Administratively provided initial credentials and security configuration:

1. The Grid Service has a set of X.509 credentials that uniquely identify it. This will be a X.509 EEC and associated key. The DN for these credentials could have any value, but will typically have a commonName containing the FQDN (possibly with a “host/” prefix) of the host on which the service runs.

2. The Grid client application (this is the user or a process running on the user’s behalf) has a set of X.509 credentials. These will typically be based on a X.509 Proxy Certificate.
   a) The proxy certificate optionally contains a Subject Information Access extension (exact contents TBD) which provides contact information for one or more Shib AAs which can provide attributes regarding the client. This extension will have been placed in the proxy certificate at the time of its creation by to-be-developed extensions to the grid-proxy-init program. The exact contents of the extension are TBD, including the acquisition of a suitable OID (from either the PKIX or the Grid community). The identifiers for the AAs will be acquired via a user configuration mechanism (e.g. a configuration file or commandline argument).

3. All Shib AAs have a set of X.509 credentials that uniquely identify it.

4. The Grid Service has a set of certificates identifying Shib AAs that it trusts to provide attributes suitable for use in authorization decisions.

5. It is assumed that all X.509 EECs are issued by CAs that are trusted by all parties mentioned in this document.

Use case #1, with no pseudonymity:

1. Grid client contacts Grid service and authenticates as it normally would. From this authentication the service determines:
   a. The subject name of the user;
   b. If the Subject Information Access extension is present, contact information for Shib AA(s) that can provide attributes for the client.

2. The Grid service determines it needs attributes regarding the user (based on administrative configuration). If not, authorization is done as normal (outside the scope of this document).

3. If the client certificate provided a pointer to one or more AAs, these are validated as being trustworthy by checking for presence of appropriate certificates in the list of trusted AA certificates. Untrusted AAs are silently ignored.
4. If the client certificate did not provide a pointer to one or more AAs, then a set of one or more administratively configured AAs is used.

5. Grid service contacts the Shib AA using standard Shib AA protocol and a SSL protected channel; mutual authentication is performed.
   a. Local, trusted copy of certificate of Shib AA is used to verify that the correct AA is being communicated with.
   b. Grid service authenticates with shib AA using it's own certificate & private key, so Shib AA knows identity of target service for ARP evaluation.
   c. If contact with Shib AA fails for any reason, next AA in set is attempted. If all fail, Grid services performs authorization without any attributes (which will probably result in failed authorization).

6. GridService sends an Attribute Query to the AA containing the subject name of the user and its Resource name.
   a. This query will be for either all attributes or some set in an administratively supplied namespace.
   b. AA validates that Resource name matches the identity from SSL mutual authentication and fails if not? Or ignores Resource name in Query and uses value from mutual authentication? I suspect whichever is easiest to implement.
   c. AA validates that the Service has the right to ask about the given Subject. (This seems to mesh with Note #2 in the LionShare profile.)

7. Shib AA consults ARPs to determine Grid service's right to possess attributes for user based on subject and resource names. A list of attributes to be delivered is generated.

8. Shib AA delivers list of attributes to target service over SSL-encrypted link (don't see any need for signing of attributes).
   a. TB: One thought is this might this come in handy for portal environments. I'm thinking portal conducts shib attribute marshalling on behalf of allied apps and forwards signed assertions to them. They validate they got them from their trusted portal by whatever means, and they can verify the authenticity of the attributes by validating the AA signatures using certs obtained from the same sources as those used by the portal for authenticating AAs. Deal with n-tier issue this way.

9. Target service uses attributes along with local policy to make access control decisions.

Use case #2, with pseudonymity:

[Client behavior is to get a temporary set of credentials first with pseudonymous identifier.]

1. Grid client contacts an online CA designed to provide pseudonymity:
a. The CA authenticates the client using its Grid credentials in normal fashion for a Grid service.

b. The client generates a new key pair. The public key is sent to the CA in the form of a certificate request.

c. The CA then generates a unique ephemeral identifier for the user, equivalent to the Shibboleth Handle.

d. The CA places the identifier (as a CommonName component) into a X.509 certificate bound to the public key sent over from the client. A Subject Information Access extension is also placed into the certificate to identify the Shib AA associated with the CA.

e. The CA registers the identifier with the Shib AA, binding it to the user’s attributes.

f. The client associates the new certificate with temporary identifier with the previously generated private key, henceforth dubbed as the temporary credentials.

g. The client will then set environment variables to cause subsequent Grid client applications to use the temporary pseudonymous credentials in place of the user’s normal credentials; this replacement continues until some given task is completed (i.e. a set of applications are run) or the user explicitly swaps the normal credentials back as the default.

2. Grid client contacts Grid service and authenticates using the temporary credentials. From this authentication the service determines:

   a. The identifier for the user;
   b. From the Subject Information Access extension, contact information for Shib AA that can provide attributes for the client.

   [The Grid service steps are the same as in the previous use case.]

3. The Grid service determines it needs attributes regarding the user (based on administrative configuration). If not, authorization is done as normal (outside the scope of this document).

4. The AA pointer provided in the client certificate is validated as being trustworthy by checking for presence of appropriate certificates in the list of trusted AA certificates. Untrusted AAs are silently ignored.

5. If the client certificate did not provide a pointer to one or more AAs, then a set of one or more administratively configured AAs is used.

6. Grid service contacts the Shib AA using standard Shib AA protocol and a SSL protected channel; mutual authentication is performed.

   a. Local, trusted copy of certificate of Shib AA is used to verify that the correct AA is being communicated with.
b. Grid service authenticates with shib AA using it's own certificate & private key, so Shib AA knows identity of target service for ARP evaluation.

c. If contact with Shib AA fails for any reason, next AA in set is attempted. If all fail, Grid services performs authorization without any attributes (which will probably result in failed authorization).

7. GridService sends an Attribute Query to the AA containing the identifier (in the form of a X.509 subject name) of the user and it’s Resource name.

   a. This query will be for either all attributes or some set in an administratively supplied namespace.

   b. AA validates that Resource name matches the identity from SSL mutual authentication and fails if not? Or ignores Resource name in Query and uses value from mutual authentication? I suspect whichever is easiest to implement.

   [AA acts the same as in use case #1, except for mapping identifier to long-term identifier]

8. AA maps identifier to long-term Subject identifier for user

9. AA validates that the Service has the right to ask about the given Subject. (This seems to mesh with Note #2 in the LionShare profile.)

10. Shib AA consults ARPs to determine Grid service's right to access attributes for user based on subject and resource names. A list of attributes to be delivered is generated.

11. Shib AA delivers list of attributes to target service over SSL-encrypted link (don't see any need for signing of attributes).

12. Target service uses attributes along with local policy to make access control decisions.