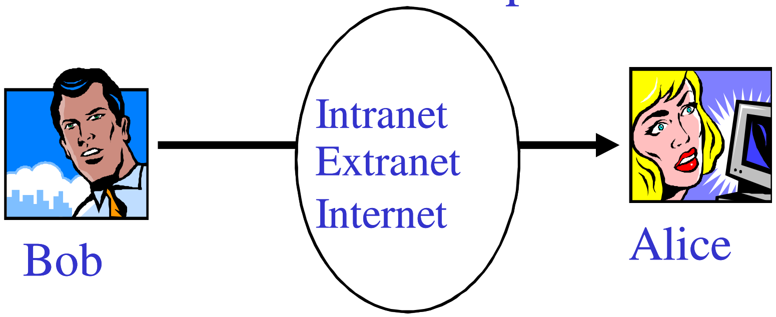
Public Key Infrastructure (X509 PKI)

Presented by : Ali Fanian

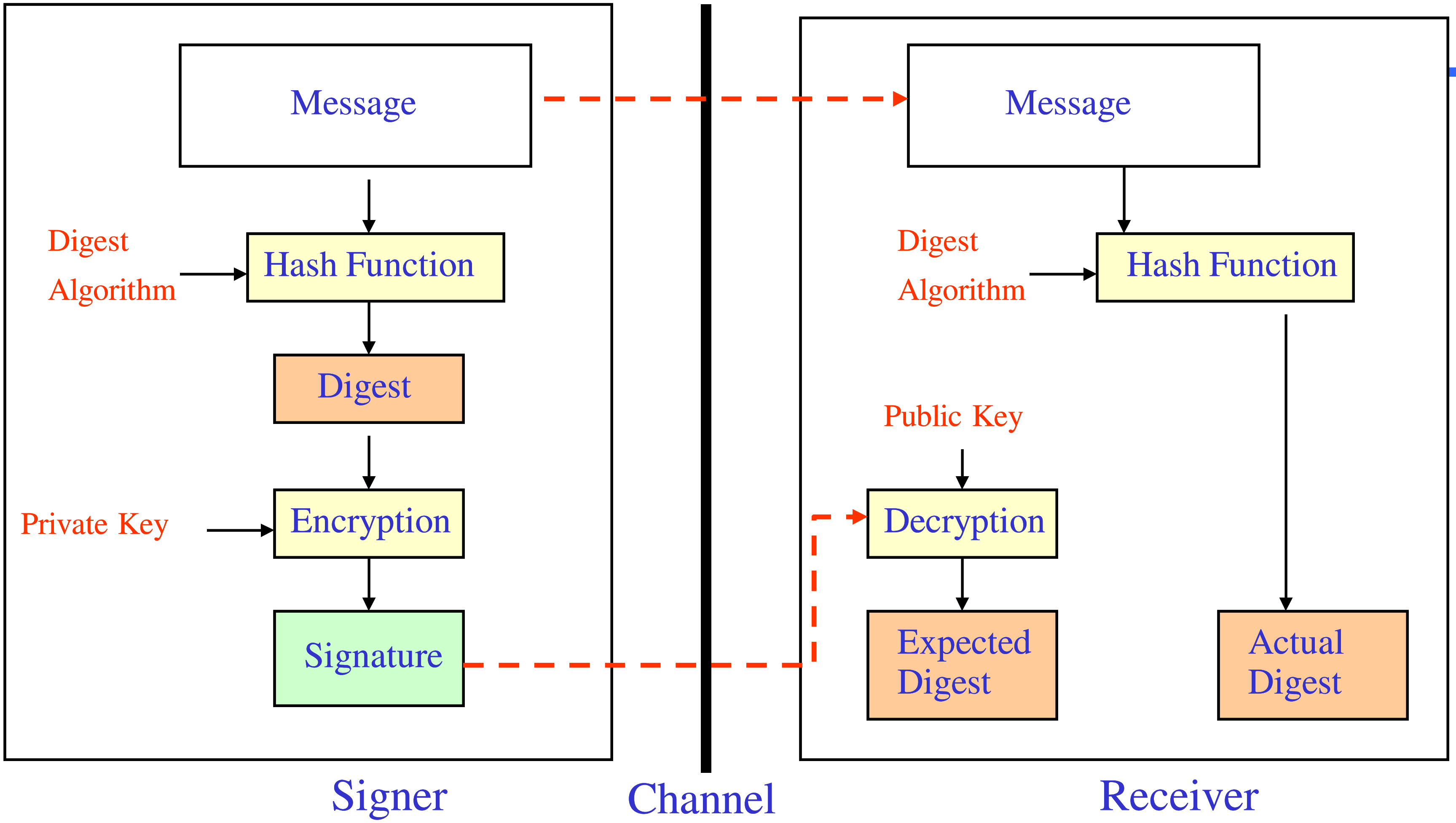
Digital Signature

A Digital Signature is a data item that vouches the origin and the integrity of a Message

- The originator of a message uses a signing key (Private Key) to sign the message and send the message and its digital signature to a recipient
- The recipient uses a verification key (Public Key) to verify the origin of the message and that it has not been tampered with while in transit



Digital Signature



Digital Signature

There is still a problem linked to the “*Real Identity*” of the Signer.

Why should I trust what the Sender claims to be?

Moving towards PKI …

Digital Certificate

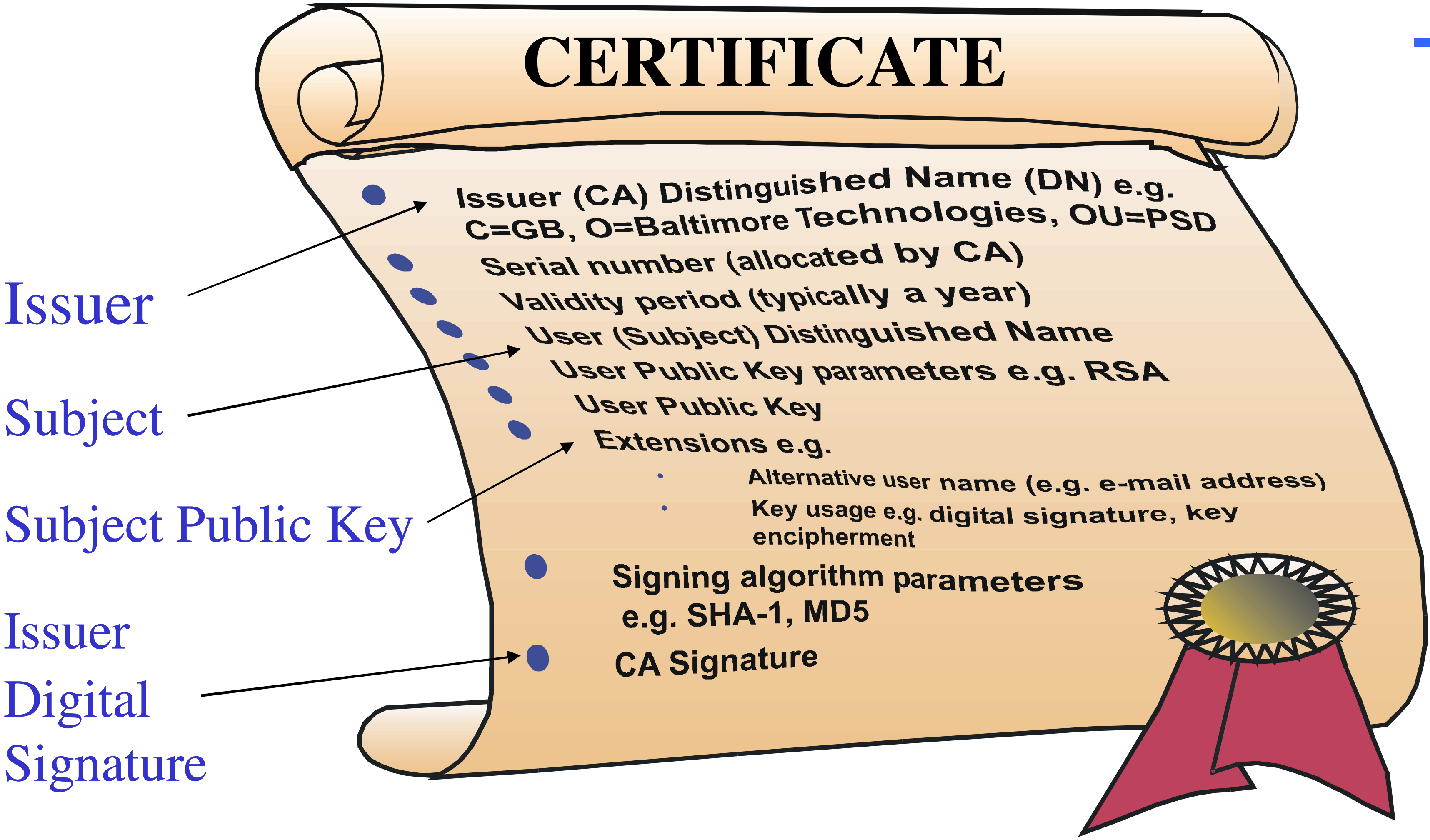
Digital Certificate

A Digital Certificate is a binding between an entity's Public Key and one or more Attributes relating its Identity.

- The entity can be a Person, an Hardware Component, a Service, etc.
- A Digital Certificate is issued (and signed) by someone

  -Usually the issuer is a Trusted Third Party (TTP)
- A self-signed certificate usually is not very trustworthy

Digital Certificate



CERTIFICATE

- Issuer (CA) Distinguished Name (DN) e.g. C=GB, O=Baltimore Technologies, OU=PSD
- Serial number (allocated by CA)
- Validity period (typically a year)
- User (Subject) Distinguished Name
- User Public Key parameters e.g. RSA
- User Public Key
- Extensions e.g.
  - Alternative user name (e.g. e-mail address)
  - Key usage e.g. digital signature, key encipherment
- Signing algorithm parameters e.g. SHA-1, MD5
- CA Signature

Issuer

Subject

Subject Public Key

Issuer Digital Signature

Digital Certificate

Problems

- How are Digital Certificates Issued?
- Who is issuing them?
- Why should I Trust the Certificate Issuer?
- How can I check if a Certificate is valid?
- How can I revoke a Certificate?
- Who is revoking Certificates?

Moving towards PKI …

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI)

A Public Key Infrastructure is an Infrastructure to support and manage Public Key-based Digital Certificates

Public Key Infrastructure (PKI)

"A PKI is a set of agreed-upon standards

- Certificate structure

- Structure between multiple CAs

- Methods to discover and validate Certification Paths

-Operational Protocols

-Management Protocols

"Digital Certificates" book – Jalal Feghhi, Jalil Feghhi, Peter Williams

Public Key Infrastructure (PKI)

X509 Digital Certificates standard

➔ Standards defined by IETF, PKIX WG:

http://www.ietf.org/

… *however X509 is not the only approach (e.g. PKI)*

X509 PKI – Technical View

Basic Components:

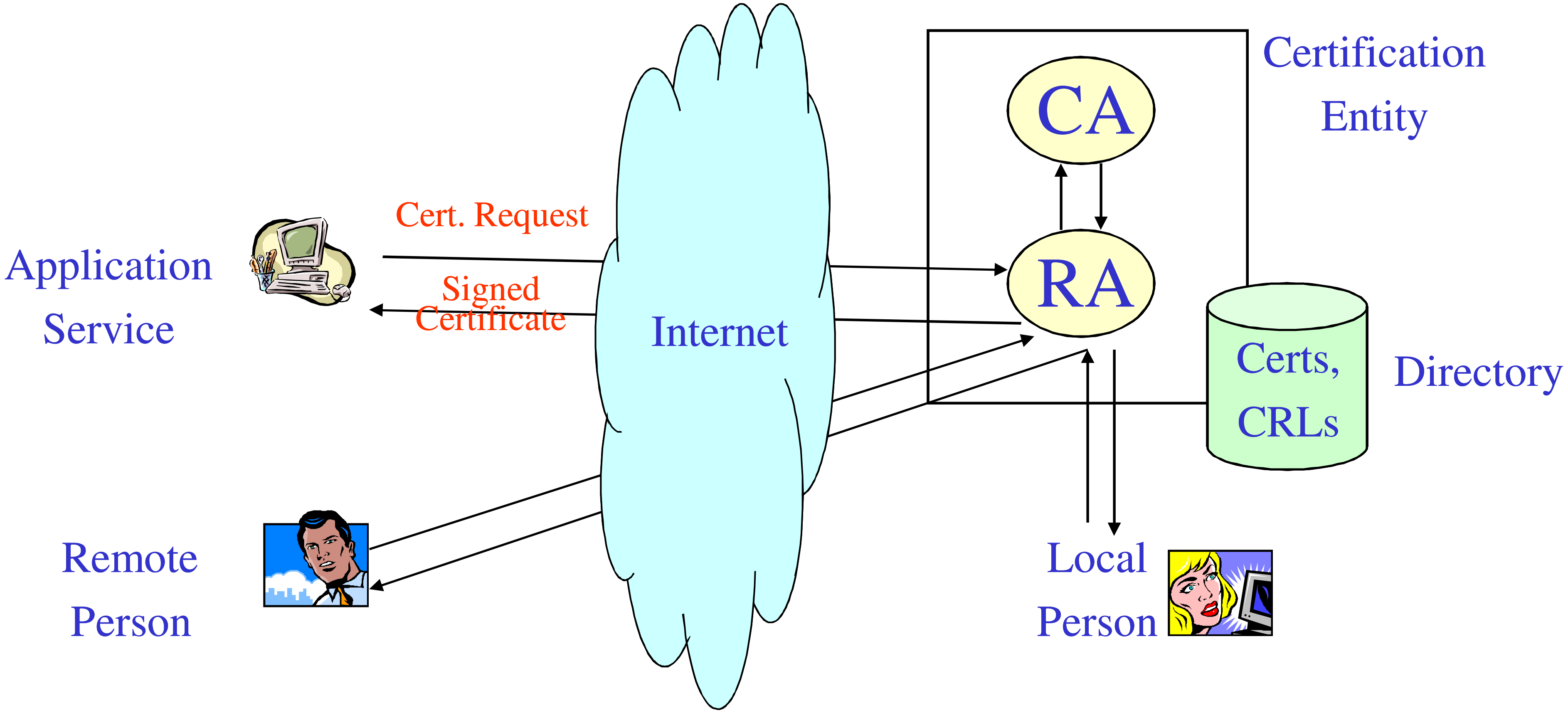
- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate Distribution System

“Provider” Side

- PKI enabled applications

“Consumer” Side

X509 PKI – Simple Model



X509 PKI
Certificate Authority (CA)

Basic Tasks:

- Key Generation
- Digital Certificate Generation
- Certificate Issuance and Distribution
- Revocation
- Key Backup and Recovery System
- Cross-Certification

X509 PKI
Registration Authority (RA)

Basic Tasks:

- Registration of Certificate Information
- Face-to-Face Registration
- Remote Registration
- Automatic Registration
- Revocation

X509 PKI
Certificate Distribution System

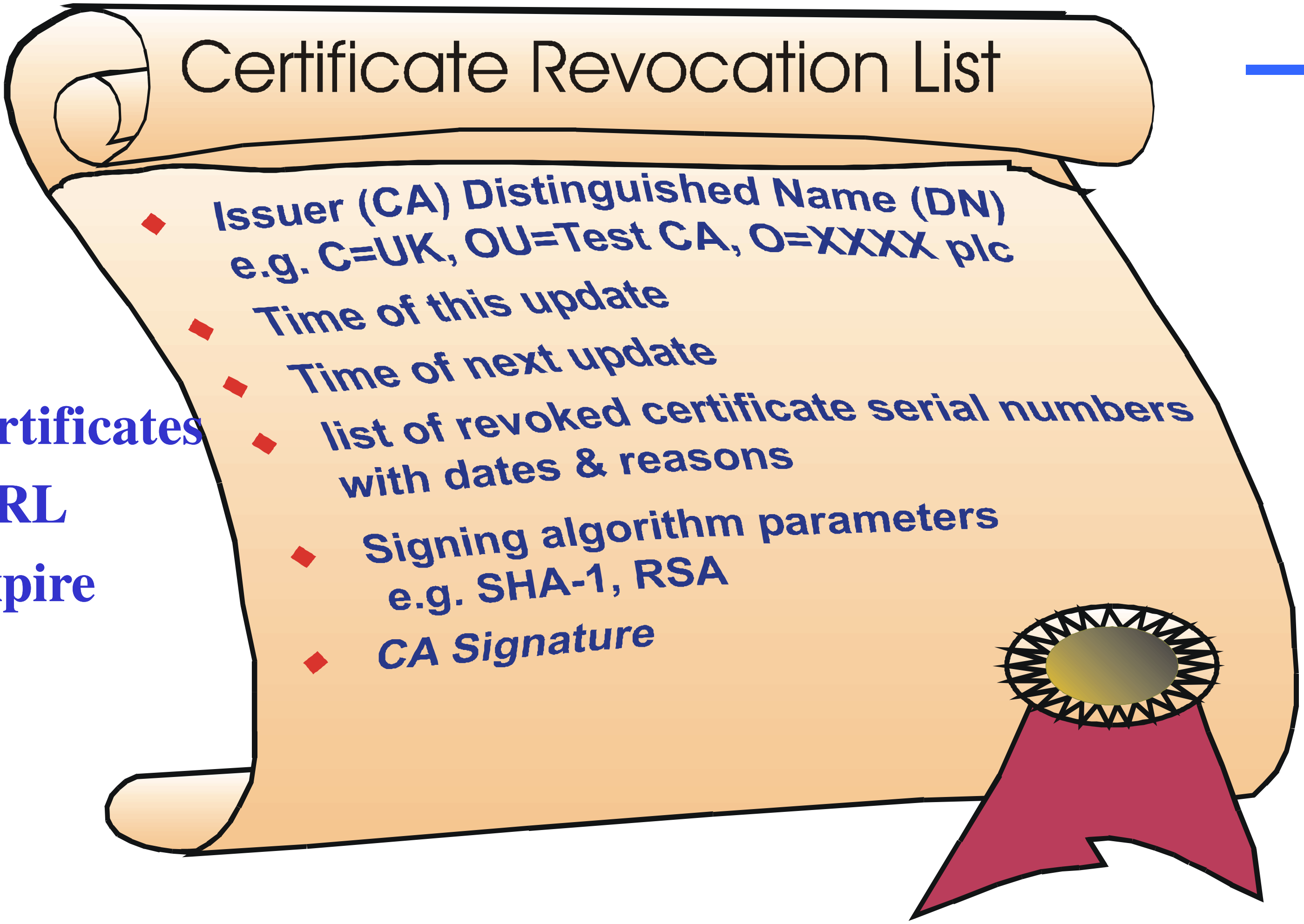
Provide Repository for:

- Digital Certificates
- Certificate Revocation Lists (CRLs)

Typically:

- Special Purposes Databases
- LDAP directories

Certificate Revocation List



Certificate Revocation List

- Issuer (CA) Distinguished Name (DN) e.g. C=UK, OU=Test CA, O=XXXX plc
- Time of this update
- Time of next update
- list of revoked certificate serial numbers with dates & reasons
- Signing algorithm parameters e.g. SHA-1, RSA
- *CA Signature*

Revoked Certificates
remain in CRL
until they expire

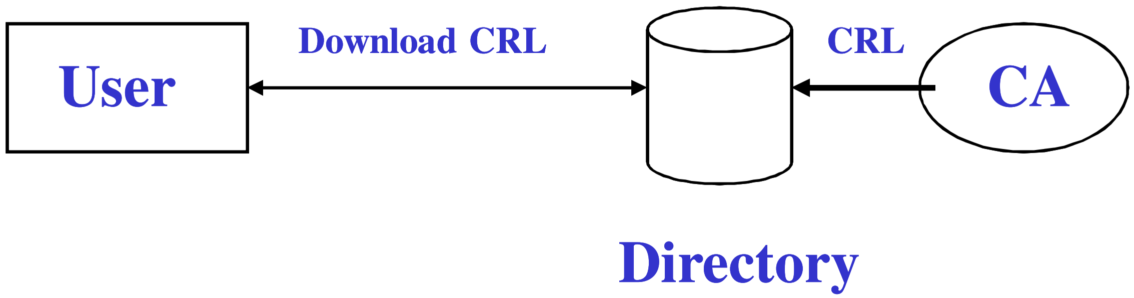
Certificate Revocation List (CRL)

- CRLs are published by CAs at well defined interval of time
- It is a responsibility of “Users” to “download” a CRL and verify if a certificate has been revoked
- User application must deal with the revocation processes

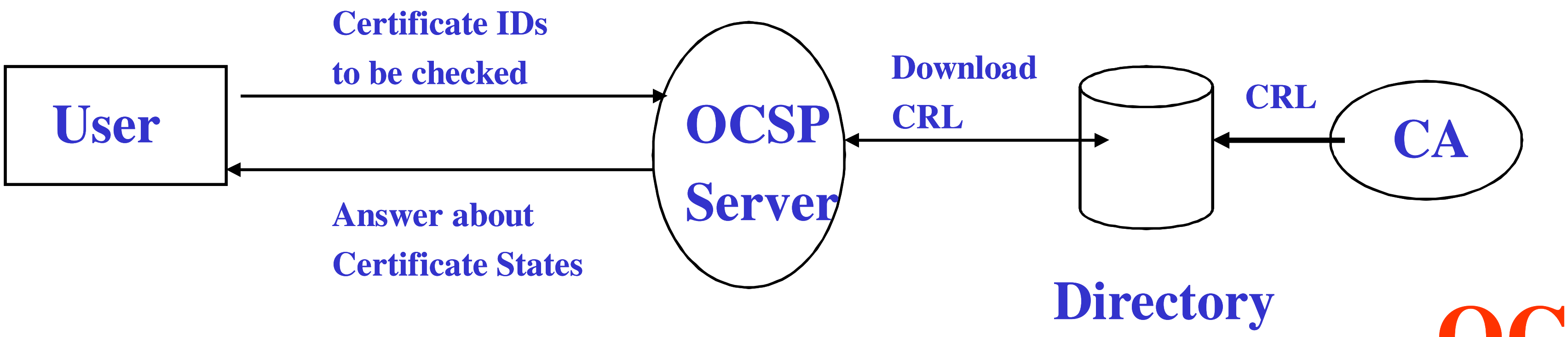
Online Certificate Status Protocol (OCSP)

- An alternative to CRLs
- IETF/PKIX standard for a real-time check if a certificate has been revoked/suspended
- Requires a high availability OCSP Server

CRL vs OCSP Server



CRL



OCSP

X509 PKI
PKI-enabled Applications

Functionality Required:

- Cryptographic functionality
- Secure storage of Personal Information
- Digital Certificate Handling
- Communication Facilities

X509 PKI
Trust and Legal Issues

X509 PKI
Trust and Legal Issues

- Why should I Trust a CA?

- How can I determine the liability of a CA?

X509 PKI
Approaches to Trust and Legal Aspects

- Why should I Trust a CA?

  ⇨ Certificate Hierarchies, Cross-Certification

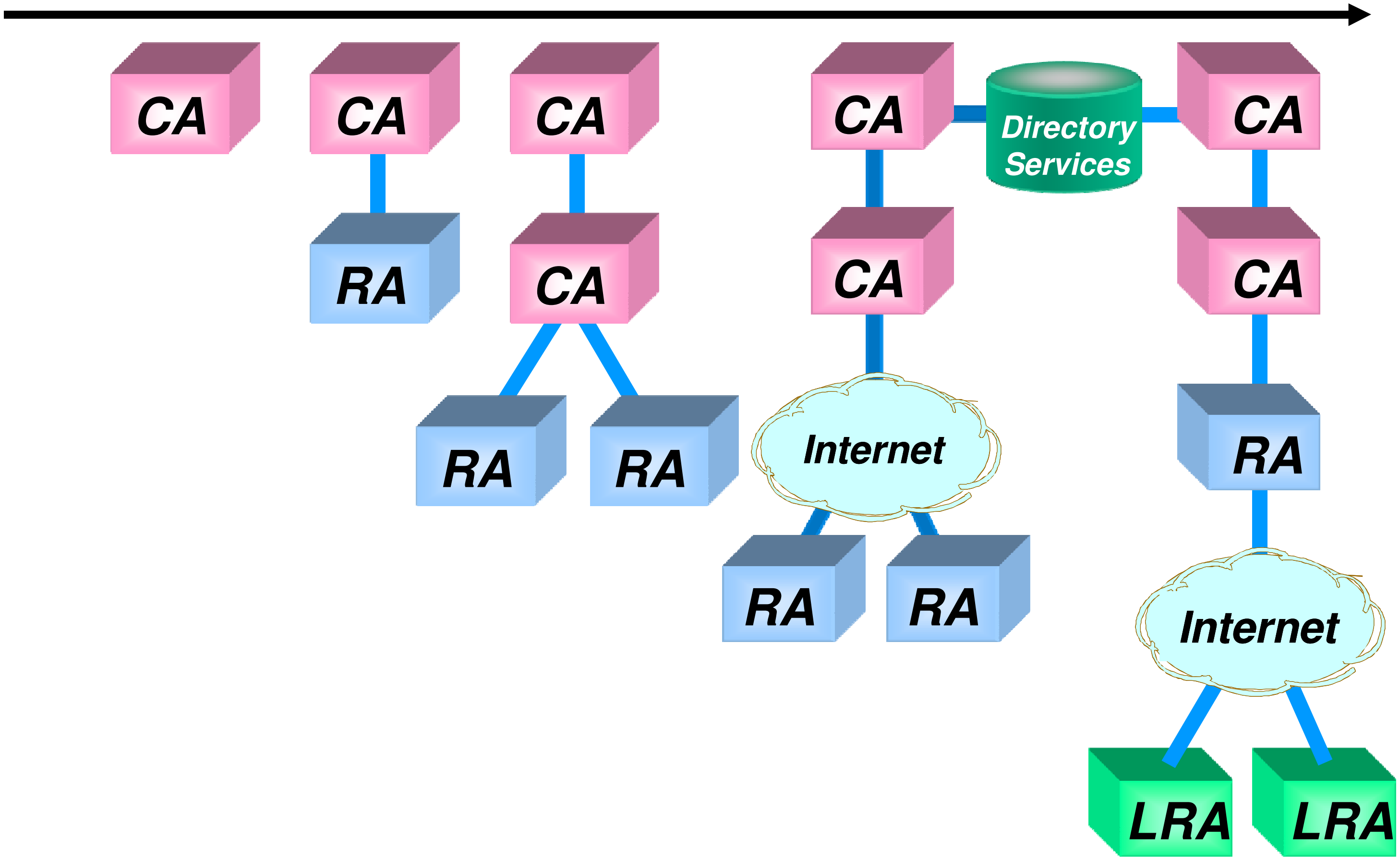
- How can I determine the liability of a CA?

  ⇨ Certificate Policies (CP) and Certificate Practical Statement (CPS)

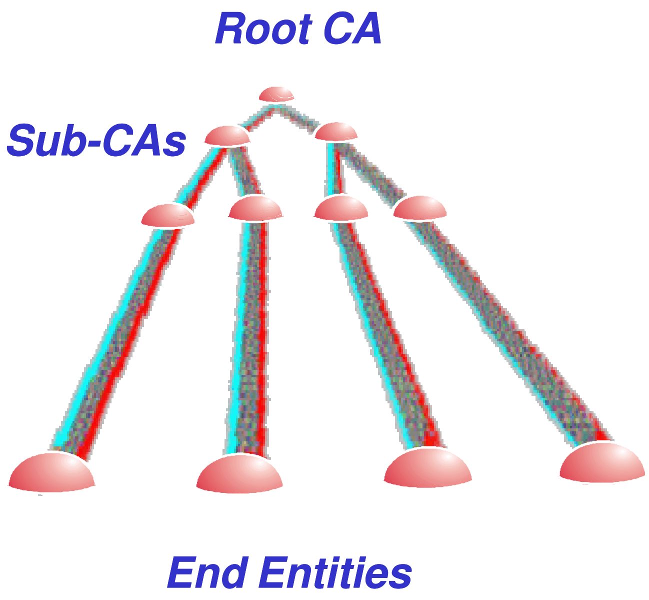
X509 PKI
Approach to Trust

Certificate Hierarchies
and
Cross-Certification

CA Technology Evolution



Simple Certificate Hierarchy

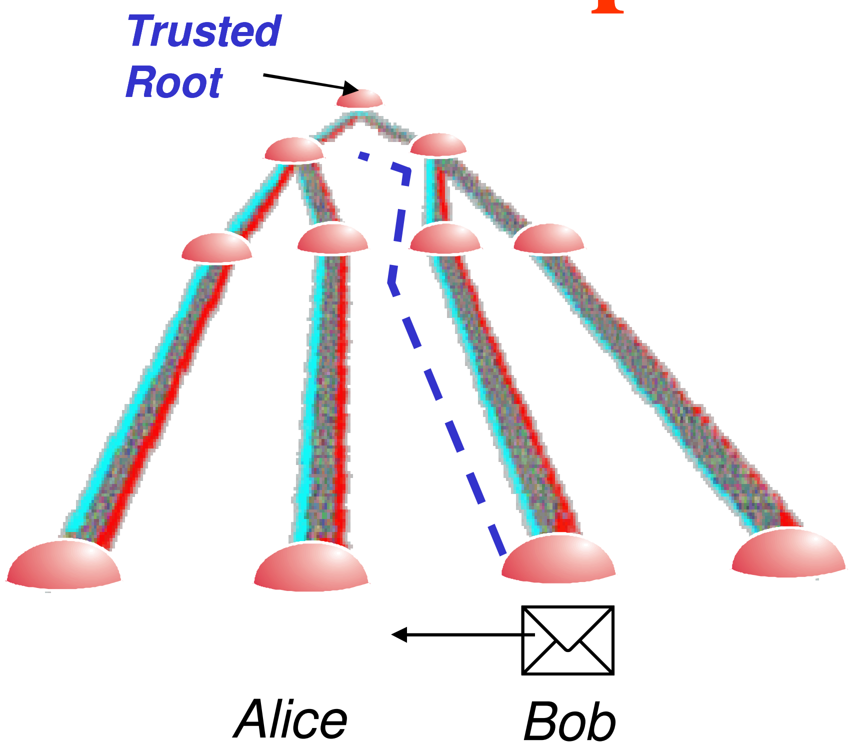


Each entity has its own certificate (and may have more than one). The root CA's certificate is self signed and each sub-CA is signed by its parent CA.

Each CA may also issue CRLs. In particular the lowest level CAs issue CRLs frequently.

End entities need to "find" a certificate path to a CA that they trust.

Simple Certificate Path



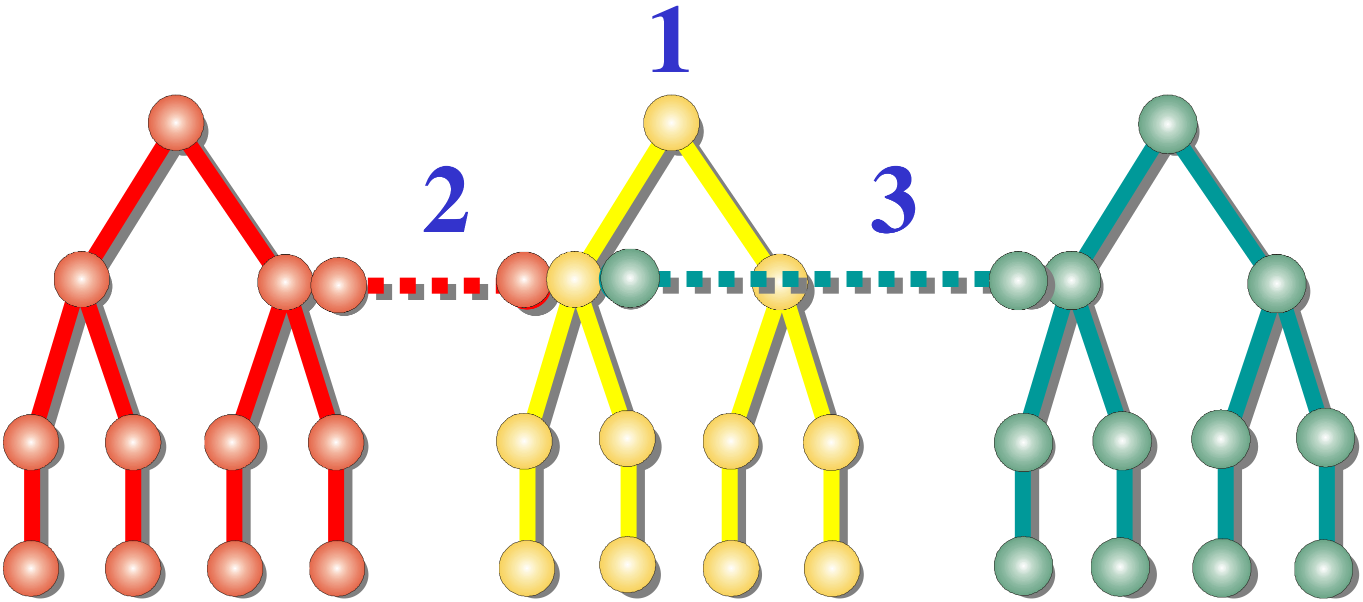
Alice trusts the root CA
Bob sends a message to Alice

Alice needs Bob’s certificate, the certificate of the CA that signed Bob’s certificate, and so on up to the root CA’s self signed certificate.

Alice also needs each CRL for each CA.

then Alice can verify that Bob’s certificate is valid and trusted and so verify the Bob’s signature.

Cross-Certification and Multiple Hierarchies

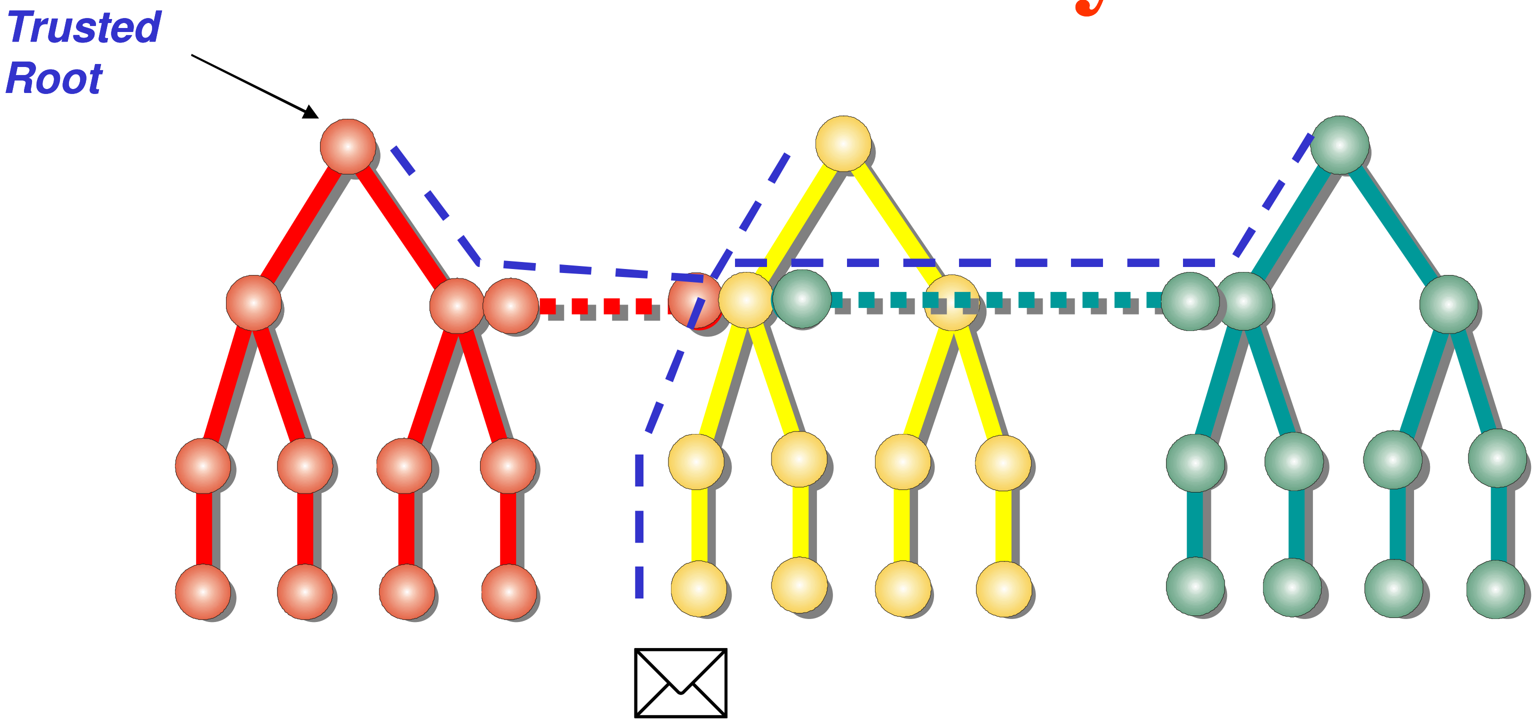


1. Multiple Roots
2. Simple cross-certificate
3. Complex cross-certificate

X509 PKI
Approach to Trust : Problems

Things are getting more and more complex if Hierarchies and Cross-Certifications are used

Cross-Certification and Path Discovery



X509 PKI
Approach to Legal Aspects

Certificate Policy

And

Certificate Practice Statement

Certificate Policy (CP)

- A document that sets out the rights, duties and obligations of each party in a Public Key Infrastructure
- The Certificate Policy (CP) is a document which usually has legal effect
- A CP is usually publicly exposed by CAs, for example on a Web Site (VeriSign, etc.)

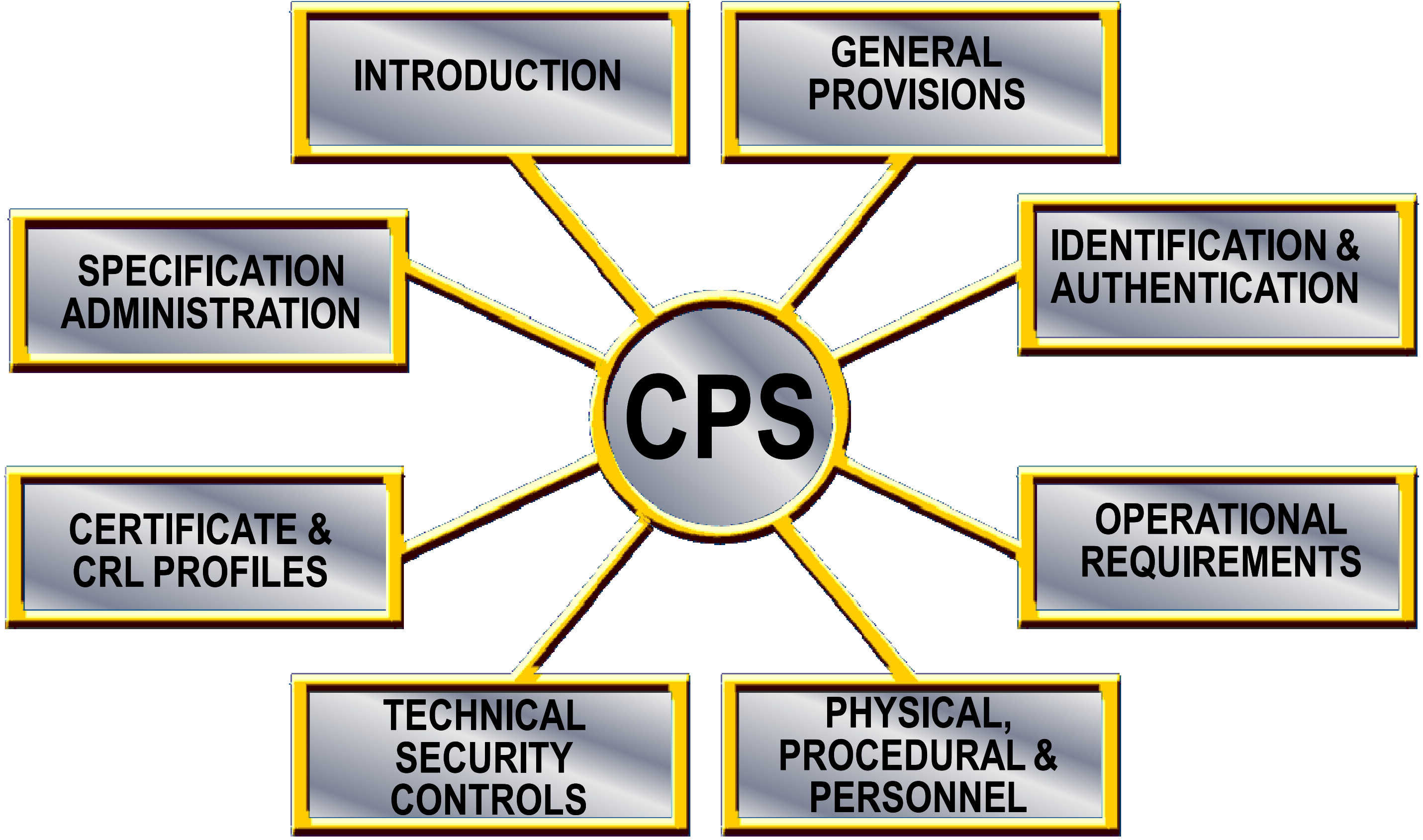
Policy Issues (CP)

- Liability Issues
- Repository Access Controls
- Confidentiality Requirements
- Registration Procedures
  - Uniqueness of Names
  - Authentication of Users/Organisations
- Certificate Acceptance
- Revocation (Online/CRL)
- Physical Security Controls

Certificate Practice Statement (CPS)

- A document that sets out what happens in practice to support the policy statements made in the CP in a PKI

Certificate Practice Statement (CPS)


INTRODUCTION
GENERAL PROVISIONS
SPECIFICATION ADMINISTRATION
IDENTIFICATION & AUTHENTICATION
CPS
CERTIFICATE & CRL PROFILES
OPERATIONAL REQUIREMENTS
TECHNICAL SECURITY CONTROLS
PHYSICAL, PROCEDURAL & PERSONNEL

IETF (PKIX) Standards

- X.509 Certificate and CRL Profiles
- PKI Management Protocols
- Certificate Request Formats
- CP/CPS Framework
- LDAP, OCSP, etc.

http://www.ietf.org/

Identity is Not Enough: Attribute Certificates

IETF (PKIX WG) is also defining standards for Attribute Certificates (ACs):

- **Visa Card vs. Passport (Identity)**
- **Attribute Certificates specify Attributes associated to an Identity**
- **Attribute Certificates don’t contain a Public key but a link to an Identity Certificate**