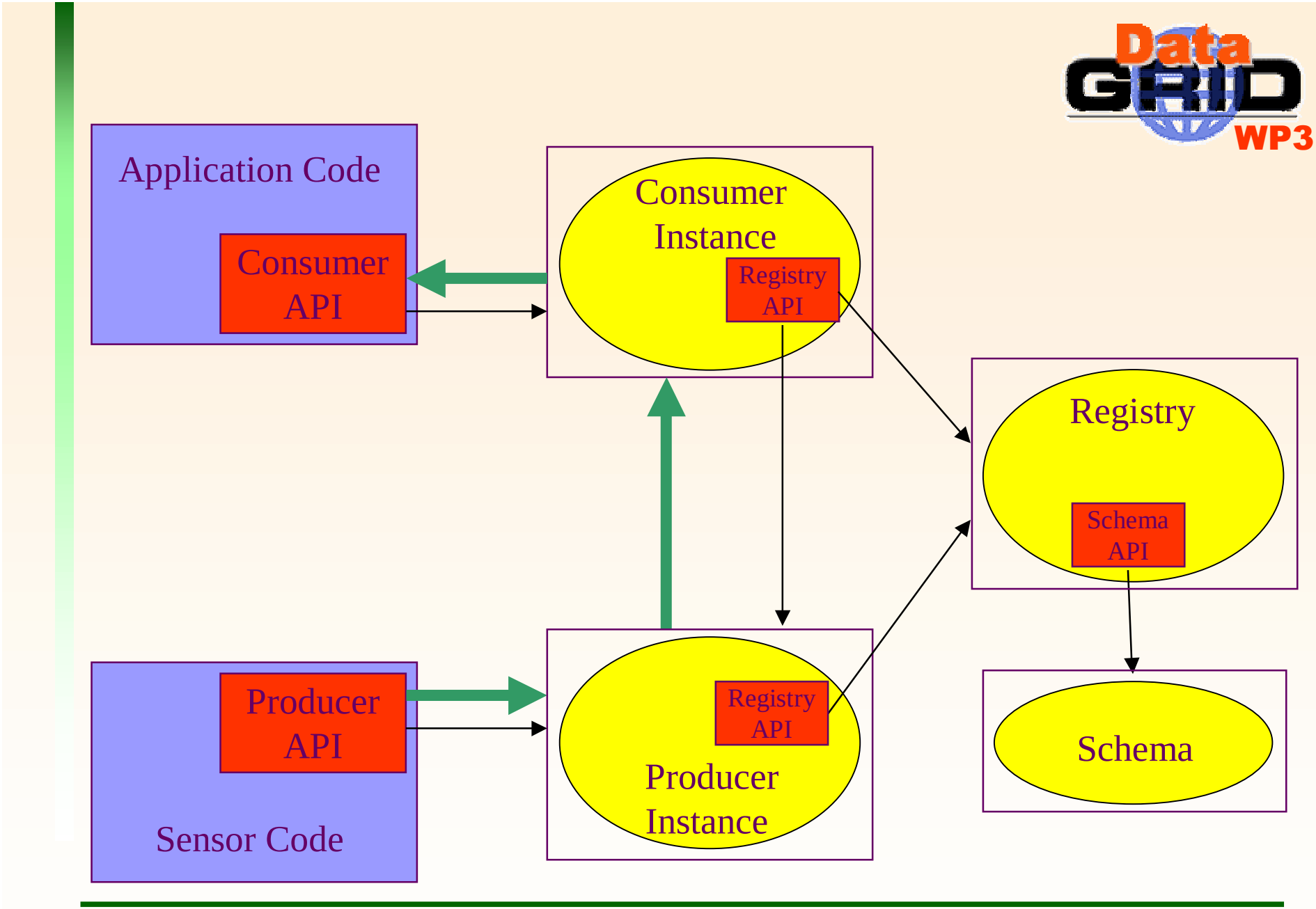
WP3 Security Implementation for TB3

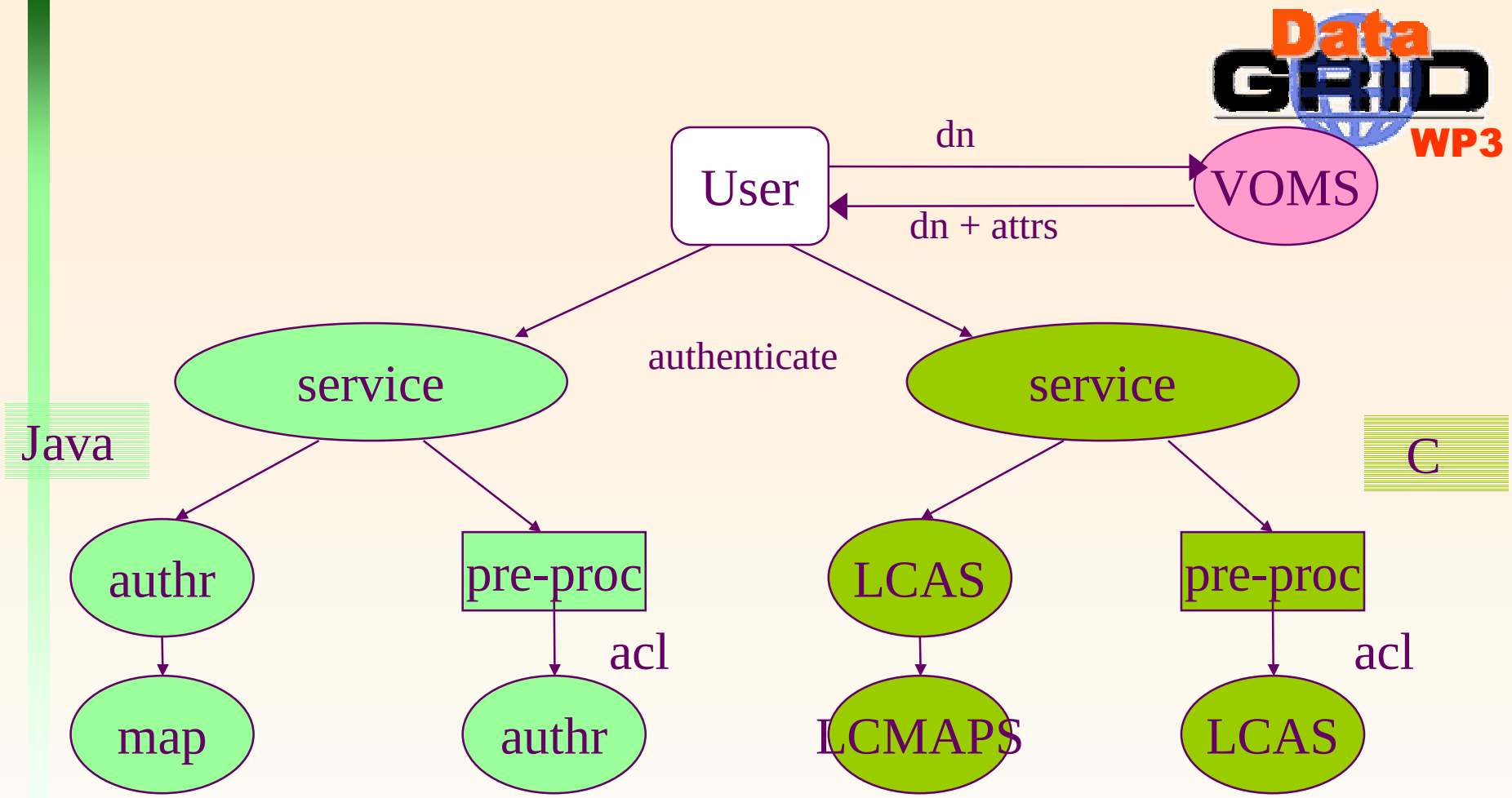
Linda Cornwall

SCG meeting 10th July 2003

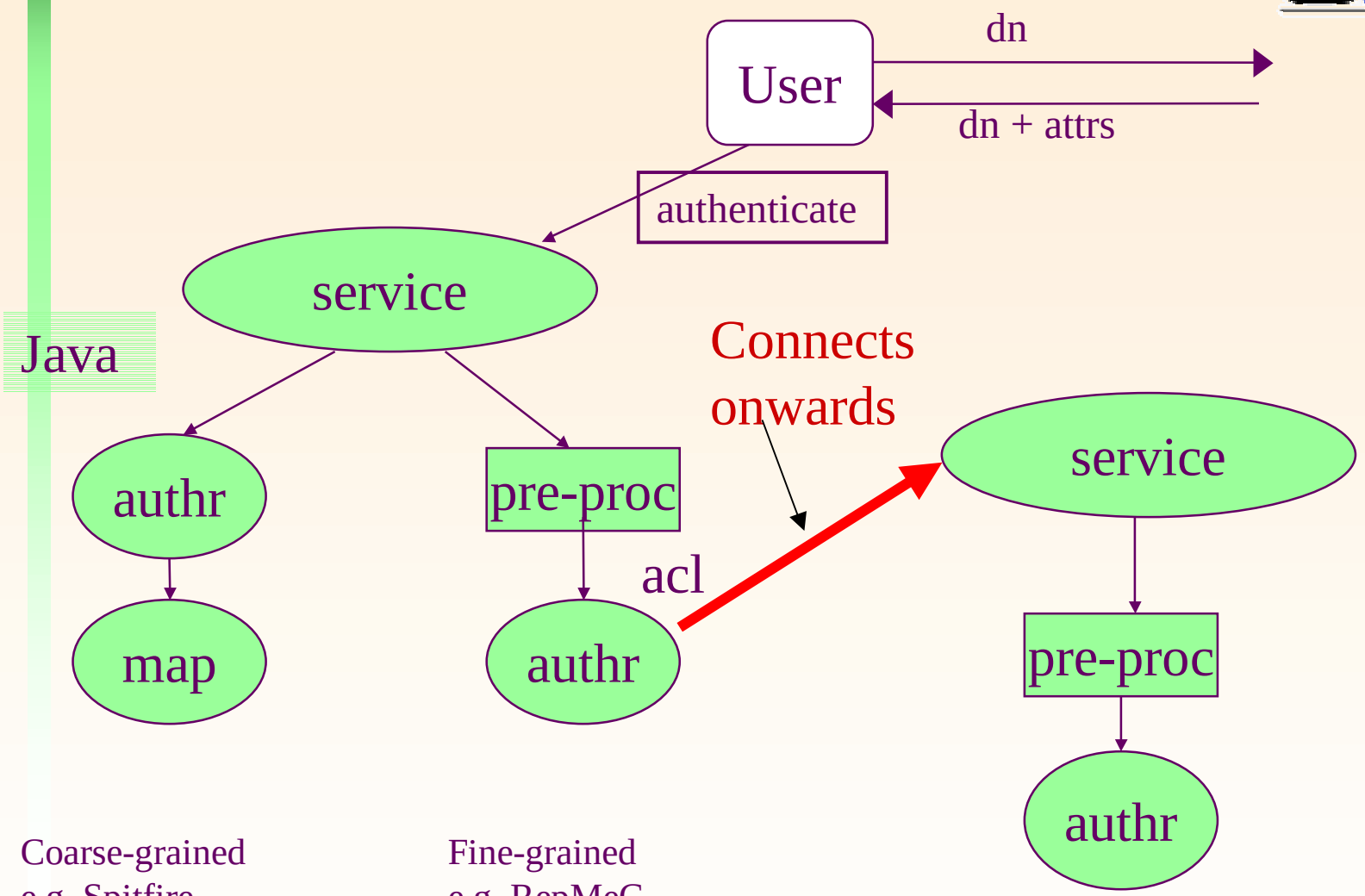
What is R-GMA?

- R-GMA is a Relational Grid Information and Monitoring system being developed by WP3
- Based on the Grid Monitoring Architecture (GMA) from the GGF
- Information system has the appearance of one large relational database (but it's not).


Application Code
Consumer API
Consumer Instance
Registry API
Registry
Schema API
Producer API
Sensor Code
Registry API
Producer Instance
Schema



Coarse-grained e.g. Spitfire	Fine-grained e.g. RepMeC	Coarse-grained e.g. CE, Gatekeeper	Fine-grained e.g. SE, /grid
WP2	WP2/WP3	WP4	WP5



Coarse-grained
e.g. Spitfire

WP2

Fine-grained
e.g. RepMeC

WP2/WP3

Getting Real

- Talked a lot in the past about the complexity of R-GMA, and how to make it secure.
  - Especially the complexity of Authorization
- Now presenting what we are doing during the next few weeks
- We will ‘trust’ the R-GMA instances, after Authenticating them. This simplifies both Authentication and Authorization
  - No need for delegation
  - Authz decision can be made by the servlet the user connects to.
  - This strategy is used by other services which collect information from many places.

Authentication for next testbed

- The user Authenticates with the servlet they connect to.
- Each Servlet Authenticates with each other servlet.
- We use the EDG trustmanger to carry out Authentication.
- Each client and servlet has a trustproperties file – stating where to find the certificate and key.

Current Status for Authentication

- Java Authentication works
  - Including using the service proxy for Authenticating Servlets.
- No default host name verifier
  - That provided in httpsURLConnection checks the host name in the certificate against the host name connected to.
  - So this has been replaced by always returning O.K..
  - No host name verifier means a user could connect to a rogue service with a stolen certificate and not know.
- C/C++ API not complete

Authentication – TO DO

- C/C++ API
  - Can't lift other people's
  - Probably base ours on what Jens/WP5 has done
- Ideally add host name verifier – helps avoid user connecting to 'rogue' r-gma

Authorization

- Turn off non-ssl connections – thus everyone must have a certificate to do anything.
- Add very simple Authorization – largely hard-coded, where job control information is only issued if DN=DN OR if another R-GMA service requests this information.
  - Since there's a generic service certificate rather than an r-gma service certificate – not very secure.
- At least this is a step towards Authz

After EDG

- R-GMA (we are hoping/assuming) will continue to be developed.
- We will address the Security issues – especially Authorization.
- We have written a first draft of a security document for R-GMA
  - includes plans for introducing full, general Authorization functionality in stages.
  - Includes caveats on R-GMA security – including reference to EDG disclaimer.