CAS (alpha release)

- Current release thought for grid-ftp only
  - CAS issues restricted proxy certificates
- Missing features:
  - subgroups;
  - replicas;
  - confidentiality for the GSI delegation request;
  - absence of a CAS superuser (feature?);
  - user info missing (feature?);
  - documentation (in particular API's).

Considerations

- Do we need a CAS or a VO Membership server?
  - server should contain user membership and role info only;
  - access rights should be located with the resources and enforced by the entity which controls them.
- Users may need more than one CAS certificate simultaneously (even more so if we are going towards "pure" authentication certificates).
- User info should be present in CAS certificate:
  - required by local sites (e.g. to ban specific users);
  - required for automatic proxy renewal (?);
  - required for ACL of local resources;
  - for mapping to Unix UID/GID (*grid-mapfile*).
- **Without proof of the user's consent, CAS is a CA with its private key online and unencrypted!**
  - **user info into CAS cert is not sufficient.**

Possible Alternative?

1. The user submits his request to CAS.
2. CAS returns (**signed**):
   User Info,
   CAS Id,
   User Id,
   Timestamp,
   Validity Period.
3. The user repeats above steps for each CAS.
4. The user generates the proxy with CAS info into extensions.

- Advantages:
  - compatibility with the current system;
  - ease of integration of info from more than one CAS.
- ACL checking?

TestBed 2 (9/02)

- CAS? No, thank you!
  - looking at CAS code
- VO LDAP system enhancements:
  - the user can choose the VO
    - this opens the way to other possibilities (e.g. roles);
  - *grid-mapfiles* are no longer published (WP1);
  - access to LDAP directories restricted to selected nodes/users (e.g. only bearers of “valid” certificates).

DataTAG / iVDGL

- Authentication: ok
  - Mutual Trust Treaty has been signed:
    - DOE CA certs accepted by EDG testbeds
      - CRL's issues (?);
    - EDG CA's certs accepted by PPDG experiment testbeds (except BaBar?).
- Authorization:
  - CAS unsuitable at the moment;
  - DataTAG proposal:
    - VO LDAP Directories, mkgridmap, VO management tools by C. Steenberg.
  - iVDGL:
    - still discussing.
- Next meeting: 23-24 May.