Who are the certification authorities?

- whom will you trust in your context?
- private CAs: good for in-house work, etc.
- telecomms providers (AT&T, MCI)
- IBM
- Thawte, Verisign, Globalsign — making a business of certification

Functions of a certification authority

- accept enrollments for certificates
- authenticate the (identity) information to be included in the certificate
- generate certificates
- distribute the certificates, either directly to the requesting entity or by including them in a directory (or both)
- revoke certificates when requested to do so
- maintain status information about certificates it has issued which are currently within their validity period
- may use *registration authority* — agency and verification functions; not certification and revocation themselves

How does a certification authority work? The approach

- will depend on the clientele
- inputs will differ, depending on what the certificate is to certify
- appropriate measures:
  - certifying an email address: ensure the party can receive mail there
  - certifying a merchant for high-value transactions: much more exhaustive checks

Example

A CA issuing certificates for use with SSL/TLS on web servers might request as part of its application process:

- a certificate signing request (CSR) produced on the web server to be secured which will include the company's name and location and the name of the web server that they wish to secure
- supporting information about the company, such as a registration number (if it is a registered company), DUNS number and registered address, plus documentation confirming this information
- names and contact details for relevant personnel
- the type of software being used