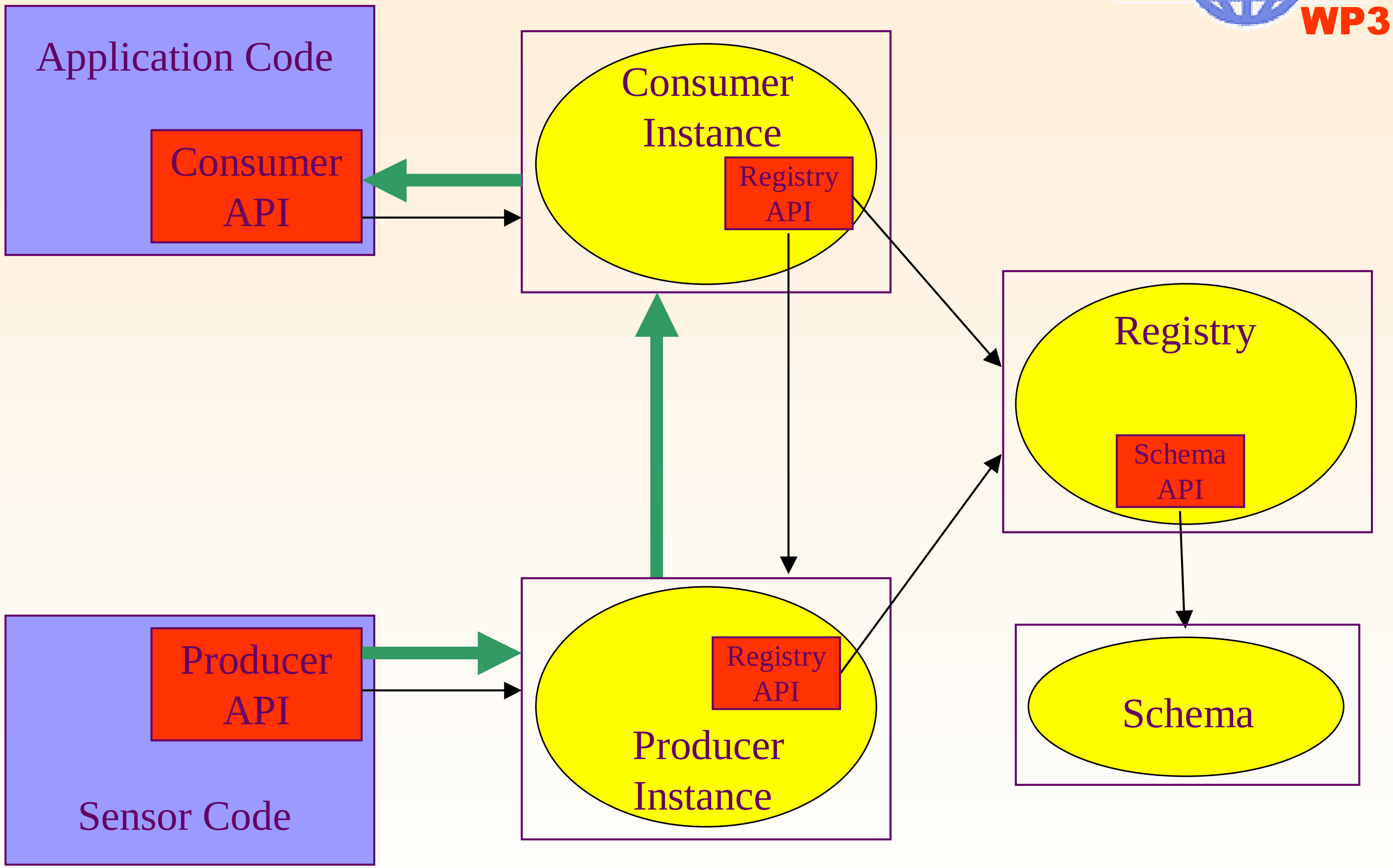
Security Implementation for WP3

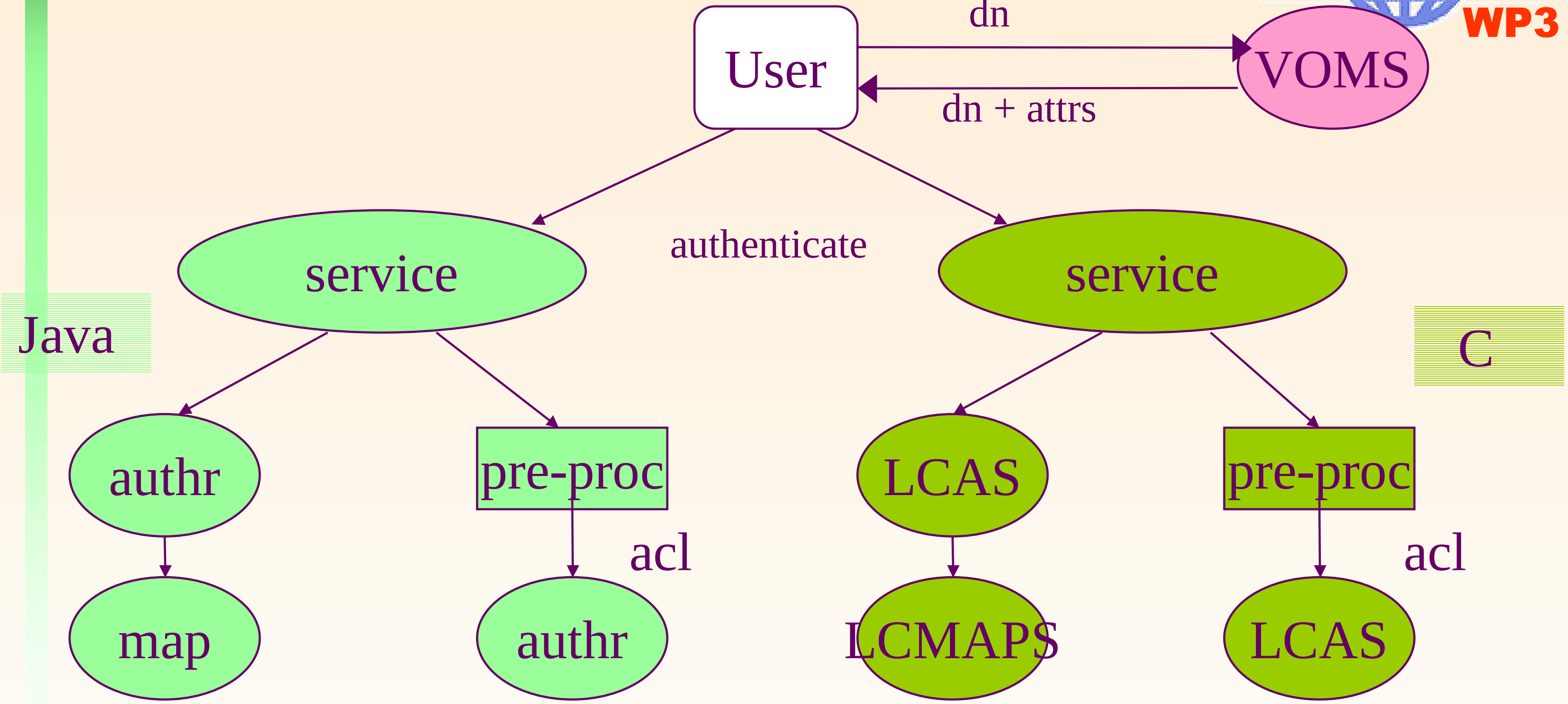
Linda Cornwall

SCG meeting 12th May 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



User

dn

VOMS

dn + attrs

authenticate

Java

service

service

C

authr

pre-proc

LCAS

pre-proc

acl

acl

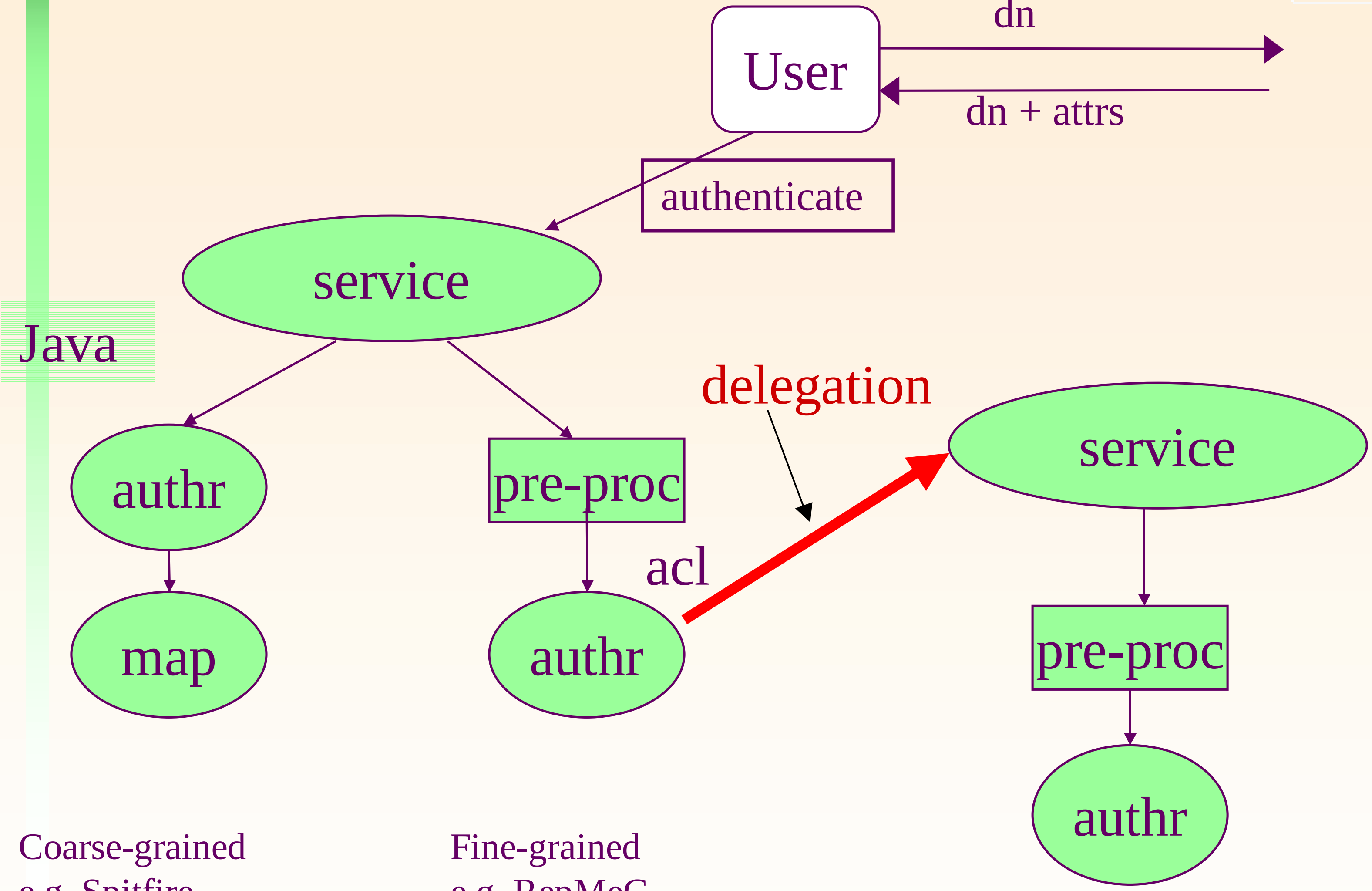
map

authr

LCMAPS

LCAS

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



User

dn

dn + attrs

authenticate

service

Java

authr

pre-proc

map

authr

acl

delegation

service

pre-proc

authr

Coarse-grained
e.g. Spitfire

WP2

Fine-grained
e.g. RepMeC

WP2/WP3

Authentication in R-GMA

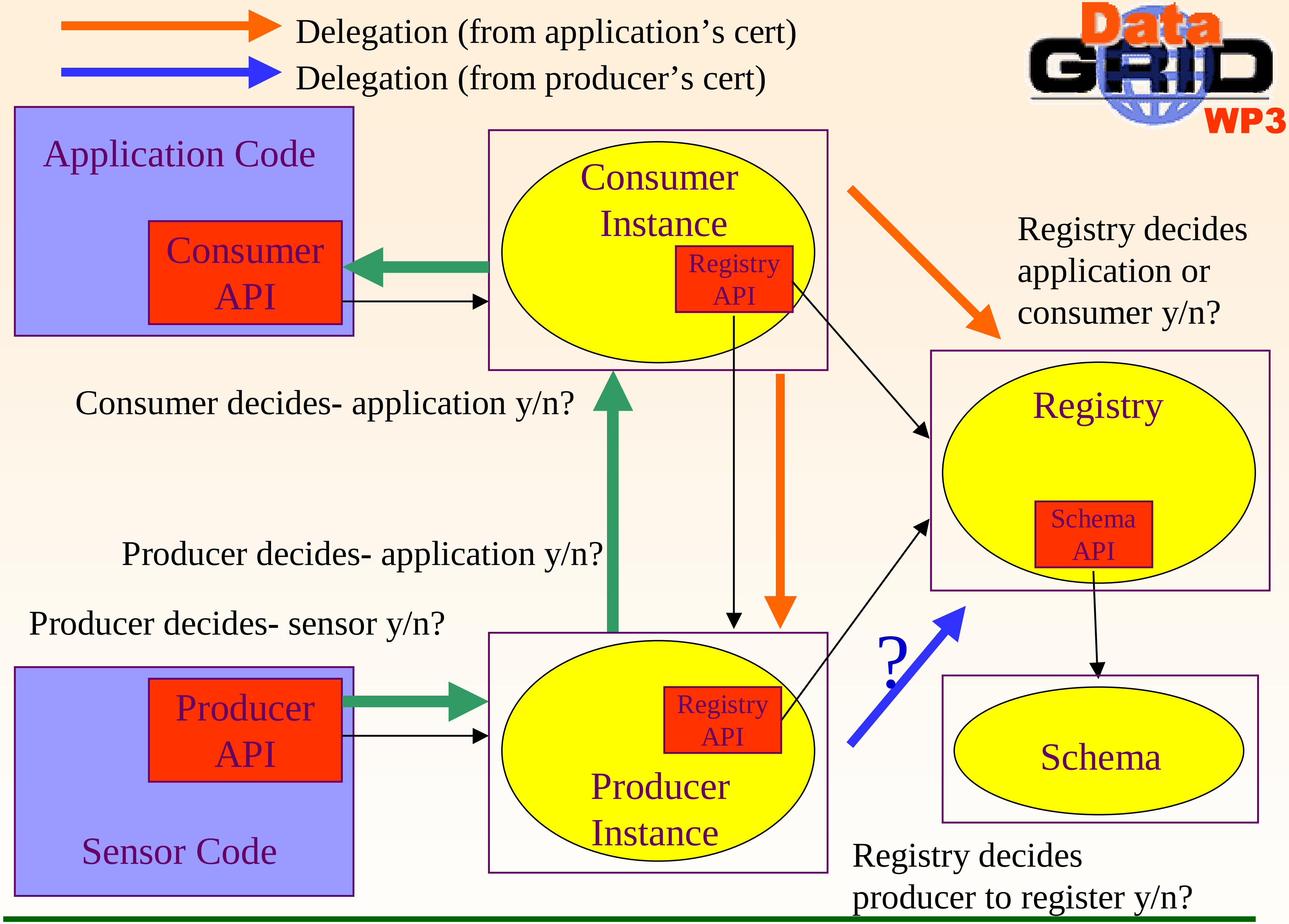
- In R-GMA servlets connect onto other servlets – so to properly authenticate the client with all the servlet that get connected onto we need delegation.
- But, in it's absence the trustmanager has been integrated such that the client authenticates with the first servlet they connect to, then each servlet authenticates with the next servlet.
- Each client and servlet has a trustproperties file – stating where to find the certificate and key.

Current Status

- No delegation – a rogue r-gma can do what they like if they have a service certificate.
  - (This is more serious for authorization.)
- 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.
  - Need to know exact form of service certificates in edg to do this properly.
  - No host name verifier means a user could connect to a rogue service and not know.

R-GMA (Special) Authz requirements

- R-GMA handles tables of info
- In some cases, certain rows of data may only be available to one user.
- Summary information on a table may be available to another group of users
- Simple e.g. GACL on table/row not adequate
- Complex decisions need to be made within the process- still should be based on
  - DN
  - VO membership, Groups and roles
- There is a requirement to hide existence of producers of information from those not authorized



Delegation (from application’s cert)

Delegation (from producer’s cert)

Application Code

Consumer API

Consumer Instance

Registry API

Registry decides application or consumer y/n?

Registry

Schema API

Consumer decides- application y/n?

Producer decides- application y/n?

Producer decides- sensor y/n?

Producer API

Sensor Code

Registry API

Producer Instance

?

Schema

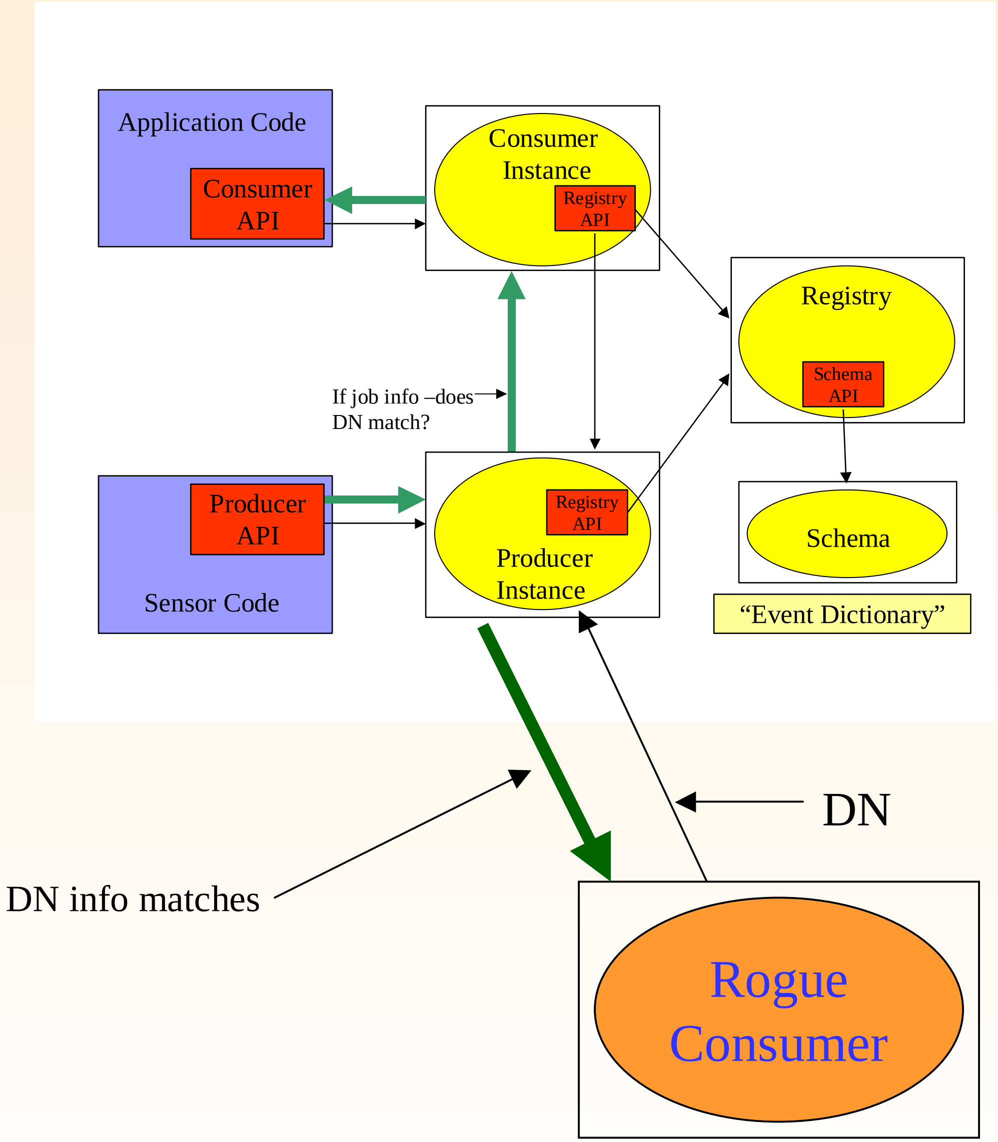
Registry decides producer to register y/n?

Authz Strategy for R-GMA

- Authz decisions all made within Service
- Use Delegated VOMS proxy's (when available).
  - Need ability to extract DN, VO, Groups and Roles .
- Publish Policy in Registry
  - Allows ability to only ask producers questions they are likely to answer.
- Final Authorization Decision made by the end Producer.
- Combination of delegation AND decision being made by the producer preserves confidentiality.

Confidentiality

- There are certain requirements on confidentiality. To satisfy these an authorization decision at the source or producer of info AND a delegated VOMS proxy is needed.
- If a third party can say ‘tell me if Linda is banned’ without the use of a delegated certificate – then the fact Linda is banned can be found out without Linda’s permission.
- Similarly for any info – a hacked or rogue R-GMA can get any info they want. Can only make things difficult.



Without Delegation it is possible to obtain info one is not authorized to see. But it requires a consumer to be hacked or written.

Rogue Consumer has acceptable Certificate.

How to prevent copying to unauthorized sites?

- R-GMA has more complications that this – there are Archivers, Producer/Consumers – which collect and re-publish info.
  - Need to ensure Authz information is copied with the info and adhered to.
  - Need to ensure these do not store confidential data.
- 2 way authorization been talked about in context of storing sensitive data
  - Thus – we should only allow data to be archived/replicated/copied to consumer/producer if those are trusted.
- Better only allow sensitive data to be accessed directly?
- The more I think about it, the more I think we are opening a can of worms.