UnitelmaSapienza
Università degli Studi di Roma

SAPIENZA
Università di Roma
Dipartimento di Informatica

Digital Certificates and X.509 Authentication Service

Francesco Parisi Presicce

UnitelmaSapienza.it

Public-Key Certificates

reliable distribution of public-keys

- public-key encryption
  - sender needs public key of receiver
- public-key digital signatures
  - receiver needs public key of sender
- public-key key agreement
  - both need each other’s public keys

Public-Key Infrastructure PKI

Manages the certificates during their lifetime

- User registration
- User identification and authentication
- Certificate publishing
- Certificate renewal
- Certificate revocation
- Revocation list publishing

Digital Certificates

- A digital certificate is:
  - An assertion
  - Digitally signed by a “certificate authority”
- An assertion
  - Can be anything
  - Usually an identity assertion
  - Can also be a list of authorizations
- A certificate authority (CA) is
  - Someone who signs certificates
  - Has a “known” public key
  - Is “famous” enough for this to be useful

Thus, a certificate is

- A cryptographic proof that the CA believes the assertions

X.509 Certificate Authority Scope

A CA can vary dramatically in scope.

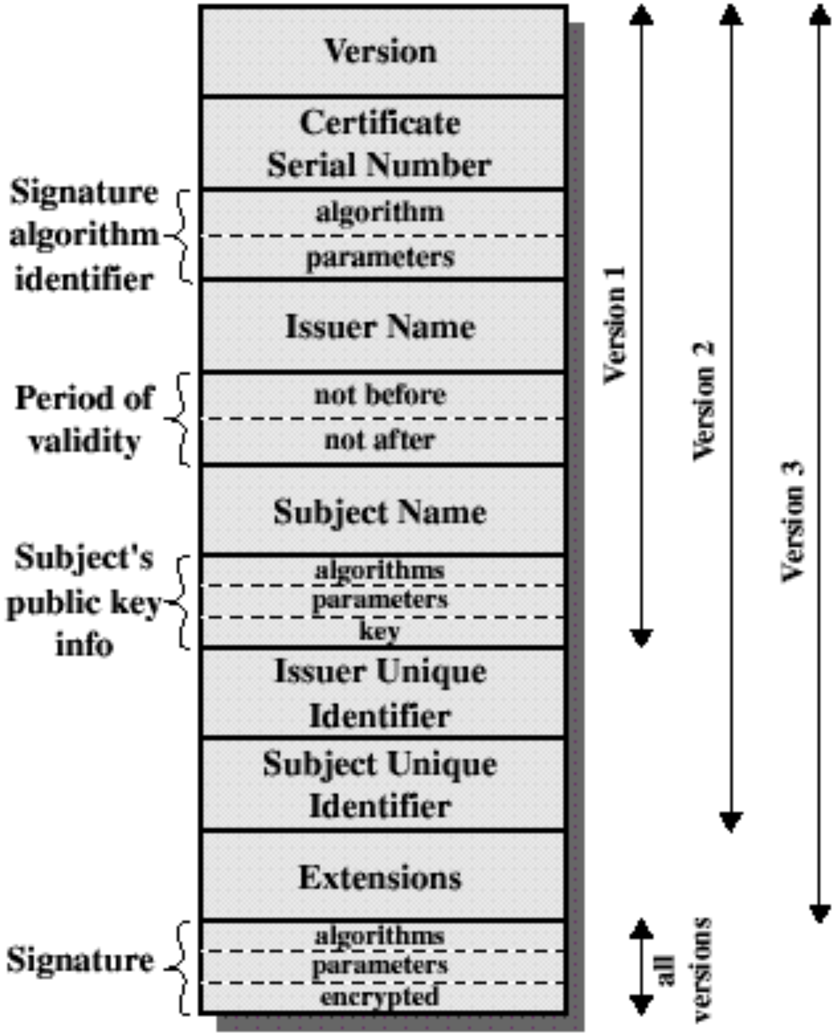
At the large end are commercial CAs like Thawte, Verisign, Belsign, GTE Cybertrust or others.

- These commercial CAs issue certificates to millions of users.

At the smaller end are CAs operated by departments within a company:

- These CAs issue certificates to a small number of users.
- These smaller CAs may be intermediate CAs whose certificates are signed by higher-level CAs inside the organization.

X.509 Public-key Certificate Formats



Courtesy of W.Stallings: Cryptography and Network Security, Prentice Hall 2011

Example of X.509 certificate

```
Certificate:
  Data:
     Version: 1 (0x0)
     Serial Number: 7829 (0x1e95)
     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: Jul  9 16:04:02 1998 GMT
        Not After : Jul  9 16:04:02 1999 GMT
     Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
           OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
     Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
           Modulus (1024 bit):
              00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb: 33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
              66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66: 70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
              16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b: c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
              8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3: d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
              e8:35:1c:9e:27:52:7e:41:8f
           Exponent: 65537 (0x10001)
  Signature Algorithm: md5WithRSAEncryption
     93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
     ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67: d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
     0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1: 5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
     8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:68:9f
```

X.509 certificate format

- The general format for a certificate is:

• Version	V
• Serial number	SN
• Signature algorithm identifier	AI
• Issuer Name	CA
• Period of Validity	T_A
• Subject Name	A
• Subject's Public-key Information	A_p
• Issuer Unique Identifier (added in Version 2)	
• Subject Unique Identifier (added in Version 2)	
• Extensions (added in Version 3)	
• Signature	

X.509: obtaining a user certificate

User certificates generated by a CA have the following characteristics:

- Any user with access to the public key of the CA can recover the user public key that was certified.
- No party other than the CA can modify the certificate without being detected.

Since they are unforgeable, they can be placed in a directory without the need for the directory to make special efforts to protect them.

X.509: CA Trust Issues

If all users subscribe to the same CA, then there is a common trust of that CA.

- All user certificates can be placed in the directory for access by all users.
- Any user can transmit his/her certificate directly to other users.

Once B is in possession of A’s certificate, B has confidence that:

- Messages it encrypts will be secure.
- Messages signed with A’s private key are unforgeable.

X.509: multiple CAs

Large User Community

- Not Practical to Support All Users
- More Practical to Have Multiple CAs
- Each CA Provides Its Public Key to A Smaller User Group

Consider this Scenario …

- User A obtained A’s certificate from CA X1.
- User B obtained B’s certificate from CA X2.
- If A does not know X2’s public key, B’s certificate is useless.
    - A can read B’s certificate
    - A cannot verify the signature

X.509: multiple CAs solution

Solution: CAs X1 and X2 exchange their public keys

Now…

- A gets X2’s certificate signed by X1
- A gets B’s certificate signed by X2
- Now, A has a trusted copy of X2’s public Aey
  - Verifies X2’s signature on B’s certificate
  - Obtains B’s public key

X.509: certificate revocation

Certificates have a period of validity, a *lifetime*.

- Normally, a new one is issued just prior to the expiration of the old one.

In some cases, a certificate may need to be revoked prior to its expiration:

- User's secret key is assumed to be compromised.
- User is no longer certified by this CA.
- CA certificate is assumed to be compromised.

X.509: certificate revocation list CRL

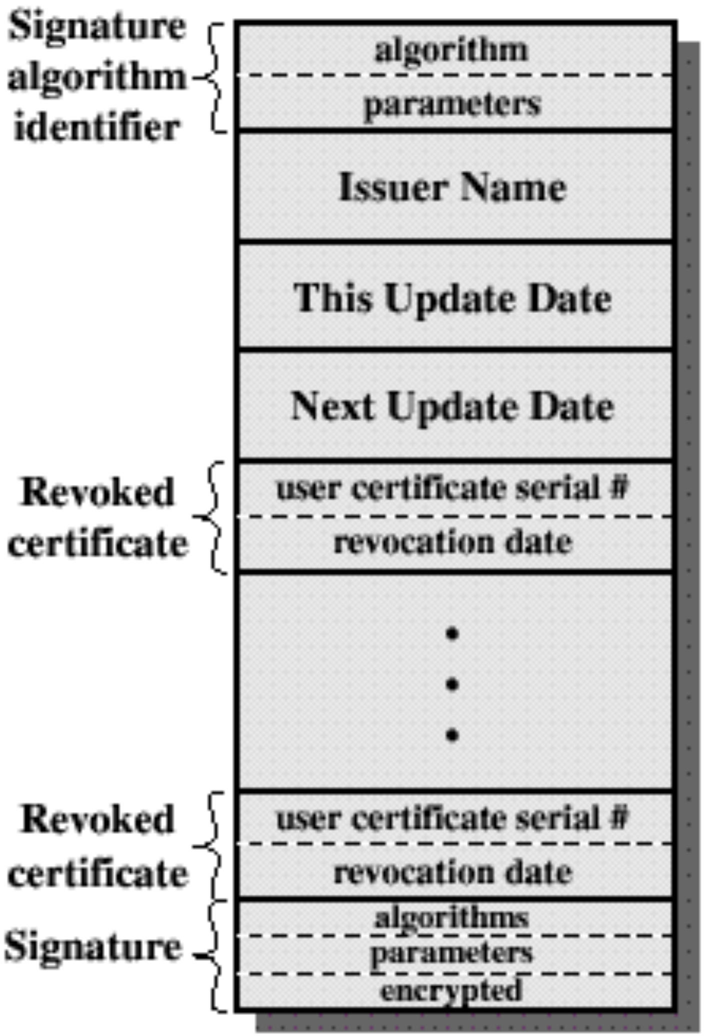
Each CA maintains a list of all revoked not-expired certificates.

- issued by that CA to users
- issued to other CAs

Certificate Revocation List (CRL) posted to the directory is signed by the issuer and includes:

- issuer’s name
- list creation date
- next CRL creation date
- revoked certificate entries (serial number and revocation date)

X.509: certificate revocation list CRL



Courtesy of W.Stallings: Cryptography and Network Security, Prentice Hall 2011

X.509: CRL pros and cons

Pros

- Simple
- No need for a secure channel to distribute CRLs

Cons

- Timeliness: window of vulnerability
- CRLs can be huge
- How to distribute CRLs reliably?

Two basic Certificate Revocation List delivery models:

Polling: the current CRL is requested by the certificate user when he/she needs to use a key on a digital certificate

- time delay between revocation and publication

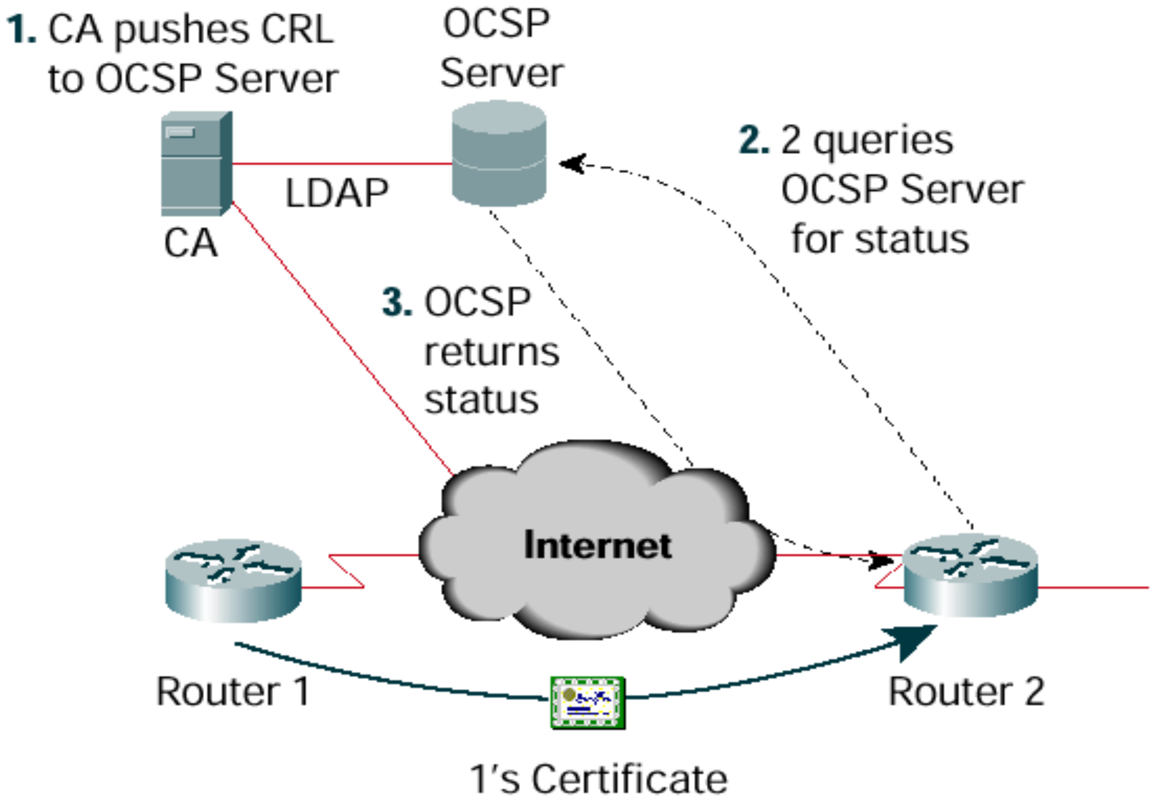
Pushing: the new CRL is delivered by the CA to the user as soon as a new revocation occurs

- storage of new pushed CRLs even if irrelevant
- danger of interception and deletion

NOTE: CRL in an offline mechanism

Alternative Revocation

Online Certificate Status Protocol (OCSP)



- 1 sends certificate to 2
- 2 requests certificate staus from OCSP Server
- OCSP replies with status

Online Certificate Status Protocol (OCSP)

Request

- Protocol version
- Service request
- Target certificate identifier
- Optional extensions which MAY be processed by the OCSP

Response

- Version
- Responder’s name
- Responses for each of the certificates in the request

Possible Responses:

- Good (not revoked)
- Revoked (permanently or temporarily)
- Unknown

NOTE: this is also a “black list” approach

X.509 Authentication Procedures

The standard proposes also three alternative authentication procedures

- Each use public-key signatures
- Each assumes that the two parties know each other’s public key.
  - either obtained from Directory
  - or obtained in an initial message

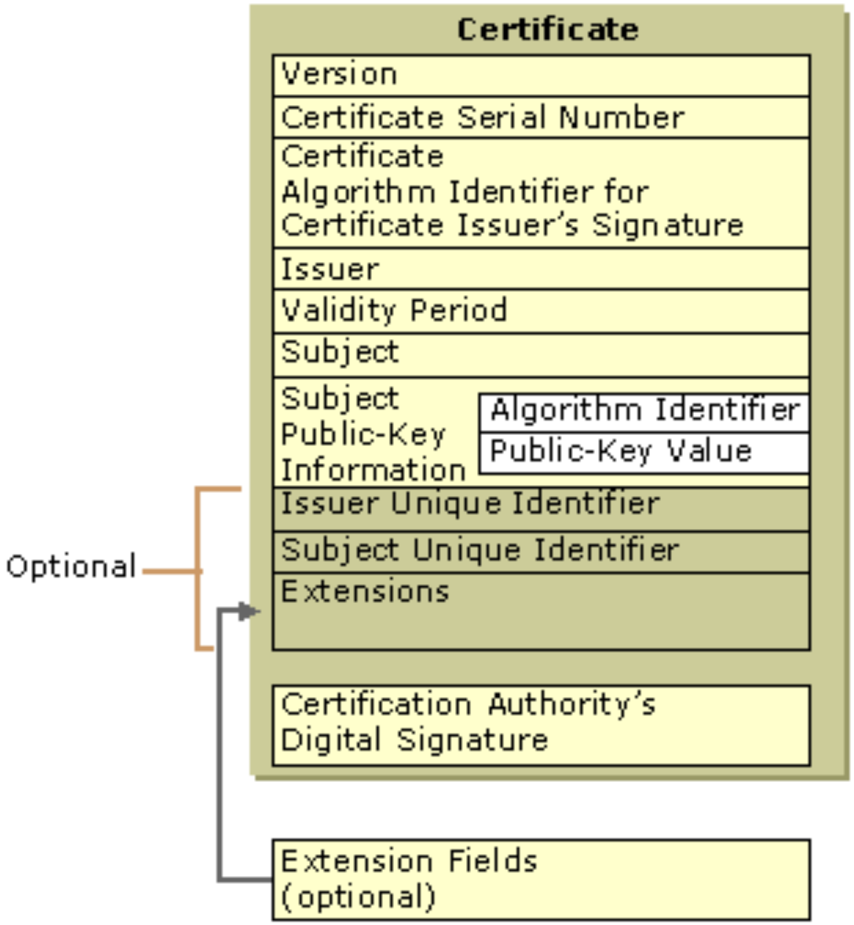
X.509 Version 2 inadequacies

Insufficient information conveyed in the certificate

- Subject field issues
  - inadequate to identify key owner
  - inadequate for many applications (that require, for example, e-mail or URL)
- No security policy information
- No method to limit damage (in case of faulty or malicious CA)
- No key differentiation
- Solution: two approaches
  - either add fields to version 2 format
  - or add optional extension fields (!!)

X.509 Version 2 inadequacies

Extensions: Additional information that can be specified for optional use by public key infrastructures. Common extensions include a list of specific uses for certificates (for example, S/MIME secure mail or IPSec authentication), CA trust relationship and hierarchy information, a list of publication points for revocation lists, and a list of additional attributes for the issuer and subject.


Certificate
Version
Certificate Serial Number
Certificate Algorithm Identifier for Certificate Issuer's Signature
Issuer
Validity Period
Subject
Subject Public-Key Information
Algorithm Identifier
Public-Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Optional
Certification Authority's Digital Signature
Extension Fields (optional)

X.509 Version 3 certificate

3 extension categories

- Key and policy information
- Subject and issuer attributes
- Certification path constraints

X.509 Extensions: Key and Policy

- Subject and issuer keys information
- Indicators of certificate policy
- Extension fields
  - Authority key identifier (to differentiate keys of the same CA)
  - Subject key identifier (to differentiate keys of the same subject)
  - Key usage (bit string for 9 possibilities, such as key and/or data encryption, signature verification on certificates/CRLs, …)
  - Private-key usage period (for signatures)
  - Certificate policies (used for issuing and for certificate usage)
  - Policy mappings (from CA to CA, for matching policies of different CAs)

X.509 Extensions: Certificate Subject Attributes

- Alternate names for either the certificate subject or the certificate issuer

- Extension fields
  - Subject alternative name (additional identities to be bound to the subject)
  - Issuer alternative name (to associate, e.g., internet style identities to issuer)
  - Subject directory attributes (such as DoB or clearance, to be used by X.500 directory)

X.509 Extensions: Certificate Path Constraints

Provide constraints for certificates issued by CAs for other CAs.

Extension fields

- Basic constraints (can subject be CA and length of allowed certification path from this CA)
- Name constraints (name space for allowed subjects in subsequent certificates)
- Policy constraints (for path validation, either prohibiting or requiring policy)

(crypto-) vulnerabilities

- In 2005, shown "how to use hash collisions to construct two X.509 certificates with identical signatures and differerent public keys", using a collision attack on the MD5 hash function.
- In 2008, presented a practical attack to create a rogue Certificate Authority, accepted by all common browsers, by exploiting the issuing X.509 certificates based on MD5.
- X.509 certificates based on SHA-1 appeared to be secure until April 2009 when researchers produced a method to increase the likelihood of a collision
- In 2017 collisions for SHA-1 were produced (Chrome and Firefox reject certificates using SHA-1 since then)

other vulnerabilities

- There are implementation errors with X.509 that allow e.g. falsified subject names using null-terminated strings or code injections attacks in certificates
- Implementations suffer from design flaws, bugs, different interpretations of standards and lack of interoperability.
  - Different notations, unspecified length of attributes, …
  - Many implementations turn off revocation check, key usage ignored using first certificate in list, and policies are not enforced