

EGEE Fabric, Infrastructure and Middleware

Jan Aсталos
Institute of Informatics
Slovak Academy of Sciences

- **EGEE structure**
- **Infrastructure and fabric**
- **Middleware**



32 Million Euros EU funding over 2 years starting 1st April 2004

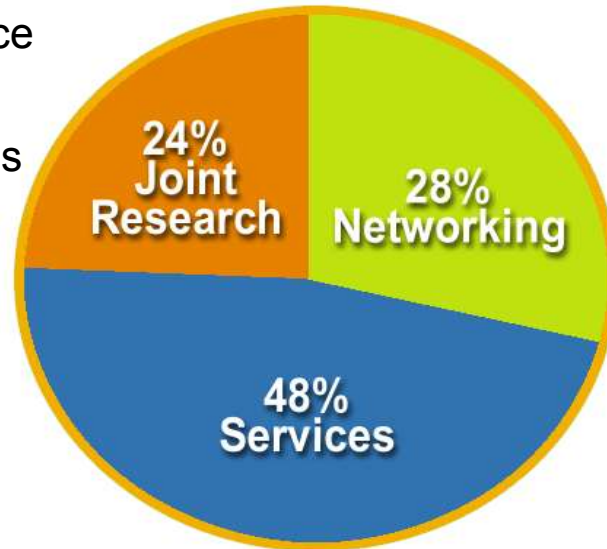
24% Joint Research

JRA1: Middleware Engineering and Integration

JRA2: Quality Assurance

JRA3: Security

JRA4: Network Services Development



48% Services

SA1: Grid Operations, Support and Management

SA2: Network Resource Provision

28% Networking

NA1: Management

NA2: Dissemination and Outreach

NA3: User Training and Education

NA4: Application Identification and Support

NA5: Policy and International Cooperation

Emphasis in EGEE is on operating a production grid and supporting the end-users

- **Core Infrastructure services:**
 - Operate essential grid services
- **Grid monitoring and control:**
 - Proactively monitor the operational state and performance,
 - Initiate corrective action
- **Middleware deployment and resource induction:**
 - Validate and deploy middleware releases
 - Set up operational procedures for new resources
- **Resource provider and user support:**
 - Coordinate the resolution of problems from both Resource Centres and users
 - Filter and aggregate problems, providing or obtaining solutions
- **Grid management:**
 - Coordinate Regional Operations Centres (ROC) and Core Infrastructure Centres (CIC)
 - Manage the relationships with resource providers via service-level agreements.
- **International collaboration:**
 - Drive collaboration with peer organisations in the U.S. and in Asia-Pacific
 - Ensure interoperability of grid infrastructures and services for cross-domain VO's
 - Participate in liaison and standards bodies in wider grid community

1 Operations Management Centre – OMC

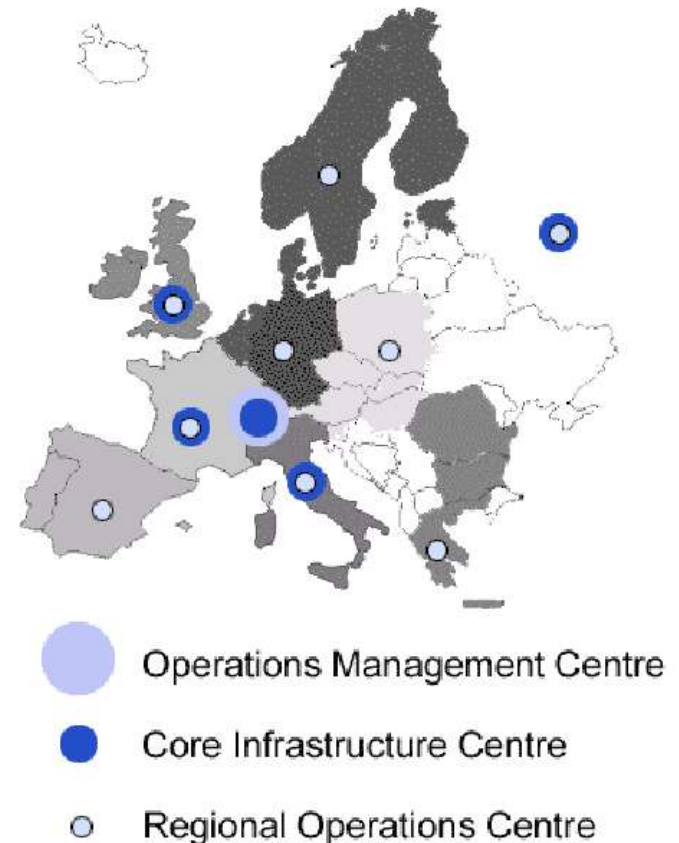
- Coordinator for CICs and for ROCs
- Team to oversee operations – problems resolved, performance targets, etc.
- Operations Advisory Group to advise on policy issues, etc.

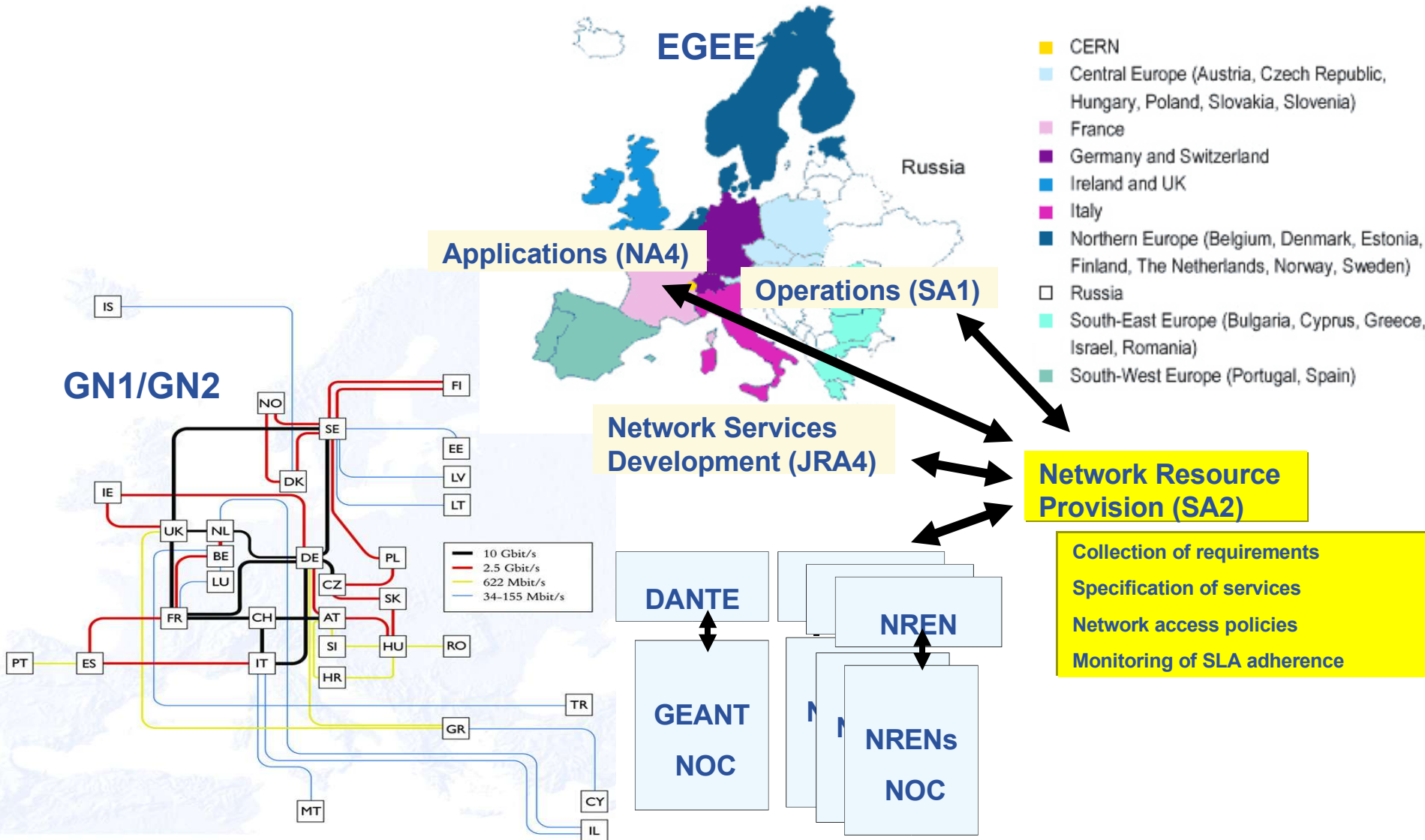
5 Core Infrastructure Centres – CIC

- Day-to-day operation management– implement operational policies defined by OMC
- Monitor state, initiate corrective actions, eventual 24x7 operation of grid infrastructure
- Provide resource and usage accounting, security incident response coordination, ensure recovery procedures

~11 Regional Operations Centres – ROC

- Provide front-line support to users and resource centres
- Support new resource centres joining EGEE in the regions





| Region | CPU nodes Month 1 | Disk (TB) Month 1 | CPU Nodes Month 15 | Disk (TB) Month 15 |
|--------------------------|----------------------|----------------------|-----------------------|-----------------------|
| CERN | 900 | 140 | 1800 | 310 |
| UK + Ireland | 100 | 25 | 2200 | 300 |
| France | 400 | 15 | 895 | 50 |
| Italy | 553 | 60.6 | 679 | 67.2 |
| North | 200 | 20 | 2000 | 50 |
| South West | 250 | 10 | 250 | 10 |
| Germany + Switzerland | 100 | 2 | 400 | 67 |
| South East | 146 | 7 | 322 | 14 |
| Central Europe | 385 | 15 | 730 | 32 |
| Russia | 50 | 7 | 152 | 36 |
| Totals | 3084 | 302 | 8768 | 936 |

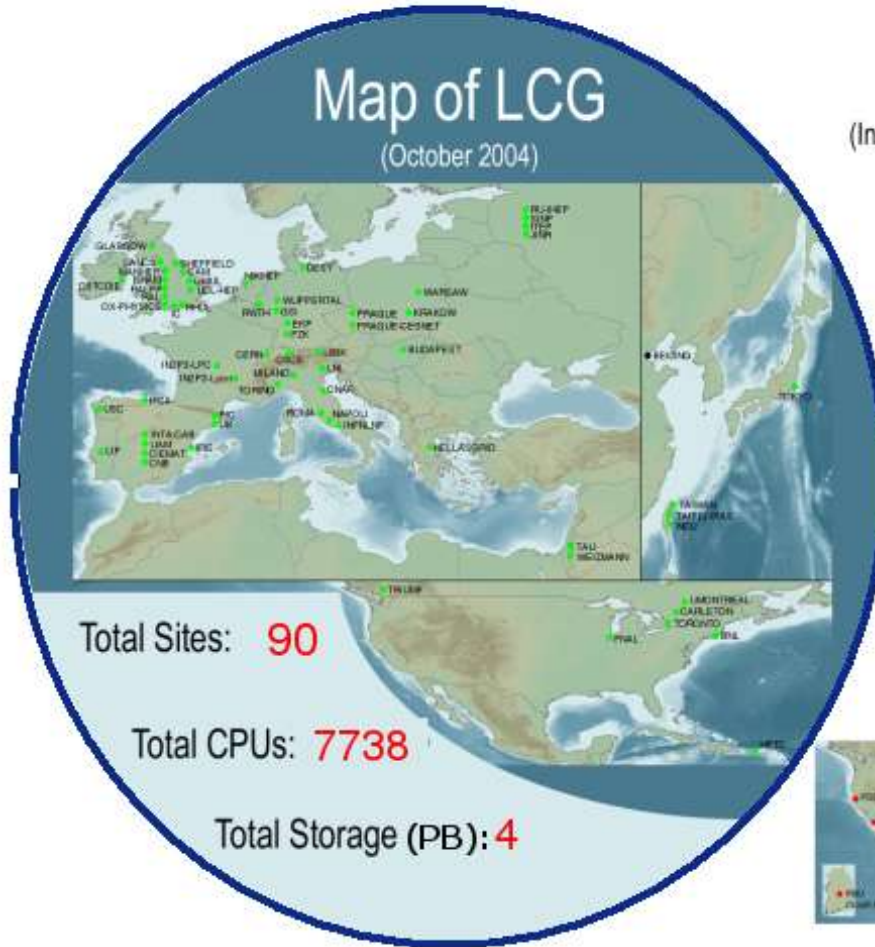
Month 24

resource centres

10

20

50

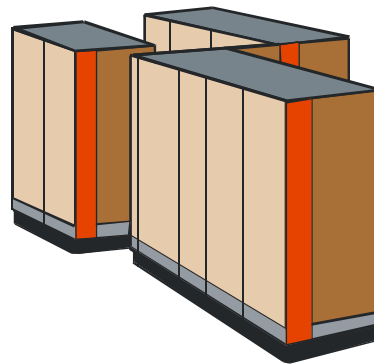


<http://goc.grid-support.ac.uk/lcg2>

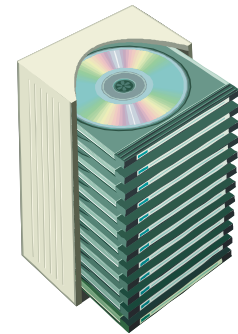
- **Building blocks of the Grid**
 - Computers, storage systems, networks
- **Logical machine types:**



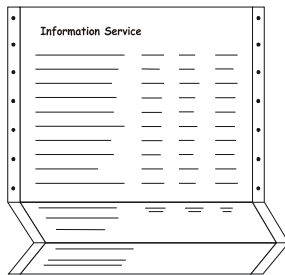
User Interface (UI)



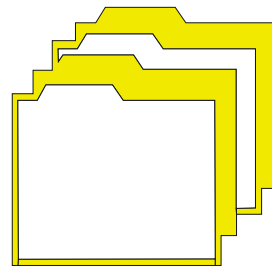
Computing Element (CE)



Storage Element (SE)



Information Service (IS)

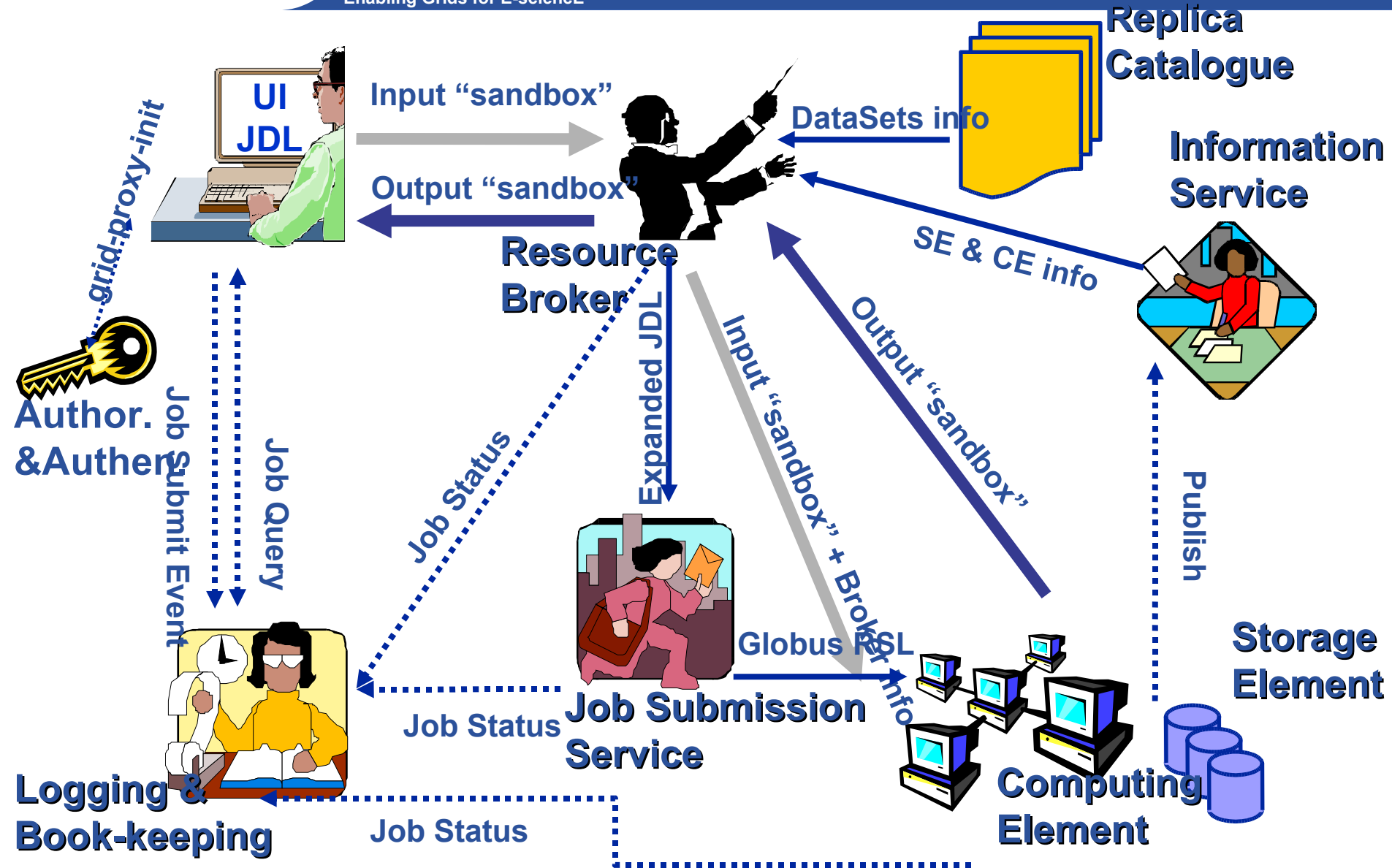


Replica Catalog (RC, RLS)



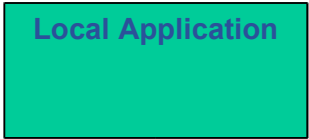
Resource Broker (RB)

The lifecycle of an EGEE job

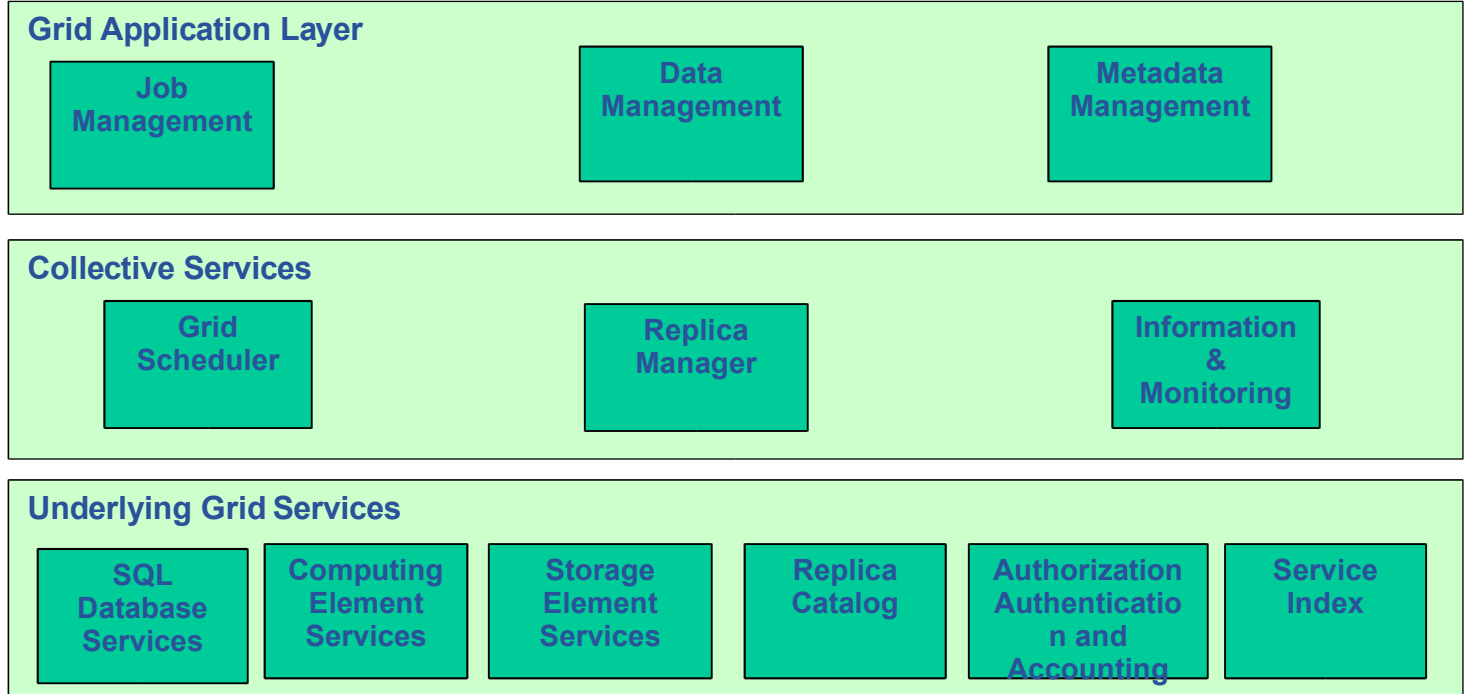


- **EGEE middleware built upon the VDT toolkit provides generic Grid services:**
 - Information
 - Job submission
 - Data management
 - Security
 - Logging
 - Monitoring
- **EGEE supports computation and data storage by multiple virtual organisations**

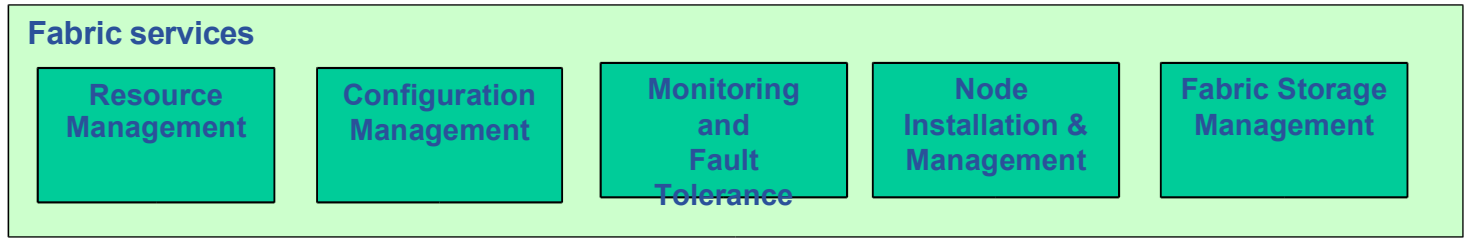
APPLICATIONS

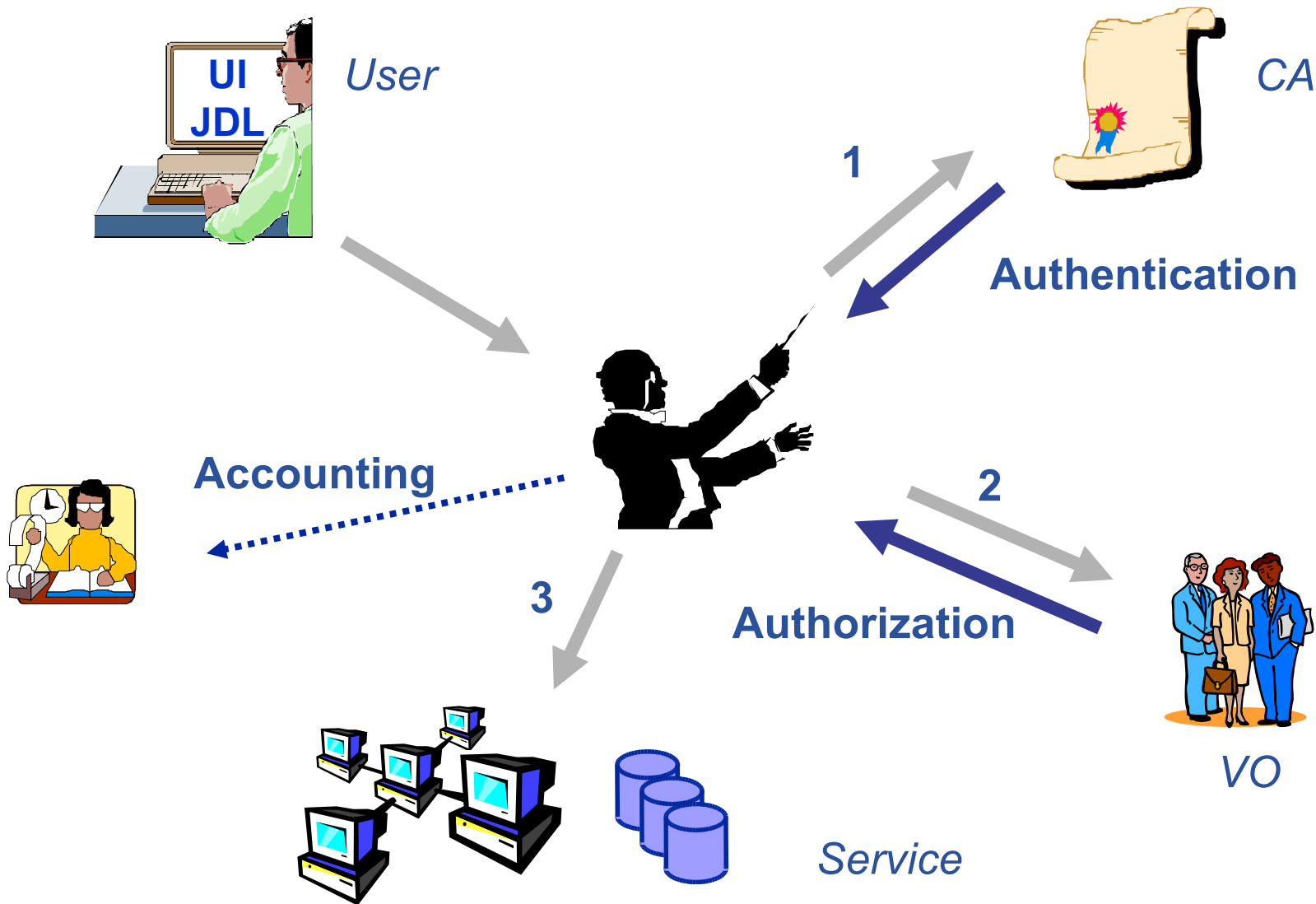


MIDDLEWARE

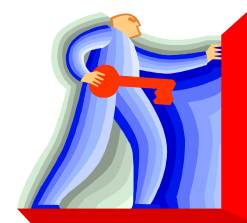


FABRIC



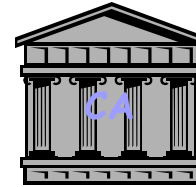


- **Distribution of resources: secure access is a basic requirement**
 - secure communication
 - security across organisational boundaries
 - single “sign-on” for users of the Grid
- **Two basic concepts:**
 - **Authentication: *Who am I?***
 - “Equivalent” to a pass port, ID card etc.
 - Certificates
 - **Authorisation: *What can I do?***
 - Certain permissions, duties etc.
 - Virtual organizations



- **In industry, several security standards exist:**
 - **Public Key Infrastructure (PKI)**
 - PKI keys
 - SPKI keys (focus on authorisation rather than certificates)
 - RSA
 - **Secure Socket Layer (SSL)**
 - SSH keys
 - **Kerberos**
- **Need for a common security standard for Grid services**
 - Above standards do not meet all Grid requirements (e.g. delegation, single sign-on etc.)
- **Grid community mainly uses X.509 PKI for the Internet**
 - Well established and widely used (also for www, e-mail, etc.)

Certificate Authority



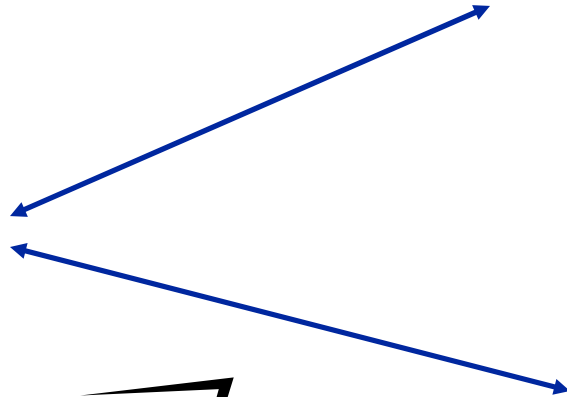
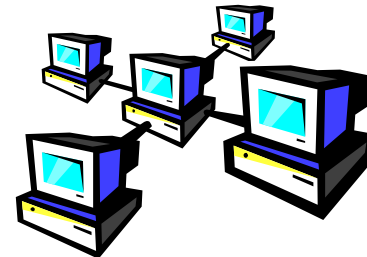
User



Public key
Private key
certificate

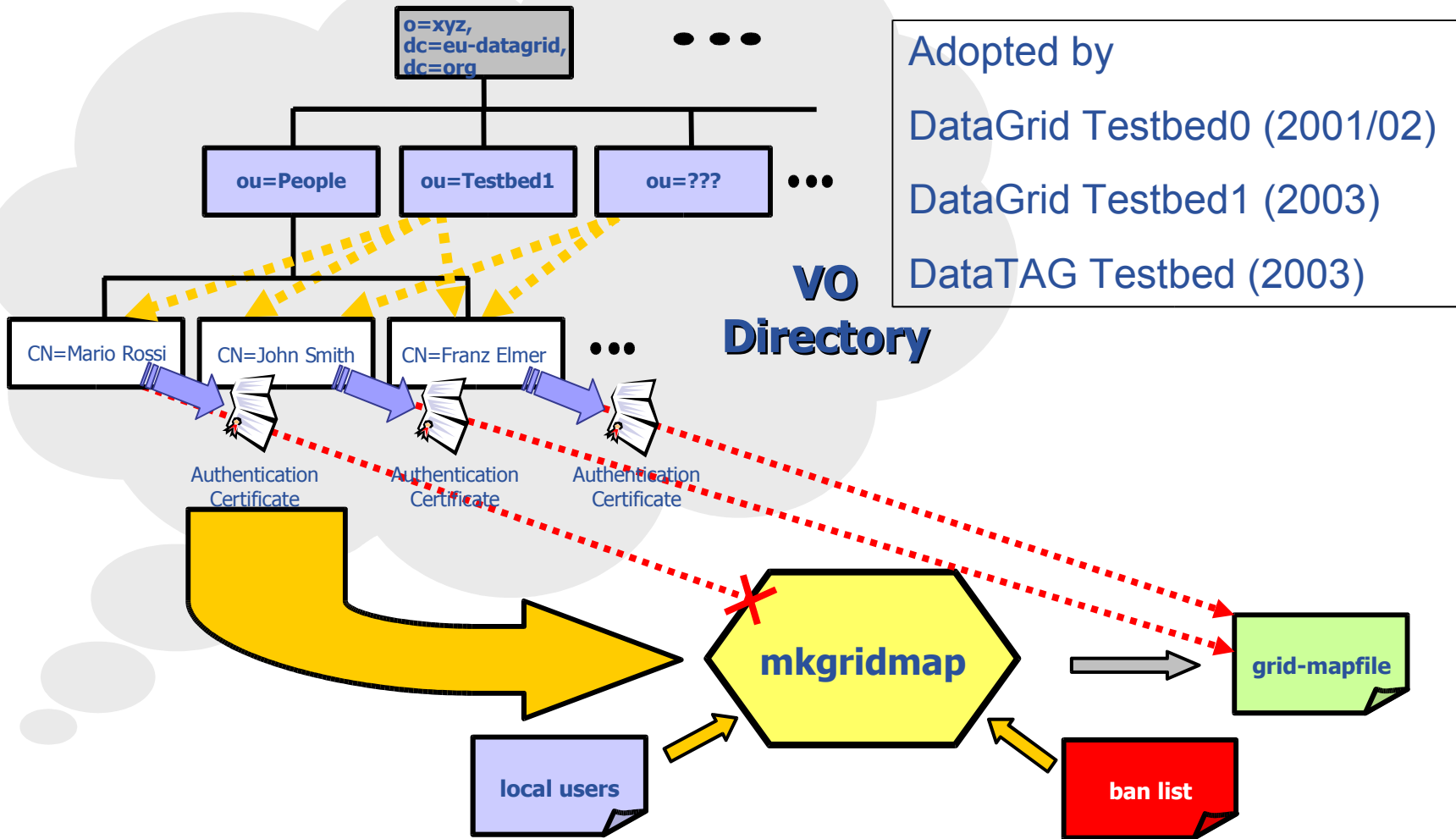


Resource
(site offering services)



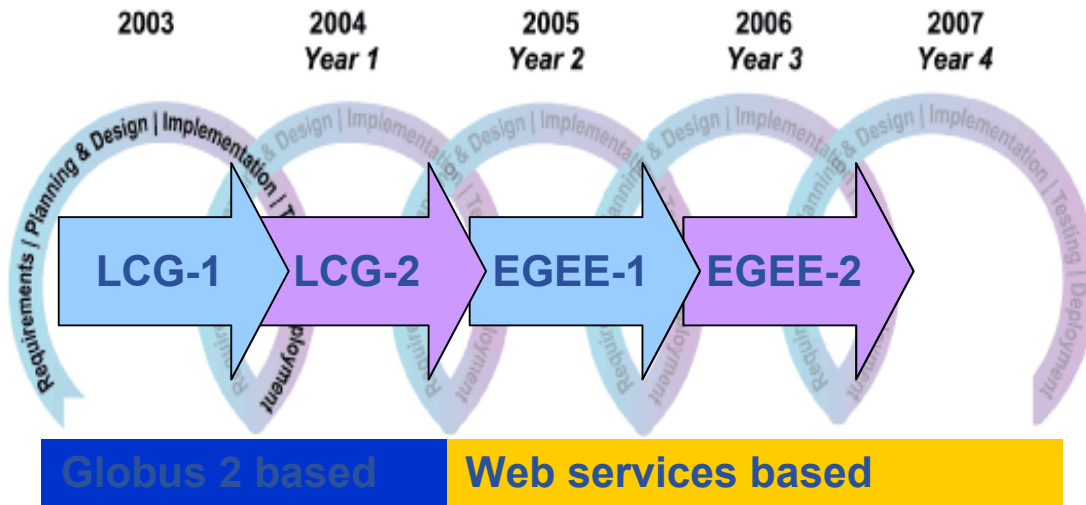
- **Globus Toolkit™** proposed and implements the **Grid Security Infrastructure (GSI)**
 - Protocols and APIs to address Grid security needs
- **GSI protocols extend standard public key protocols**
 - Standards: X.509 & SSL/TLS
 - Extensions: X.509 Proxy Certificates (single sign-on) & Delegation
- **GSI extends standard GSS-API (Generic Security Service)**
 - The GSS-API is the IETF standard for adding authentication, delegation, message integrity, and message confidentiality to applications.
- **Proxy Certificate:**
 - Short term, restricted certificate that is derived from a long-term X.509 certificate
 - Signed by the normal end entity cert, or by another proxy
 - Allows a process to act on behalf of a user
 - Not encrypted and thus needs to be securely managed by file system

- Detailed **user rights** need to be centrally managed and assigned
 - User can have certain group membership and roles
- **Involved parties:**
 - **Resource providers** (RP, provides access to the resource)
 - keep full control on access rights
 - traceability user level (not VO level)
 - **Virtual Organisation** (VO) of the user (member of a certain group should have same access rights independent of resource)
- **Agreement required between resource providers and VO**
 - RPs evaluate authorisation granted by VO to a user and map into local credentials to access resources
- **Need tool to manage membership for large VOs (10,000 users)**



- **Hardware:**
 - EDG Information Service
 - Information Providers
- **Data:**
 - Replica Catalog
 - LDAP (release 1.4)
 - RLS (release 2.0)
- **Software & Services:**
 - EDG Grid Services:
 - Information Service
 - *MDS*
 - *R-GMA*
 - Application Services:
 - Currently only EDG applications directly supported
- **Machine Types:**
- **Information Service (IS)**
 - Top level MDS
 - R-GMA registry
- **Replica Catalog (RC, RLS)**

- From day 1 (1st April 2004)**
 Production grid service based on the **LCG infrastructure** running **LCG-2** grid middleware
 LCG-2 will be maintained until the new generation has proven itself (fallback solution)
- In parallel develop a “next generation” grid facility (www.glite.org)**
 Produce a new set of grid services according to evolving standards (Web Services)
 Run a development service providing early access for evaluation purposes



- **The EGEE Grid requires resources, an infrastructure and middleware that allows for:**
 - Authentication and Authorization
 - Information services
 - Job and Data Management
 - Monitoring and fault recovery
- **We have seen the main components of the EGEE Grid Service and Organization**
 - The Grid Operations Management Structure monitors and controls the overall functionality
 - EGEE is VO based
- **The EGEE tutorials ensure training at all levels with hands-on on the GILDA dedicated testbed**