Security Group

TODO

E-mail: Akos.Frohner@cern.ch

1. CAS/VOMS strategy

- grid-proxy-init –-vo Alice –role admin
  client application, PAM module?!

- Membership administration – admin interface

- VOMS: WP1/WP2/CAS implementation

- Encoding of the information: XML vs. ASN.1
  basically it is an attribute certificate

- Format of attributes: group/role/VO
  /O=Grid/O=Alice/Role=RM-admin

- Where to put the extra info: inside or beside the proxy cert?

- Libraries for the services (C/Java/?)

2. ACL syntax and semantics

- ◆ AND?: yes (multi-VO requirement from WP10)
  but have only allow xor deny

- ◆ XML, C, Java and database representation of ACLs

- ◆ ACL manipulation library API -> Andrew's GACL for C is the current nominee, but we probably need it in Java and Perl as well.

- ◆ Transport format: probably XML (write grammar!)

3. SE/RM interaction

The interaction is as described earlier.

◆ Transport of ACL and metadata: needs common format

◆ Delegation: file transfers between SE nodes – they must act on behalf of the initiator of the transfer

◆ (Checksum on files – signatures?)

4. SE/MSS interaction

Mixed access to files (local and grid)

- SE authz to replace and/or emulate existing authorization

- Conflict of ownership

- Semantical differences in access rights

5. WP10 confidentality issues

Protecting the owner's identity

- In access control lists (protected storage and evaluation)

- Log/audit records (different name for audit)

- Key to read data (encrypted for the session)

See slides from the earlier meeting.

- Requirements along contracts – „implement" them as policies!

6. Accounting user/group/VO level?

Granularity of accounting and/or quotas

◆ User level: OK, based on the identity
„accounted user" field in file metadata

◆ VO level: OK, in a replica manager
files are mixed in an SE – „accounted VO" field?

◆ Group level: ?
Group may change over time – „accounted group" field?

Extra fields

◆ Do we allow modifications?

◆ Who can modify them (ACL)?

7. Mutual authorization - client

Service can also obtain authorization information from a VOMS.

User may configure, which „group of service" is acceptable.

◆ Do we need this?

◆ Semantics of client applications

8. CE/LCAS interaction with VOMS

VOMS provides group/role info

- Mapping identity to local credentials - OK

- Mapping group information to local groups?

- Enforcement of group level access rights in a CE?

9. Multiple vs. single VO

- See WP10 requirements -> multiple VOs

10. VO LDAP servers

VOMS vs. VO-LDAP servers

◆ VO membership information (VOMS, LDAP)

◆ User information (LDAP)

◆ Which is the primary data source?

◆ Updating of user information – site authorities

◆ Tracking of incidents -> plan

11. Auditing

Tracking changes for incidents and debugging

◆ Pool of assigned user accounts
(who was using N userid at T time?)

◆ Membership information
(was X member of group Y at T time?)

◆ Software versions
(what version of software W was running at T time?)

◆ Authorization decisions
(why user X was allowed to access R resource at T time?)

12. GGF presentation

◆ What shall be in the presentation?