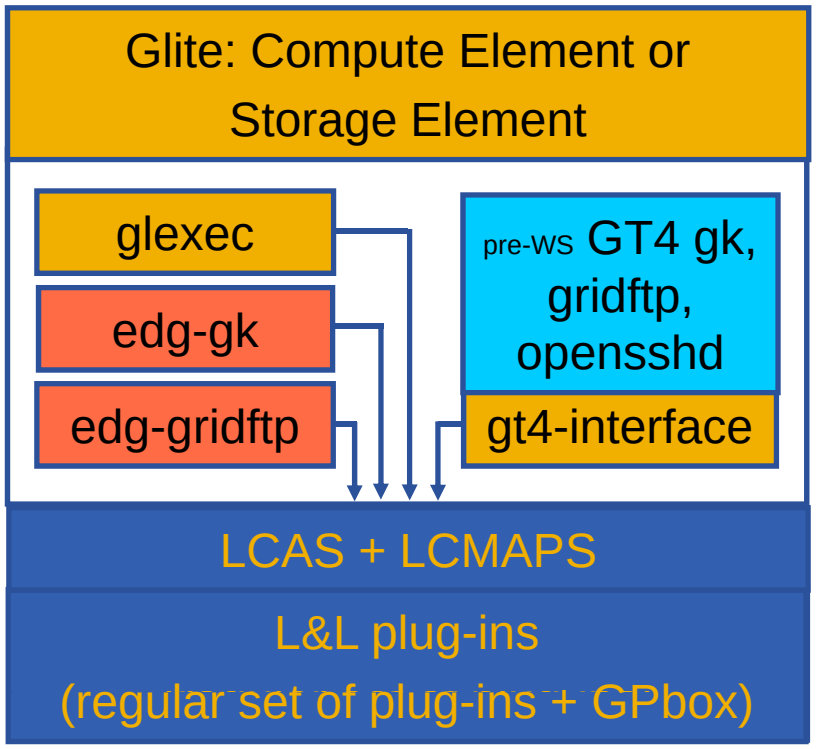
SAML-XACML interoperability

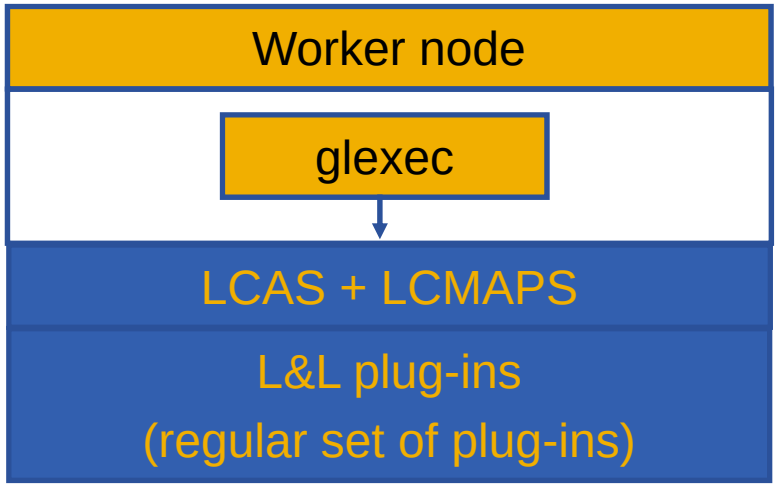
Oscar Koeroo

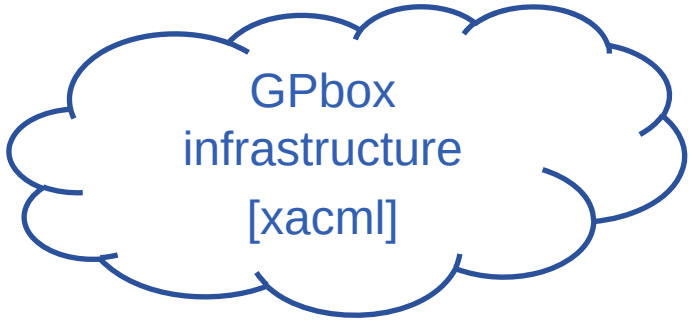
index

- The current setup
- The architectural big picture (EGEE/OSG)
- How will this work
- The requirements
- Work done and decisions made
- Stuff to do

Our current architecture



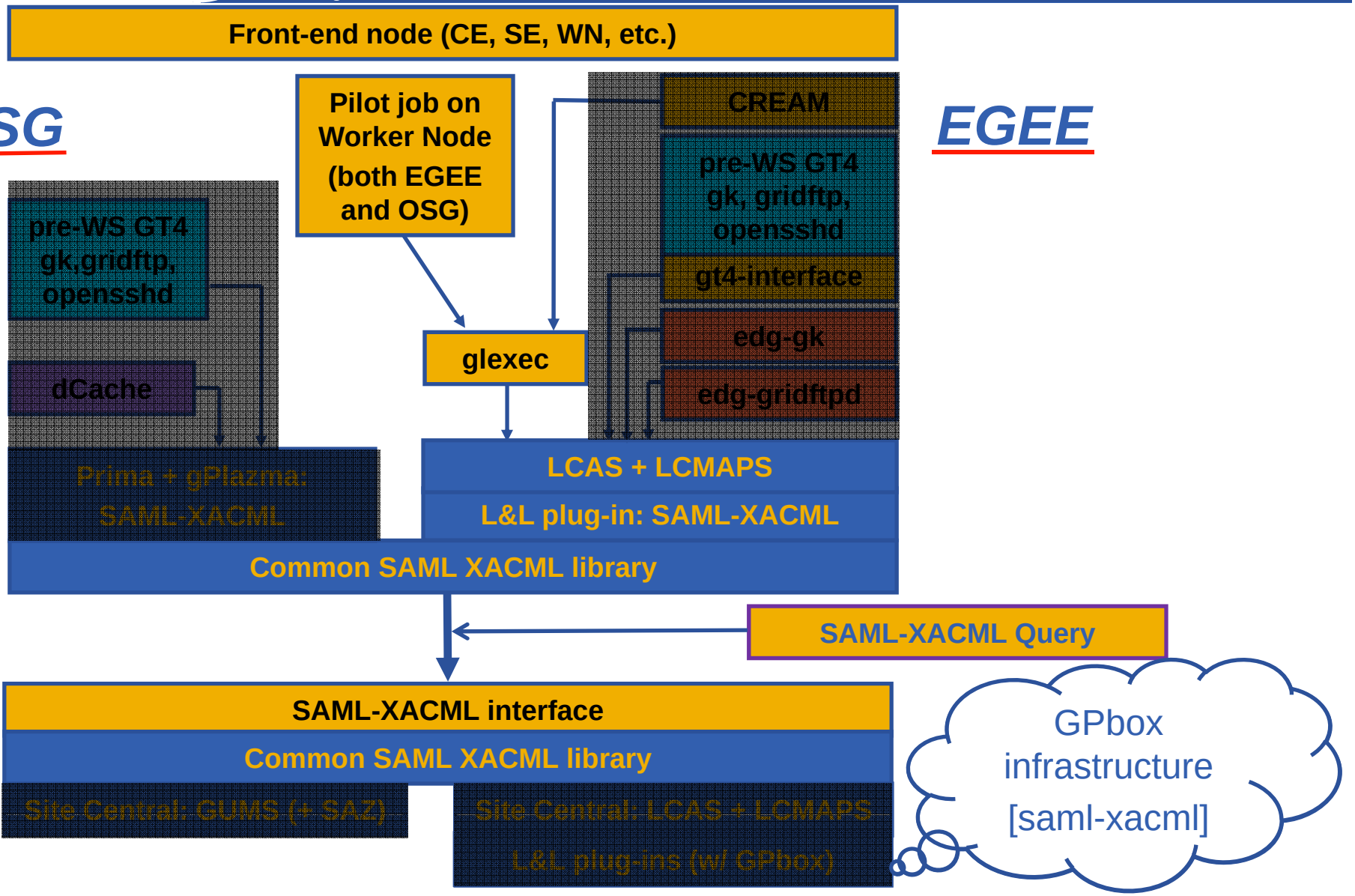




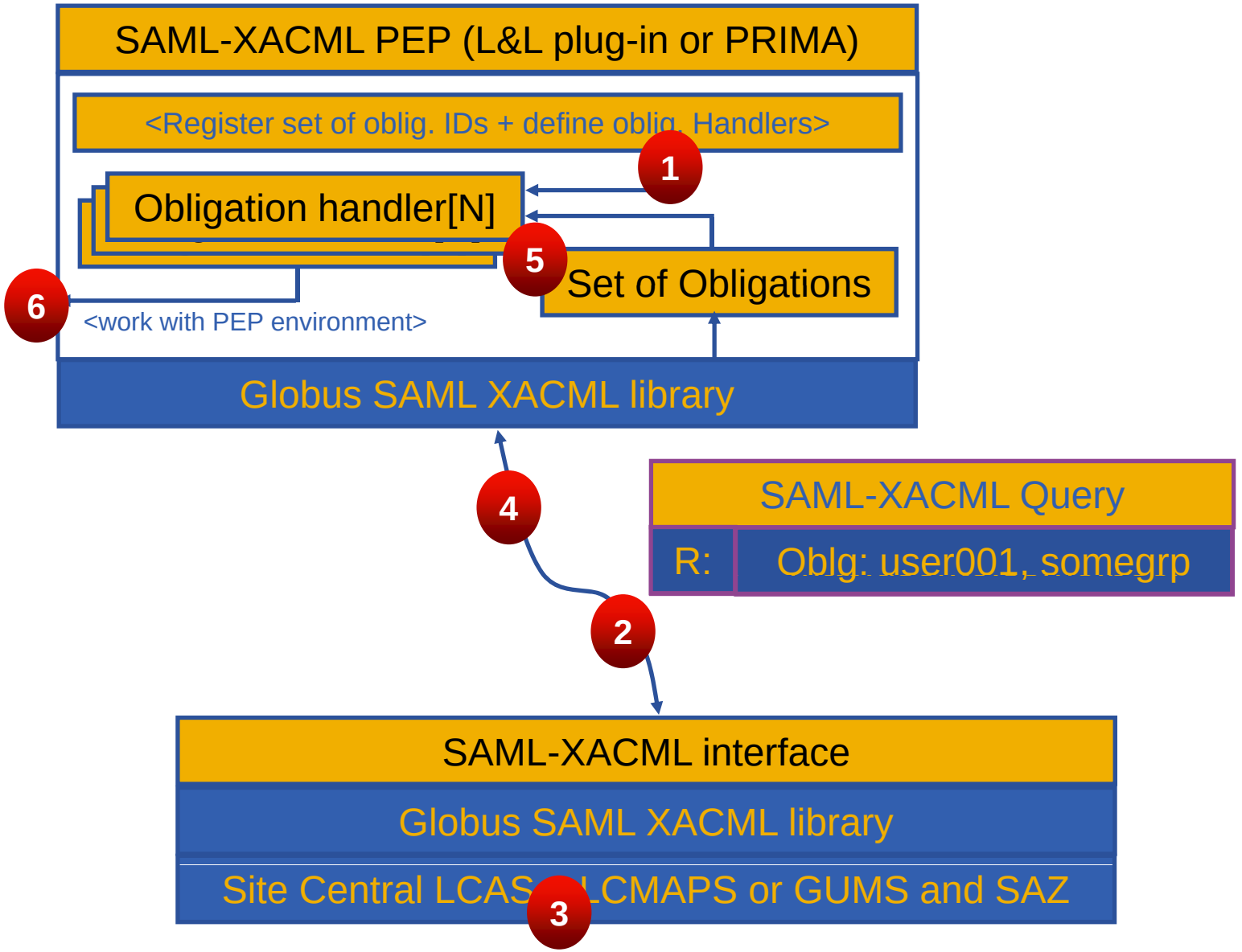
Issues with this setup:

- share/distribute the **gridmapdir** for mapping consistency
- share/distribute the **configurations** for the nodes
- share/distribute **authorization** files, like **grid/groupmapfiles** and a **blacklisting** file
- **Scaling** issues; lots of node will probably **overload** an NFS server

The big picture



How it should work (conceptual)



SAML-XACML lib requirements

- **Requirements to Globus**
  - Initial focus on Java and C environment
    - C-clients (PEP) & C-service (PDP)
      - *Prima & gPlazma*
      - *LCAS and LCMAPS plug-ins*
      - *Newly to be created Site Central service with the LCAS and LCMAPS back-end will be C-based*
    - Java initially server-side only (PDP)
      - *The GUMS server is a Java-Tomcat environment*
  - Uses TLS connection for client (PEP) / server (PDP) comm.
  - Must be able to mix our PDP and PEP implementations
  - Must be separate from the existing Globus Toolkit
    - We want the library to be lightweight and easily portable

SAML-XACML lib requirements

- **Requirements to ourselves**
  - Easy interoperation
    - Understand a common set of obligations and its attributes
  - Scalability
    - Low network traffic
    - Low overhead at the end points
  - Keeping compatibility with existing LCAS and LCMAPS plug-ins and their functionalities

Work done and decisions made

- **Understanding the scope of usage**
  - *Interesting for everybody who was not at the MWSG UCSD lunch*
- **Understanding the term *stateful PDP***
  - Note: XACML PDP is (usually only) stateless
  - Passing stateful information (the results of a pool account mapping) from the obligations' attributes
- **Discussing SAML-XACML protocol details**
  - "Using standard protocols" != "Being standards compliant"
  - Generation of the protocol stack must be reproducible
- **Using Globus SAML-XACML instead of OpenSAML**
  - Globus is committed to fix potential deviation to the specs
- **Testing the alfa version of the SAML-XACML library**
  - C and Java; Ongoing process…
- **Compilation of a tentative lists of obligations**
  - for EGEE and OSG *(next slide…)*

Tentative lists of obligations

- **EGEE Obligations:**
  - UID + GID
  - Optional multiple 2ndary GIDs
  - Optional AFS token (type string)

- **VO Services Obligations (to be checked with representative from Storage):**
  - Username (for CE)
  - UID + GID (common w/ EGEE)
  - RootPath + HomeDir (gPlazma)
  - Priorities (gPlazma)
  - File creation mask + directory creation mask

Stuff to do….

- **Other obligations (or no obligation, just a binary AuthZ decision)**

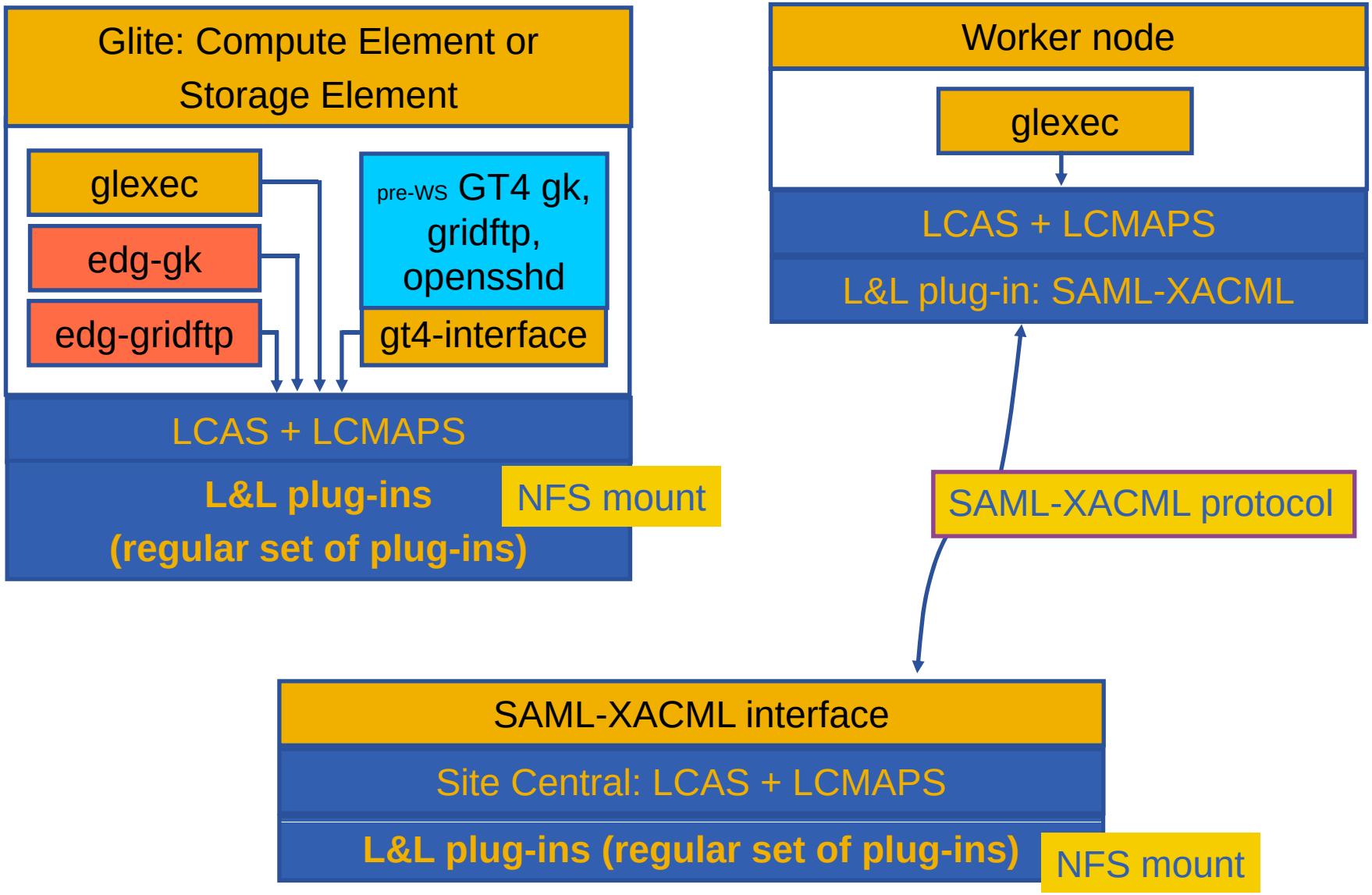
- **Reproducibility of the protocol stack, credits to:**
  - Yuri Demchenko
  - Valerio Venturi
  - Vincenzo Ciaschini
  - Alberto Forti
  - and others…

- **Timeline:**
  - Library beta: ~end of October ‘07
  - Client (LCMAPS plugin) Library beta + 1 month
  - Service (beta) Library beta + 2 months
  - Service (production) ~Q1 2008

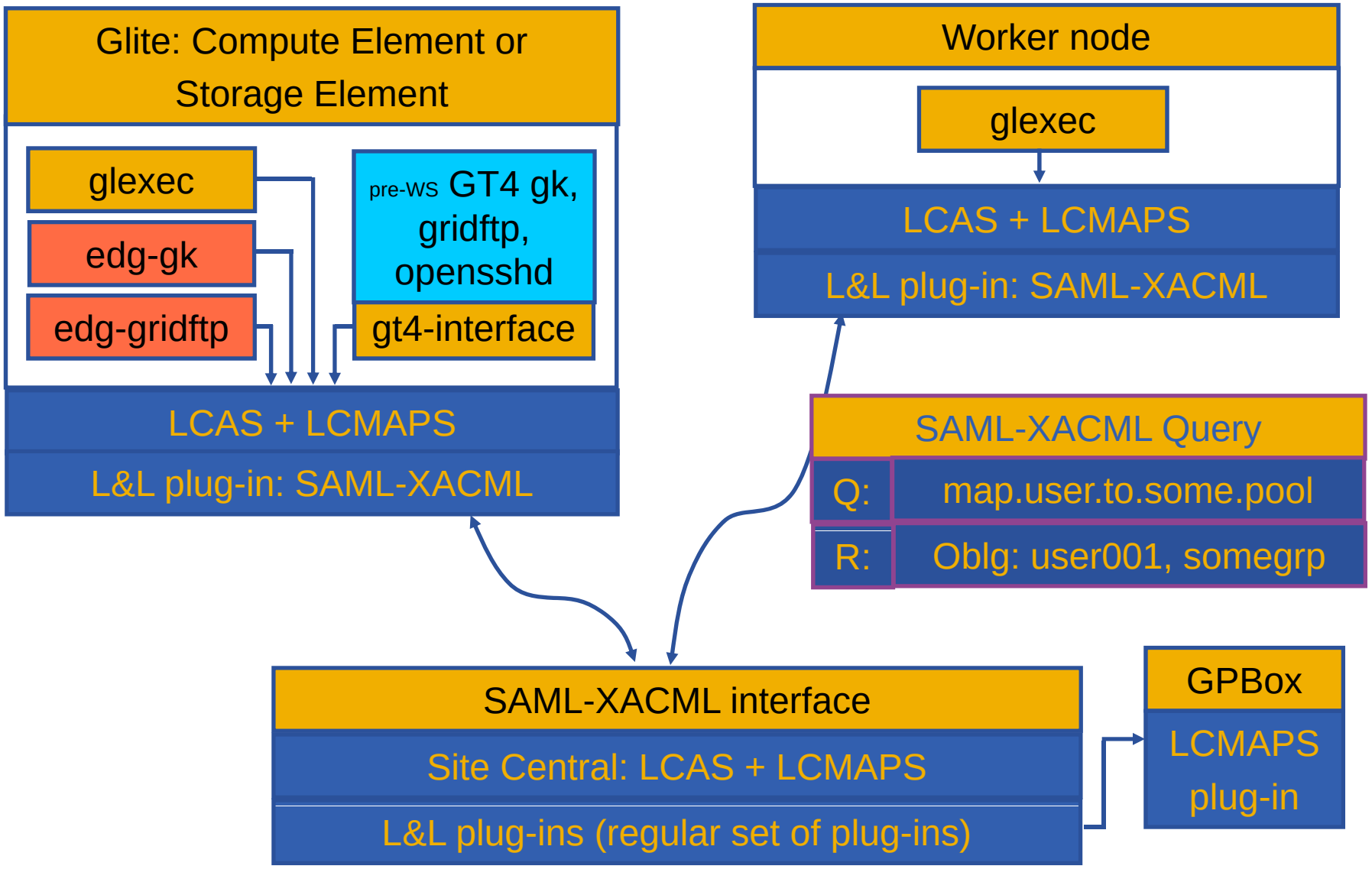
Final words

- **The site central solution allows for improved emergency response**
  - Central blacklist
  - Consistent mappings across a cluster or a site for all the services
- **The interface is going to be standards compliant with SAML2-XACML2**
- **Globus library will be the first implementation of the protocol stack, hopefully many to follow**

Alterative setups



The big picture (Glite)



The big picture (OSG)