Authorization Working Group Status

Roberto Cecchini
Authorization Working Group

WP6 Meeting
11 December 2001, CERN

M9 Authorization Structure

- Each CA manages an LDAP Directory with the issued certificates.
- Each VO manages an LDAP Directory (o=xyz,dc=eu-datagrid,dc=org):
  - members (**ou=People**);
  - groups (e.g. **ou=Testbed1**):
    - each user **must** belong to at least one group;
  - each user entry contains:
    - the URI of the certificate on the CA LDAP server;
    - the Subject of the user's certificate (to speed up *grid-mapfile* generation).
- **grid-mapfile**s are generated from the VO Directories:
  - looking for the members of the groups;
  - according to users' attributes (the Certificate Subject, for the moment);
  - according to the existence of an entry with the same Certificate Subject in an "Authorization Directory";
  - with different local names, according to local requirements (e.g. McNab patch).

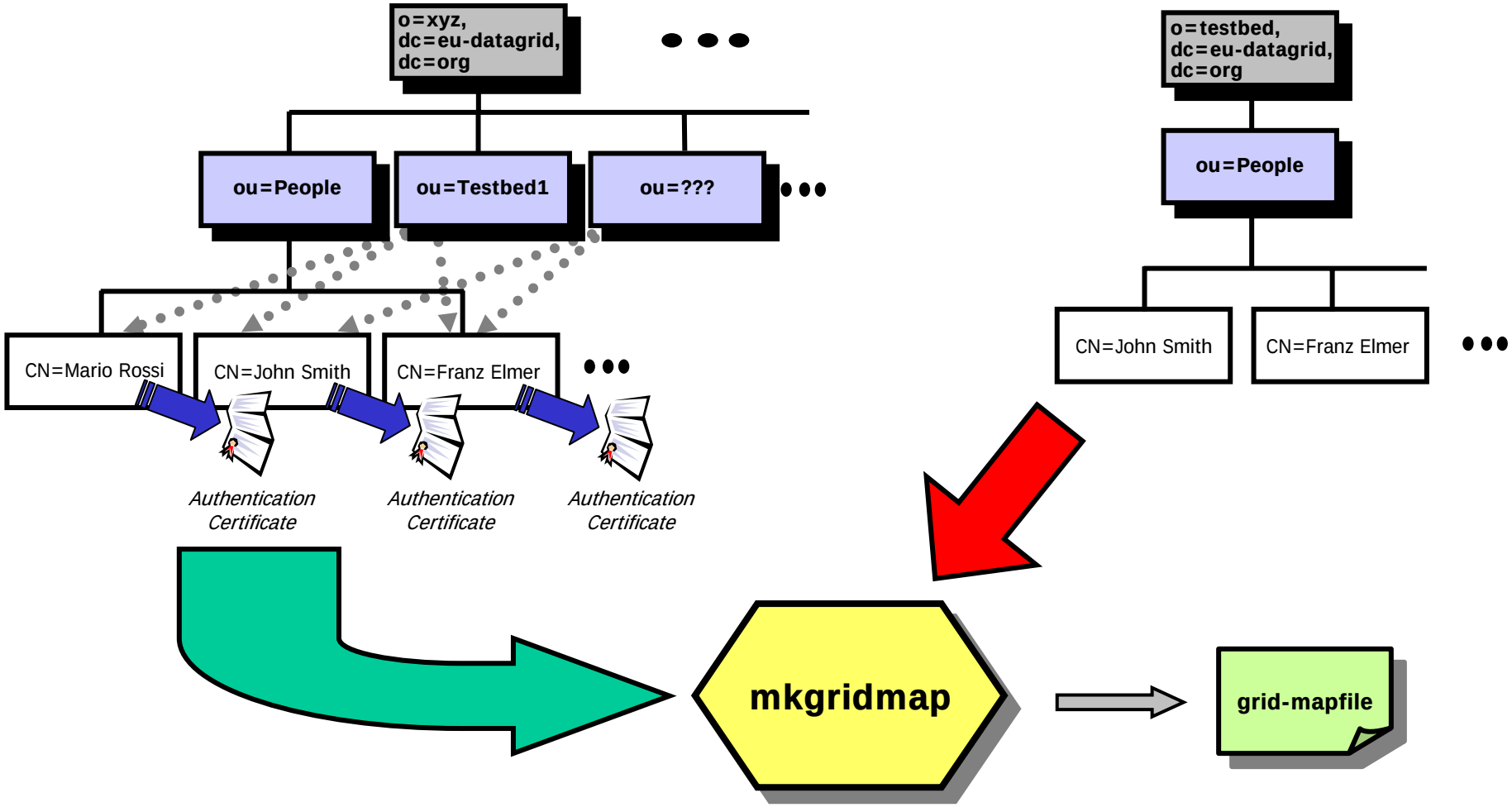
Authorization Tools

- Available from the Authorization WG CVS server:
  - CA Directory management: http://cvs.infn.it/cgi-bin/cvsweb.cgi/Auth/LDAP-CA/
  - VO Directory management: http://cvs.infn.it/cgi-bin/cvsweb.cgi/Auth/VO/
  - *grid-mapfile* generation: http://cvs.infn.it/cgi-bin/cvsweb.cgi/Auth/edg-mkgridmap/
- Developers' mailing list: sec-grid@infn.it
- Authorization WG mailing list: dg-eur-auth@services.cnrs.fr

CA Directory Management

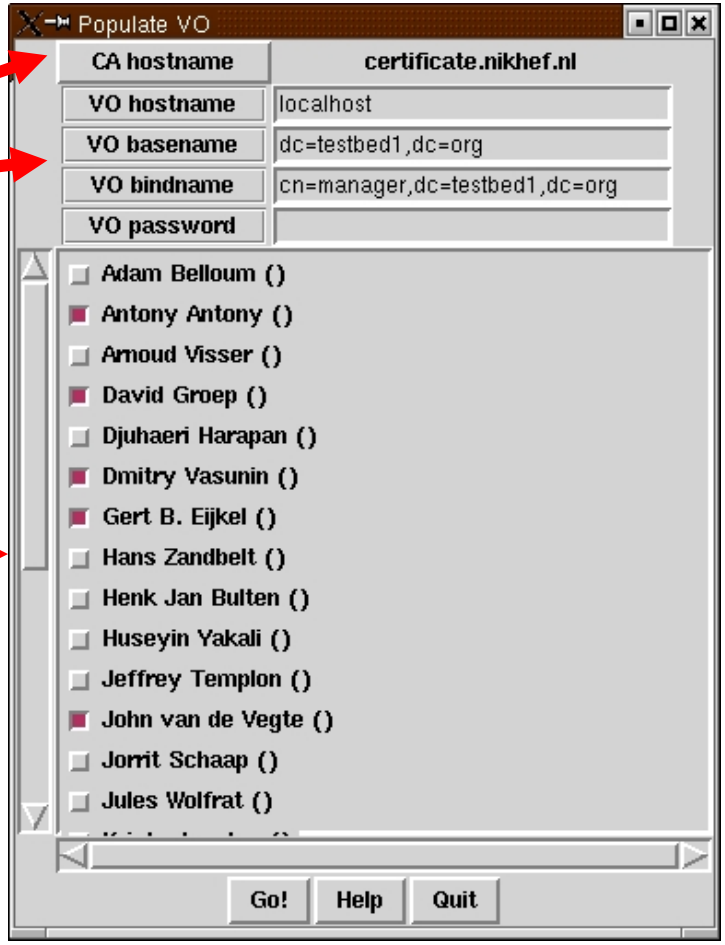
- Tools:
  - **pem2ldif.pl**: initial loading;
  - **crtUpd.pl**: insertion of certificates;
  - **crlUpd.pl**: insertion of CRLs;
  - **delUser.pl**: removal of users.
- Available DataGrid CA Directories (9/12/01):
  - CESNET: **ldap://tady.ten.cz**
  - INFN: **ldap://security.fi.infn.it**
  - NICKEF: **ldap://certificate.nikhef.nl**

grid-mapfile generation



VO Directory Management 1/2

- Insertion of users:
  - from CAs LDAP servers: **vop.pl**
    1. VO manager specifies CA and VO Directories
    2. users' entries are read from the specified CA Directory;
    3. validity of users' certificates is checked;
    4. VO manager selects the users to be inserted.
  - from certificate files: **cert2ldif.pl**
    - reads user certificate;
    - produces an LDIF file for the insertion of the user.
- Consistency check between VO and CA Directories: **chkusers.pl**



VO Directory Management 2/2

- Creation of groups: **creategroup.pl** (same interface of **group.pl**)
- Population of groups: **group.pl**
  1. VO Manager indicates the group;
  2. the list of all the users and of those already in the group are shown;
  3. VO manager selects the users to be inserted in the group.

grid-mapfile generation: **mkgridmap**

- perl script, to be run at appropriate intervals by the local site manager.
- Produces a *grid-mapfile* from the entries in the VO Directories, according to the directives specified in a configuration file: **mkgridmap.conf**.
- Mapping between Certificate Subjects and local user names is customizable by the local site managers.

mkgridmap.conf directives

- **`group`** *<VO group URI> [<lcluser>]*
  selects the VO Directories. *<lcluser>,* if specified, is the local username to be inserted in the *grid-mapfile* for the users belonging to the group.
- **`allow`** (**`deny`**) *<pattern>*
  users allowed (banned) in the *grid-mapfile*:
  - *<pattern>* may contain wildcards;
  - the test is done on the user certificate subject;
  - parsing stops at the first match;
  - if there is at least an **`allow`**, there is an implicit **`deny *`** at the end.
- **`auth`** *<Auth Server URI>*
  the user is inserted only if there is an entry on the Auth Server with the same Certificate Subject.
- **`default_lcluser`** *<username>*
  the local username in the grid-mapfile (e.g. "**`.`**" for McNab patch)
  If **`AUTO`**, the local username is generated by an external program (**subject2user**).
- **`gmf_local`** *<filename>*
  <filename> is a local *grid-mapfile* to be inserted.

Sample *mkgridmap.conf*

```
#### GROUP: group URI [lcluser]
group ldap://grid-vo.nikhef.nl/ou=testbed1,o=alice,dc=eu-datagrid,dc=org
#group ldap://grid-vo.nikhef.nl/ou=testbed1,o=atlas,dc=eu-datagrid,dc=org
#group ldap://grid-vo.nikhef.nl/ou=testbed1,o=cms,dc=eu-datagrid,dc=org
#group ldap://grid-vo.nikhef.nl/ou=testbed1,o=lhcb,dc=eu-datagrid,dc=org
#group ldap://grid-vo.nikhef.nl/ou=testbed1,o=earthob,dc=eu-datagrid,dc=org
#group ldap://grid-vo.nikhef.nl/ou= testbed1,o=biology,dc=eu-datagrid,dc=org
#group ldap://marianne.in2p3.fr/ou=wp6,o=testbed,dc=eu-datagrid,dc=org
#group ldap://grid-vo.cnaf.infn.it/ou=testbed1,o=infn,c=it

#### Optional - DEFAULT LOCAL USER: default_lcluser lcluser
default_lcluser AUTO

#### Optional - AUTHORIZED VO: auth URI
auth ldap://marianne2.in2p3.fr/ou=people,o=testbed,dc=eu-datagrid,dc=org

#### Optional - ACL: deny|allow pattern_to_match
allow *INFN*

#### Optional - GRID-MAPFILE-LOCAL
#gmf_local /opt/edg/etc/grid-mapfile-local
```

grid-mapfile customization: **subject2user**

- External program called by **mkgridmap** when `default_lcluser` or `lcluser` is `AUTO`.
- It allows local sites to customize the output of **mkgridmap**:
  - it is called with the user certificate subject as argument.
  - it must write to the standard output the local username associated with the user certificate subject.
- The version supplied maps *cn=Name Surname* to *nsurname* (e.g. *cn=Pinco Pallino* to *ppallino*).

Future Plans

- Better VO Directory management;
- Support for replicas of VO Directories;
- Support for users' attributes in the VO Directories;
- Authorization Certificates;
- CAS (or VOAS).