“Directory” Server Issues

X.509 in LDAP

- **Most apps can’t deal with multiple CAs and multiple certs**
  - **essential - people will have multiple identities**
- **Leaf node aliases are essential**
  - **email aliases - I have never gotten Netscape S-MINE mail to work because mail gateways rewrite the return addr**
  - **people use the same identity on different systems (wej@nas.nasa.gov and wejohnston@lbl.gov are equivalent from my point of view - I use a single identity cert.)**

Certificate Servers

- "Bridge" CAs are essential
  - top level CAs (i.e. most of today's CAs) have self-signed CA certs, which makes their cert. servers vulnerable - need a higher-level, "policy-neutral" CA whose only function is to sign and distribute CA certs.
- Secure DNS is important so that we can treat and authenticate "system" identity in the same way the we do human identity
- Hashed lookup in certificate servers (directory servers?) is important for performance (esp. when using "vanilla" Web servers, which we use for all non-CA (e.g. stakeholders) signing authorities
  - alias (human_readable, content_hash1, content_hash2)