Applications of crypto, namely of public key techniques

PV018

Vašek Matyáš

Crypto applications

- Related lectures
  - Block ciphers and modes of operation. DES, AES.
  - Key management and protocols
  - Standards (in security and cryptography)
  - Authentication
  - Secure hardware (next week)
- Today
  - Positioning of crypto functions
  - Digital signatures
  - PKI, Trust management

Crypto mechanisms

- Workstation vs. LAN/firewall granularity
- Traffic analysis, privacy services
  - Traffic padding
- Considerations (as usual):
  - Cost
  - Security
  - Administration/Logistics requirements

End-to-end vs. Link encryption

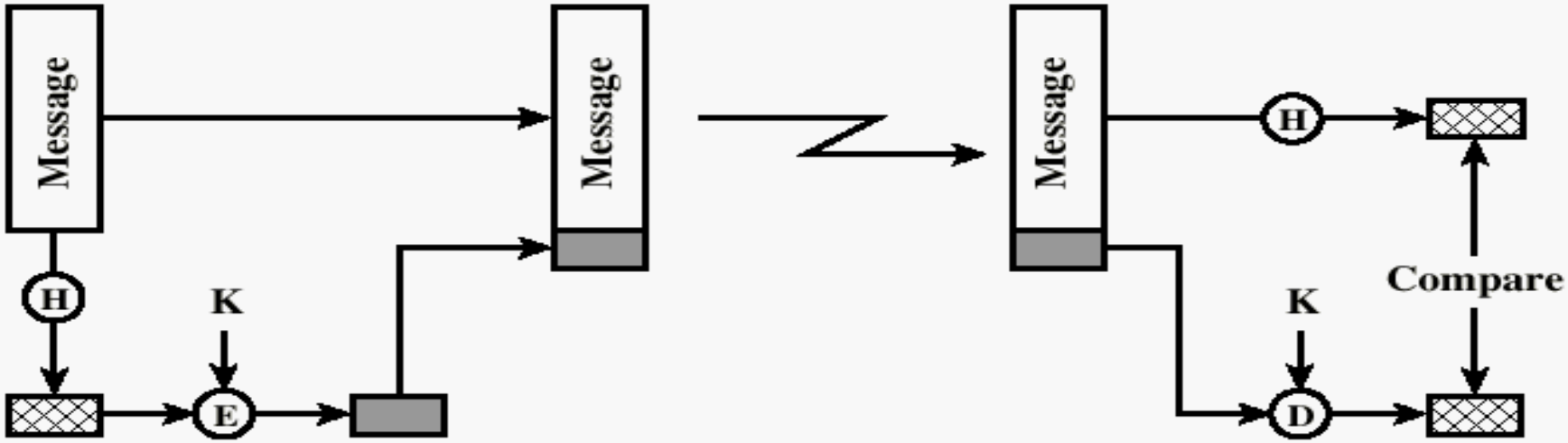
- En-/De-cryption device at sender/recipient ends
- Packet content protected at all nodes
- Headers available to all nodes on the way
- Many services cannot be provided
- IPsec

- En-/De-cryption device at ends of each link
- Processing and message avail. at each node
- Headers can be encrypted on the link (onion routing)
- Advanced network services can be provided

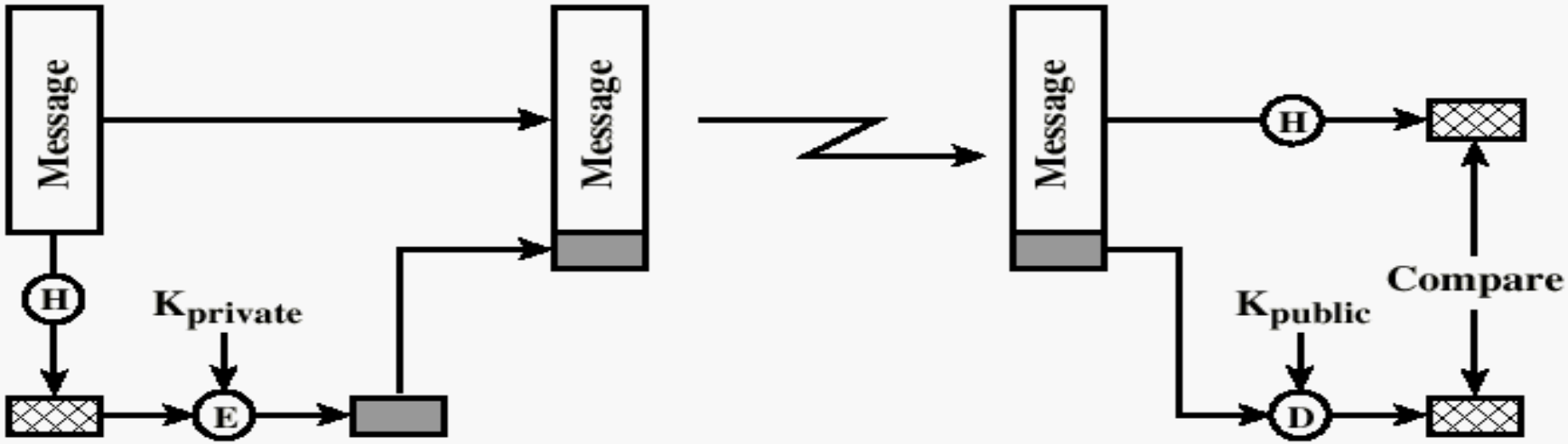
Public-key cryptography

- Shared-key crypto: good security vs. Key Distribution Center (involuntary reliance)
- Authentication of data
  - Hash functions (MAC)
  - Symmetric ciphers (MAC-like)
- GCHQ (UK, 1970) – non-secret encryption
  - Principles of Diffie-Hellman (76), RSA (78)
  - More at *www.gchq.gov.uk*

Data authentication



(a) Using conventional encryption



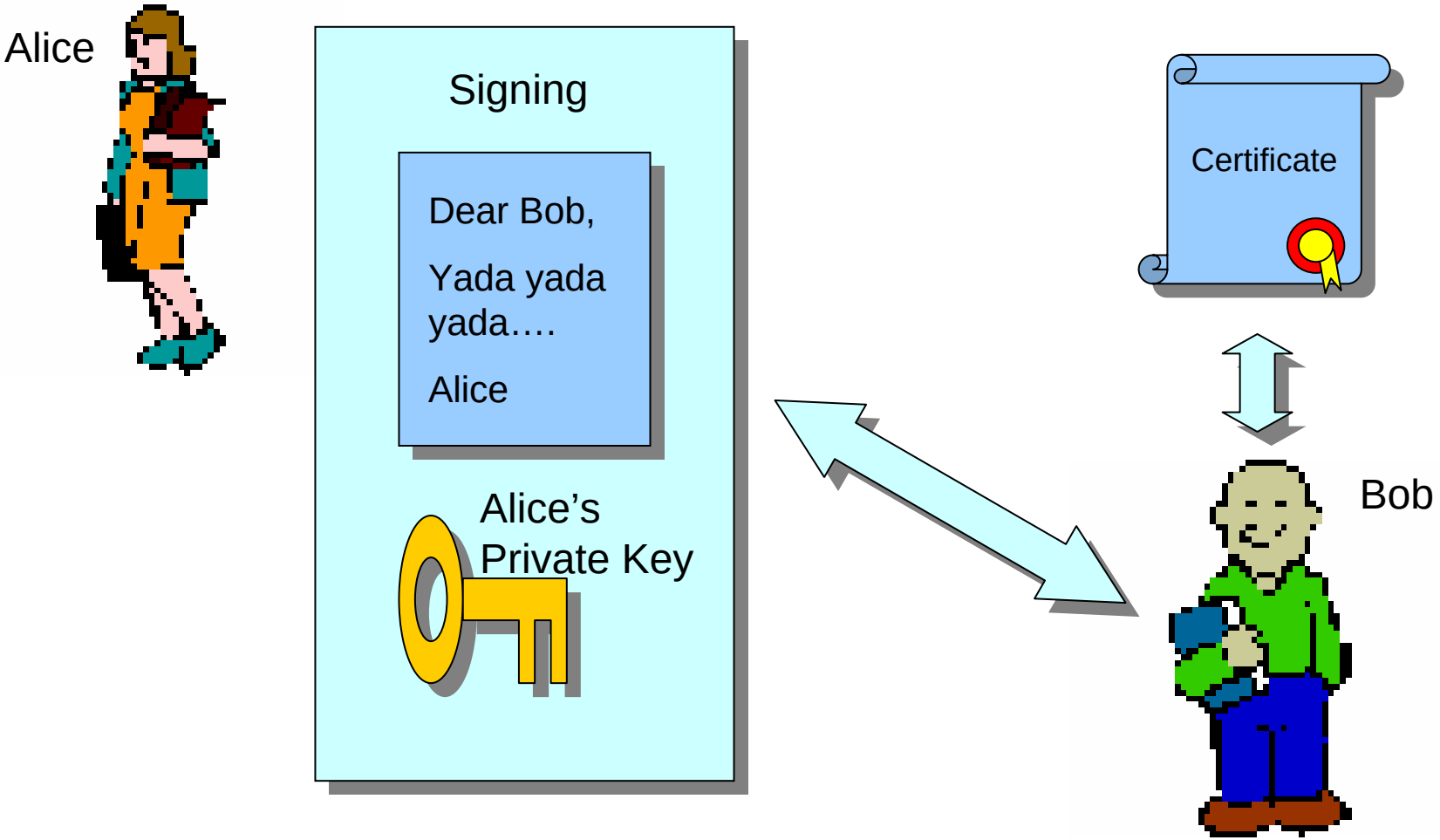
(b) Using public-key encryption

Shared-key data authentication

- Use the shared key to encrypt the data image
- Only those able to decrypt such message can verify the image correctness

- Use the shared key to create a Message Authentication Code (**MAC**) representing both the data and the key
- Only those able to recalculate the MAC can verify the image correctness

What are digital signatures?



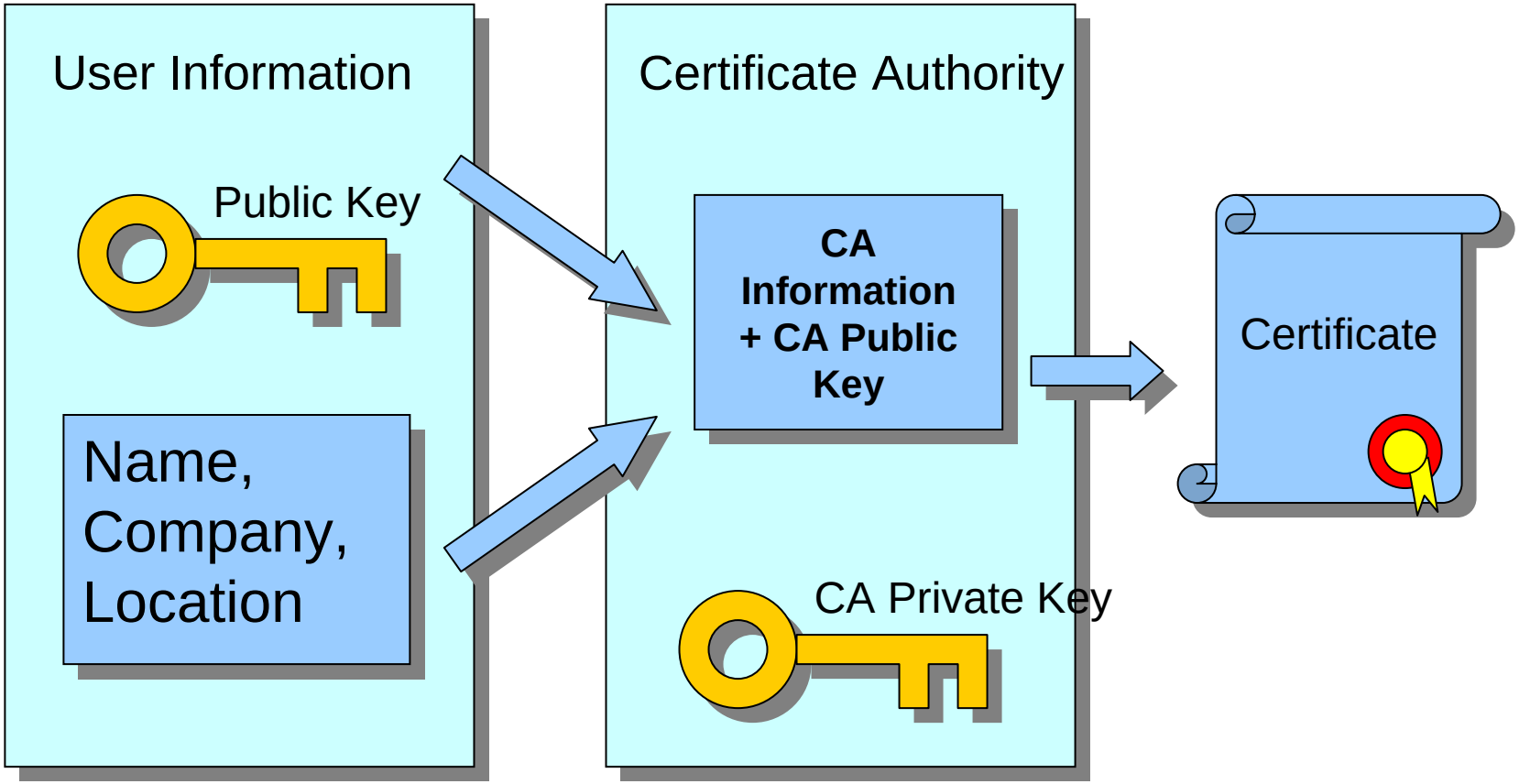
Public-key management

- Yellow Pages-like directory
  - Diffie-Hellman, “phonebooks”
  - Electronic form (browsers)
  - Efforts like Global Trust Register
- Trust models of PGP vs. (?) X.509
  - Web of trust vs. (?) Certification authority
  - PGP modified to accept X.509 certificates
  - Trust model not defined by software, but by the environment (that also implies type of S/W used)

X.509 based authentication

- X.509 specifies the format for public-key certificates.
- The certificate contains the public key of a user and is signed with the private key of a Certification Authority (CA).
- Distributed environment using a database with certificate (user) information.
- Used in S/MIME, IP Security, SSL/TLS, SET.

What is a certificate?



The role of the Certification Authority

- "I, Bob Bloggs, declare that my public key is 1234...321"
- **Which Bob Bloggs? What about impersonators?**

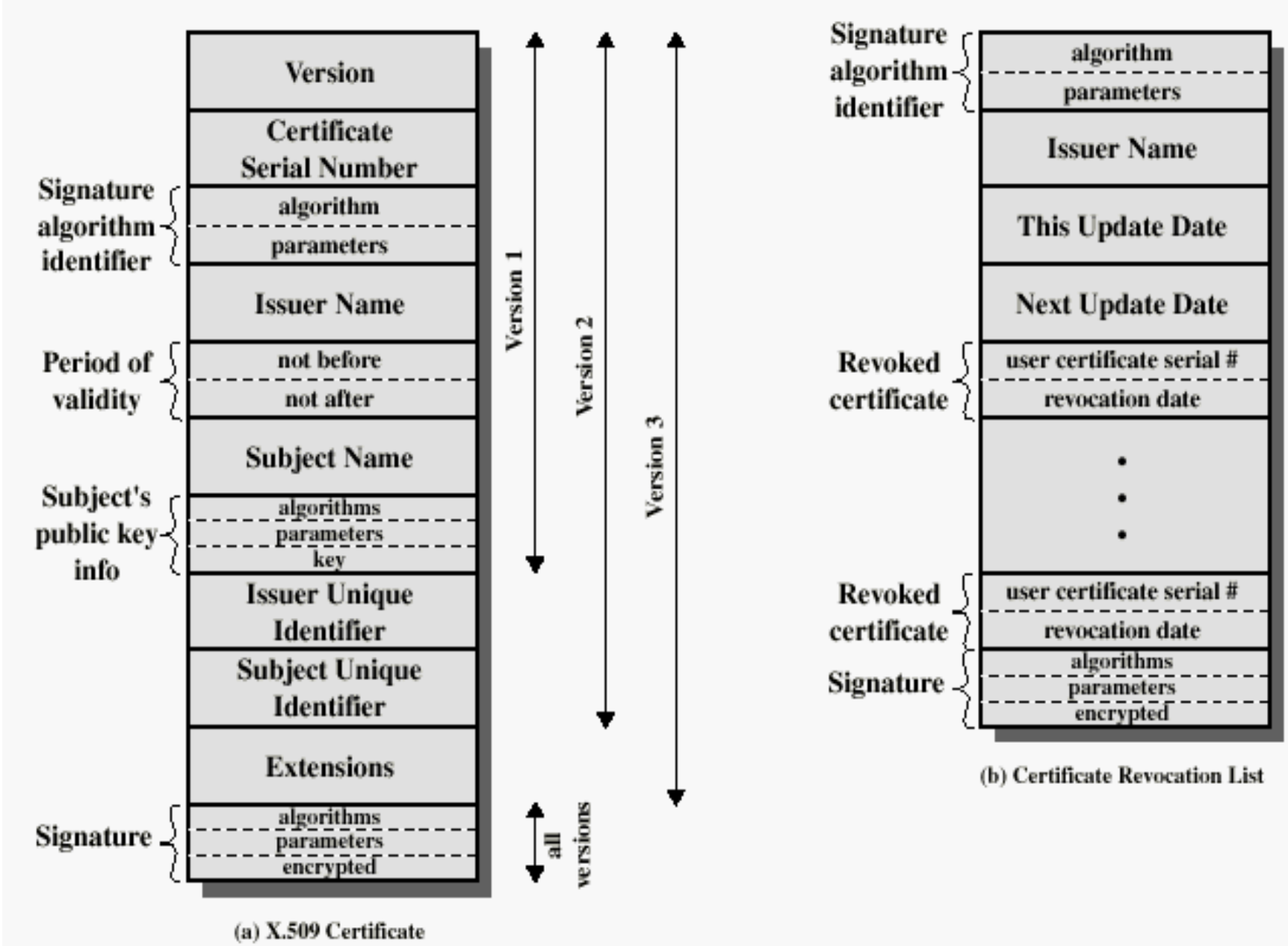
- Solution: Public Key Certificates signed by certifiers

- Certifiers have to be trusted parties with declared policies
- Complete management of certificates (issuance, revocation…)
- Customer relation:
  - Closed User Group
  - Public Certification Authority

Reliance on the CA

- Anyone (with user X's certificate) can verify with X's CA that X's certificate is valid
  - That this CA created it (possibly off-line using CA's own public key)
  - That the CA still considers it valid (both off-line and on-line)
- No-one (except for the CA = owner of the CA's private key) can create/modify X's certificate

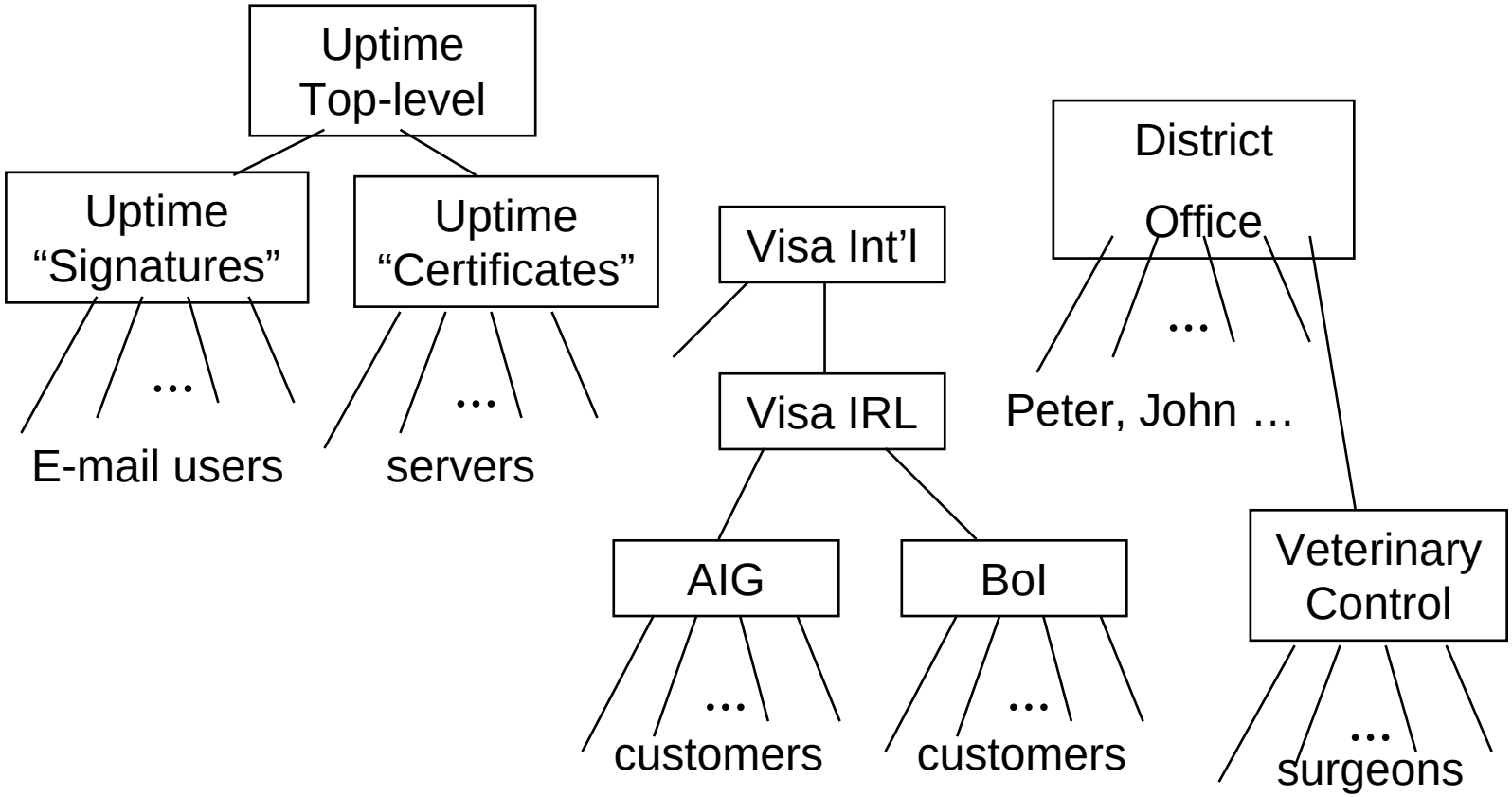
X.509 certificate



Public-key (X.509v3) certificate

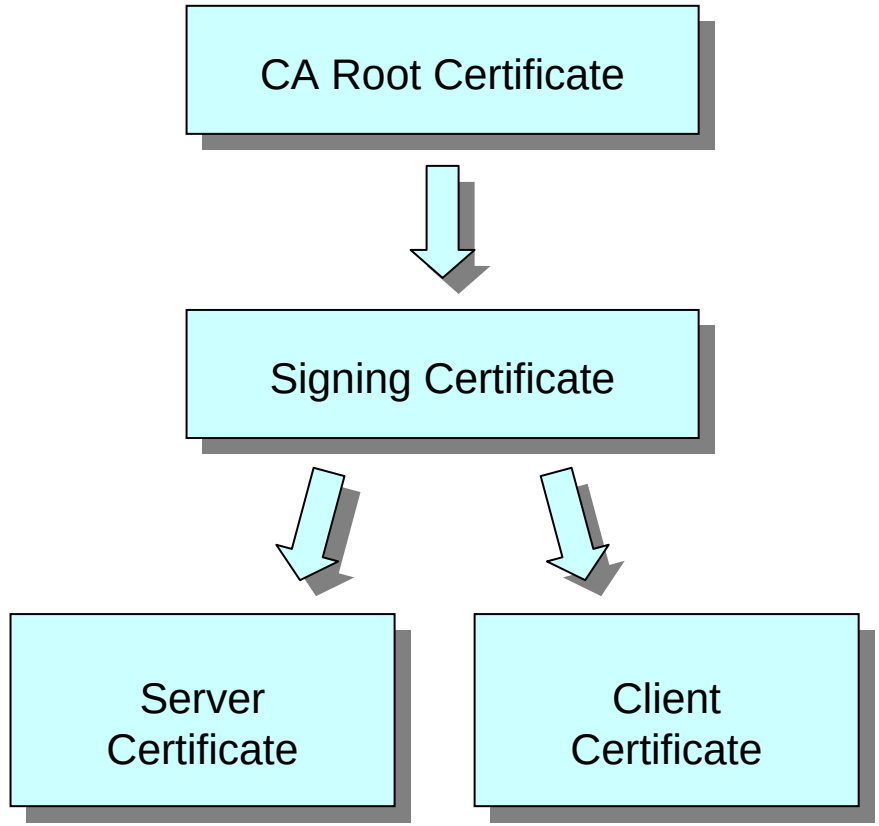
```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signature            BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
     version         [0]  Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,       -- notBefore, notAfter
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,  -- algID, bits
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
     extensions      [3]  Extensions OPTIONAL
        -- sequence of: extnID, crit, value }
```

CA hierarchy

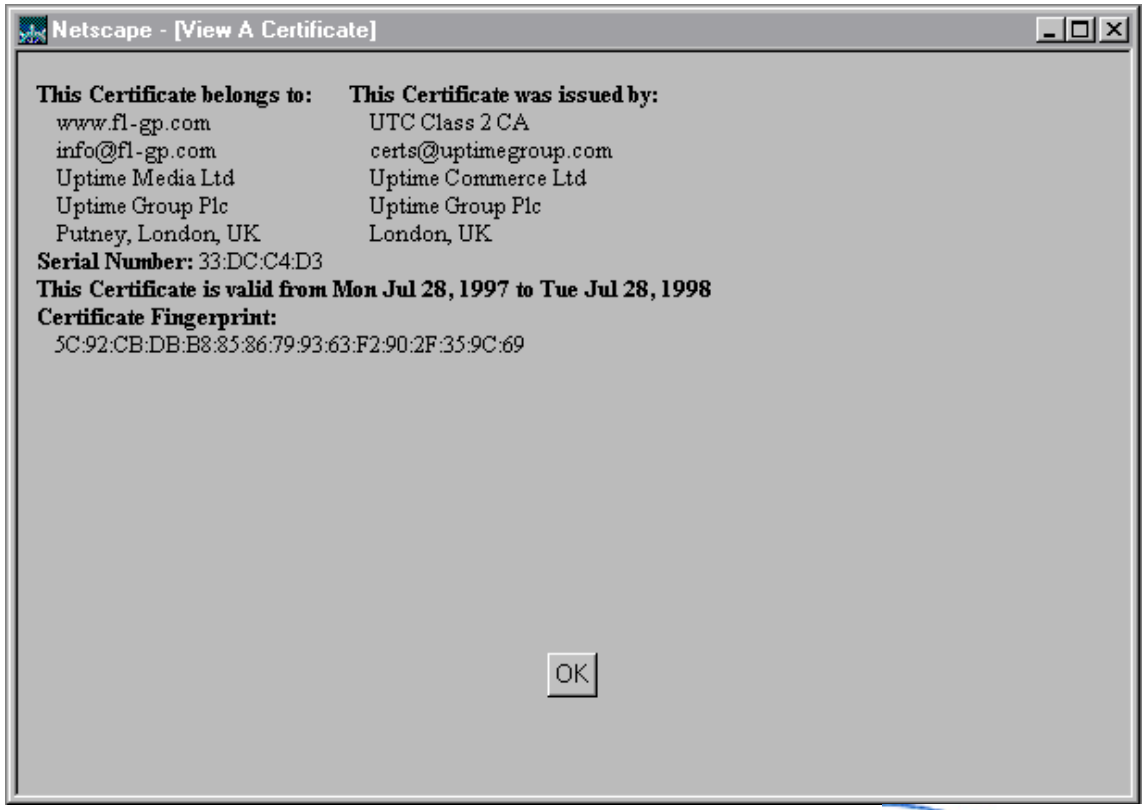


Certificate types

- Certificate Hierarchy
  - CA Root Certificate
  - Signing Certificates
  - Web Server Certificates
  - Client Certificates
- Certificate Chains

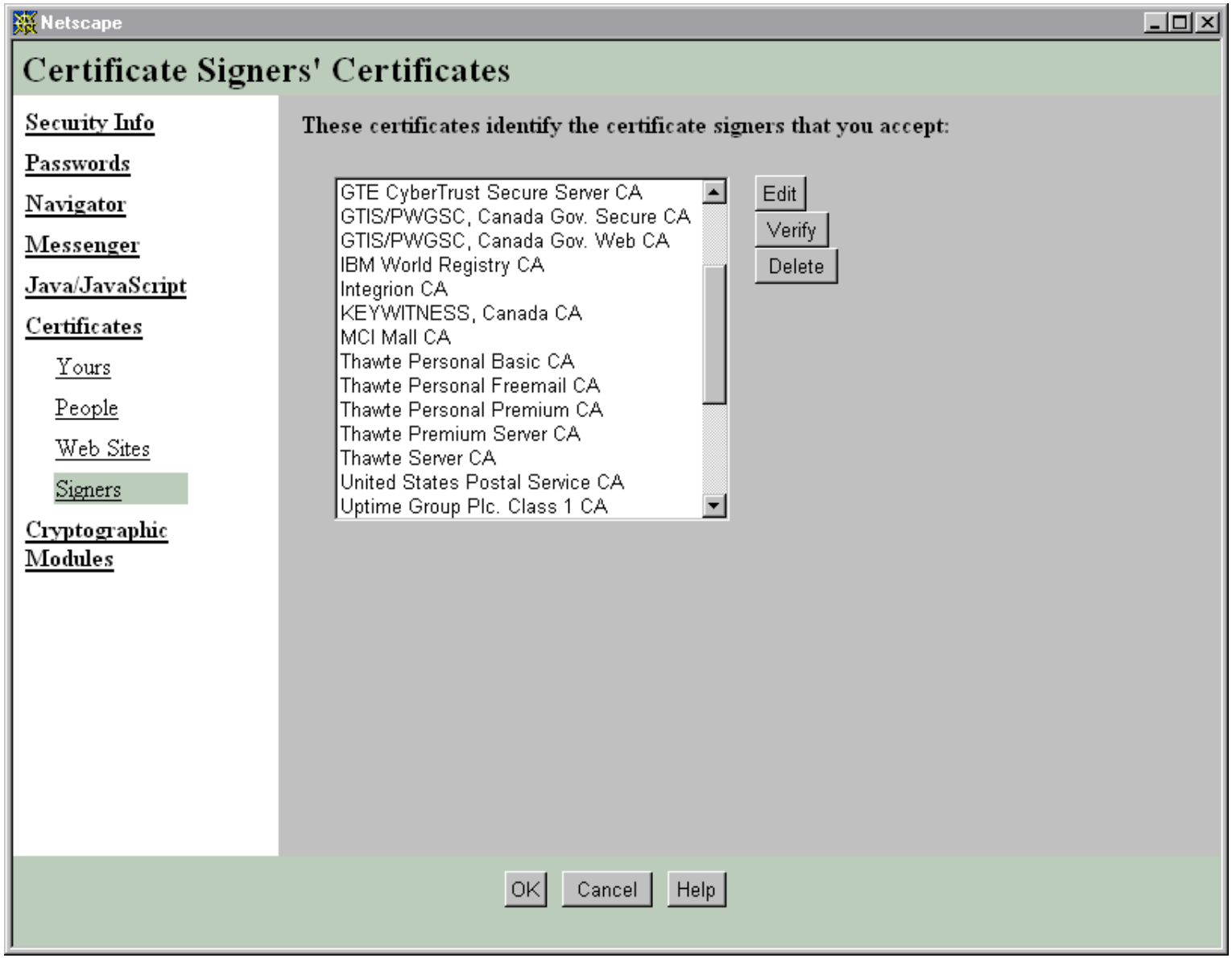


… Certificate from the server



UPTIME COmmerce

… Is in your database???



What about the private key...

…when you lose it?
…when it’s compromised?
…when you change employer?
…when escrowed by an escrow agent?
…when required by court?
…when temporarily absent from work?
…when…

Certificate revocation

- Certificate revocation != key revocation
- User-lead (PGP) or CA-lead (X.509) revocation
- Reasons for certificate revocation
  - The user is no longer certified (represented) by a given CA
  - CA's certificate misused
  - User's private key misused

Key/Certificate control

- **Liberal**: key/certificate is **valid** unless we are not explicitly and reliably told otherwise.
  - CRL – Certificate Revocation List.

- **Conservative**: key/certificate **invalid** unless we are explicitly and reliably told otherwise.
  - fresh confirmation, from a trusted party, and useful in case of dispute.
  - OCSP – Online Certificate Status Protocol

- **Revocation is the matter of highest importance!!!**

Revocation – Technical note

- PGP users can revoke their key without certifier's knowledge
- X.509 CAs can revoke user's key without her knowledge

PGP lessons

- Obviously, key servers unreliable <president@whitehouse.gov>
- Key IDs unreliable
  - should not be used for binding
- Key fingerprints better (yet not unique!!!)

CA operations

- Immature public service market
- Technology reliable, implementations
  and operations mostly not!
- Governments weaken the growth basis - by
  unclear escrow and liability “statements”
- Banks uncertain where to step in

- Closed User Groups (Extranets, Intranets)
- Token-based (smart-card) applications
- SET did not bring the break-through

PKI in use today

1) Internal systems (authentication in distributed environments)

2) With existing customers (online banking)

3) Communication with other players (partners, etc.) that have been previously known

Global Trust Register

- Paper-based Register (off-line top-level CA) in 1998-99
- Keys and other info (URL, address, phone...)
- Keys verified and rated D➢ C➢ B➢ A (highest)
- Reliable, convenient, free press privilege

- Top-level X.509 CAs (and secure websites)
- Important PGP keys
- EDI and Entrust/Solo(X.509) keys

Authenticity of documents

- Current approaches to digital signatures unsuitable to publishing, unclear liability issues, etc.
- Possible solutions:
  - Signing keys with shorter life than verification key(s)
  - Hash trees

Recommended reading – week 3

- Paper "*Tamper Resistance - a Cautionary Note*", Ross Anderson, Markus Kuhn, 2nd USENIX Workshop on Electronic Commerce
- `http://www.cl.cam.ac.uk/users/rja14/tamper.html`

- Extremely useful for next week ☺

To be continued

- Block ciphers and modes of operation. DES, AES.
- Key management and protocols

- Secure hardware
  - Critical for security & performance
- Standards
  - how to use crypto

Reminder – term project report

- Approvals after March 9 with 25% penalty
  - And 50% penalty if not approved by March 23rd
- Your report should be:
  - Focused on the topic, analytical in nature (your own view/comments, at least in conclusions, is critical!)
  - 5-7 pages, sharp! Single lines, equiv. Times N. R. 10/11
  - Delivered on/before the deadline May 25th