



TM and © Laurent de Brunhoff

Authentication and Authorisation

Tim Adye

Rutherford Appleton Laboratory

Workshop on
Distributed Analysis at Tier A Centres
SLAC

15th December 2001

Authentication and Authorisation

- Authentication
 - Identifies **who** you are
 - Does not say whether you are allowed to use the resource
 - Each user should have their own certificate
- Authorisation
 - Specifies which users can do **what**
 - Once certificate has been authenticated, authorisation can be done using **Certificate ID**.

Authentication

- We plan to use **Grid certificates** issued by national Certificate Authorities
- **Tier A sites** must recognise these CAs
 - What about **client machines**?
 - Users without a national CA (eg. US) can apply for a French (CNRS) certificate
- See **DataGrid WP6** pages
 - <http://marianne.in2p3.fr/datagrid/ca/ca-testbed-ca.html>

Authorisation

- Currently maintain a **grid-mapfile** by hand
 - Contains mapping between **Certificate ID** and local **username**
 - Smaller sites may want to use “**generic accounts**”, so all Certificate IDs map to the same set of accounts
- This will not scale to 811+ users
 - Use a **central BaBar grid-mapfile**
 - Already do this for the UK (but only 8 users so far 😊)
 - How can maintainer tell that a user is a BaBarian?
 - If manually-maintained, user has to send another e-mail
 - Tells maintainer her Certificate ID
 - This adds another delay to get started

Central grid-mapfile

For this reason, would like to allow users to add themselves to this list

- BaBar Personnel database?
- Something analogous to HyperNews registration?
- Use SLAC AFS ACLs?

Using AFS ACLs

- Result of a discussion with Doug Smith
- Many SLAC AFS ACLs – including list of SLAC account names of **BaBar members** (`g-babar:member`)
 - May prefer to use (or combine with) `g-babar:com-obj`
 - Don't want to break Objectivity licence agreement
- Cron job checks each user's home directory for a special file
 - Eg. `~adye/.babar-grid-certid`
 - Not in `.globus` which is private
 - This gives Certificate ID (and other info?)
- Cron job outputs BaBar **grid-mapfile**
 - Probably want a bit more info (eg. username)
 - Each site updates from this (stripping unused info)

AFS ACL features

- Later, could make **several lists** by using different ACLs
 - Eg. **Priority users, SP managers, etc.**
- Under each user's control
 - Can add/remove themselves from the list
 - Latency depends on cron job and sites' update frequency
- Relies on SLAC and users' security
 - **Primary security is Grid certificate** (and national CA)
 - If this system were compromised, it would allow non-BaBarians access to BaBar resources, but would not allow one person to masquerade as another
 - If this system were compromised, non-BaBarians would already have access to BaBar data and resources