Authentication

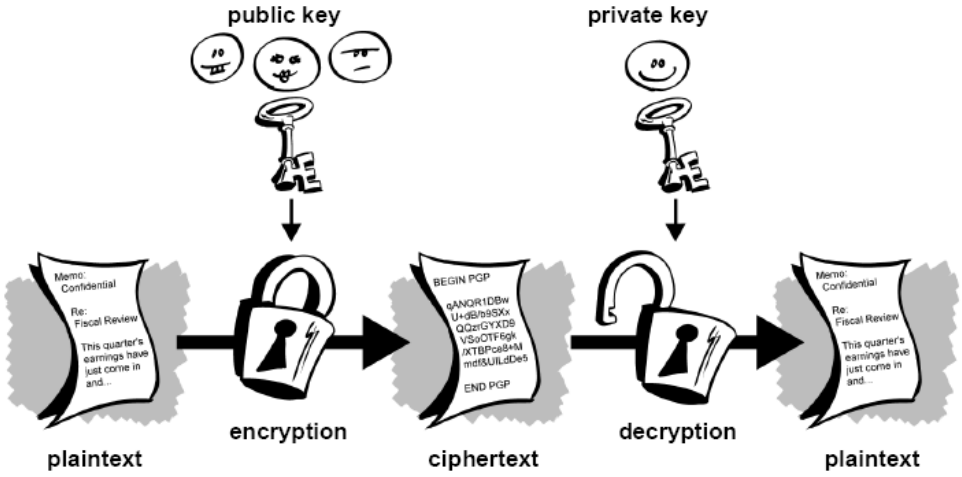
Cristian Solano

Virginia Tech

Cryptography

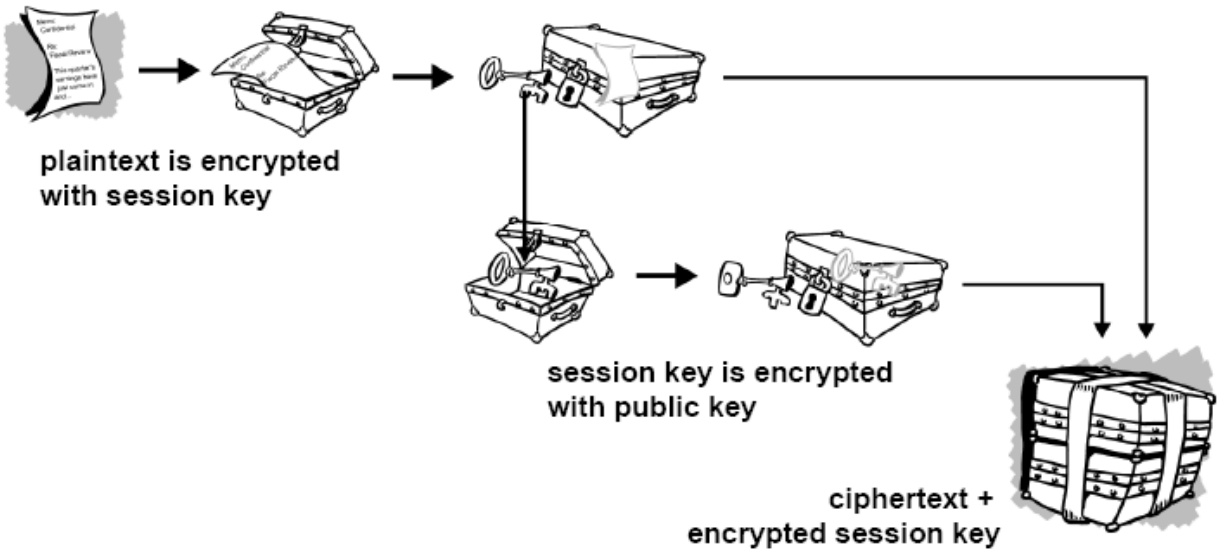
- **Cryptography** is the science of using mathematics to encrypt and decrypt data.

- **Public Key Cryptography**
  - Problems with key distribution are solve with Public Key Cryptography.
  - Uses a public key and a private key.



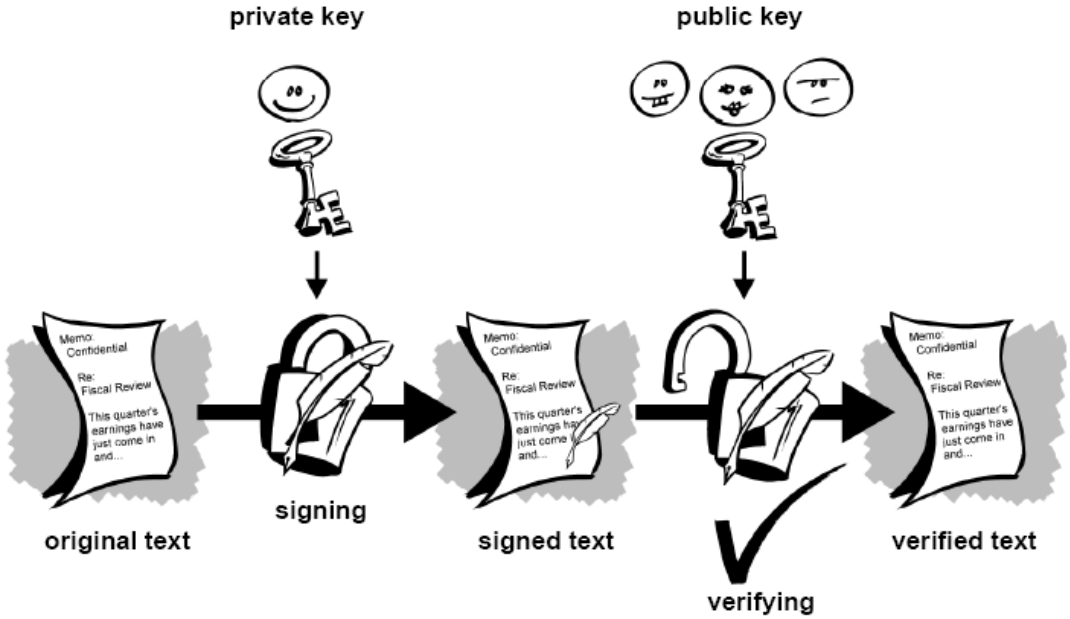
Pretty Good Privacy (PGP)

- PGP is an application and protocol for secure email and file encryption.
- PGP provides encryption, authentication, message integrity and key management.
- It uses a session key, which is a one time-only secret key generated from the random movements of the mouse and keystrokes typed.
- PGP stores the keys in two files on your hard disk; one for public and one for private keys. These files are called keyrings.



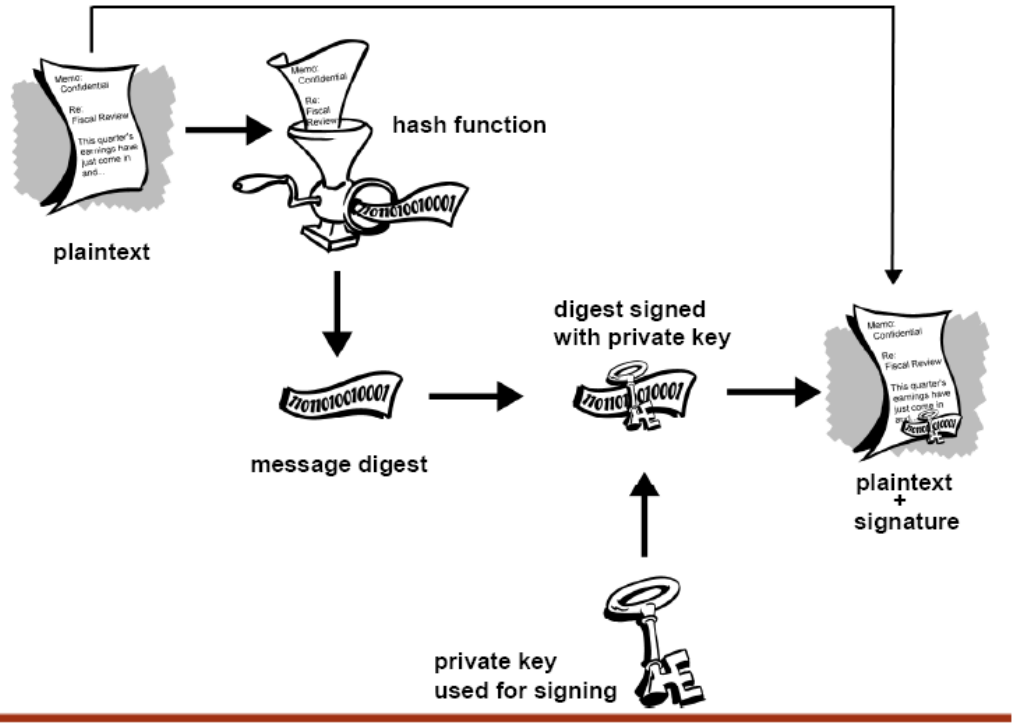
Digital Signatures

- Digital Signatures enable the recipient of information to verify the authenticity of the information's origin, and also to verify the information is intact.
- Digital Signatures provide authentication, data integrity and non-repudiation (it prevents the sender from claiming that he/she did not actually send the information.



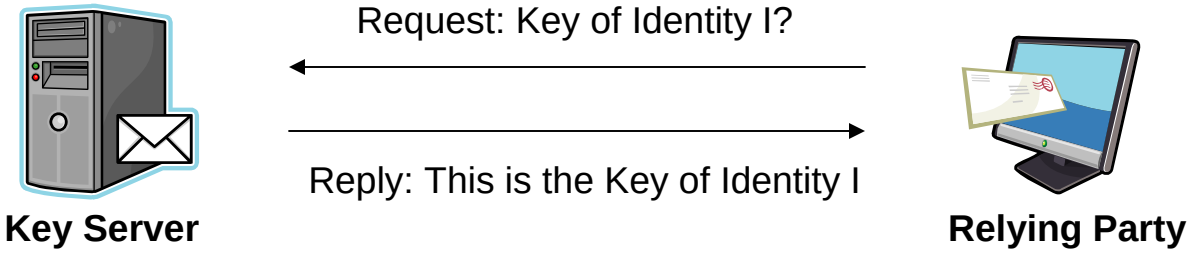
Digital Signatures

- Hash functions
  - Resolves the problem of enormous volume of data produced by the previous method by producing a fixed-length output.
  - The Previous method produced at least double the size of the original information.
- PGP uses this method.

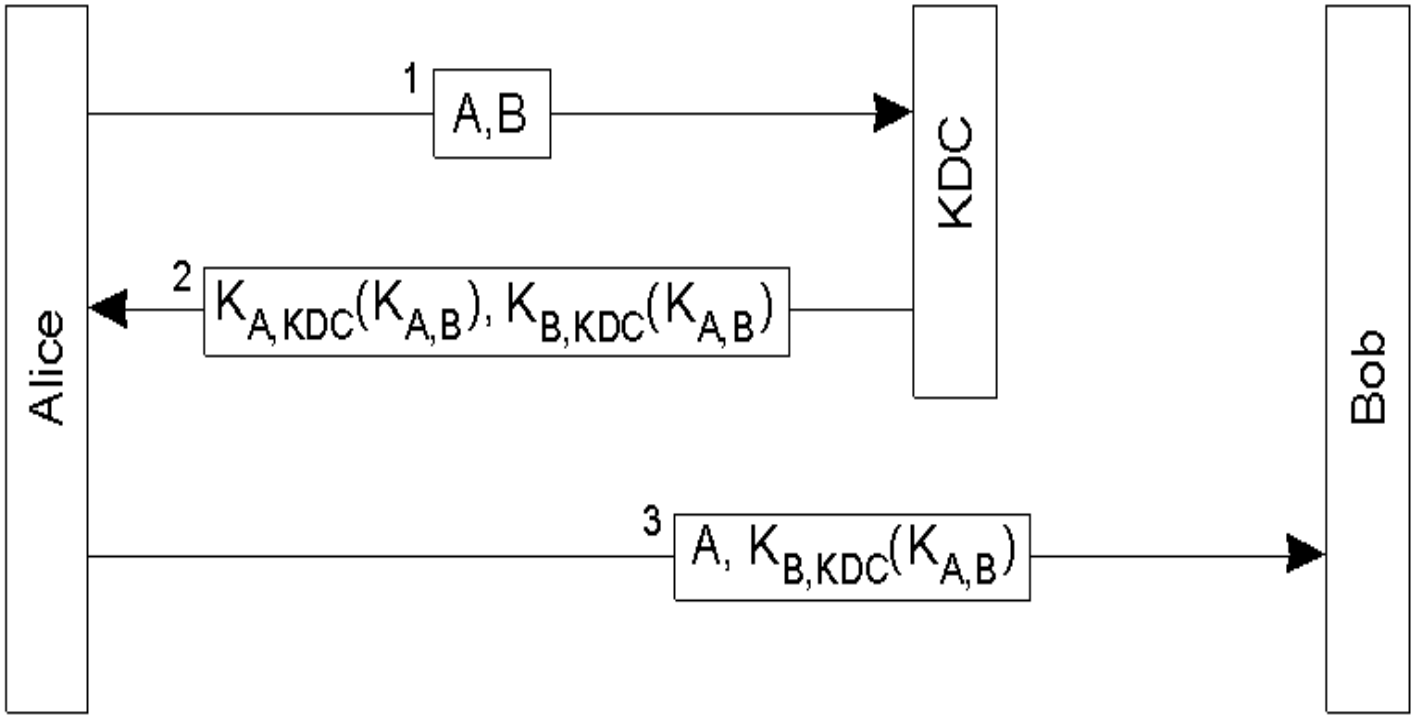


Authentication

- Authentication is a mechanism that verify a claim of authenticity.
- How do we know that a public key really belongs to its owner?
  - Key Server
  - Digital 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 server
  - The key server must be trustworthy.



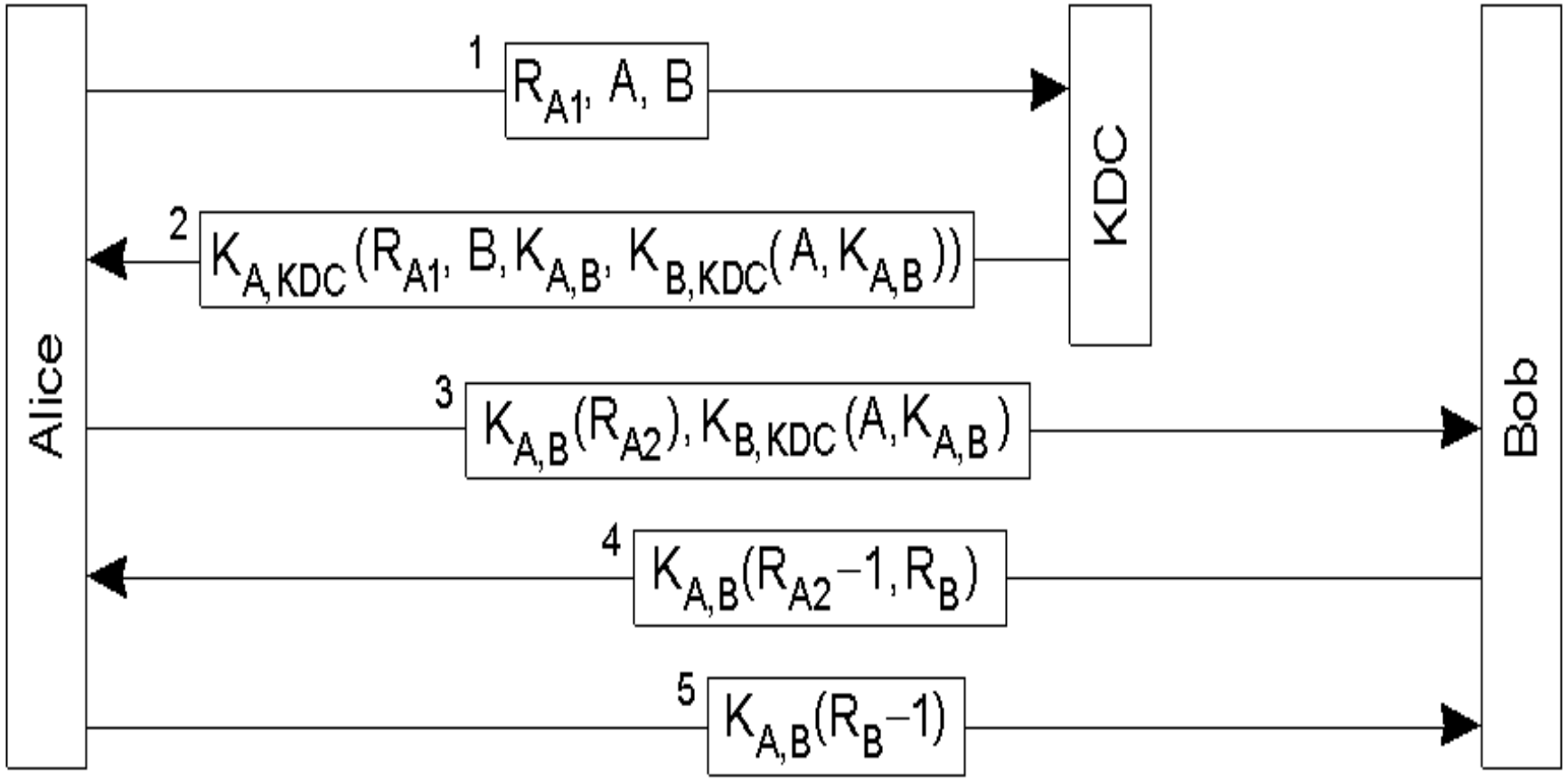
Authentication using a Key Server



Problems:

- Message 2 can be compromised to allow someone else to act as Bob.
- Message 3 can be compromised to allow someone else to act as Alice.

Needham-Schroeder Protocol



Digital Certificates

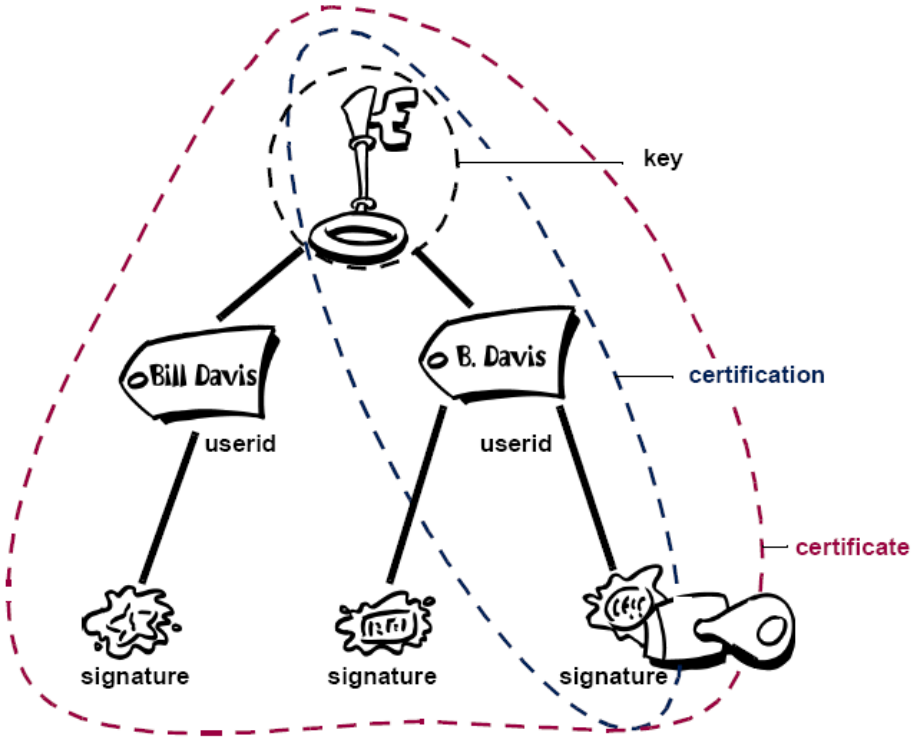
- **Digital certificates** or **certs** simplifies the task of establishing whether a public key truly belongs to the purported owner. It is a form of credential.

- A digital certificate consists of three things:
  - A public key
  - Certificate information. (Identity)
  - One or more digital signatures from the attesters.

- A certificate is a public key with one or two forms of ID attached, plus the approval from some other trusted individual.

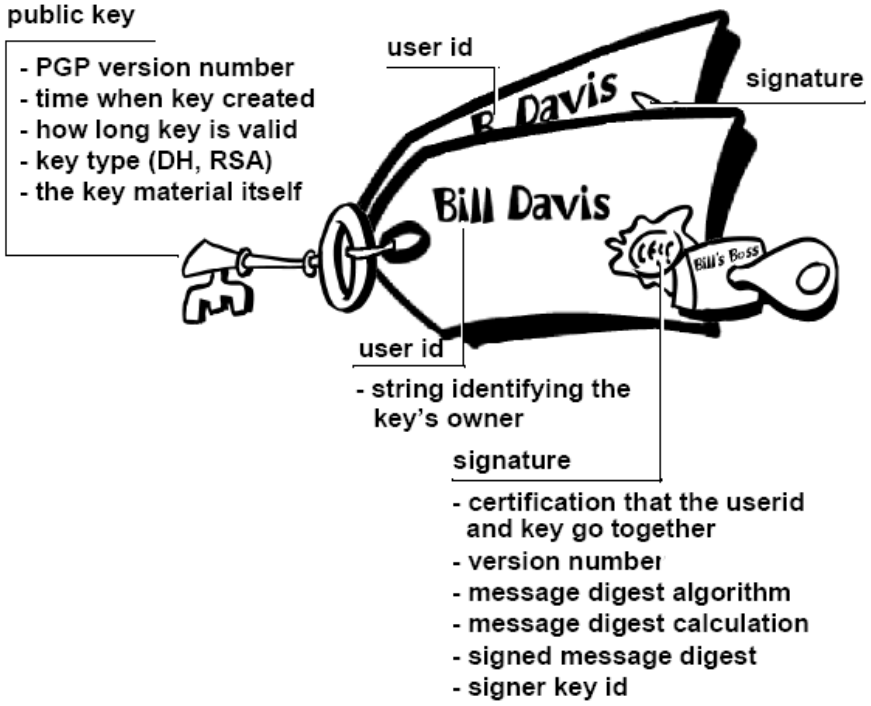
- Certificate servers store certs.

- Public Key Infrastructures (PKIs) are structured systems that provide additional key management features.

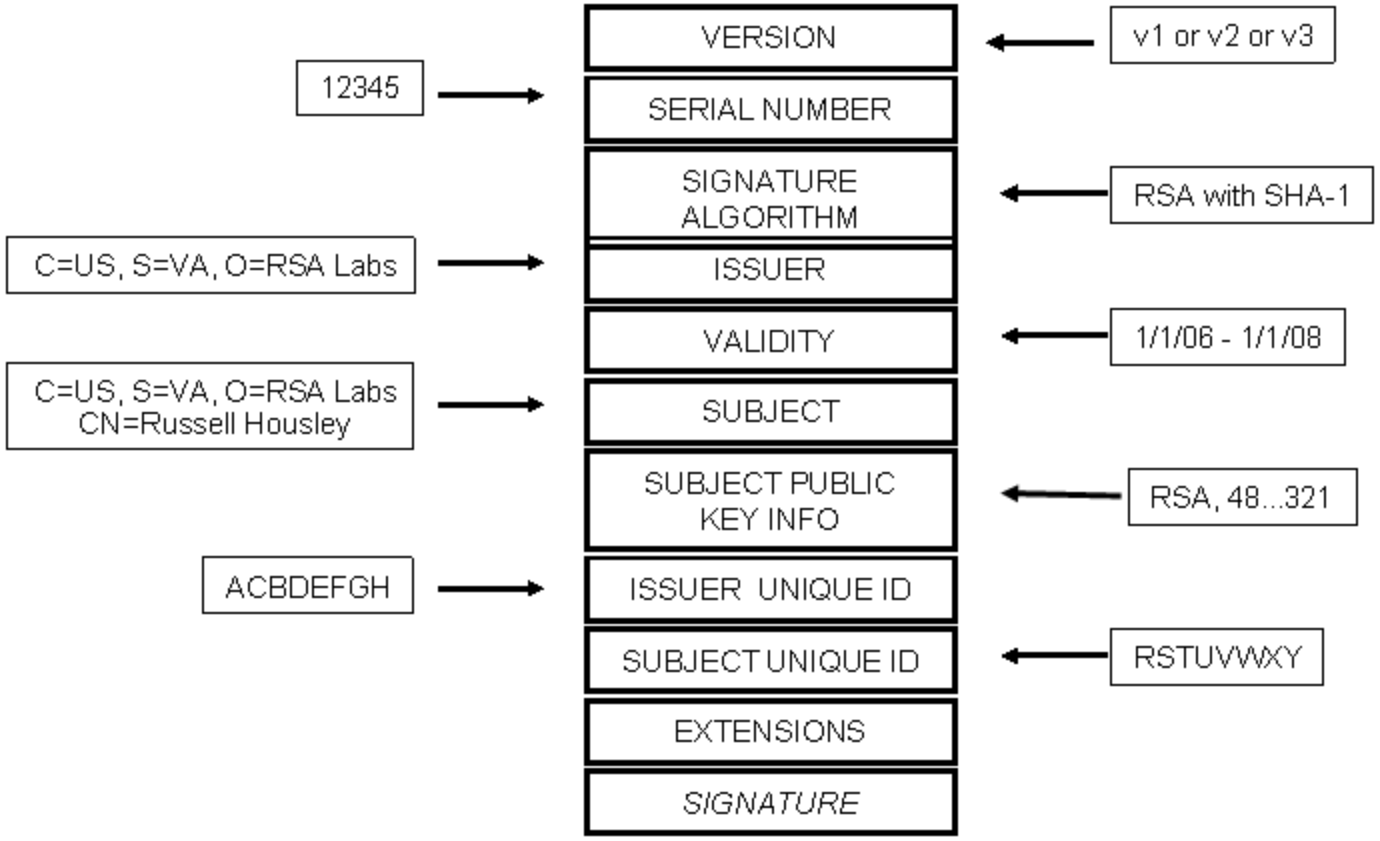


PGP Certificate Format

- A single certificate can contain multiple signature from the attesters.
- Some PGP certificates consist of public key with several labels which contains different means of identifying the key owner.



X.509 Certificate Format



X.509 Certificate Example

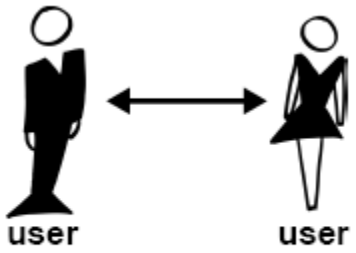
```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
        OU=Certification Services Division,
        CN=Thawte Server CA/emailAddress=server-certs@thawte.com
    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
```

Public Key

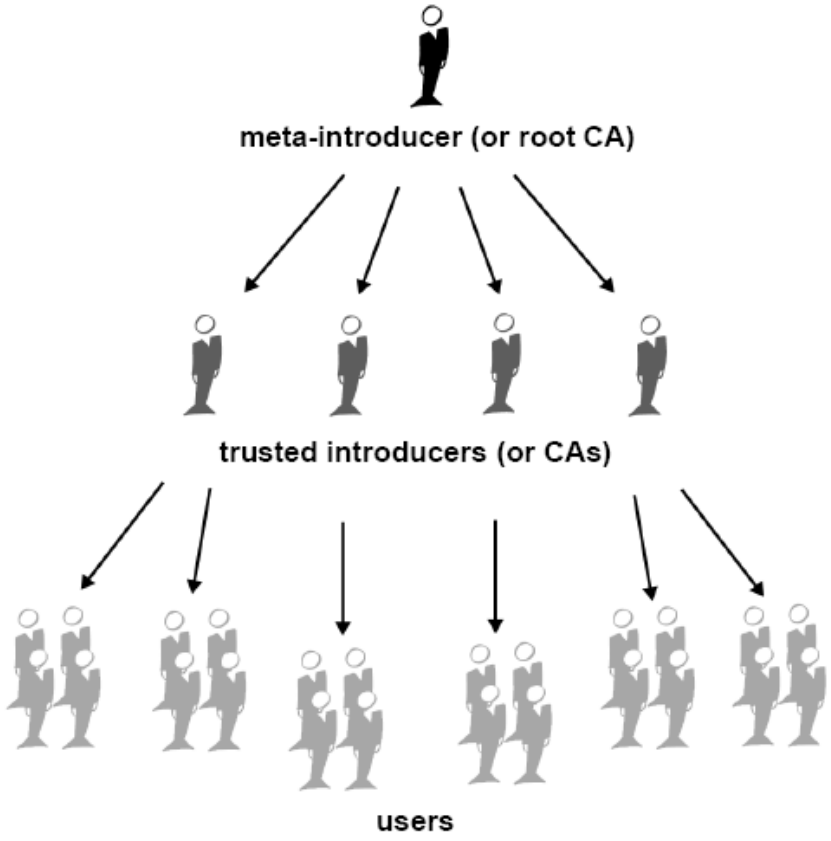
Signature

Establishing Trust

- Trust Models for PGP:
  - Direct Trust
  - Hierarchical Trust
  - A Web of Trust

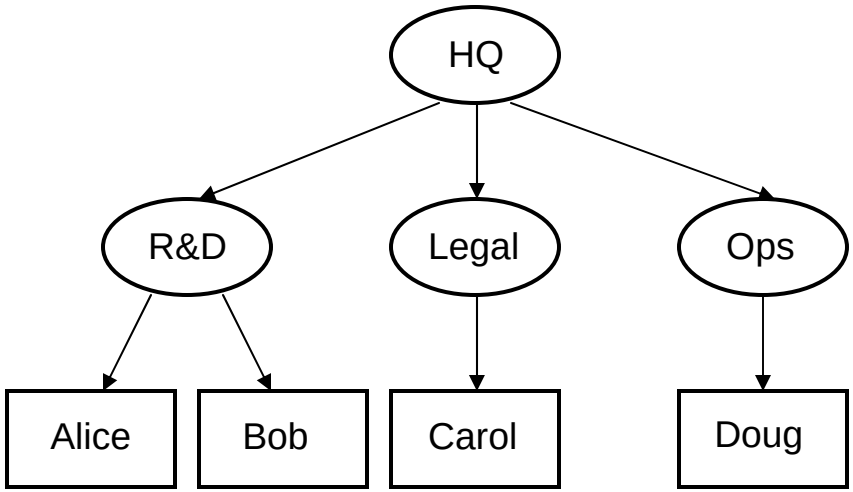


Direct trust

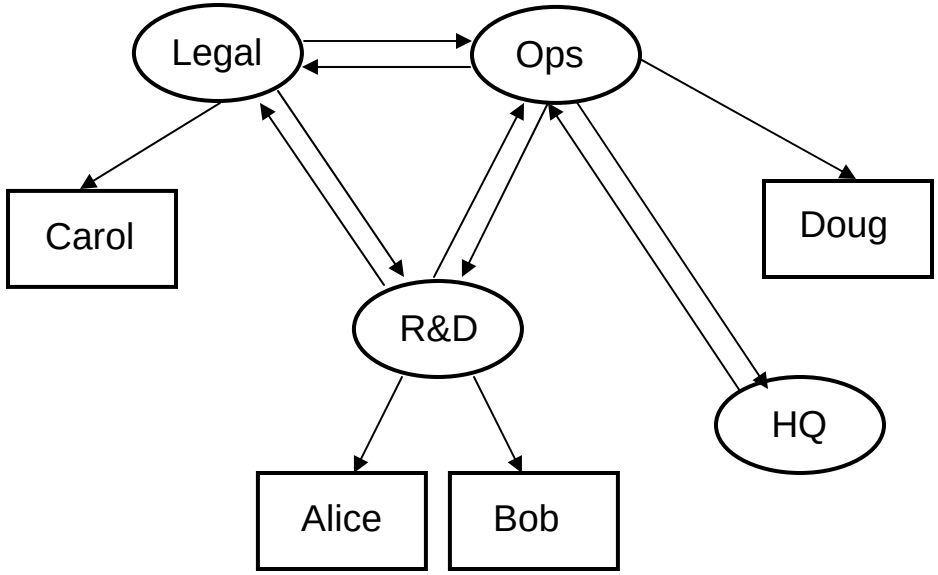


Hierarchical trust

CA Topologies

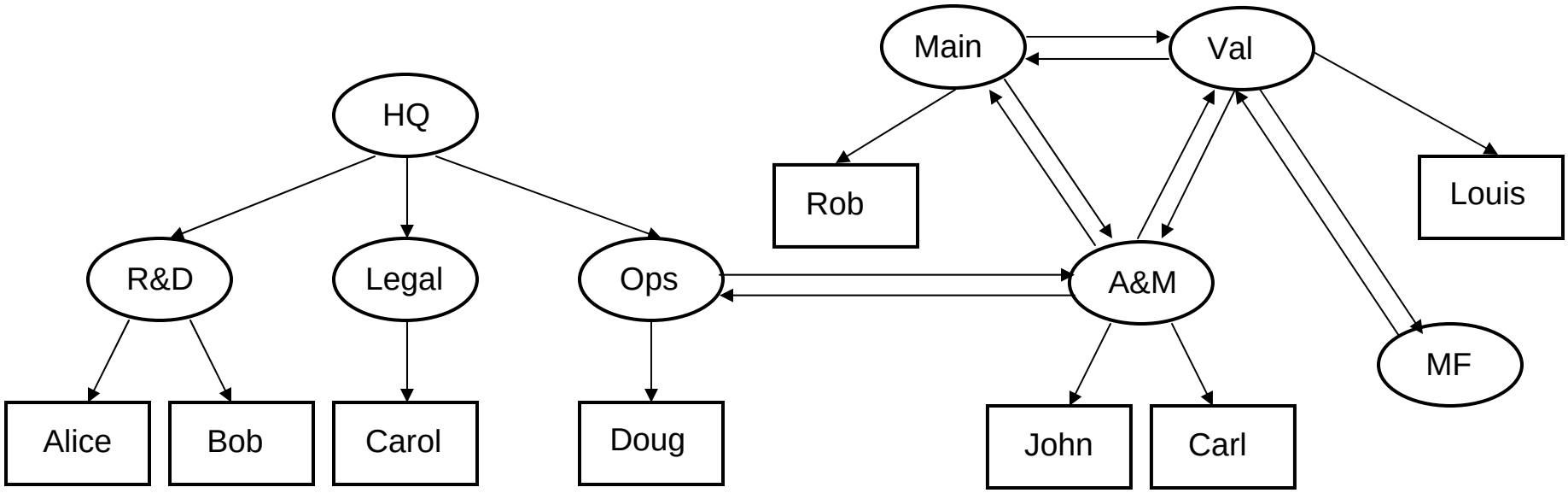


HIERARCHI PKI



MESH PKI

CA Topologies

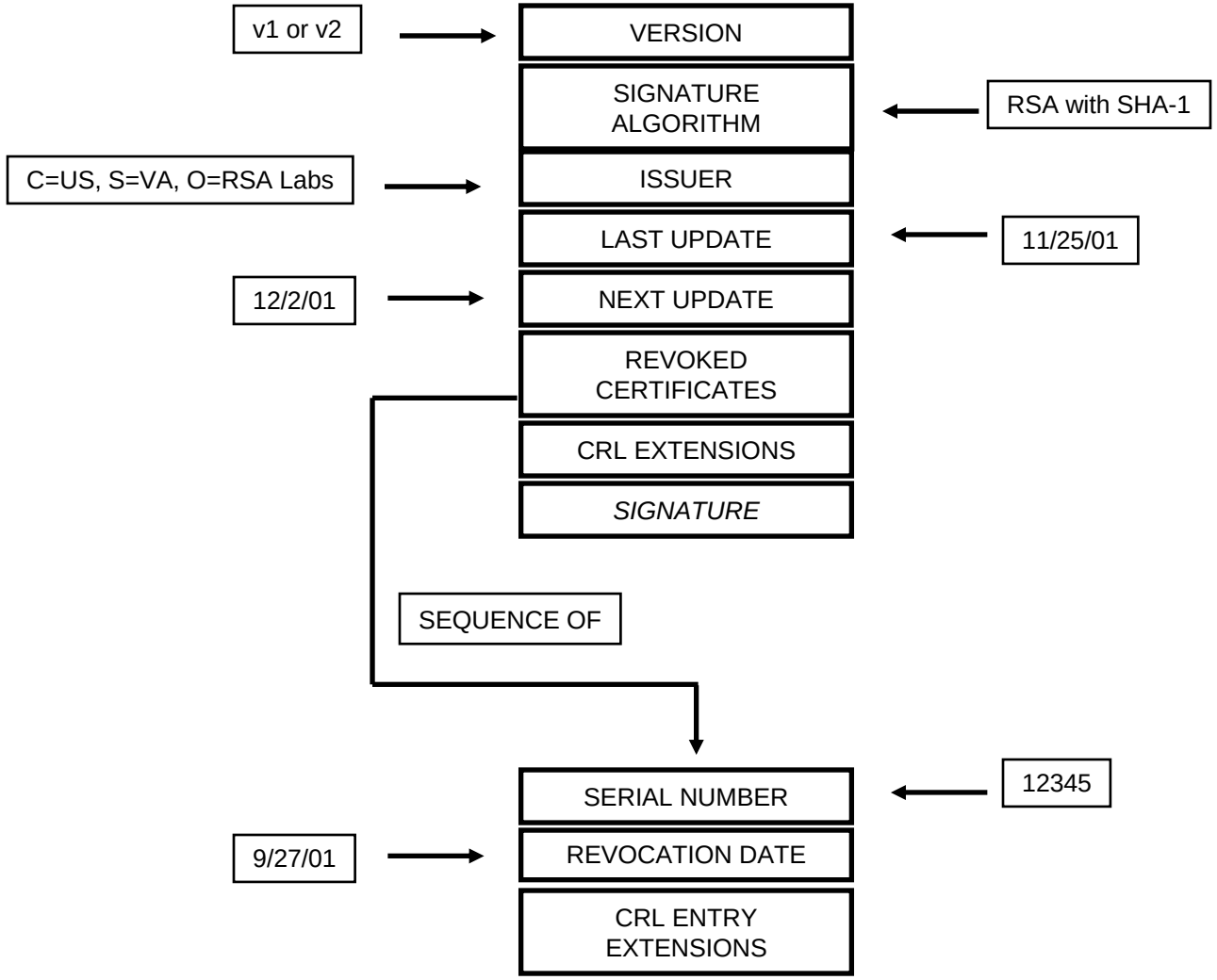


CROSS CERTIFICATION

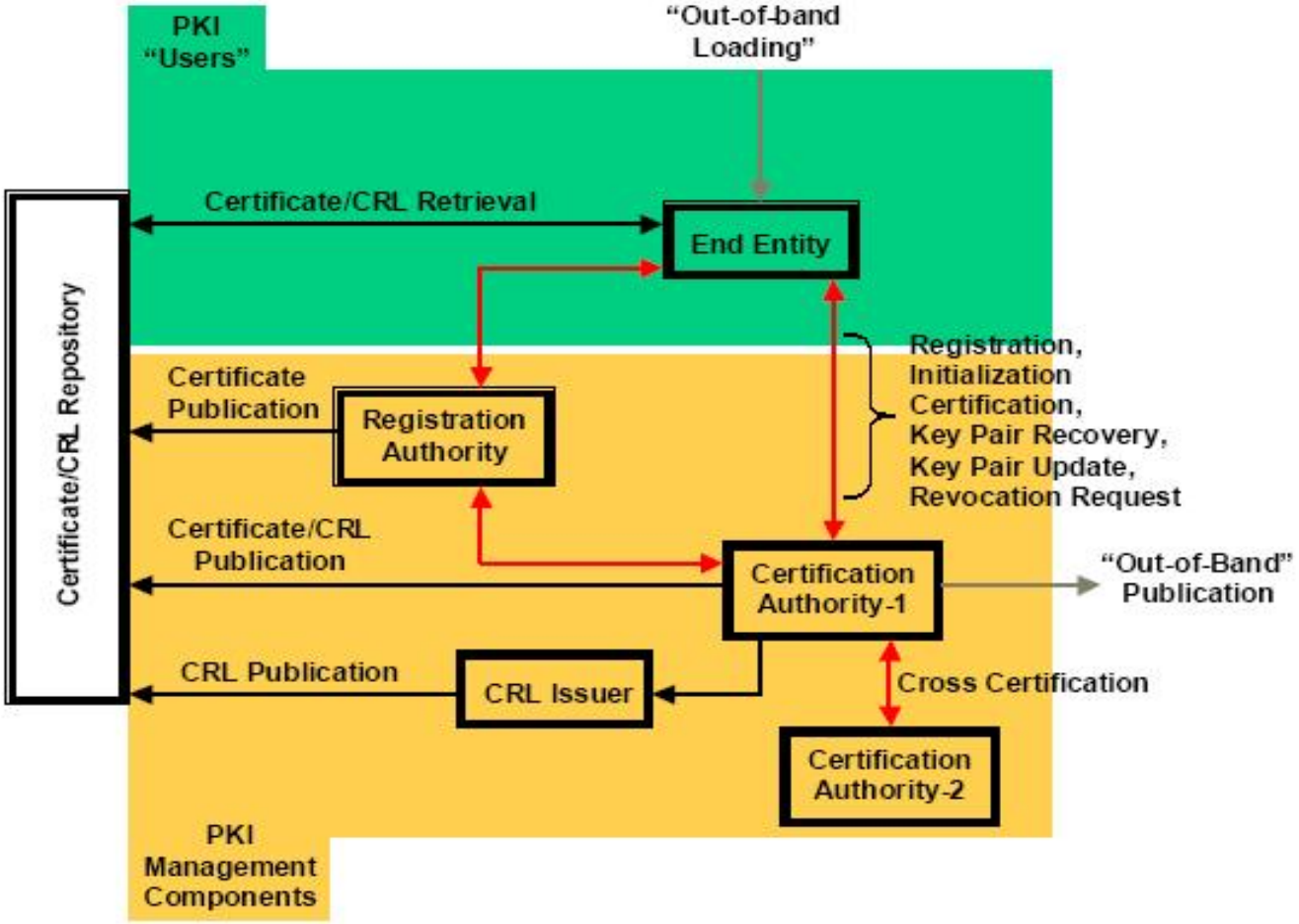
Certificate Revocation

- When a certificate holder terminates employment with a company or suspects that the certificate's corresponding private key has been compromised, they have to invalidate a certificate prior to its expiration date.
- Only the certificate's owner or someone whom the certificate's owner has designated as a revoker can revoke a PGP Certificate.
- Certificate Revocation List (CRL) provides a list of the unexpired certificates that should no longer be used.
- Certificate Authority (CA) distributes the CRL to users periodically.

CRL Format


v1 or v2
VERSION
SIGNATURE ALGORITHM
RSA with SHA-1
C=US, S=VA, O=RSA Labs
ISSUER
LAST UPDATE
11/25/01
12/2/01
NEXT UPDATE
REVOKED CERTIFICATES
CRL EXTENSIONS
SIGNATURE
SEQUENCE OF
SERIAL NUMBER
12345
9/27/01
REVOCATION DATE
CRL ENTRY EXTENSIONS

PKIX Infrastructure



Certificate Authorities (CA)

- The primary role of the CA is to publish the key bound to a given user.
- This is done using the CA's own key, so that trust in the user key relies on one's trust in the validity of the CA's key.
- CA generates public keys. (Optional service)
- CA revokes certificates if information change or if private key is disclosed.

Thank You

Questions

?

Comments