eGee

Enabling Grids for E-sciencE

Authorization in the Match-making

Salvatore Monforte - INFN
Francesco Giacomini - INFN

JRA1 All Hands meeting
CERN, 24-26 October 2007

www.eu-egee.org

www.glite.org

Information Society
and Media

Enabling Grids for E-sciencE

- **The WMS keeps CE information in memory in ClassAd format (ISM)**
  - according to the GLUE schema
  - the information is retrieved by querying the BDII for the following object classes
    - gluece, gluecesebind, gluecluster, gluesubcluster, gluevoview
    - an attribute published in the subschema without the SINGLE-VALUE tag is converted to a list
  - other mechanism are supported (CEMon, RGMA)
- **For each VOView the CE ClassAd and the VOView ClassAd are merged**
  - CE attributes values are overridden by VOView ones
  - The result is inserted in the ISM
- **ISM contains a lot of duplicated information**

Enabling Grids for E-sciencE

- **The CE/VOView ClassAd contains authorization information as a list of ACBRs**

- **While populating the ISM, the space of authorization rules the CE provides should be preserved:**

  – If the set of CE ACBRs is not entirely covered by the union of the VOViews ACBRs, also the CE ClassAd is inserted in the ISM

    ▪ CE ACBRs include only those not covered by the VOViews

- **Within the same CE, the VOView ACBRs may overlap**

- **Match-making means evaluating the requirements expression contained in a ClassAd against another ClassAd**
  - The MM is *symmetric* if the evaluation goes in both directions
- **The MM in the WMS is symmetric**
  - The requirements expression in the JDL is specified by the user
  - The requirements expression in the CE/VOView Ad is as follows

```
Requirements = AuthorizationCheck && ... ;
AuthorizationCheck = (
  member(other.CertificateSubject, GlueCEAccessControlBaseRule)
  || member(strcat("VO:",other.VirtualOrganisation),GlueCEAccessControlBaseRule)
  || FQANmember(strcat("VOMS:",other.VOMS_FQAN), GlueCEAccessControlBaseRule)
) &&  ! FQANmember(strcat("DENY:",other.VOMS_FQAN), GlueCEAccessControlBaseRule);
```

  - FQANmember returns true iff the FQAN is *member* of ACBR list
  - **Within the same CE multiple VOViews can match!**