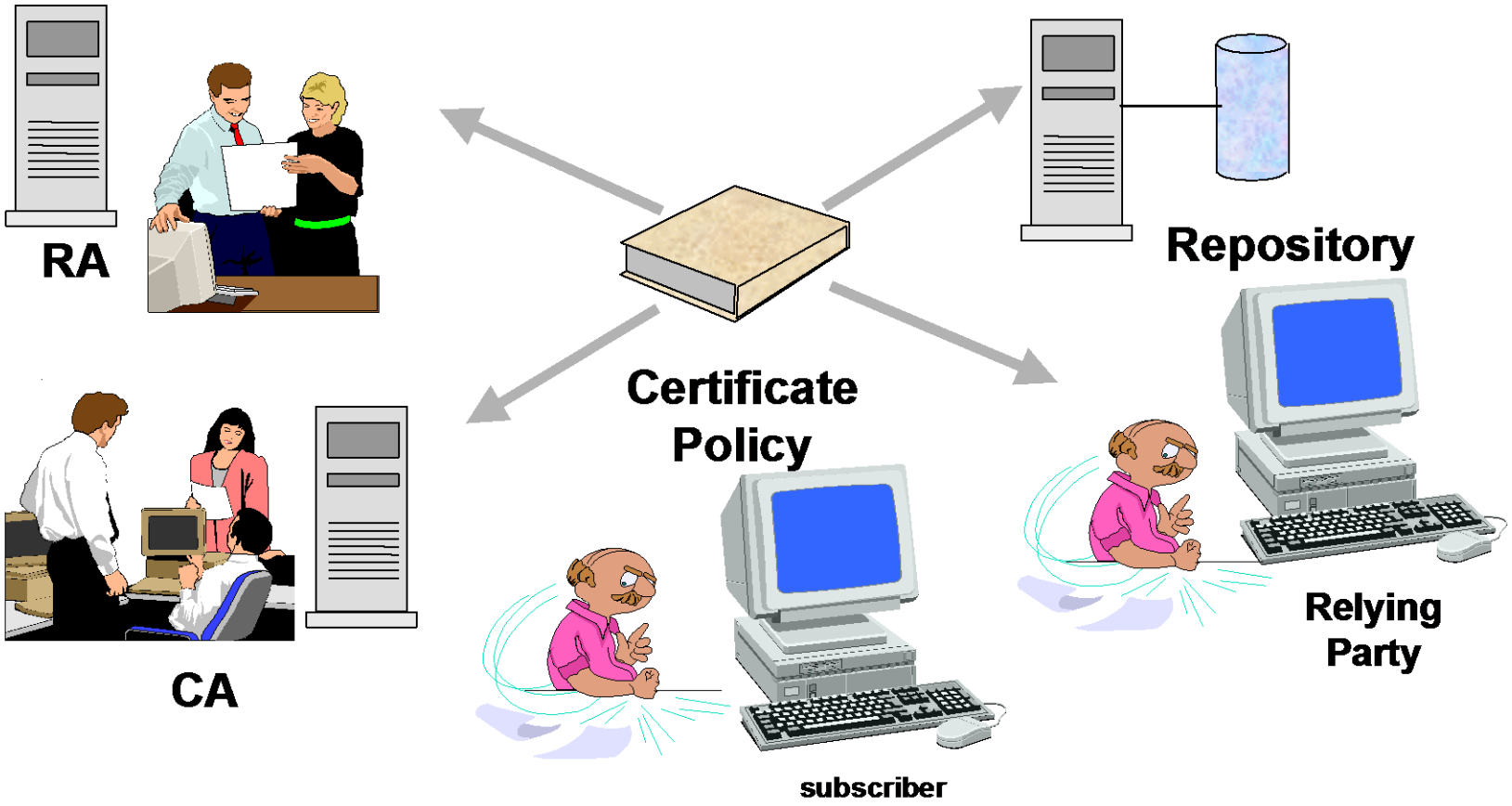
PUBLIC KEY INFRASTRUCTURE

Enterprise PKI



Why PKI?

- PKI is not the goal
- Scalable security services are the goal
- PKI supports scalable security services using public key cryptography

What is PKI?

Public/Private key pair

The public key is a string of bits

A public key certificate answers the following questions (and many more)

- Whose certificate is it?
- What can it be used for?
- Is it still valid?

- Example uses:
  - Is this really the key for Jack Nathan?
  - Can this key be used to send an encrypted message to John Smith?
  - Was the key used for digitally signing this document valid at the time of signing?
  - Fetch me the key of Mike Jones

Security Services That Can Be Supported By PKI

- Authentication - Ability to verify the identity of an entity
- Confidentiality - Protection of information from unauthorized disclosure
- Data Integrity - Protection of information from undetected modification
- Non-repudiation - Prevention of an entity from denying previous actions
- Key estalishment

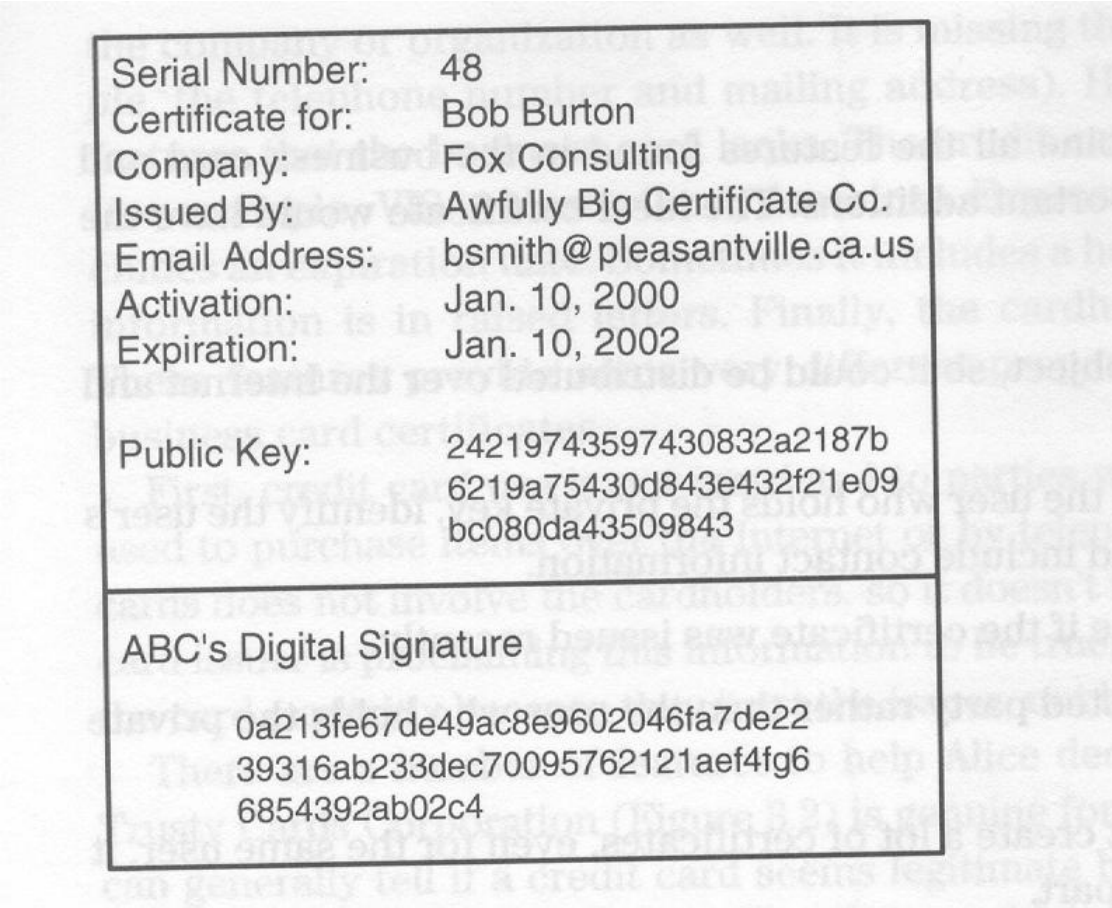
A Fully Functional PKI

- Certification authority
- Certificate repository
- Certificate revocation
- Key backup and recovery
- Automatic key update
- Key history management
- Cross-certification
- Support for non-repudiation
- Time stamping
- Client software

Why Do We Need Certificates?

- Associate the public key with a name or entity
- What is this key good for?
  - Signatures or encryption?
  - Authorization
  - Secure mail, secure web, or digital signatures
  - How can I trust it?

Example Public Key Certificate

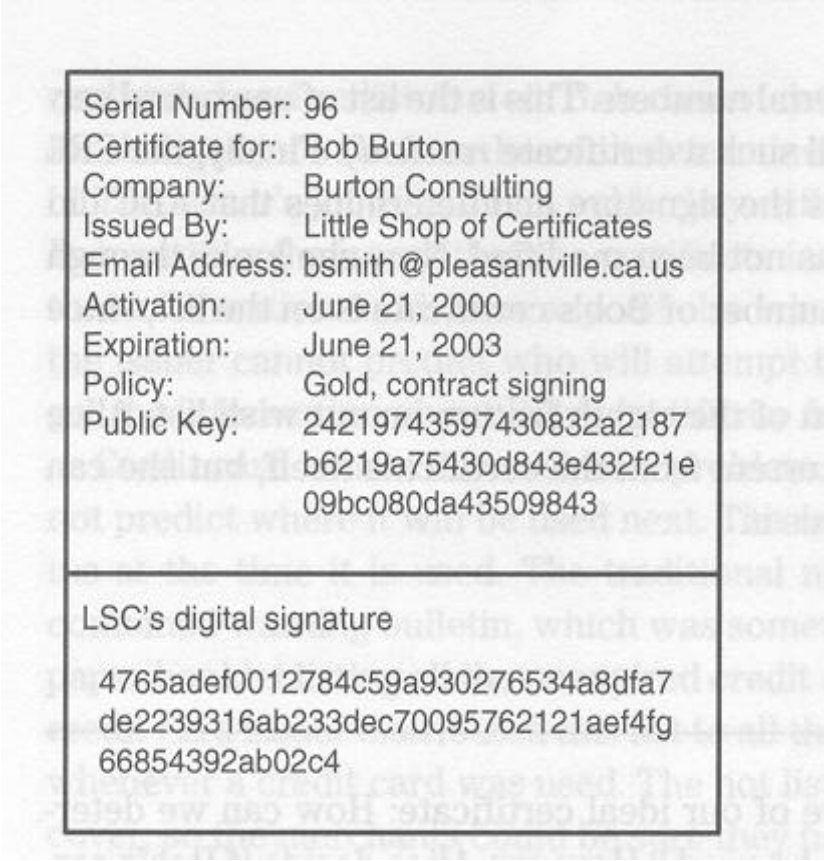


Serial Number:	48
Certificate for:	Bob Burton
Company:	Fox Consulting
Issued By:	Awfully Big Certificate Co.
Email Address:	bsmith@pleasantville.ca.us
Activation:	Jan. 10, 2000
Expiration:	Jan. 10, 2002
Public Key:	24219743597430832a2187b 6219a75430d843e432f21e09 bc080da43509843

ABC's Digital Signature

0a213fe67de49ac8e9602046fa7de22
39316ab233dec70095762121aef4fg6
6854392ab02c4

A Certificate with Policy Information



Problems with Identity Certificates

- Which "Don Smith?" does this certificate corresponds to?
- Suppose there are two "Don Smith" s in the same organization, how do we know to whom a given certificate belongs?
- Where directory do we look up for "Don Smith?"
- Examples:
  - PGP: Used for email encryption
    - Identity is name + email address
  - SPKI: Used for authorization/access control
    - Identity is a name meaningful within the domain of application
      - Account name on a server
      - Credit card number
      - Merchant ID
  - PGP and SPKI also use the public key as a unique ID

More on Public Key Certificates

- Features
  - Tamper-evident
  - Issued by a Trusted third party (TTP) called CA
  - Complete user identification
  - Fixed expiration
- Drawbacks
  - Must trust issuer

X.509: A Standard for PKI

- Defined and standardized a general, flexible certificate format.
- Three nested components in an X.509 certificate
  - Tamper evident envelop (outer most)
  - Basic certificate contents
  - Certificate extensions (options)

X.509

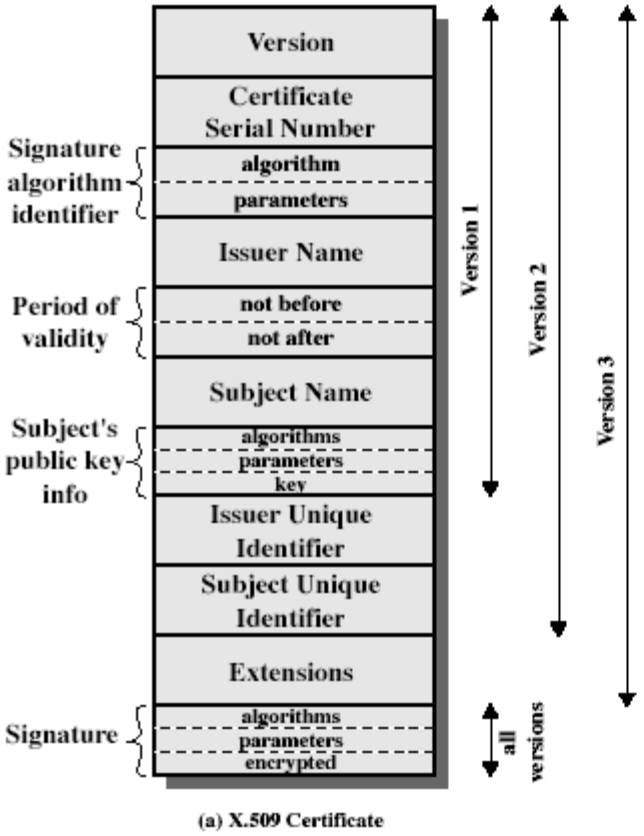
X.509 Authentication Service

- part of CCITT X.500 directory service standards
  - distributed servers maintaining some info database
- defines framework for authentication services
  - directory may store public-key certificates
  - with public key of user
  - signed by certification authority
- also defines authentication protocols
- uses public-key crypto & digital signatures
  - algorithms not standardised, but RSA recommended

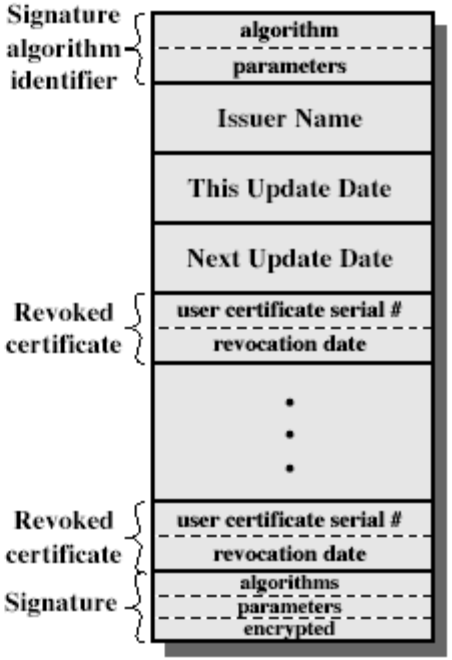
X.509 Certificates

- issued by a Certification Authority (CA), containing:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (from - to dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (of hash of all fields in certificate)
- notation `CA<<A>>` denotes certificate for A signed by CA

X.509 Certificates



(a) X.509 Certificate



(b) Certificate Revocation List

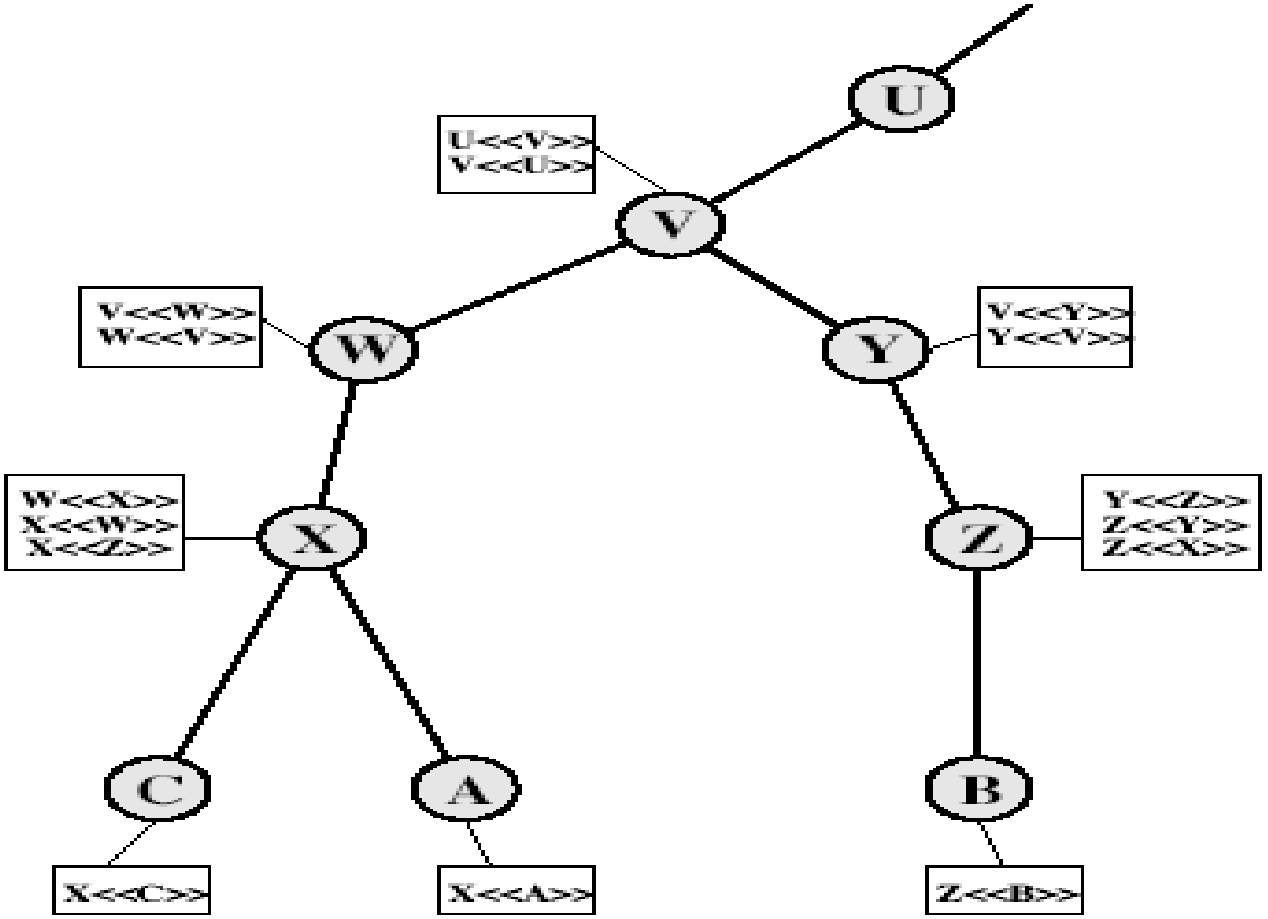
Obtaining a Certificate

- any user with access to CA can get any certificate from it
- only the CA can modify a certificate
- because cannot be forged, certificates can be placed in a public directory

CA Hierarchy

- if both users share a common CA then they are assumed to know its public key
- otherwise CA's must form a hierarchy
- use certificates linking members of hierarchy to validate other CA's
  - each CA has certificates for clients (forward) and parent (backward)
- each client trusts parents certificates
- enable verification of any certificate from one CA by users of all other CAs in hierarchy

CA Hierarchy Use



Certificate Revocation

- certificates have a period of validity
- may need to revoke before expiry, eg:
  1. user's private key is compromised
  2. user is no longer certified by this CA
  3. CA's certificate is compromised
- CA's maintain list of revoked certificates
  - the Certificate Revocation List (CRL)
- users should check certs with CA's CRL

Authentication Procedures

- X.509 includes three alternative authentication procedures:
- One-Way Authentication
- Two-Way Authentication
- Three-Way Authentication
- all use public-key signatures

One-Way Authentication

- 1 message (A->B) used to establish
  - the identity of A and that message is from A
  - message was intended for B
  - integrity & originality of message
- message must include timestamp, nonce, B's identity and is signed by A

Two-Way Authentication

- 2 messages (A->B, B->A) which also establishes in addition:
  - the identity of B and that reply is from B
  - that reply is intended for A
  - integrity & originality of reply
- reply includes original nonce from A, also timestamp and nonce from B

Three-Way Authentication

- 3 messages (A->B, B->A, A->B) which enables above authentication without synchronized clocks
- has reply from A back to B containing signed copy of nonce from B
- means that timestamps need not be checked or relied upon

X.509 Version 3

- has been recognised that additional information is needed in a certificate
  - email/URL, policy details, usage constraints
- rather than explicitly naming new fields defined a general extension method
- extensions consist of:
  - extension identifier
  - criticality indicator
  - extension value

Certificate Extensions

- key and policy information
  - convey info about subject & issuer keys, plus indicators of certificate policy
- certificate subject and issuer attributes
  - support alternative names, in alternative formats for certificate subject and/or issuer
- certificate path constraints
  - allow constraints on use of certificates by other CA's

Summary

- have considered:
  - Kerberos trusted key server system
  - X.509 authentication and certificates