

An overview of the EGEE infrastructure and middleware

Flavia Donno
CERN



EGEE is funded by the European Union under contract IST-2003-508833

Acknowledgement

- This talk is based on the work of many people:
 - the EDG developers
 - the EDG training team
 - the NeSC training team

Goals

- To introduce the major components of the EGEE grid
 - Infrastructure and fabric
 - Middleware
 - Organisation

Overview

- Enabling Grid Computing:
fabric + infrastructure + middleware
 - Authentication and Authorization
 - Information services
 - Other Grid services
 - The major components of the infrastructure
 - The software stack
- EGEE grid organisation

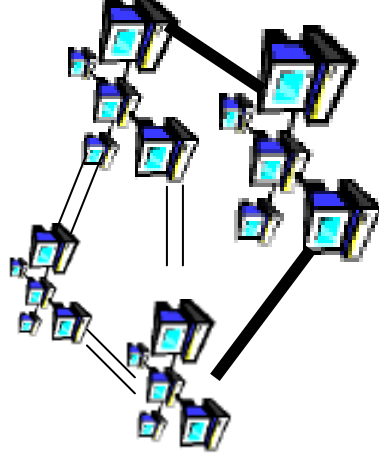
What are the characteristics of a Grid system?

Numerous Resources

**Ownership by Mutually
Distrustful Organizations
& Individuals**

**Different Security
Requirements
& Policies Required**

**Potentially Faulty
Resources**



**Connected by
Heterogeneous,
Multi-Level Networks**

**Different Resource
Management
Policies**

**Geographically
Separated**

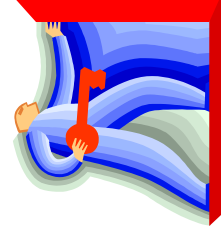
**Resources are
Heterogeneous**

How do I login on the Grid ?

- 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.



- **Authorisation: *What can I do?***
 - Certain permissions, duties etc.

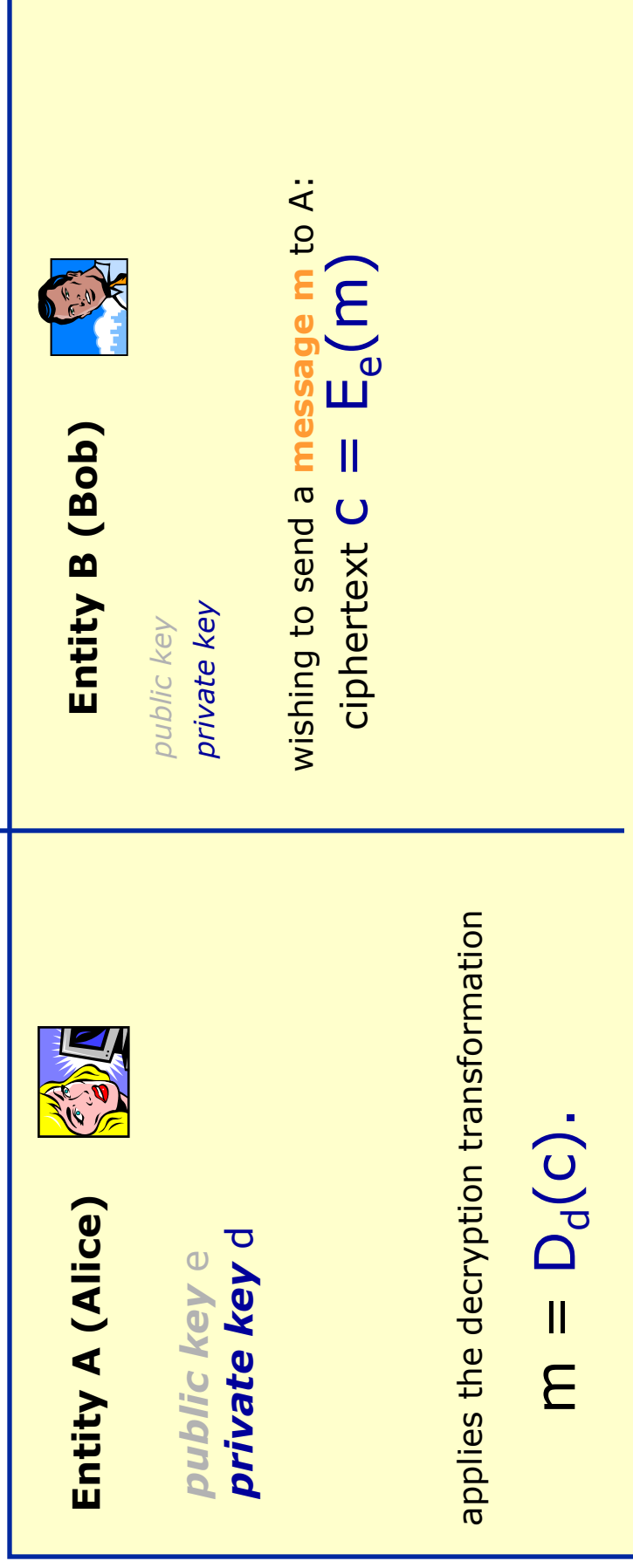


Security in the Grid

- 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.)

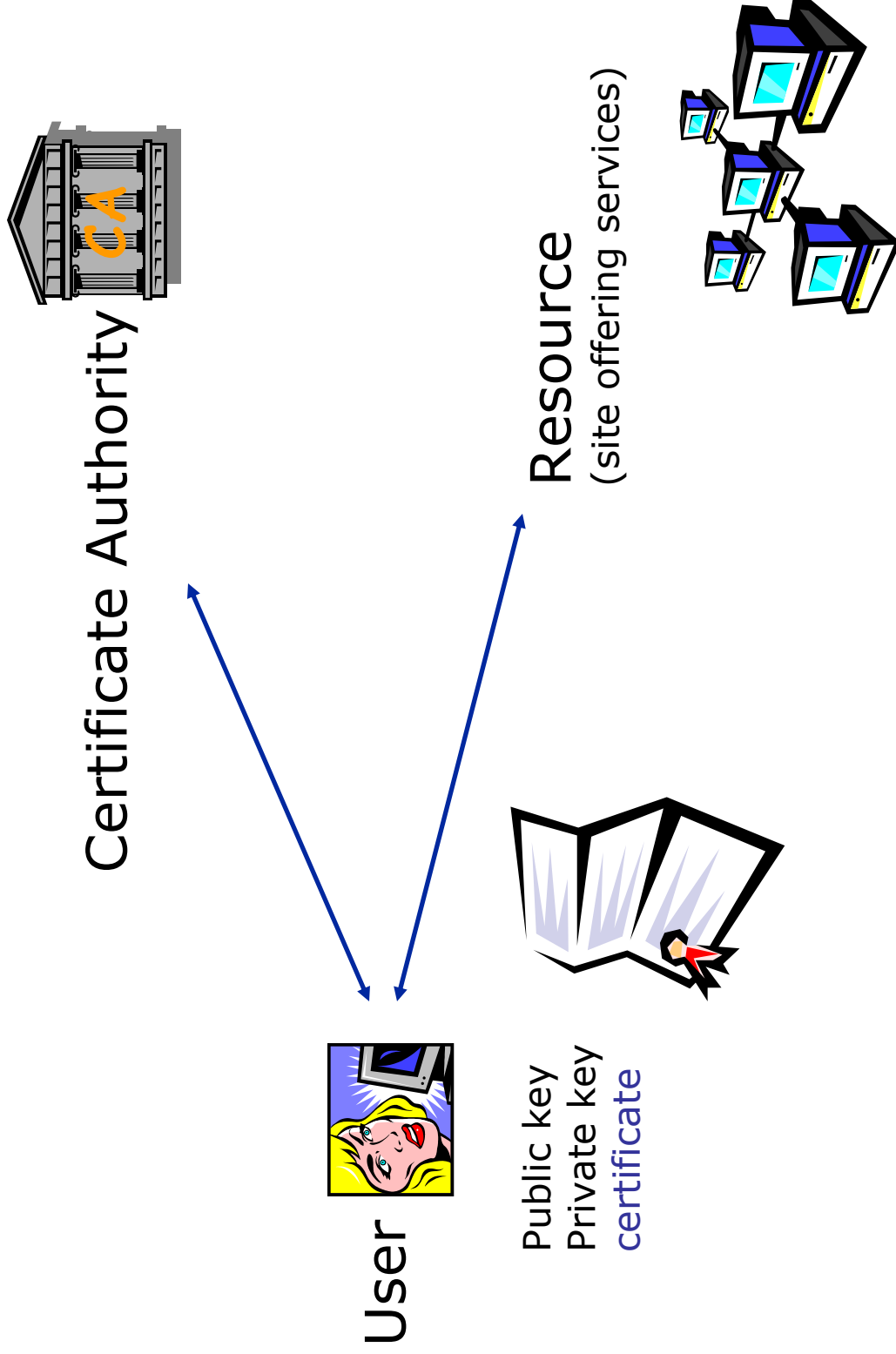
PKI – Basic overview

- Public Key Infrastructure (also called asymmetric cryptography)
- One primary advantage: it is generally easier than distributing secret keys securely, as required in symmetric keys



encryption transformation E_e
decryption transformation D_d

Involved entities



X.509 alias ISO/IEC/ITU 9594-9

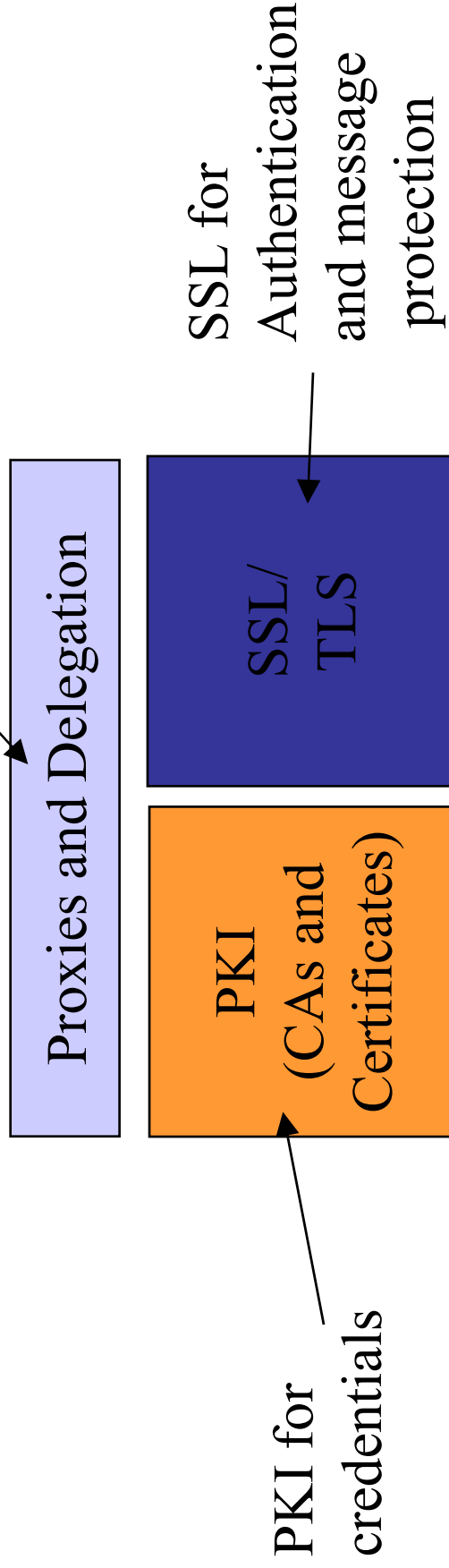
- X.509 is ITU Standard:
 - ITU-T Recommendation X.509 (1997 E). Information technology - Open Systems Interconnection - The Directory: **Authentication Framework**
 - Defines a **certificate format** (originally based on X.500 Directory Access Protocol)
 - Latest standard: X.509 version 3 certificate format
- X.509 certificate includes:
 - User identification (someone's subject name)
 - Public key
 - A "signature" from a Certificate Authority (CA) that:
 - Proves that the certificate came from the CA.
 - Vouches for the subject name
 - Vouches for the binding of the public key to the subject

Grid Security Infrastructure (GSI)

- 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

GSI General Overview

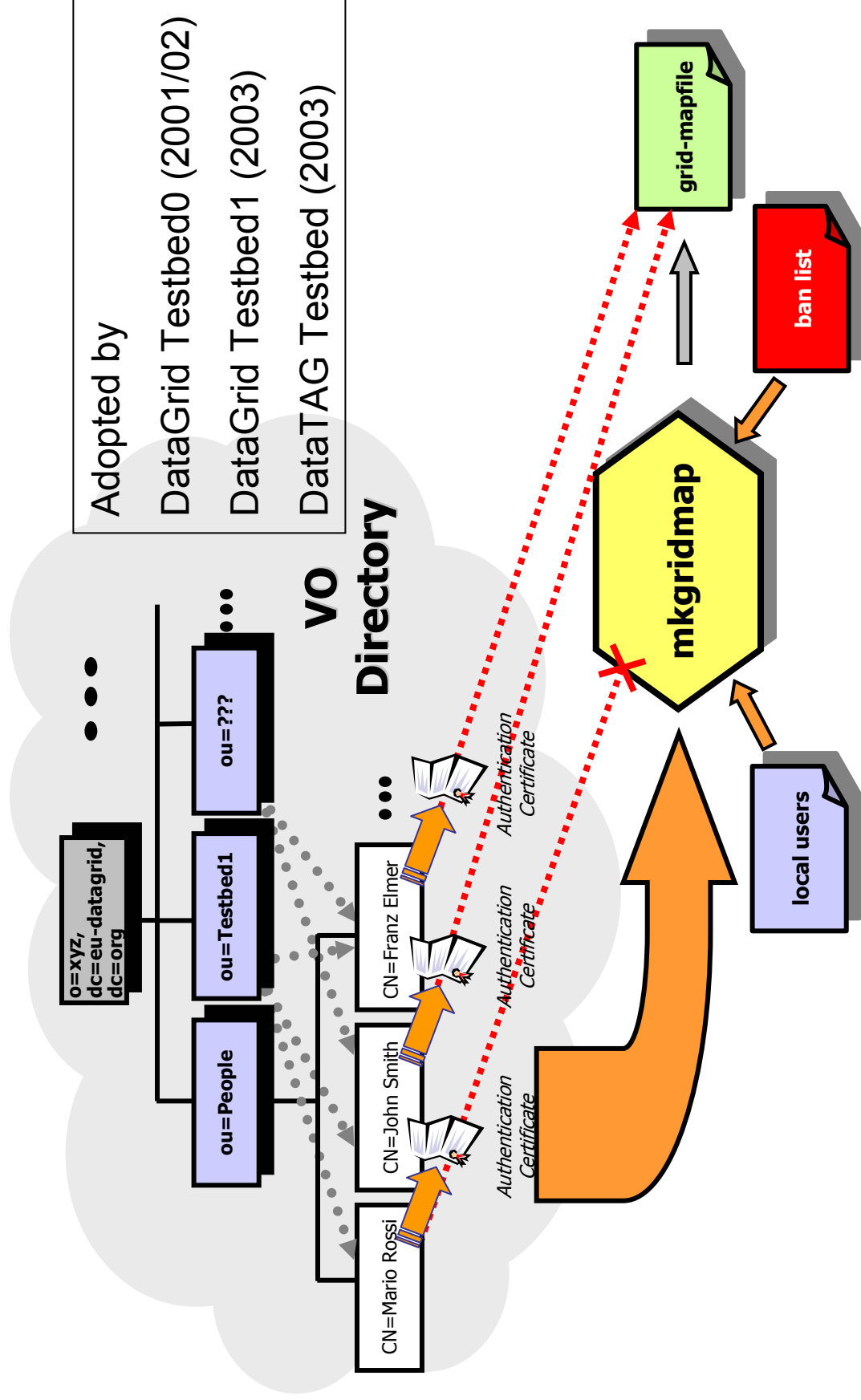
Proxies and delegation (GSI
Extensions) for secure single
Sign-on



Authorisation Requirements

- 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)

Example: VO-LDAP server for Authorisation



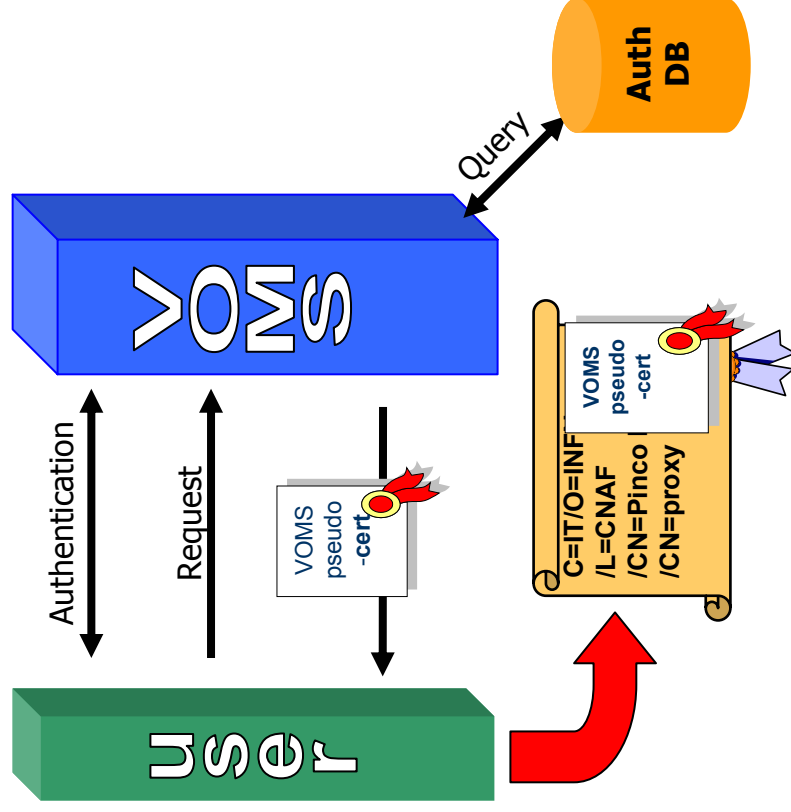
Improvements/Extensions

- ◆ Community Authorisation Service (CAS)
 - Provided by the Globus Alliance
 - Original concepts

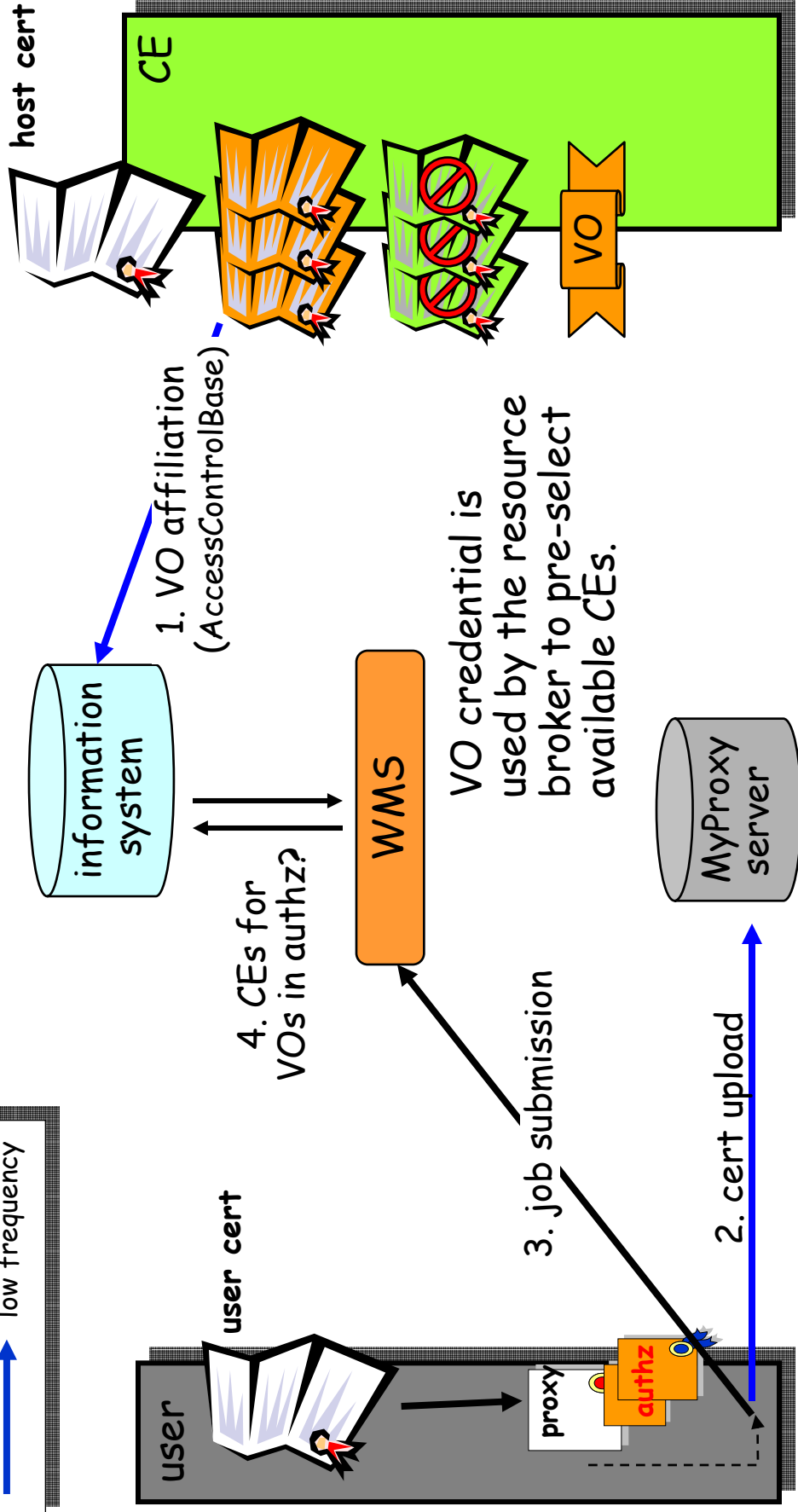
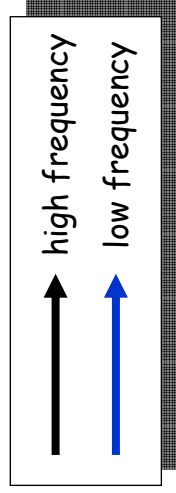
- ◆ Virtual Organisation Membership Service (VOMS)
 - Provided by EU DataGrid and DataTAG projects
 - Some different concepts

VOMS Operations

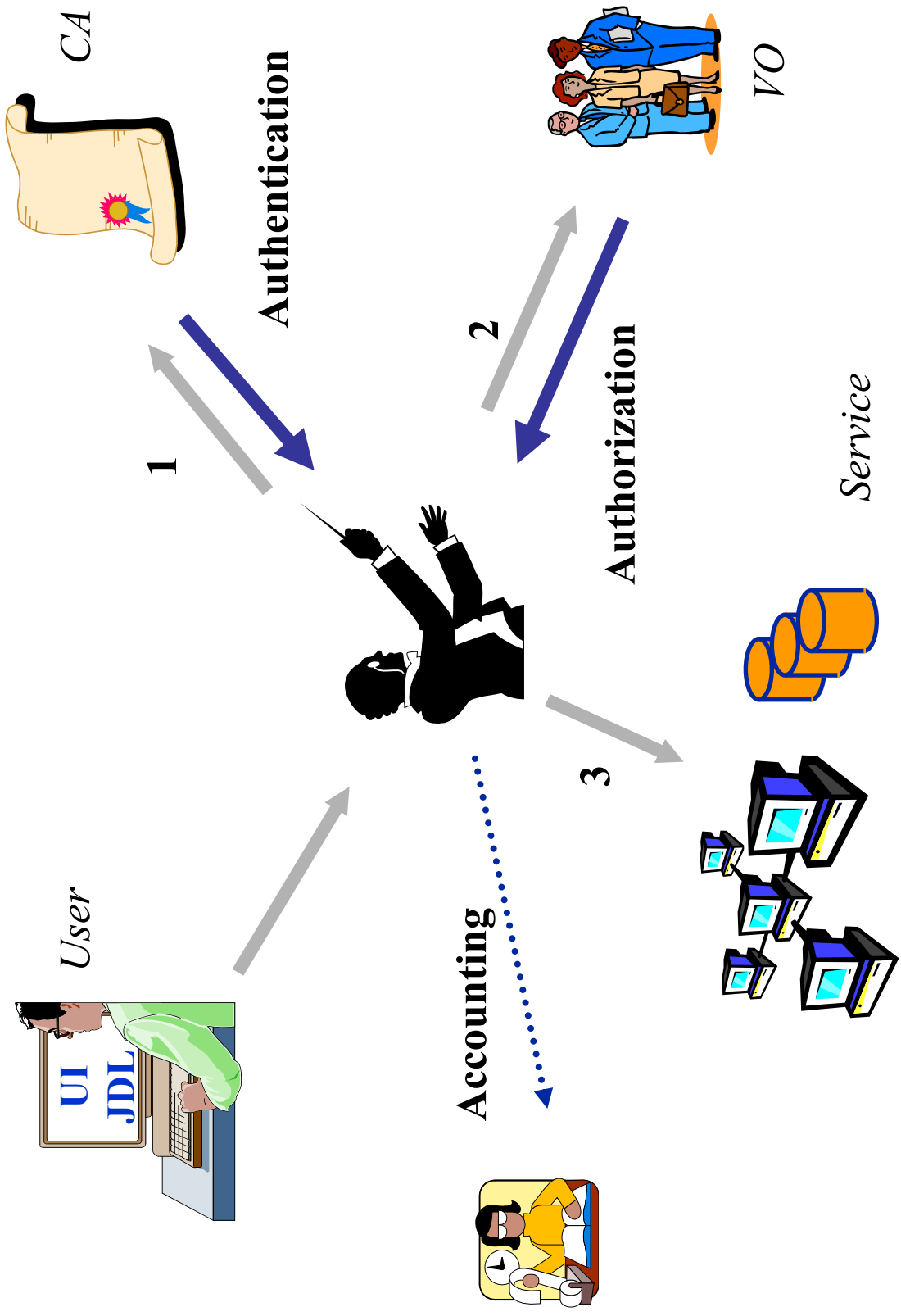
1. Mutual authentication Client-Server
 - Secure communication channel via standard Globus API
2. Client sends request to Server
3. Server checks correctness of request
4. Server sends back the required info (signed by itself) in a "Pseudo-Certificate"
5. Client checks the validity of the info received
6. Optionally: [Client repeats process for other VOMS's]
7. Client creates proxy certificates containing all the info received into a (non critical) extension
8. Client may add user-supplied auth. info (kerberos tickets, etc...)



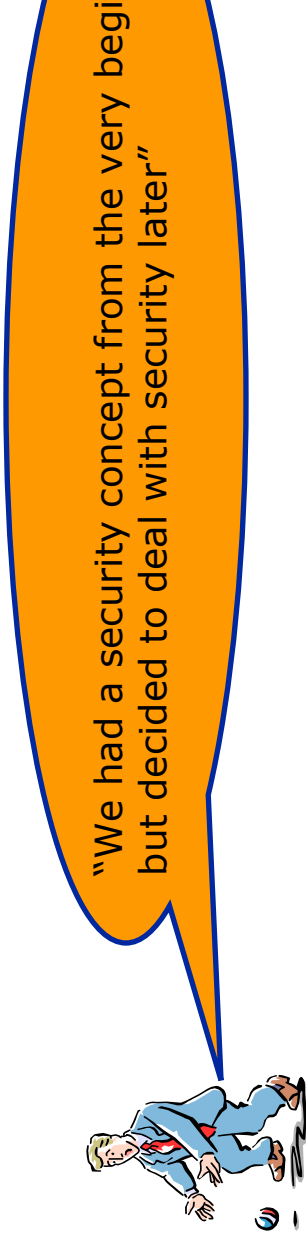
Job Submission using VOMS



Authentication and Authorization



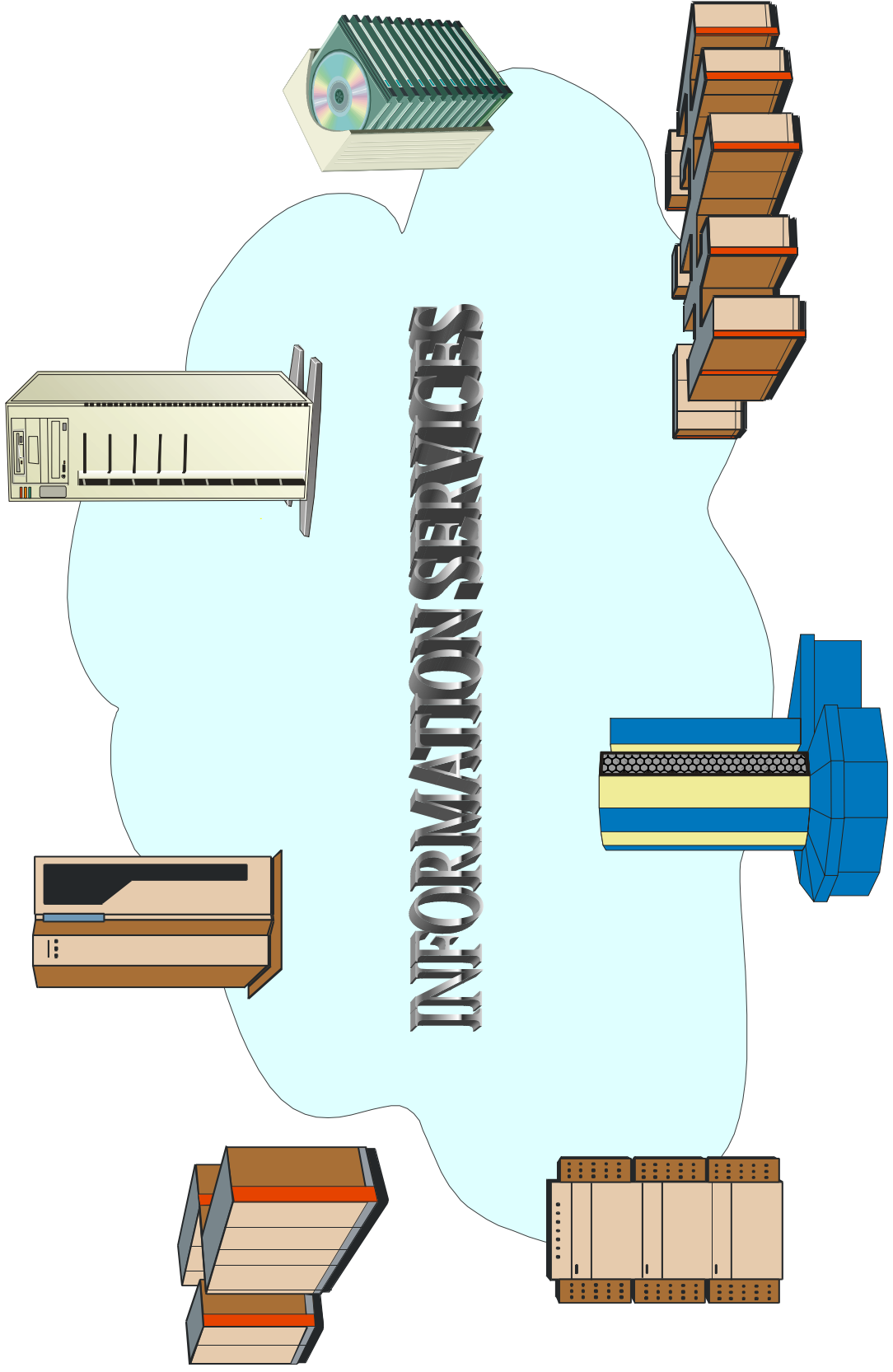
Security Summary

- Security is important for Grid middleware:
 - In particular in commercial use
 - Security solutions need to be integrated from the very beginning
- 
- Grid security relies on PKI
 - Requires: authentication & authorization
 - Basic entities:
 - Users – CA (Certificate Authorities) – Resource Providers

The middleware

- 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

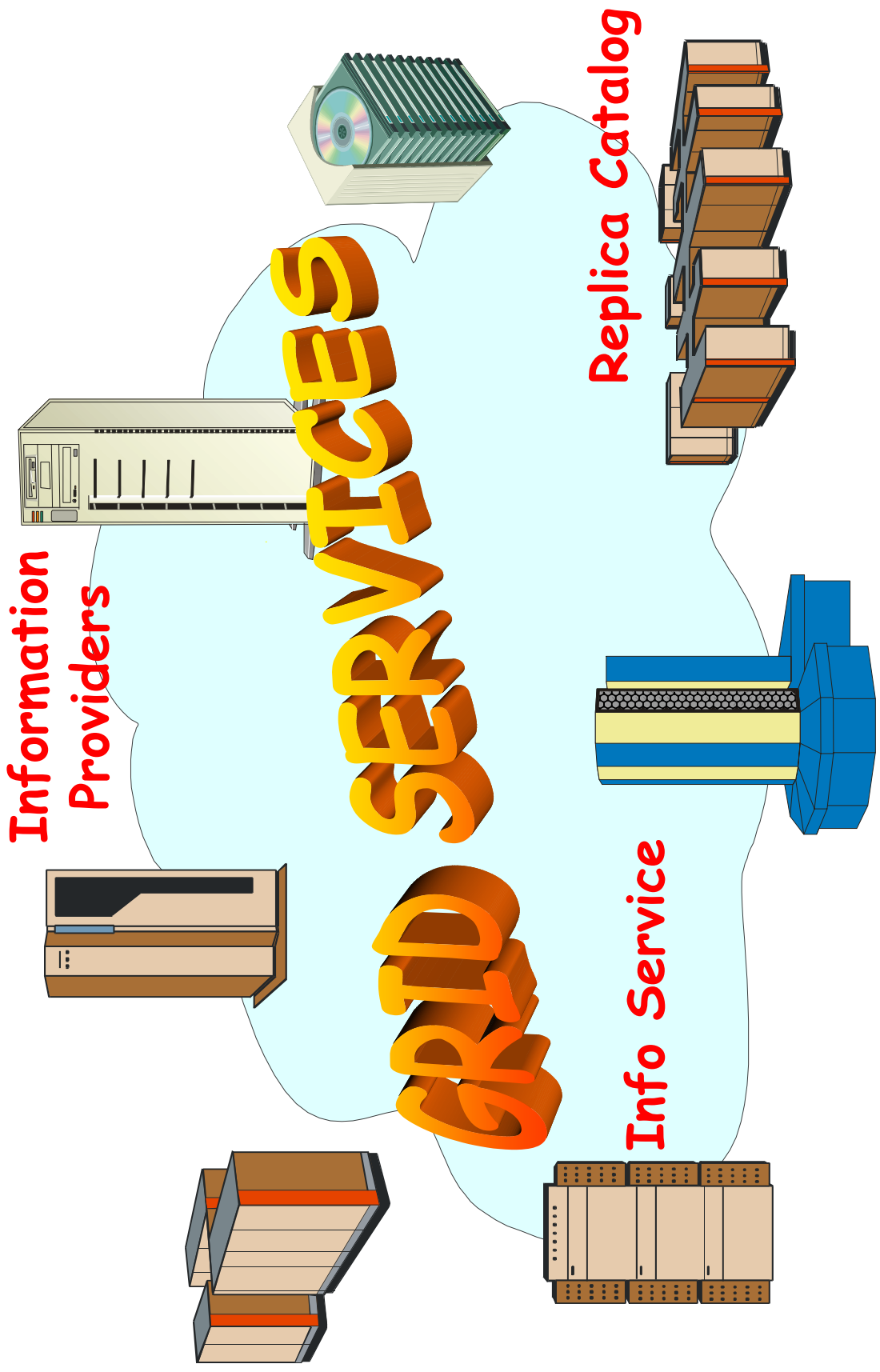
Situation on a Grid



Features of a grid information system

- Provides information on both:
 - The Grid itself
 - Mainly for the middleware packages
 - The user may query it to understand the status of the Grid
 - Grid applications
 - For users
- Flexible infrastructure
 - Able to cope with nodes in a distributed environment with an unreliable network
 - Dynamic addition and deletion of information producers
 - Security system able to address the access to information at a fine level of granularity
 - Allow new data types to be defined
 - Scalable
 - Good performance
 - Standards based

Situation on a Grid Cont'd



Information Services

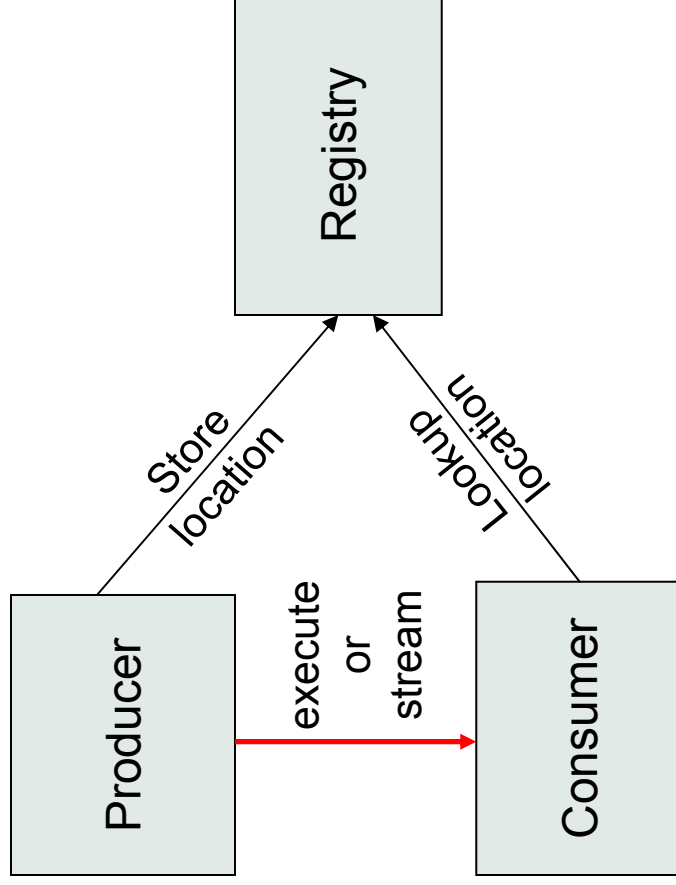
- **Hardware:**
 - EDG Information Service
 - Information Providers
 - **Data:**
 - Replica Catalog
 - LDAP (release 1.4)
 - RLS (release 2.0)
 - **Software & Services:**
 - EDG Grid Services:
 - Information Service
 - MDS
 - R-GMA
 - Application Services:
 - Currently only EDG applications directly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

EDG Information Providers

- EDG information providers
 - Software that provides information about resources and infrastructure
 - Provided by the developer of a service or the responsible for the resource
- The information providers produce data in LDIF format
 - This is a legacy from when Globus MDS was the primary information system (LDAP based)
- R-GMA publishes the data
 - Gin (gadget in) is used to invoke the information provider scripts and publish via StreamProducers
 - Gout (gadget out) republishes the data via a LatestProducer and then to an OpenLDAP database
 - This is to provide backwards compatibility during the transition from MDS to R-GMA

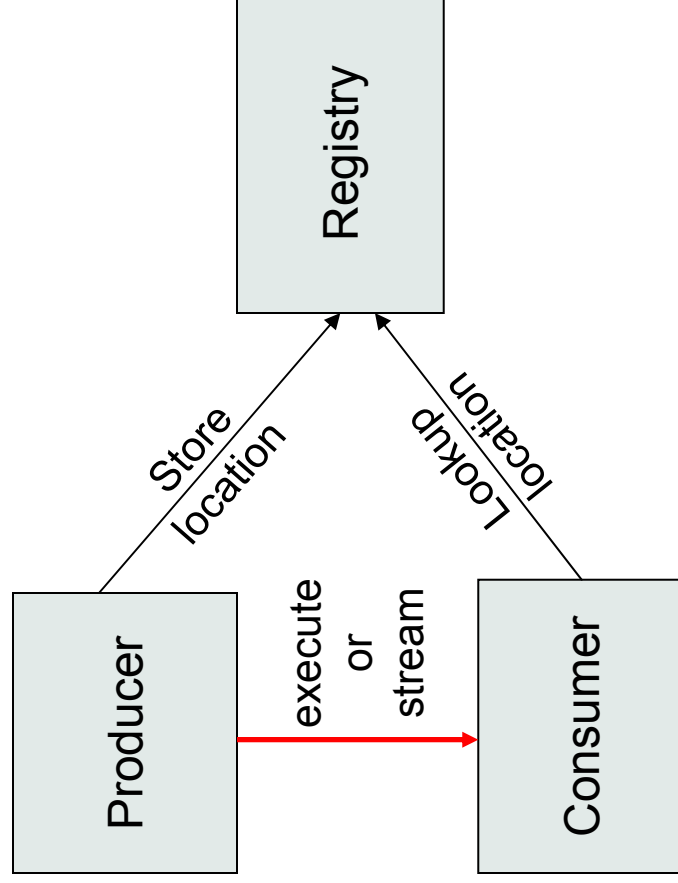
GMA

- From GGF
- Very simple model
- Does not define:
 - Data model
 - Data transfer mechanism
 - Registry implementation



R-GMA

- Use the GMA from GGF
- A relational implementation
 - Powerful data model and query language
 - All data modelled as tables
 - SQL can express most queries in one expression
- Applied to both information and monitoring
- **Creates impression that you have one RDBMS per VO**



Main EDG Grid Services

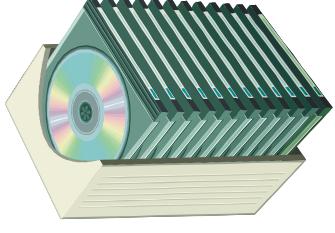
- Authentication & Authorization
- Job submission service
 - Resource Broker
- Replica Management
 - EDG-Replica-Manager
 - Mass storage system support
- Logging & Bookkeeping
- Monitoring

Main Logical Machine Types

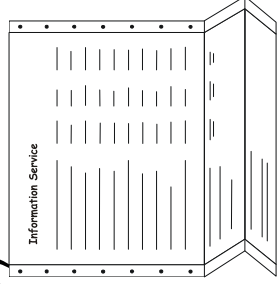
- User Interface (UI)



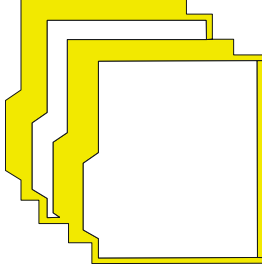
- Storage Element (SE)



- Information Service (IS)

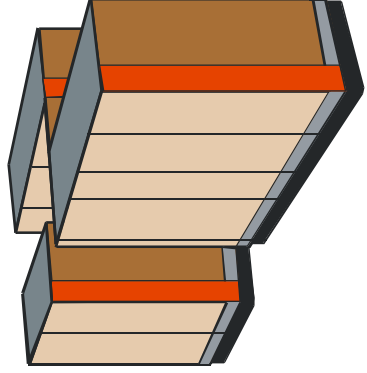


- Replica Catalog (RC, RLS)

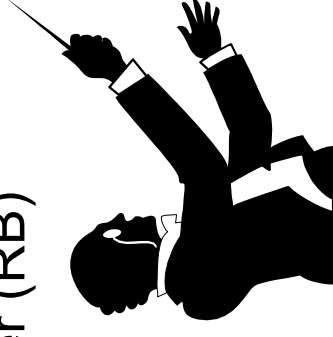


- Computing Element (CE)

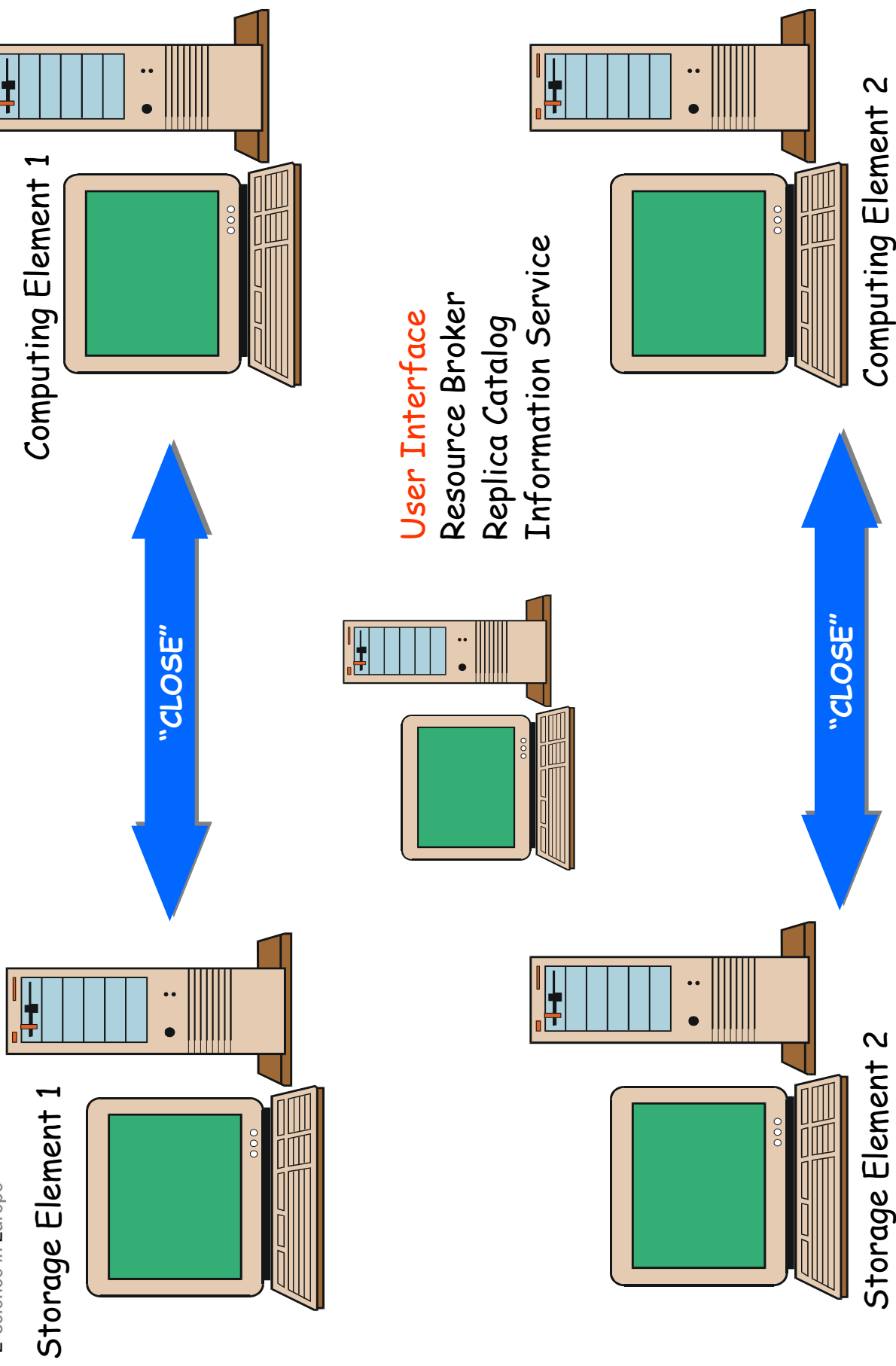
- Frontend Node
- Worker Nodes (WN)



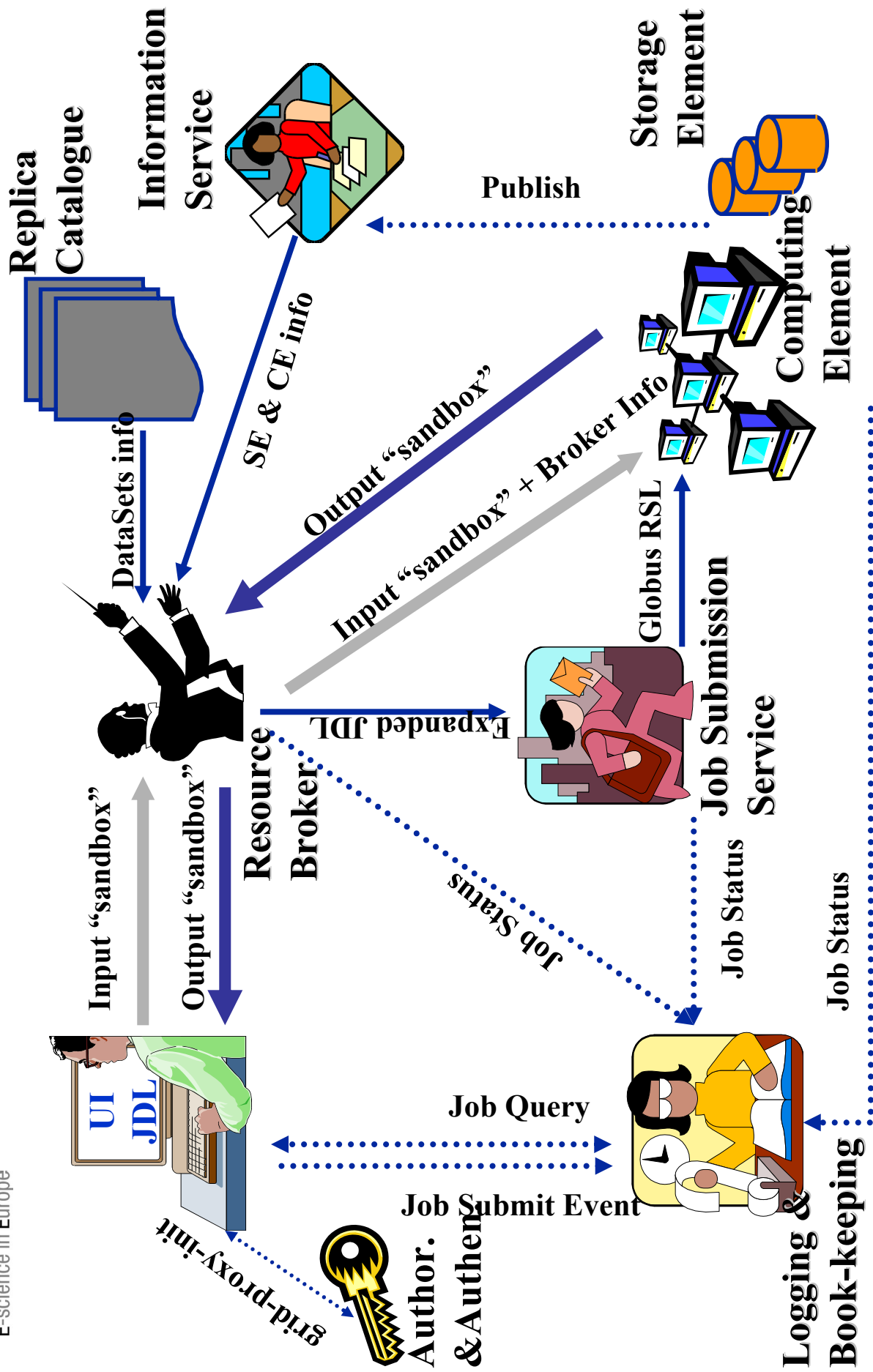
- Resource Broker (RB)



A Simple Testbed Configuration



The lifecycle of an EGEE job



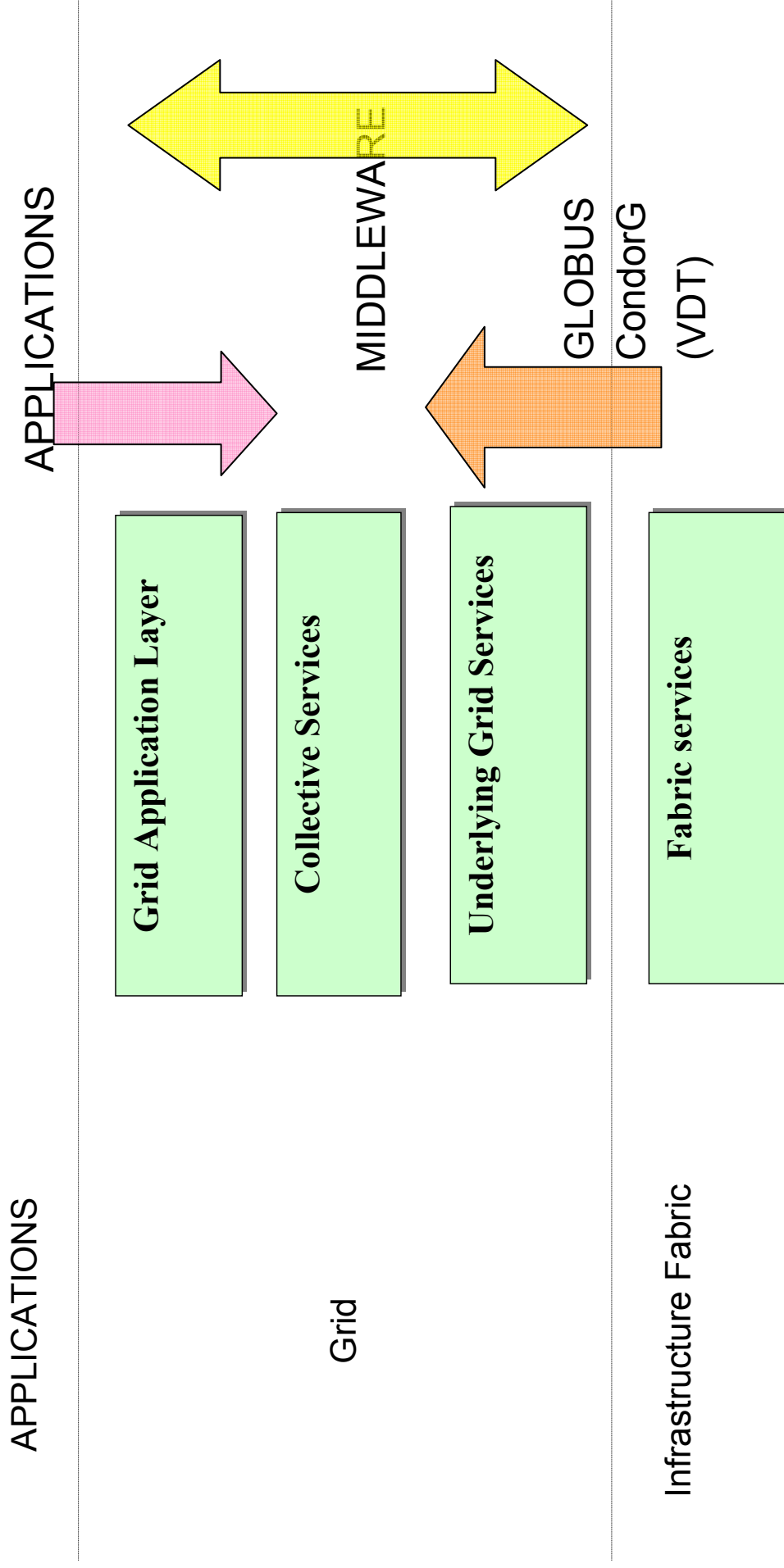
Main Services per Machine Type

Daemon	UI	IS	CE (frontend)	WN	SE	RLS	RB
Globus Gatekeeper	-	-	✓	-	-	-	-
RLS-LRC	-	-	-	-	-	✓	-
RLS-RMC	-	-	-	-	-	✓	-
GridFTP	-	-	✓	-	✓	-	✓
R-GMA	-	✓	-	-	-	-	-
R-GMA GOUT	-	-	-	-	-	-	✓
R-GMA GIN	-	-	✓	-	✓	-	-
Broker (Network server, job control)	-	-	-	-	-	-	✓
CondorG Job submission	-	-	-	-	-	-	✓
Logging & Bookkeeping	-	-	-	-	-	-	✓
Local Logger	-	-	✓	-	-	-	✓
CRL Update	-	-	✓	-	✓	-	✓
Grid mapfile Update	-	-	✓	-	✓	-	✓
RFIO	-	-	-	-	✓	-	-
EDG-SE	-	-	-	-	✓	-	-

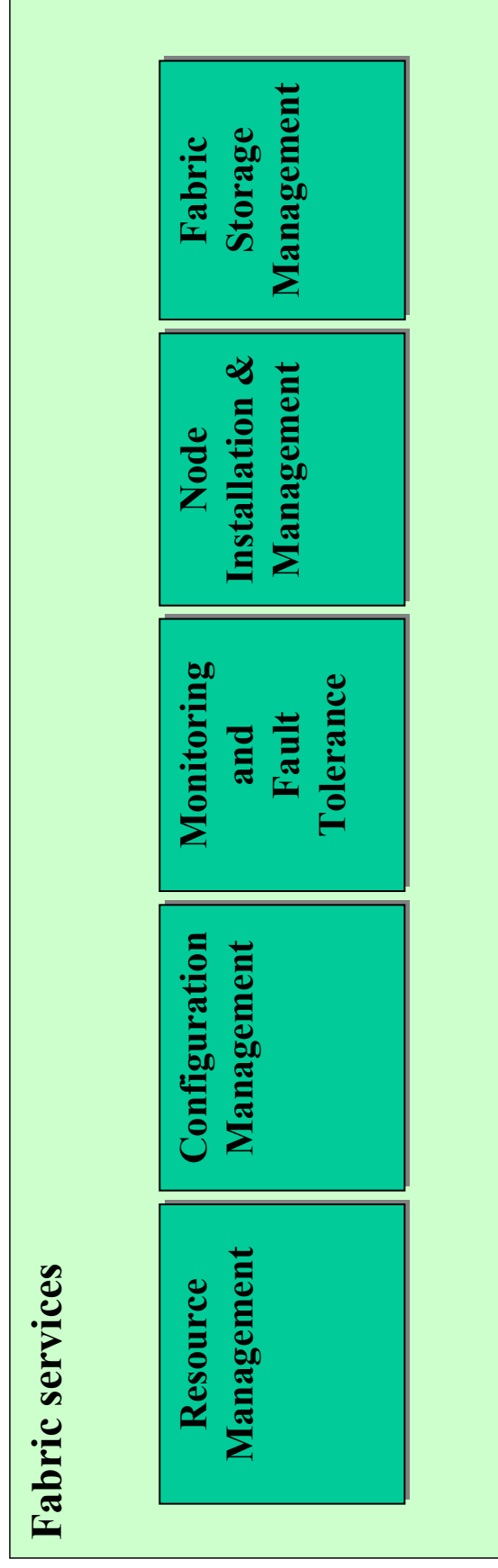
Where are we now?

- Enabling Grid Computing:
fabric+infrastructure+ middleware
 - Information services
 - Grid services
 - The major components
 - **The software stack**
- EGEE grid organisation

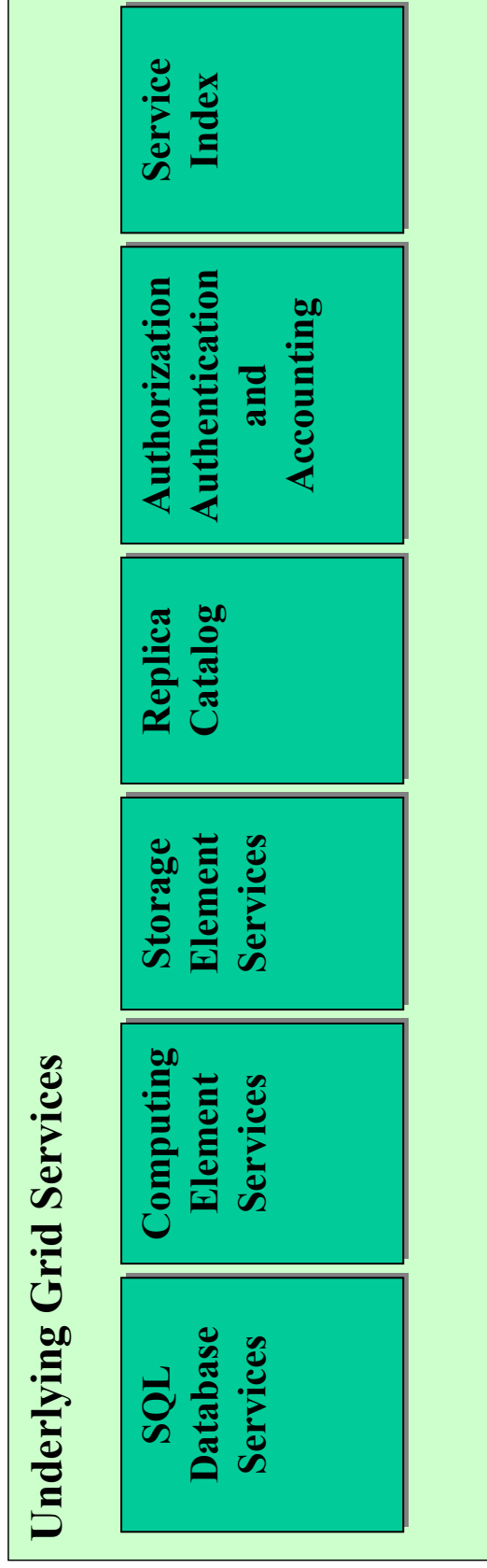
The grid software stack



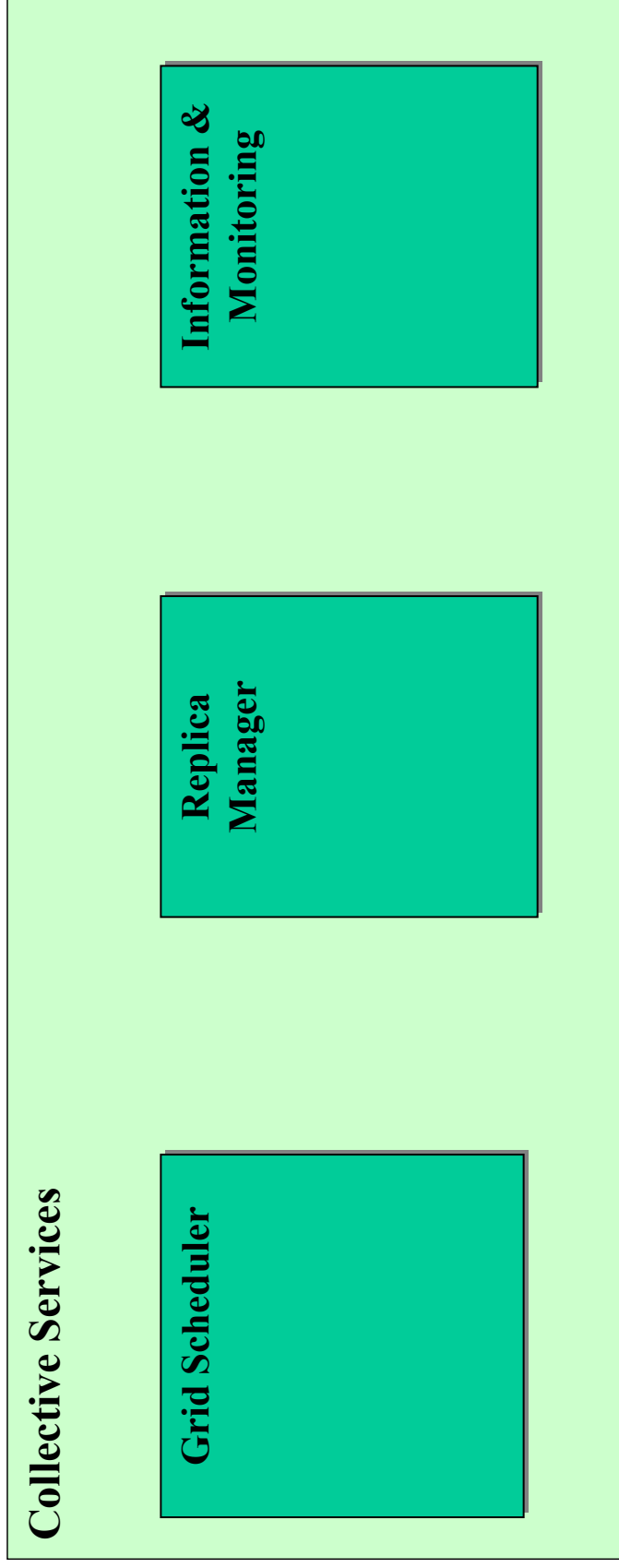
The grid software stack - Fabric



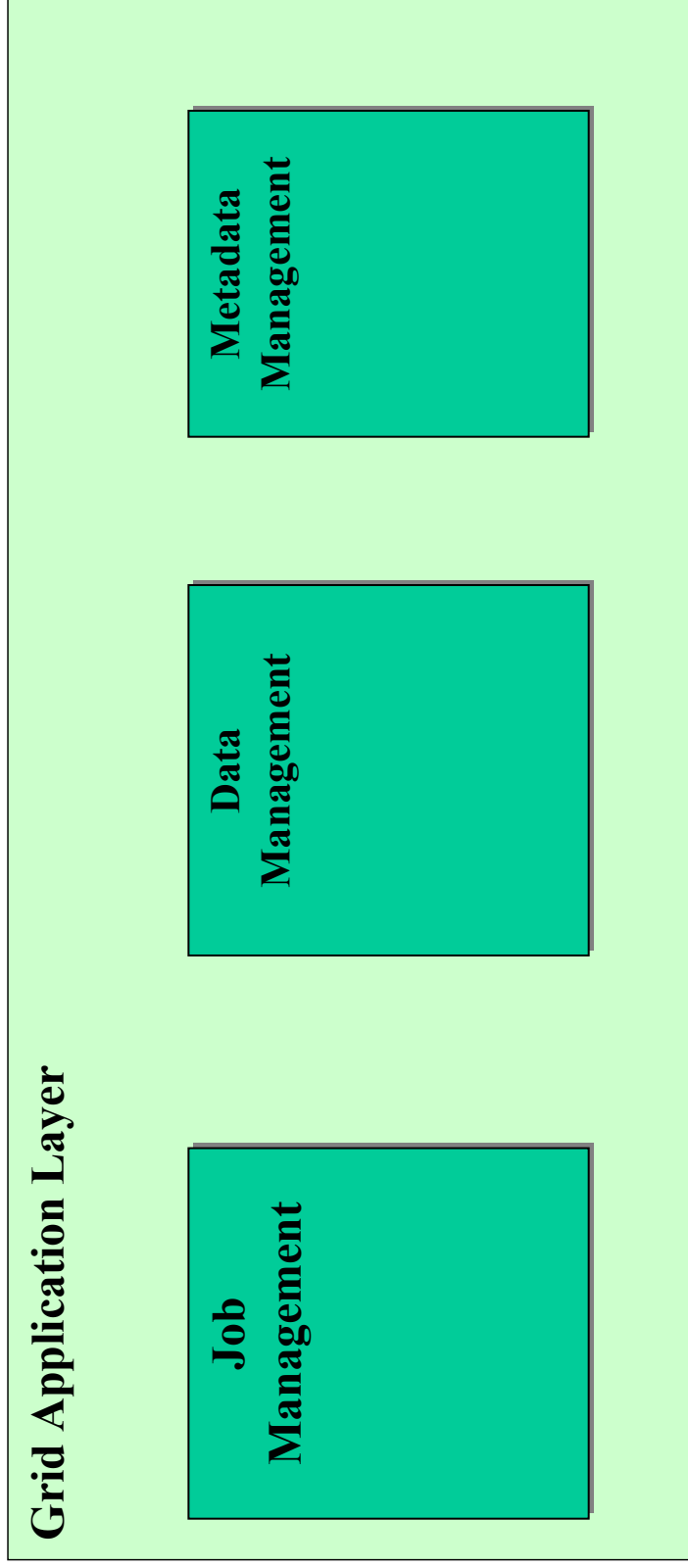
The grid software stack – Grid services



The grid software stack – Collective services



The grid software stack – Application layer



- EGEE is distinctive because of the emphasis on :
 - Production quality of service
 - Multiple virtual organisations

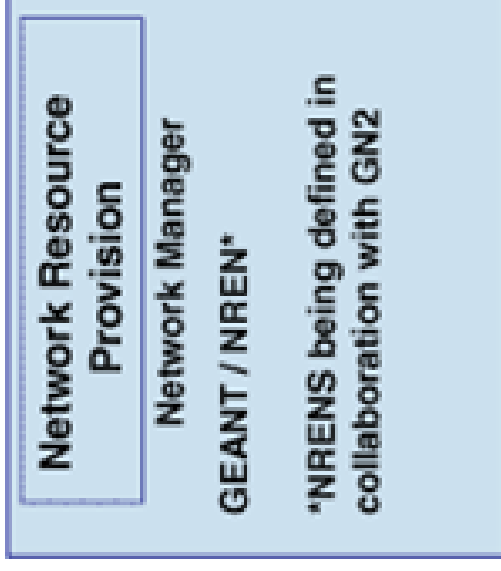
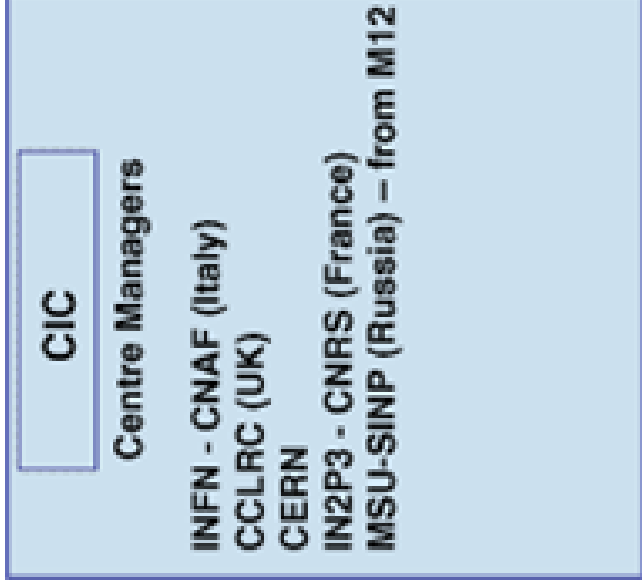
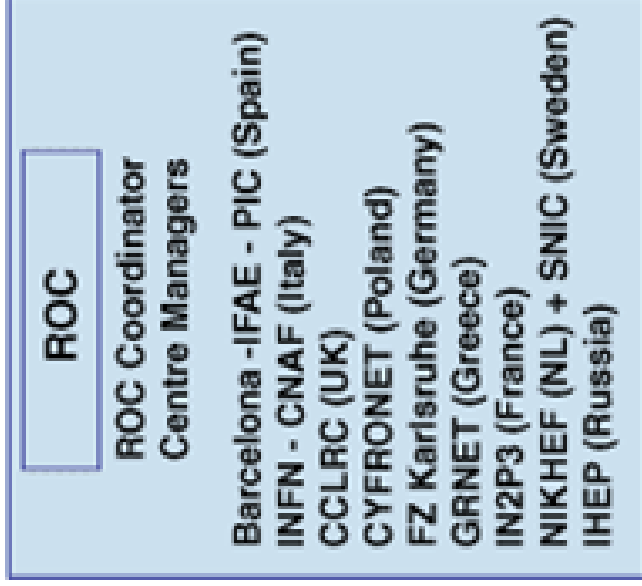
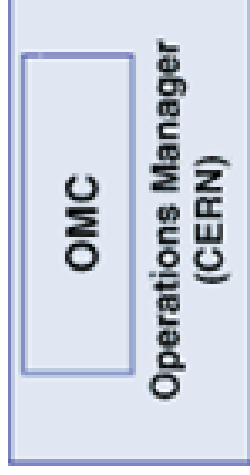
Where are we now?

- Enabling Grid Computing:
fabric+infrastructure+ middleware
- EGEE grid organisation
 - **Virtual Organisations**
 - Operations management and testbeds

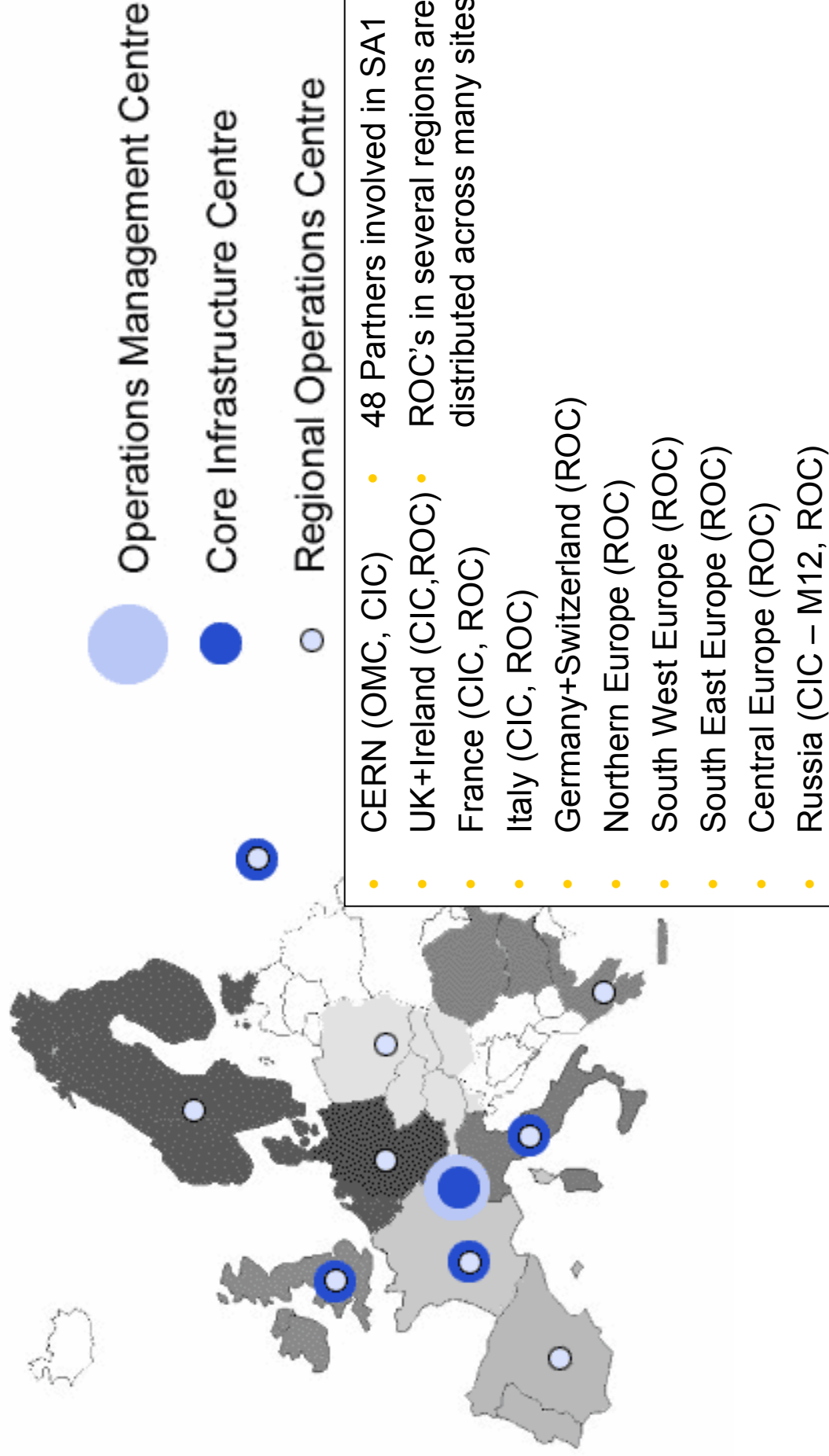
Virtual organisations

- An EGEE user must belong to a VO
- A VO
 - Controls access to specified CE, SE
 - Usually comprises geographically distributed people
 - Requires the ability to know who has done what, and who will not be allowed to do it again.... Security.
- Current VO's:
 - HEP communities, biology, astronomy,....
- VOMS: enhanced flexibility in VO management

Grid Operations Management Structure



Operations Infrastructure



Pre-production service

- For next version middleware
- Initially – start with EGEE middleware as soon as there is a basic release
 - For year 1 pre-production will run EGEE m/w, production will run LCG-2
 - When EGEE middleware is ready – move to production and pre-production service will be next EGEE candidate release
 - Even incremental component changes – get away from big-bang changes
 - Expect to updated services on pre-production even one by one
- Initial resources – come from EDG application testbed sites, perhaps also some of the new smaller sites
- While waiting for first EGEE release – could deploy LCG-2 to get pre-production system up
- Support is 8 hours x 5 days

Training/demo service

- Permanent need for tutorials, demonstrations etc.
- Cannot disturb production system, or guarantee pre-production
- Ideally need dedicated (small) service
 - Kept in an operational state
 - Need sufficient resources to be available (another testbed!)
- Currently fulfilled by GILDA service (via GENIUS portal)

Conclusions

- 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
 - EGEE is VO based
 - The Grid Operations Management Structure monitors and controls the overall functionality
- The EGEE tutorials ensure training at all levels with hands-on on the GILDA dedicated testbed