Meeting Object: **WP7 Security Co-ordination Group (SCG)**

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

Meeting Date: **2nd July 2002**
Meeting Place: **CERN**

Attendees:	**David Kelsey**	**SCG RAL Chairman**
	Linda Cornwall	**SCG/WP3 RAL Secretary**
	Andrew McNab	**WP6 Manchester**
	Franck Bonnasseiux	**SCG/WP7 CNRS**
	Olle Mulmo	**KTH**
	Gavin Lowe	**SCG Oxford**
	Lee Momtahan	**Oxford**
	David Groep	**WP4 NIKHEF**
	Mika Silander	**WP2 HIP**
	Akos Frohner	**WP6 CERN**
	Karoly Loreutey	**ELTE**
	Alberto Gianoli	**WP6 INFN**
	Denise Heagerty	**CERN**

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

1. ACTIONS

N°	Initials	Partner	Subject	Deadline
1.	AF		Whenever Security is discussed at the ATF, provide either a brief summary/report to the SCG list or provide a pointer to the minutes or other information.	N/A
2.	ALL		(Suggested by Secretary) If you become aware of a discussion, either within your own workpackage or within a list you are a member of which you think is of interest to the SCG – forward it to the SCG list	N/A
3.	JJ		Find what is required by WP8, WP9, WP10 for file access via conventional login when files have been generated via Grid use. And vice versa. In order to satisfy IOP-01.	05/09/02
4.	DK		Raise issue of quotas to the PTB.	03/07/02
5.	DK		Raise issue of service certificates at the CA meetings	

N°	Initials	Partner	Subject	Deadline
6.	DK		E-mail GGF to request an Authorization BOF session at the next GGF, with view to starting a GGF Authorization WG	10/07/02
7.	FB		Find out exactly what is being proposed by CNRS re-checking security implementation.	
8.				

2. TODO LIST

TODO	Description	Date	Notes
1	CAS/VOMS Strategy: What shall we use? How should it work?	02/07/02	See minutes
2	ACL syntax and semantics	02/07/02	See minutes
3	SE/RM interaction	02/07/02	See minutes
4	SE/MSS interaction	02/07/02	See minutes
5	WP10 confidentiality issues		
6	Accounting user/group/VO level?	02/07/02	See minutes
7	Mutual Authorization: what does it mean for a client?	02/07/02	See minutes
8	CE/LCAS interaction with VOMS	02/07/02	See minutes
9	Multiple vs single VO		
10	VO LDAP server, (Grid security Response Team?)	02/07/02	See minutes
11	Auditing: Tracking changes of group membership	02/07/02	See minutes
12	Presentation(s) at GGF on Authorization	02/07/02	See minutes DPK to E-mail
		12/07/02	Will have to wait until next GGF as all BOF sessions full
13	How to handle service certificates within DataGrid.	02/07/02	See minutes Ask for Service Certs from CA's for now.

3. INTRODUCTIONS AND AGREE AGENDA

The agenda was agreed.

4. MINUTES OF LAST MEETING AND MATTERS ARISING

The last meeting took place on 17th May 2002.

Note that no action list was placed in the minutes, but there were some implicit actions, now included in the above action list.

Action on WP7 to consider how to look for security holes. This matter is discussed later in the meeting.

Consider how we look at quotas.

Mass storage and file ownership – SCG encourages WP5 to talk to experiments to sort this out. Probably going to have to compromise, for RM files will be owned by the RM. Exactly what is needed and how file ownership is managed, such that requirement IOP-01 is satisfied is an on-going action.

We believe WP1 is working on Accounting, but we don’t know whether this is for TB2 or TB3.

5. REVIEW OF THE ‘TO-DO’ LIST

Also see Akos Slides attached to the agenda.

The TODO list is tabulated above. The idea is this will go onto the SCG web page, the notes could include links to relevant meeting minutes or any other relevant as well as the odd sentence describing an outcome.

5.1. CAS/VOMS STRATEGY

We are planning to implement something ourselves, i.e. modify grid-proxy-init to give VO membership and Roles. Implementation is already taking place. (see slide) However, the implementers haven’t really thought about how to command more than 1 VO. And haven’t decided whether they will need more than 1 proxy certificate or 1 certificate covering the 2 VO’s.

When a user requests confirmation of membership of a VO, they need to authenticate them self, this will include generating a proxy to authenticate themselves with the VO.

We need to consider membership administration, and how this will be done.

We were promised the new CAS at the end of May, it always seems to be 1 month away. Laura Pearlman is keen to talk to people at GGF.

What extension(s) should we have to the X509 certificates to provide information on role and VO? Can we agree on the format of the attributes? It would be nice to agree something at GGF. There doesn’t seem to be any 1 standard, e.g whether we use o or vo for a virtual organisation. Information is based on DNS – for uniqueness. One idea is that they should be the same as ACL’s. Within a VO, the VO should be able to name and define roles as they choose.

We think we should carry out the minimum possible changes to Globus – if we add extra attributes then ask Globus to ignore them.

Andrew McNab has implemented a PAM module – which he thinks can be used in the Testbed.

(PAM = Pluggable Authentication Modules)

5.2. ACL SYNTAX AND SEMANTICS

We need to define the format of ACL’s.

We will also need an ACL manipulation library, including API’s.

5.3. SE/RM INTERACTION

Truck FTP was mentioned? Idea of this being equivalent to loading all data on an SE onto tapes and moving it to another site in a truck.

We need some sort of checksum of files to prove they are the same when they are moved to another site.

Someone asked, doesn't SSL do that anyway? Answer yes, but SSL is not suitable for transferring terabytes – something simpler is needed.

5.4. SE/MMS INTERACTION

There is the problem of conflict of file ownership when we consider mixed access to files between conventional login and Grid access.

Action still on Jens.

It is also one of the planned sessions in Budapest.

5.5. WP10 CONFIDENTIALITY ISSUES

5.6. ACCOUNTING – USER/GROUP/VO LEVEL?

We should find out what WP1 are actually doing w.r.t. accounting.

For accounting to work, whenever any action is carried out it is necessary to preserve the original DN of the user.

The most immediate need is for some sort of quota, so that no one user can e.g. fill up a disk. Many, if not all, resources will need a quota associated with their use.

Hope to have an accounting meeting, and a quotas meeting at Budapest.

5.7. MUTUAL AUTHORIZATION – CLIENT

It is necessary for the client (or the VO which owns the data) to authorize a resource to e.g. store data. WP10 only want to store confidential data on trusted resources.

This and WP10 confidentiality issues will be discussed as part of our session with WP10 at Budapest.

5.8. CE/LCAS INTERACTION WITH VOMS

LCAS = Local Central Authorization Service.

WP4 will provide some basic modules.

Something has been written by Argonne which allows the querying of a kerboros service using GSI certificates.

There is also the need for Conversion of certs to Kerboros tokens. Code developed has only been used at a small no. of sites – there may be vulnerabilities.

Andrew McNab is person to talk to about BaBar.

5.9. MULTIPLE VS SINGLE VO

5.10. VO LDAP SERVERS

The developers are considering replacing LDAP completely with some sort of database, e.g. MySQL.

This helps limit access.

There is a need to protect client server exchange.

Eventually grid-mapfile will be replaced with access control lists.

There is a need to store information on people by the VO, but this must not conflict with confidentiality requirements. If a user miss-uses a system, it is for the VO to sort this out.

5.11. AUDITING

There may be a need to keep information on what versions of software was running previously? This includes what versions of both middleware and applications were running.

5.12. GGF PRESENTATION

(See later)

6. WP2 SECURITY – MIKA SILANDER

Transparencies were shown, including the diagram of Authentication and Authorization from 'WP2 Security and Transparent Access: Spitfire security enhancements.' Which is available from `http://wikihip.cern.ch/twiki/pub/WP2/SpitfireAuthorization/spitfiretyot.ps`

For Authentication, Mika believes the SSL handshake does happen between the spitfire server and the user.

The plan is to have an independent Authentication servlet (TrustManager), and Authorization servlet. These should be independent of the Spitfire software.

In version 1.2 there is an initial version of the TrustManager and authorization servlet.

The biggest problem at present is that the CRL (Certificate Revocation List) is only read at startup time.

There was a question 'how is the CRL authenticated'. It is believed that authentication takes place between the host and CA producing the list.

At present, WP2 uses personal certificates as service certificates. This is highly unsatisfactory.

CA's do not want to issue service certificates, which initiated another discussion.

There are several possibilities for dealing with service certicates.

- All services have a certificate issued by a CA.
- The host certificate is also used as the service certificate – this has the disadvantage that the service has to run as root.
- The host runs a mini CA which issues short lived service certificates. (Or long lived certificates if these are automatically revoked if the host certificate is revoked.) This would be run by the owner of root.
- A cluster has a certificate from a CA, and runs it's own mini CA to issue certificates for all services on that cluster.

For now, we will ask CA to issue certificates for services, even though it does not scale in the longer term, and add this issue to the TO DO list.

Therefore we have

TODO 13 – Work out how service certificates are to be handled within DataGrid.

There is also an organisation called the Liberty alliance, which is an industry organisation developing single sign on. It is believed they are writing standards for authentication and authorization. It is supported by Vodaphone, Nokia, Sun and others.

(Java JOG = Java Community Grid.)

7. AUTHORIZATION

7.1. REPORT FROM THE WP6 AUTHORIZATION GROUP – ALBERTO GIANOLI

Information on the LDAP server progress has been distributed to the WP6 Authorization Group list.

Could not give information on time scales for various versions. SCG expressed their concern at this.

WP6 Authorization WG has asked for information about CAS, and asked for collaboration. However, there seems to be little collaboration between Globus/CAS and the Authorization WG. The version of CAS which is currently available is not liked by the people in Bologna.

PERMIS was looked at, but ruled out by people in Bologna. There has been an E-mail from David Chadwick about this. Dave K will see David Chadwick at Oxford to discuss this.

7.2. AUTHORIZATION SCALED TO LCG

(LCG - LHC Computing Grid project.)

Currently there are 13 trusted CAs. At the meeting in Prague more CAs were approved, and we expect to have 20 soon.

Anybody who wants to use the testbed and doesn't have access to a country CA uses CNRS in France. However, this doesn't scale when consider how many countries are involved. We expect to have 10 000's users spread over approx 100 different countries. There is a need to establish cross trust – this is difficult to scale. 1 advantage of the old CAS – sites didn't have to worry about trusting the CA's. The site just had to know about community. In the old CAS, sites negotiate trust with a VO – it's for the VO to make sure of their procedure for trusting CA's.

One problem – there is a lot of emphasis on the CA checking the user's identity. This is the relatively easy bit. Tricky bit is authorization to use resources. How do we check that a person who comes along with a certificate can actually join this community? Nothing to say e.g. if they are allowed to access particle physics resources. There is a scaling problem in this.

When an individual registers the VO must keep information on the person, what institute they work for. This should not be publicly readable. We are working slowly towards a procedure.

AA in the US, is run by big labs. They are tackling these sort of issues.

We need a smooth transition between DataGrid and what comes afterwards.

CERN and FERMILAB are interested in using Kerberos CA.

CP/CPS for this is needed.

CERN checks the person who requests an account at CERN. CERN has a mechanism for finding who is the person behind it, and whether they should have an account.

At present, if people have need to use CERN facilities they can simply get an account and run jobs, without needing Grid access. Don't think it's a problem for getting started on LHC computing activities.

We need to manage growth of this – need more effort in registration for VO’s.

Service certificates are there in Kerberos.

Can use GSI Kerboros or GSI Globus.?

David K – It’s not entirely clear who is doing what? Is everything the responsibility of the Authorization Group? Do you have the resources?

The Authorization Group is supporting what has been done in past. There is as yet no time scale. E.g. what is being done for TB2? TB3?

A plan is needed for what is to be done, this will be discussed at the next WP6 Authorization group meeting.

There is concern at the lack of timetable, lack of manpower, and lack of plans for Authorization.

(VOMS - Virtual Organisation Membership Service.)

8. DELEGATION – GAVIN LOWE

Between the ----- are notes from Gavin. After that, some notes on the discussion.

Delegation from user proxy UP, acting for user U, to A of the right to access resource R.

Two techniques:

1. When A wants to access R, it contacts UP; UP carries out authentication handshake with R; UP passes process handle to A.

2. When UP sends job to A, they establish a delegation credential that allows A to access R (and maybe other resources). A creates public-key, private-key pair; delegation credential contains public key, signed by UP. A accesses R by presenting delegation credential and UP's credentials.

There are two ways of doing this:

a. Delegation credential is extended X509 certificate; A uses this in SSL (with chain leading back to U's certificate).

b. A and R carry out standard SSL handshake, and then A presents delegation credential and UP's credentials.

Comparison:

- In 1, R is authenticated to UP; this isn't true in 2, but UP does give permission for A to use R.

- In 2b, A is directly authenticated to R; in 1 and 2a, R has to trust UP.

- In 2a, credential checking is implemented in SSL; in 2b it's implemented in the layer above.

- In 1, the UP is a bottleneck.

Onwards delegation: delegation credentials can contain information to allow A to delegate to R1 the right to access R2, etc.

In scheme 2, all agents in the chain must be trusted by UP and the final resource, although UP can allow delegation only to agents it trusts, and the final resource can check it trusts every agent in the chain.

Delegation credential needs to specify what rights are delegated directly (similar to an ACL), and which of those rights can be delegated onwards to whom.

Currently version 2a is used, except with "all-or-nothing" onwards delegation.

Scheme 2 allows chaining. However, there is no mutual authentication between UP and R, which could be a problem if R is certified by a CA that UP doesn’t recognise. As scheme 2 allows chaining, there is no authentication between the original user and the resource used, and it is possible to get a long way from the original CA’s trusted by the user, to the resource where a job eventually executes.

In the contents of the credentials, we need to say what resources A can access, who A can delegate these rights to, and whether these rights can be delegated further. This needs a policy language. There is the possibility that the policy language could contain a list of CA’s trusted by the user, in order that onward delegation to an un-trusted resource does not occur. This list could be part of the policy language. This list could be defined by the VO.

For accounting purposes we need to follow the chain back so that resources are charged to the original user.

2a is the way Gavin things we should go. 2a is also what he thinks Globus does. Globus used to go by scheme 1, but changed to 2 at some point prior to version 1.1.

Philippa is carrying out a formal analysis of the above schemes. She will also look at Security Standardization papers from Globus, which include information on Proxies.

Do we allow direct submission to a resource? How does the data get back to the user? As there was no WP1 person present we cannot answer this.

Also note requirement DLG-07 – It must be possible for a VO to restrict what rights a user may delegate, and to which principals they may delegate such rights.

9. DYNAMIC ACCOUNTS IN TB 1.3 – ANDREW MCNAB

See slides.

In Slashgrid – files are owned by root, (slashgrid is run under root) and file access is by DN not UID. They are not owned by the UID of the dynamic account. This allows UID's to be re-cycled, and the user can access their files via their DN.

RPM's are in the repository, it only works on Linux at present, it doesn't work on Solaris.

To recycle UID's need to be sure no jobs are running, including no sub-processing. For TB 1.3, the recommendation is that we don't re-cycle accounts between re-booting the machine. In the longer term accounts will need to be re-cycled.

Slashgrid is available and optional in TB1.3. It is up to the local site whether or not they configure it.

This has been discussed in the Architecture group.

Originally, it was not foreseen that WP6 would write middleware.

We will need to check for security holes in the same way as for other middleware.

Also raise issue of case sensitivity in Authentication vs Authorization.

We must not use case sensitivity to distinguish between 1 user and another.

10. PLANS FOR GGF5

To form a new working group we have to start with a BOF.

Dave K should request a BOF session, with a view to starting an Authorization WG.

(Note added after meeting. It is too late to form a BOF for the GGF5. We will discuss plans for a BOF in GGF6)

11. PLANS FOR BI-LATERAL MEETINGS IN BUDAPEST

Dave K sent requests for meeting rooms, asking for 5 2 hour sessions for meetings with other WP's.

They have given us a session on the Sunday, before the meeting officially starts. No-one objected to having a meeting on the Sunday.

After discussion, we think we only need the following 4 meetings in order of priority:--

Security and Biomedical applications – SCG + WP2, WP5, WP7, and WP10.

Accounting – SCG+WP1

Quotas. SCG+?

Slashgrid, ACL's etc. SCG + WP6 +WP2 +WP5?

We agreed we should not have a meeting of SCG alone.

12. HOW TO AUDIT/CHECK SECURITY DESIGN AND IMPLEMENTATION

Franck talked about Firewalls. For the current version of the testbed, firewalls are still the same as those described in D7.5. There is a proposal to setup firewalls on Linux boxes via the installation scripts – with different rules for each element on the box. Thus the firewalls would be setup automatically, and be more restrictive than the current scheme. (Sensible IP chains rules would be set automatically.)

SCG thinks this is a good idea.

There 2 parts to auditing and checking security.

1) Verify that design is correct, there are no holes in the design, i.e. the design itself is secure.

2) Verify it is implemented securely.

Philippa Broadfoot will be able to carry out some checking of the design, using formal methods, to spot obvious holes. What is needed is a concise description of the design. This can only be carried out on parts of the design that are very well defined, so they can be modelled. D7.6 should be a tool for this, and we should develop D7.6 with this in mind.

For checking the implementation, Franck said that CNRS had proposed that private companies be used to check. And this will probably be funded by CNRS. We just give the companies the software?

Jens suggested that we look at checking TB2 for security holes.

An action was placed on Franck to find out EXACTLY what CNRS is proposing.

Note that we will eventually have to describe the security of all WP middleware.

13. PLANS FOR D7.6

D7.6 = design for the whole project (just as D7.5 was the requirements for the whole project) plus what was implemented in TB2.

D7.6 is important for us internally, it is our main tool for looking at whether we have a secure design.

Akos has feedback from Oxford. We should encourage each WP to look at Security. We should make developers aware of security matters, e.g. buffer overflows. Jens has a list of what to look for.

14. AOB

There will not be another meeting of the SCG until after Budapest. Exact date is TBD.

Everyone is reminded of the quarterly reports – and the need to feedback effort spent to their country representatives.