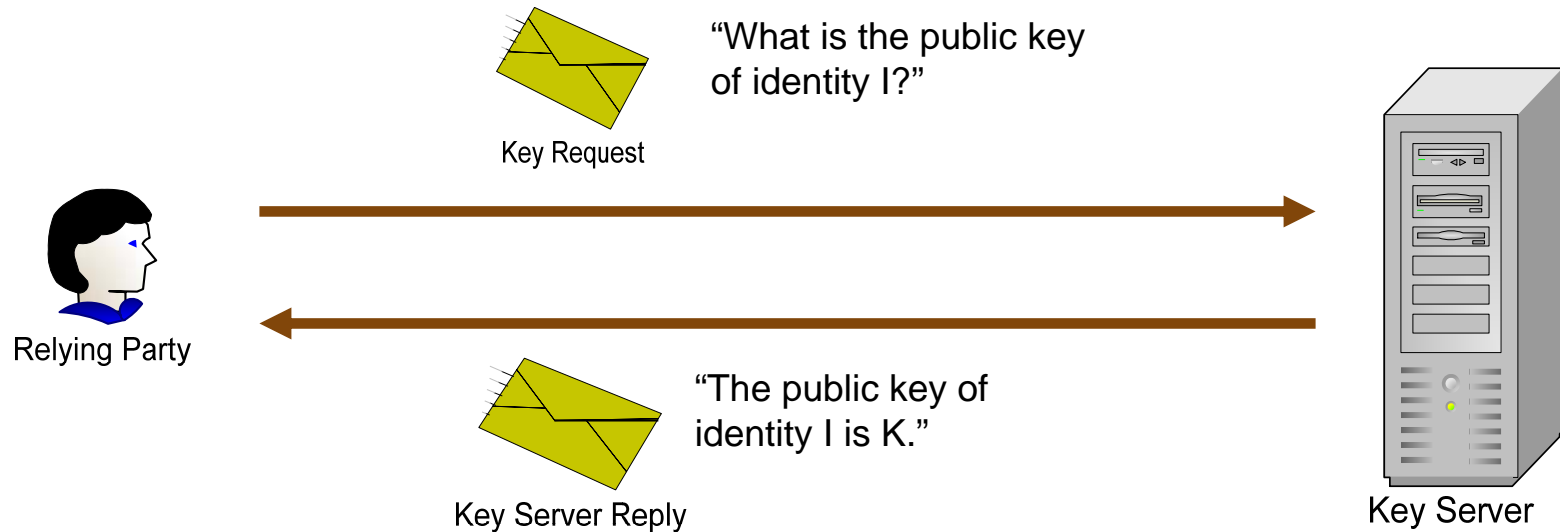


# Authentication

# Authentication

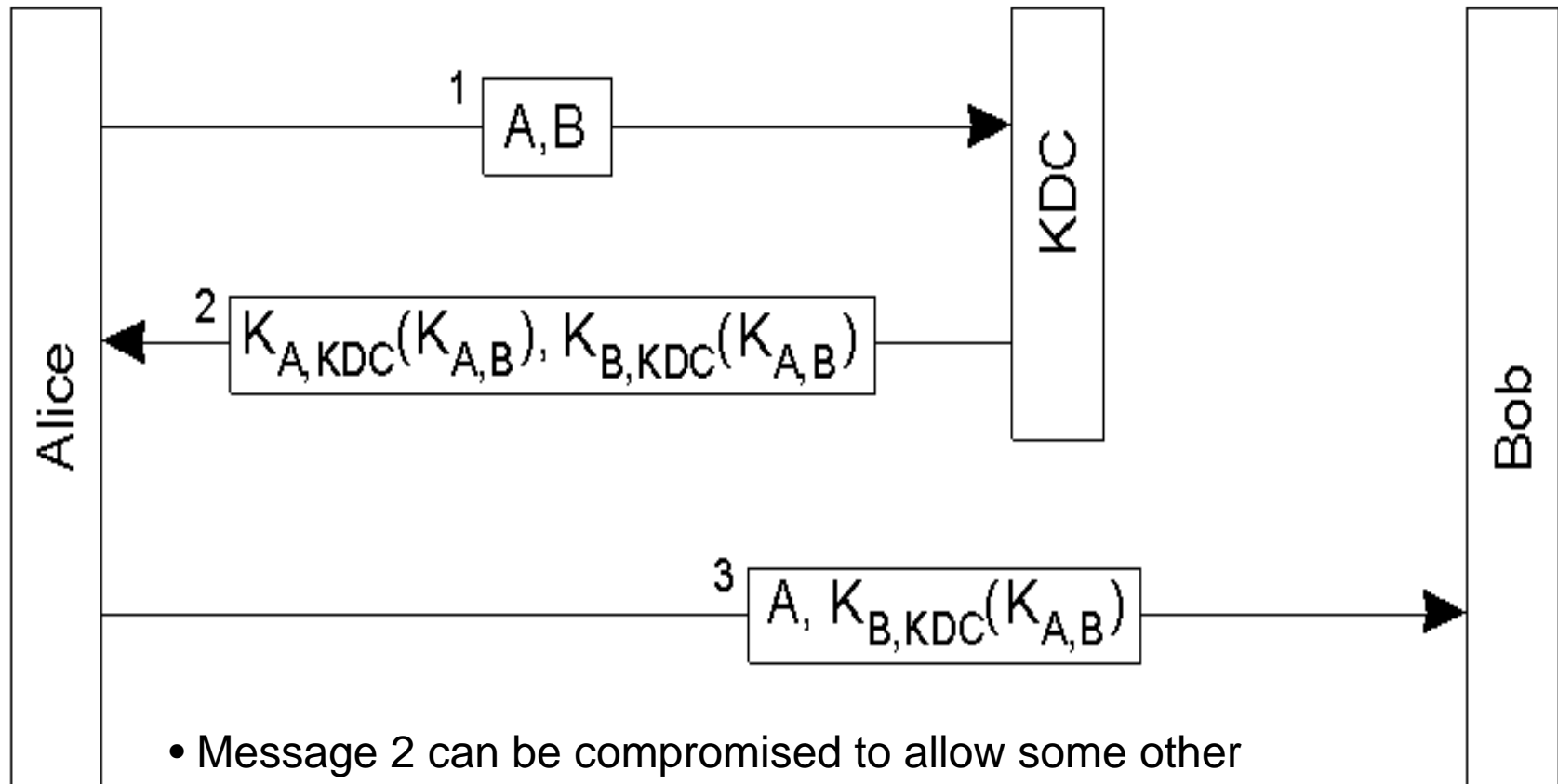
- Digital signature validation proves:
  - message was not altered in transmission
  - came from owner of the private key
  
- How does a “relying party” know to whom the private key belongs?
  - Key Servers
  - Certificates

# Key Server



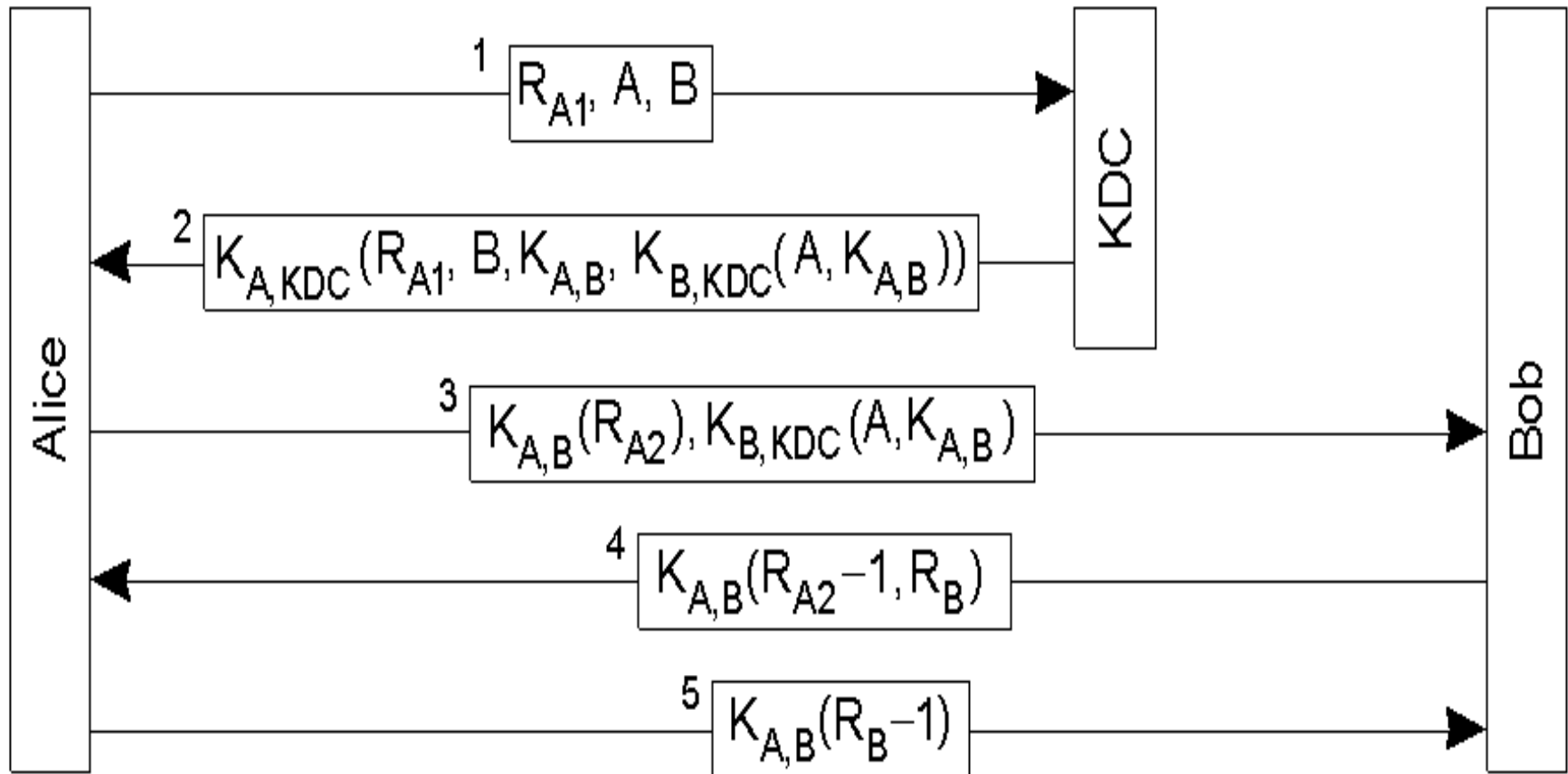
- The key server stores [identity, public key] pairs
- The key request can be in plaintext
- The key server reply is encrypted using the private key of the key server
- The public key of key server is known to the relying party
- The key server can be a point of attack or performance bottleneck
- The key server must be trustworthy
- Observations:
  - the relying party only cares about the reply
  - the reply can be precomputed and distributed

# Authentication using a Key Server

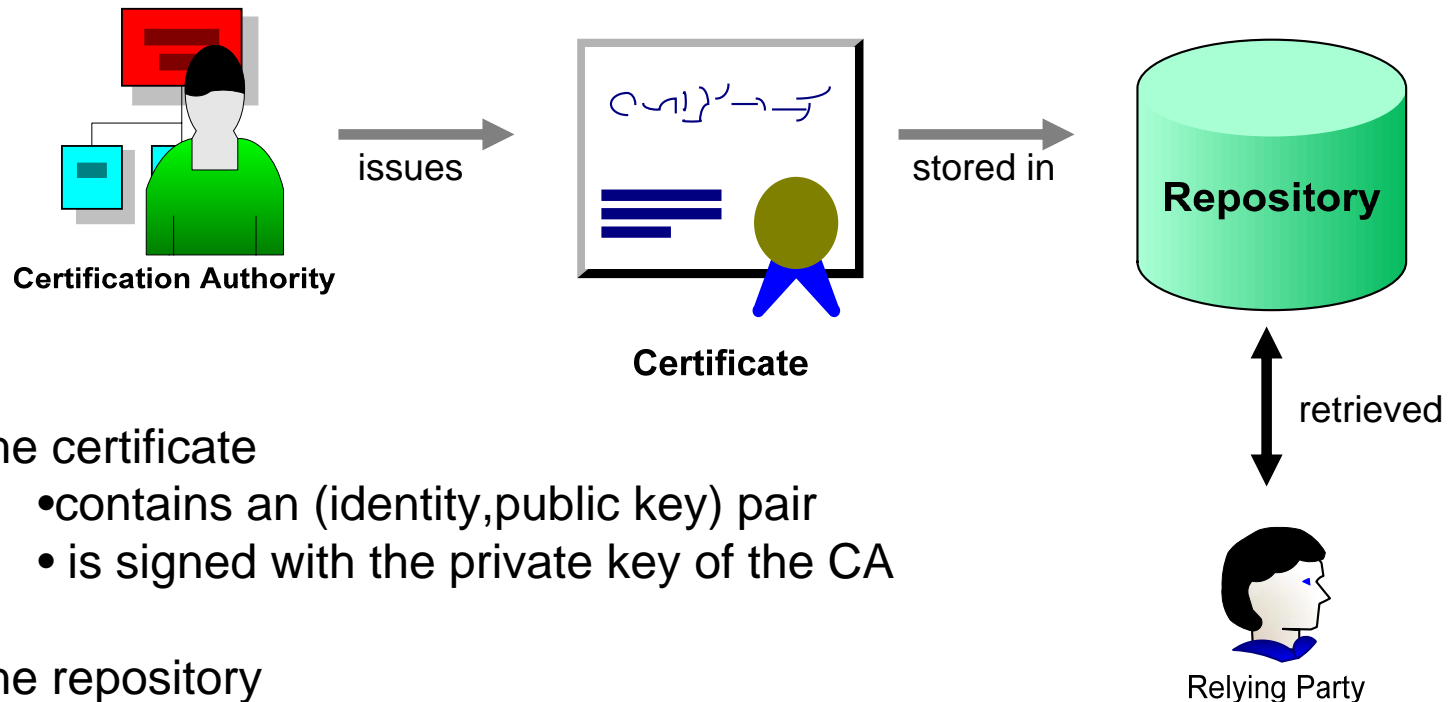


- Message 2 can be compromised to allow some other party to masquerade as Bob.
- Message 3 can be compromised to allow some other party to masquerade as Alice.

## Needham-Schroeder Protocol

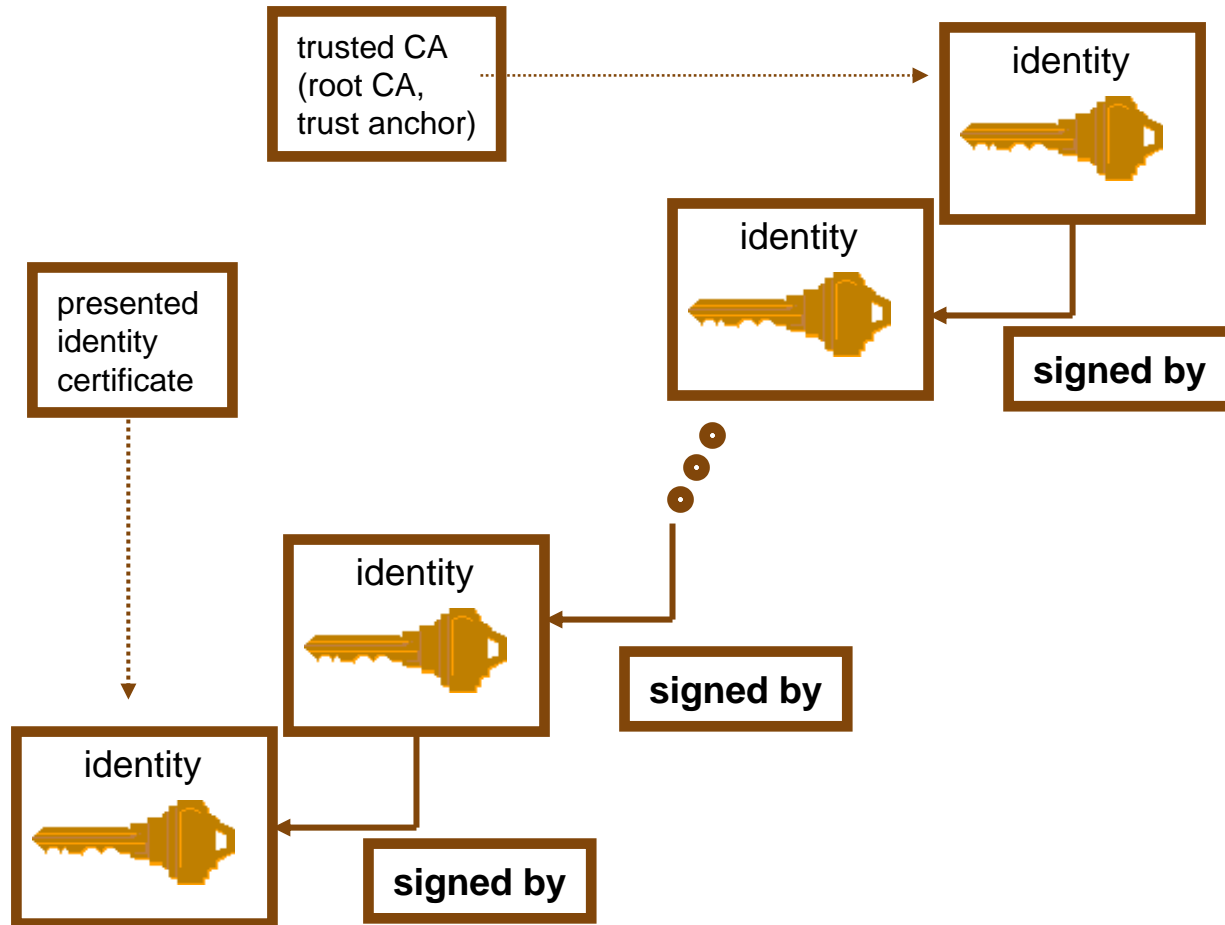


# Certificates

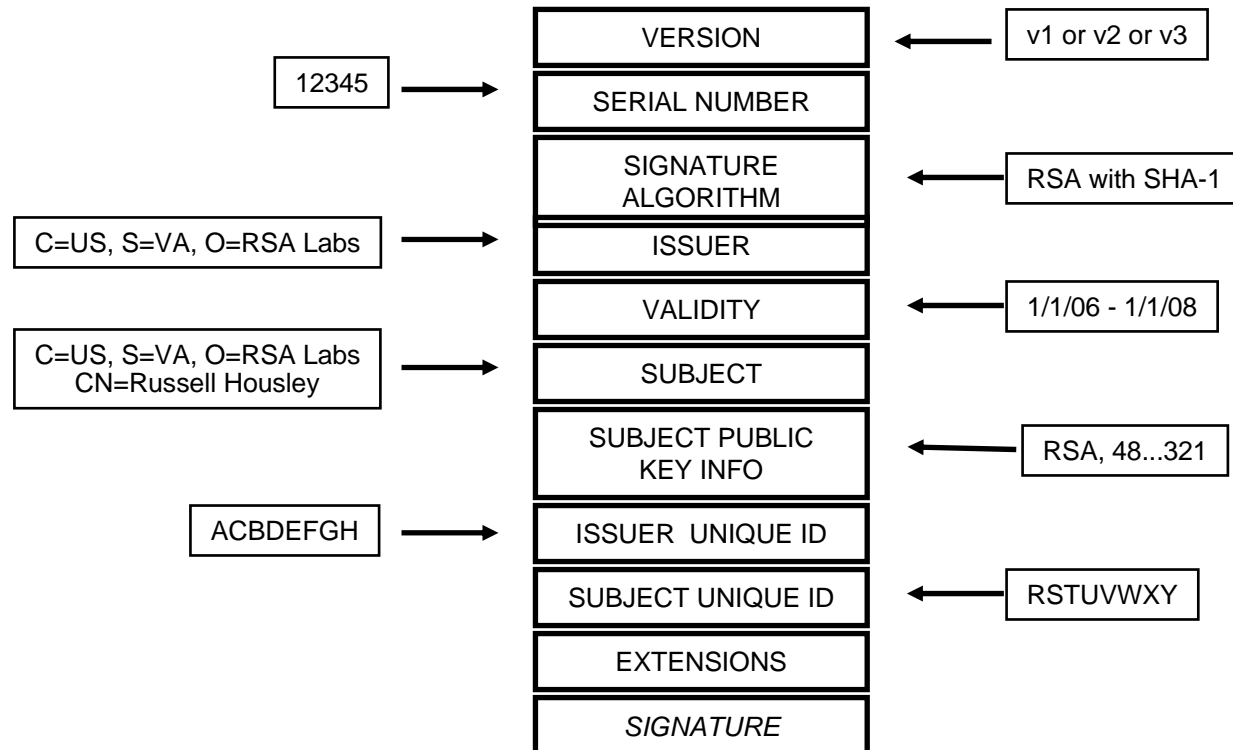


- the certificate
  - contains an (identity,public key) pair
  - is signed with the private key of the CA
- the repository
  - need not be trusted
  - is read-only
  - may be duplicated for performance
- the certificate can be “pushed” to the relying party

# Chain of Trust



# X.509 Certificate Format





# Example Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1097588 (0x10bf74)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=US, ST=Massachusetts, O=Massachusetts Institute of Technology, OU=Client CA v1

Validity

Not Before: Jul 31 14:07:49 2000 GMT

Not After : Jul 31 14:07:49 2001 GMT

Subject: C=US, ST=Massachusetts, O=Massachusetts Institute of Technology, OU=Client CA v1, CN=Jeffrey I Schiller/Email=jis@MIT.EDU

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:cf:01:0a:e5:f1:3c:60:c1:f2:c1:ca:99:96:1d:  
 7d:39:97:8c:72:cf:e8:7c:51:a1:84:a4:5b:b8:b3:  
 3a:dc:dd:c5:99:76:cb:5d:b1:24:86:67:46:52:45:  
 69:09:fb:01:b0:dd:41:02:de:27:c2:b7:cd:b1:cd:  
 47:9a:ae:55:bb:83:cd:bd:c1:aa:2b:23:3d:85:06:  
 e0:4a:6c:a8:af:b4:cb:64:ea:c9:33:f7:ef:a9:8f:  
 d9:7a:20:68:a1:09:c4:4e:62:20:00:d1:fd:a5:7c:  
 14:90:48:79:a9:7d:ef:f5:46:b6:fb:4e:c5:fc:94:  
 8f:11:bf:1a:ef:7b:2d:06:ef

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage:

....

1.2.840.113554.1.3.1:

0....]/e.ii;....m.....j....Nr....\$wF...t...QZ...

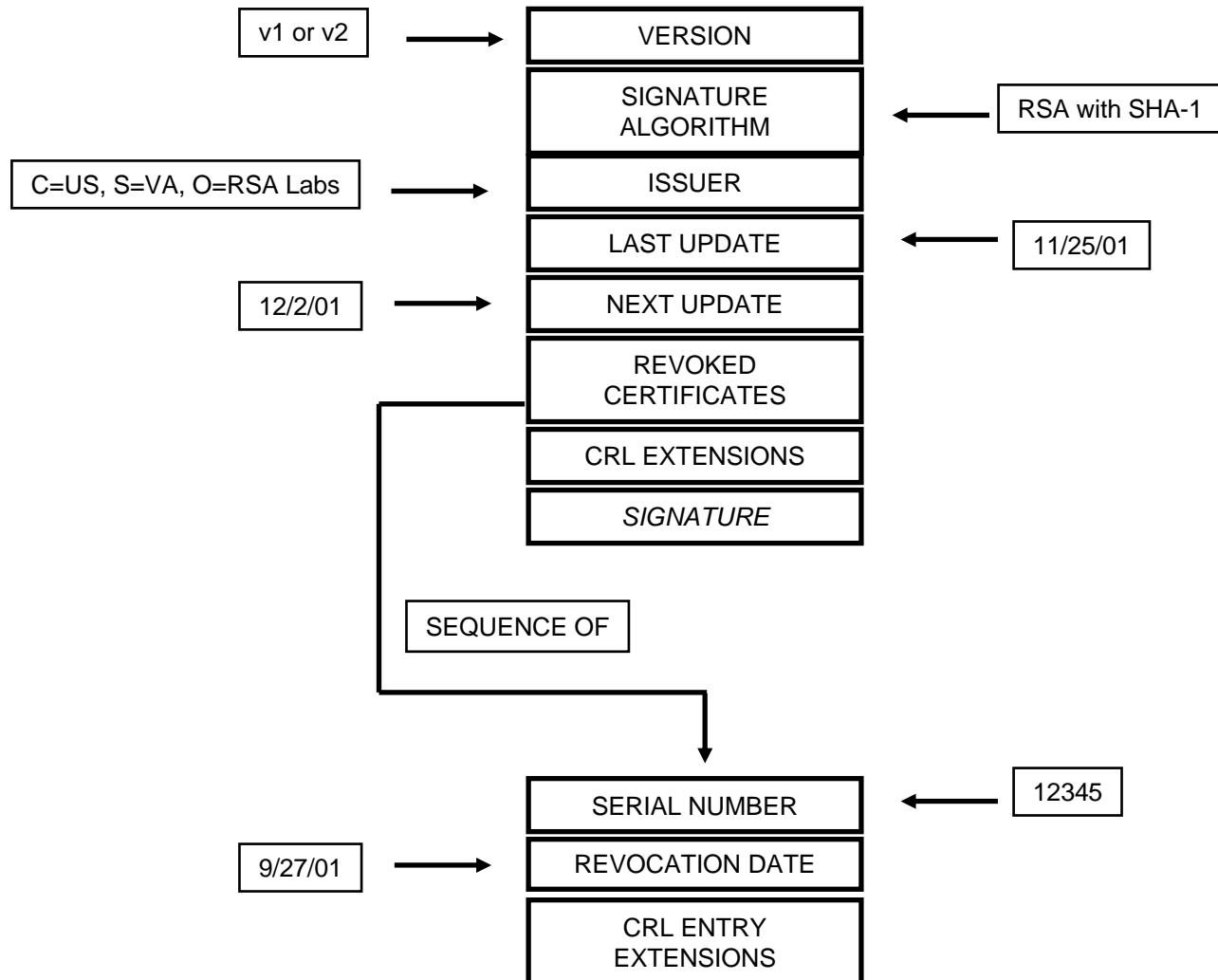
Signature Algorithm: md5WithRSAEncryption

30:4c:3b:a5:d8:11:e1:04:61:d2:39:ff:e1:74:c3:06:2f:3b:  
 52:59:9c:75:05:2e:31:cc:c3:99:5c:02:e5:67:bf:06:99:7f:  
 c8:2a:5b:dd:bd:67:a5:a7:98:74:14:44:a7:db:76:19:9c:80:  
 0a:58:1d:53:35:d0:75:82:9d:2a:e7:12:53:3f:8b:60:cc:a3:  
 c9:5b:dd:34:b6:a4:33:a9:a5:93:64:3e:50:0d:e4:ae:a8:5d:  
 c9:8d:f9:96:68:22:cd:66:3d:eb:66:11:68:04:f6:3d:64:05:  
 62:64:01:41:af:23:f9:d2:a3:5b:be:e3:33:45:71:08:05:e2:  
 2a:6e

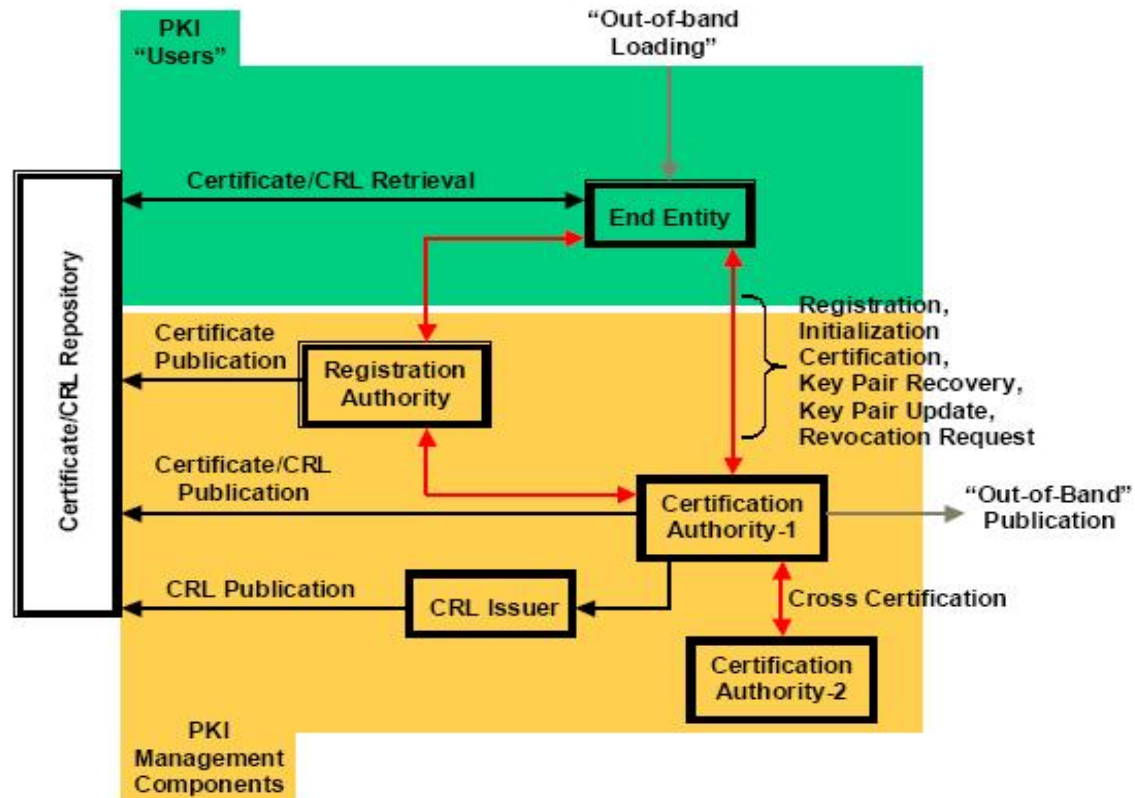
# Revocation

- Is a certificate still valid?
  - Private key compromise
  - CA compromise
  - Affiliation changed
  - Superseded
  - CA ceased operation
  - ...
- Certificate Revocation List (CRL) provides a list of the unexpired certificates that should no longer be used

# CRL Format



# PKIX Architecture



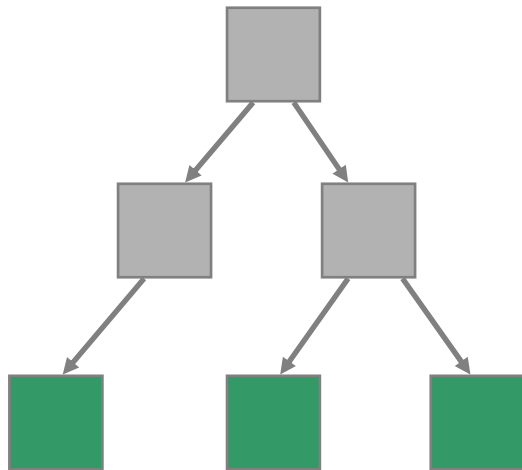
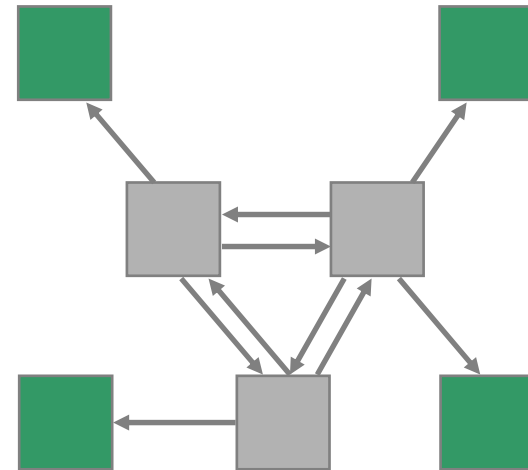
# PKIX Elements

COMPONENT	PRIMARY ROLE
<ul style="list-style-type: none"> <li>End Entity</li> </ul>	<p>End Entity is a generic term used to denote end-users, devices (e.g., servers, routers), or any other entity that can be identified in the subject field of a public key certificate. End entities typically consume and/or support PKI-related services.</p>
<ul style="list-style-type: none"> <li>Certification Authority (CA)</li> </ul>	<p>The CA is the issuer of certificates and (usually) CRLs. It may also support a variety of administrative functions, although these are often delegated to one or more Registration Authorities.</p>
<ul style="list-style-type: none"> <li>Registration Authority (RA)</li> </ul>	<p>The RA is an optional component that can assume a number of administrative functions from the CA. The RA is often associated with the End Entity registration process, but can assist in a number of other areas as well.</p>
<ul style="list-style-type: none"> <li>Repository</li> </ul>	<p>A repository is a generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by End Entities.</p>
<ul style="list-style-type: none"> <li>CRL Issuer</li> </ul>	<p>The CRL Issuer is an optional component that a CA can delegate to publish CRLs.</p>

## Role of the CA

- Verifies certificate request information
- Generates and digitally signs the certificate
- Revokes certificate if information changes
- Revokes certificate if private key is disclosed
- Support certificate hierarchies
- Optional services
  - Key generation
  - Issue hardware token

# CA Topologies

**Hierarchy****Mesh**

# Cross Certification

