Meeting Object: **WP7 Security Co-ordination Group**

Author(s): **Linda Cornwall**
Partner:

Meeting Date: **17th May 2002**
Meeting Place: **CERN**

Attendees:

David Kelsey	SCG	RAL	Chairman
Linda Cornwall	SCG/WP3	RAL	Secretary
Metery Rene	WP6	CS-SI	
Franck Bonnassieux	WP7	CNRS	
Roberto Cecchini	WP6	INFN	
Alberto Gianoli	WP6	INFN	
Gavin Lowe	SCG	Oxford	
Philippa Broadfoot	SCG	Oxford	
Akos Frohner	SCG	CERN	
Jens Jensen	RAL		
Anders Waananen	WP6	NBI	
Andrew McNab	WP6	Manchester	
David Groep	WP4	NIKHEF	
Daniel Kouril	WP1	CESNET	
Markus Schulz	CERN		
Ian Neilson	CERN		
Emanuele Leonardi	CERN		
Rafael Marco de Lucas	IFCA		

Distribution **DATAGRID-WP7-SECURITY-L@IN2P3.FR**

1. ACTIONS

N°	Initials	Partner	Subject	Deadline
1.				
2.				
3.				
4.				
5.				

6.				
7.				
8.			Click here to insert a new line below	

2. INTRODUCTIONS, AIMS OF MEETING AND AGREE AGENDA – DAVID KELSEY

The agenda was agreed.

3. SECURITY STATUS/PLANS IN EDG MIDDLEWARE

3.1. WP1 – DANIEL KOURIL

No Slides.

All components are based on X509 certificates, using the Globus GSI API.

For authorization, all components use grid mapfiles or something similar.

Proxy renewal is used for long jobs, to obtain a renewed proxy an old proxy is needed.

Proxies are stored in the proxy renewal server have a lifetime of 2 weeks and never leave the proxy server.

Documentation has been written some time ago.

3.2. WP2 – AKOS FROHNER (FOR MIKA SILANDER)

See Slides attached to agenda.

Authorization is based on the User Certificate.

The ID from the Certificate is mapped onto a role, and authorization is based on the role.

Note that after Spitfire has started up it reads the CRL, but doesn't check again later.

3.3. WP3 – LINDA CORNWALL

See Slides attached to agenda

3.4. WP4 – DAVID GROEP

See Slides attached to agenda

3.5. WP5 – JENS JENSEN

No slides

There is an issue with medical images stored in encrypted form on untrusted servers.

These are medical images stored for research purposes, with patient details removed.

People who need access will need the key to de-crypt them. If they are de-crypted on the storage element, this would be particularly insecure. It makes no sense to de-crypt on an un-trusted machine.

For replicated files ownership is transferred to the replica manager – so only certain replica managers can access the files. But the user needs access to files, thus access control needs to not be based on conventional unix file ownership.

Also WP9 wants to store a large number of small files, which is difficult to do in mass storage.

Quota management is complex, it is TBD whether this should be global or local.

3.6. WP7 – FRANCK BONNASSIEUX

No Slides

Firewalls are managed by local admin at each site.

We should consider auditing on security holes – e.g. spend 1 week at the end of the year.

Security for authorization on Network services is being considered. It might be in TB2, but more likely it will be postponed to TB3. It is not clear whether there is a need for this at all within DataGrid.

4. WP6 AUTHORIZATION GROUP AND DATATAG WP4 – ROBERTO CECCHINI

See slides

The following was noted:-

PERMIS is not considered suitable

If CAS is used, the CAS server is a single point failure.

If the CAS server is hacked it would be possible to issue usable certificates – so there needs to be some way the user proves they are aware of each certificate.

It has been suggested that CAS is used for the community, but Akenti is used for resources.

Roberto does not think CAS (at least the version he looked at prior to the meeting) is suitable for TB2.

5. SECURITY DESIGN – AKOS FROHNER

See slides and document attached to agenda

Note that this model will return a certificate with ALL group memberships within a VO, and the roles requested.

6. WP6 SECURITY ISSUES

Andrew McNab made a presentation on Slashgrid, File access and ACL's– See Slides attached to the agenda.

Andy McNab plans to have a version of Slashgrid for the DataGrid Testbed Version 1.3

There was a discussion on what basis we should deny access.

It should be possible to deny access to individual users.

We also need the ability to deny access if a combination of groups and roles are in conflict.

We should NOT deny access because a user is a member of another VO, we should not be able to obtain details of what other VOs a user is a member of. I.e. we should not contradict CNF-16. Access should only be based on Membership of VOs presented. Decision for the fist version of the software is that denial takes precedence. See if this works, and if not we should then have a better idea what we need.

Akos presented suggestions on the format of the ACL

WP4 are happy with this, they say it fits well with LCAS.

Roberto is happy with the fine grained access being handled as suggested.

WP2 are also happy.

7. AUTHORIZATION – BRAINSTORMING AND DISCUSSION

7.1. CONCLUSIONS ON AUTHORIZATION

There seems to be agreement that CAS is not suitable for DataGrid, and we should go for an Authorization server that confirms

- VO membership
- Group membership (if we are implementing groups)
- Roles.

Fine grained authorization, such as access to individual files and directories, should go with the resource. E.g. a storage element should store an ACL with the files.

However, because of e.g. replication, this cannot simply be based on Unix file ownership.

We are not sure whether we should go for User signing Authorization Server's certificate, or whether the Authorization server should sign the user's certificate.

Possibly user enters grid-proxy-init to generate the certificate, then the user sends this to the Authorization server for signature. (Roberto)

If this was the case grid-proxy-init could be replaced by a procedure that allows the user to specify exactly what rights they want to delegate, what VOs and roles they want to claim, and then the Authorization server could sign that they have VO membership and the roles they are claiming.

This is still TBD.

We will also need to do something about quotas, this will probably be discussed at the next meeting.

For Testbed-2 will probably expand the functionality of the LDAP VO server to allow for groups and roles.

Also, access to the LDAP server should be restricted to certain nodes with valid certificates.

7.2. MASS STORAGE AND FILE OWNERSHIP.

SE manages files in mass storage. The files are owned by a single user. The mass Storage facility then gives access to appropriate users

This is O.K. if all access goes through EDG.

However, some people will want to use files stored using EDG software when they are not using the grid. Thus, they will need to be able to access the correct files when they are logged on using conventional mechanisms.

Therefore, there appears to be a compatibility problem between EDG's slashgrid and conventional file access

IOP-01 NOT SATISFIED.

The SCG encourages WP5 to talk to experiments to sort this out.

We will probably need access control also via conventional unix ID as well Grid DN/role/group – the ACL and the Authorization method will probably need to cope with conventional user id as well as grid DN/role/group for the storage element and replicated data.

8. FUTURE PLANS FOR SCG AND OTHER MATTERS

Akos has presented his design for Authorization to the ATF. The ATF is now meeting for 2 days at a time.

We would appreciate it if Akos circulated a brief report on Security related matters discussed at the ATF to the SCG. Or if it is already documented in the ATF minutes, an E-mail pointing to the appropriate minutes when Security has been discussed.

D7.6 will not just be about authorization. It will also be about other aspects of security defined as within our scope in D7.5. Other people will need to work on the design in these areas.

D7.6 will also contain a report on Testbed-2, and possibly an update of the requirements.

Should there be an ACL for EDMS? At present D7.6 is world readable – as it states it is in work this is not considered to be a problem so no plans to change.

We will discuss D7.6 further in the next Security meeting.

WP1 are doing some work on accounting. We don't know whether this is scheduled for TB2 or TB3.

Accounting may be based on group quotas. (Group in the Grid context, not unix group.)

We should look at this at the next meeting.

We should present our plans for authorization at the GGF. So far within the GGF there has been little discussion on authorization. We are possibly ahead on this, so we should start a group at the GGF, possibly have a BOF and start a new WG.

We could present what we don't like about CAS

There is a very 0.0.1 web page below the WP7 web page. We plan to improve on this. Possibly this should be visible from the DataGrid home page rather than just below WP7.

9. CONCLUSIONS, DATE OF NEXT MEETING AND AOB

We will add everyone who attended the meeting who is not already on the SCG mailing list to the list. (I.e. we will ensure everyone who put their name and E-mail address on the piece of paper that was handed round will be on the SCG mailing list)

Next meeting Tuesday 2rd July at CERN (TBC)