocation List



Because certificate serial numbers must be unique within each CA, this is enough to identify the certificate