

# Site AAA Project Recommendations for Future Activities

**Bob Cowles, Dane Skow, Pls.**

January 15<sup>th</sup>, 2003

PPDG- 25

Per your request at our report, we are offering this prioritized short list of recommended activities for the immediate future. We see these as the important next steps for continuing the progress made. Certainly there is ongoing work and longer timescale work needed and not covered here, but these reflect our nearterm concerns for HEP GRID computing.

0) Expand the detailed discussion between site security infrastructure and Grid middleware security developers to include European counterparts.

It is not clear to us which role EDG plays. The LCG working groups seem the natural forum for doing this. We need to insist on input and engage our counterparts at the Tier 0 & 1 level.

1) Implement common authorization callout in Globus gatekeeper and gridFTPd.

This callout spec should be common and specified with EDG and the GGF Authorization working group. A library of modules for common checks will need to be collected and eventually something like a PAM logic handling structure developed. This last can build upon the callout specification.

2) Virtual organization as registrars for multiple sites.

There are, in principal, 3 separate user registrations that may need to happen: registration with the CA that issues the certificate, registration with the VO to affirm membership, registration with the resource provider. At this point, it looks likely that these are three separate database tiers (and probably many more instances than that depending on the number of CAs and Resources a VO uses), but the user should not have to deal with each individual instance. In the simplest case (for the user), the user registers with a VO (perhaps providing an existing, acceptable certificate) and the VO vets and passes on the information needed to register with Resources and/or CAs.

The definition of information to be collected, acceptable methods of verification, and transmission to relying sites all have to be determined. Several VOs need to engage in this activity with a representative sample of sites to survey the needs and guide implementation standardization. A standard interface for VOs to provide information and behind which sites can put their local infrastructure is very desirable. Discussions should also take place on whether

common databases can/should be utilized and what sort of interactions are needed between the CA, VO, and Resource information.

### 3) Long Running Jobs.

Solutions for this will necessarily involve services acting on behalf of users. The definition of where reauthentication and reauthorization can/must be performed in a Grid and what communications are required is needed.

There are two components: how to maintain valid authentication credentials to a job on behalf of a user without exposing the user to too big a window of vulnerability, and how to assure that jobs approved to run once are STILL approved to run (particularly relevant for cases where jobs may be consuming resources rapidly). This will probably have to be guided by a couple examples of working solutions that are acceptable to CA, user, VO and site requirements. The Condor-G/MyProxy effort is the most advanced general effort known.

There are perhaps similar issues regarding service to service interactions on behalf of users (eg. storage system to storage system transfers).

### 4) Proxy Generation Services

This is basically a different kind of user proxy generation (ie. authentication method) where the user doesn't maintain the private key (or at least that copy of it in the MyProxy case).

Whether it's a separate set of CAs, extensions of the existing CAs, a site service provided by large sites, or a combination of all is yet to be determined. There are significant policy and interface design discussions needed. The current projects should be blessed and pushed while these discussions (and the resulting standardization) takes place. This could be taken up seriously at GGF7 perhaps (though EDG did not expect to have significant presence there)

### 5) Incident handling

Methods and responsibilities for identifying, investigating, responding to, and following up on incidents of attack and misuse need to be determined across the interconnected grid.

There is no natural scale for organizing this effort short of all HEP and there is not a history of close cooperation between sites on incident handling. Indeed, since this is by definition dealing with cases where things went wrong, issues of privacy, sensitivity, authority will be extremely important.

It is time to define who's responsible for what in detail. Walking through the process for incident handling and how to deal with situations when access to the Grid is compromised (and it is guaranteed to happen) will illuminate many of these points and calm a number of nervous operations folks that they are not alone or the sole defender of a breach.

The LCG forum would be a good one to take this up with. The GGF CA operations WG may be another.

#### 6) Authorization Information

The protocols and mechanisms for expressing, enforcing and auditing authorization information need to be developed for VOs, Users and Resource Providers to use common methods. There are a number of efforts in this regard (CAS, VOMS/LCAS, VSC, etc) that should collaborate on a common framework.