Security discussion

Which took place on

3rd April 2003

Linda Cornwall 4th April 2003

Agree that:-

- Delegation is needed
- Final decision has to be made by the producer
  - For now, ignoring case where e.g. table of friends is from a different producer/location to table of people directory
- Mediator can make a first decision e.g. re-formulate a request
  - Which means that the mediator can have non-confidential authorization information on general policy
- Some confidential authorization information will have to go with the end producer
  - E.g. the mediator should not know if a user is banned.

View

- An ACL for a row or a table is not adequate.
- We need access control on a view.
- MySQL includes access rights on a view – but this is simply per user – not an ACL on a view.
- We will need some sort of policy language based on a view.
- Producer will need to publish the access control on the views.
  - When a table is created, the access control on the various views will also have to be created.

Copied information

- Information copied must have the access control copied with it.
- Information copied should only be copied to sites which we trust to enforce the security rules.
  - E.g. Registry replication – only copies to authorized DN's, which we trust to enforce the rules and not copy info to anywhere else!
- For archived information – rules must be preserved.

User's only seeing their own job information

- Simple (ish) case – user to only see their own job information
- For a first version, the producer should only provide job information if DN matches.
  - The mediator first check can be left until later
- Then there is the problem of the Archiver! Only allow certain archivers to archive – then the archiver must enforce rules too!
- Or just the simple consistent rule – no-one other than the user can get info on their own job (or at least a view on their job that includes confidential information.)

Manpower/priority

- Andy is not convinced we can even do the simplest case this year.
- Suggests that those who have these requirements write it themselves
  - Via their own Producer
  - As a canonical producer
- Also, we are not sure of exact requirements, including is it necessary to archive this data
- Lisha suggested that a user's manager will want to see their job control info
- This very simple authorization could be worse than no Authorization

Plan

- We should find out EXACT minimum requirements on job info
  - What is confidential
  - What needs archiving
  - What needs accessing by who
- Work out what we need to do to satisfy this
  - Favour the solution being as general as possible, e.g. 1 rule that is defined – extend to a whole load of rules later
- Make an estimate of the manpower needed