egee

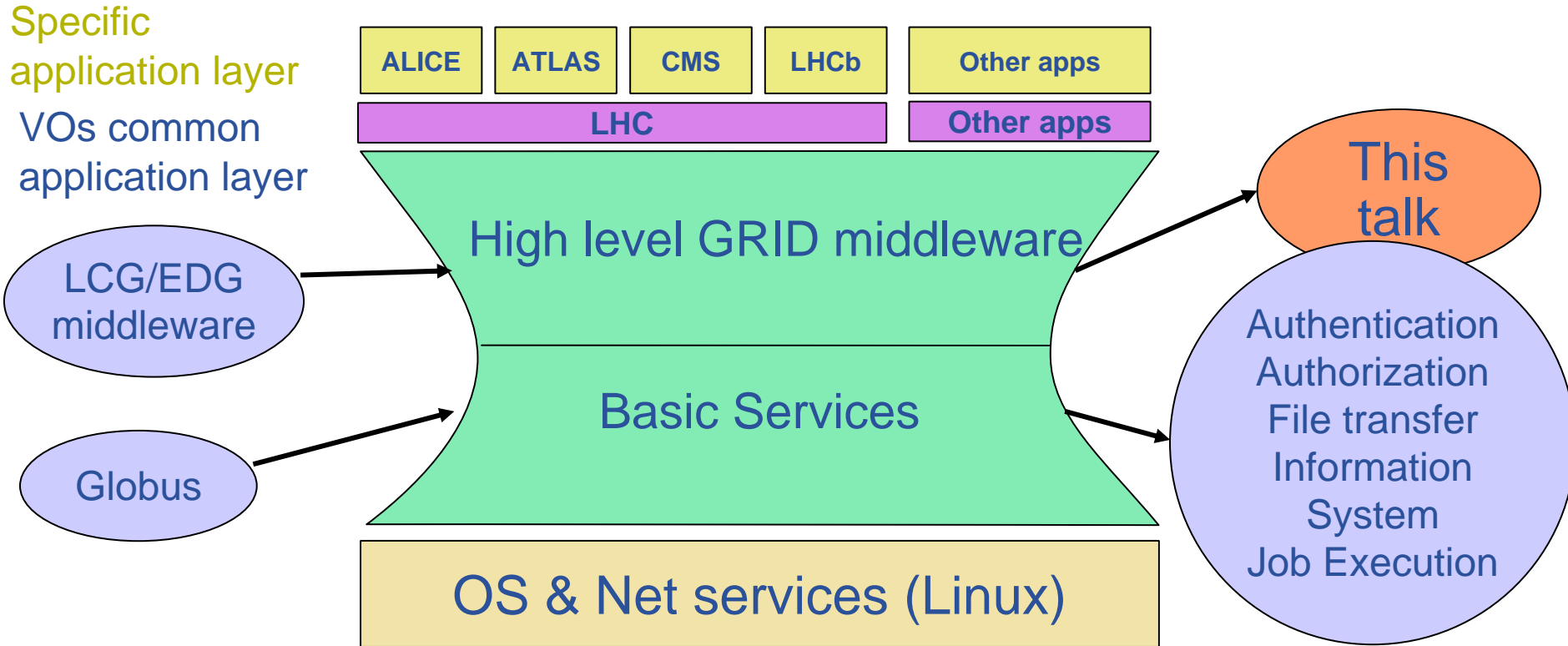# Components of LCG-2

Christopher Jung, FZK, Karlsruhe

Slides contributed by Dr. Peer Hasselmayer, Ingrid Schäffner, Marcus Hardt and Dave Berry

www.eu-egee.org

Information Society

- **LCG middleware keeps the grid together**

Specific application layer

VOs common application layer

ALICE	ATLAS	CMS	LHCb	Other apps

LHC	Other apps

High level GRID middleware

Basic Services

LCG/EDG middleware

Globus

This talk

Authentication
Authorization
File transfer
Information System
Job Execution

OS & Net services (Linux)

Enabling Grids for E-sciencE
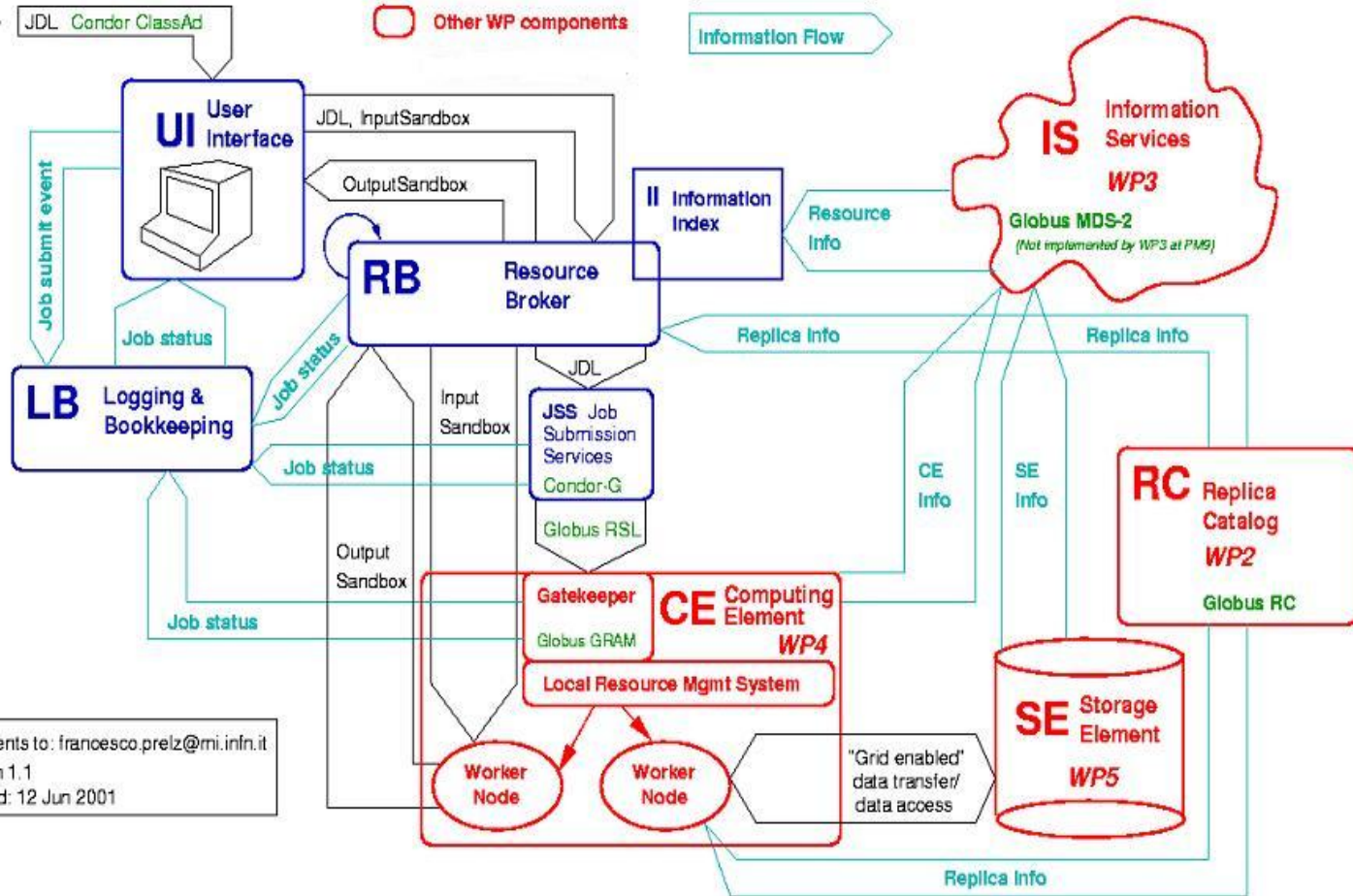
• Different sites offer different services (computing, storage, software)

• Jobs should go to the data

•Some information has to be provided by the user (e.g. which files does job need?)
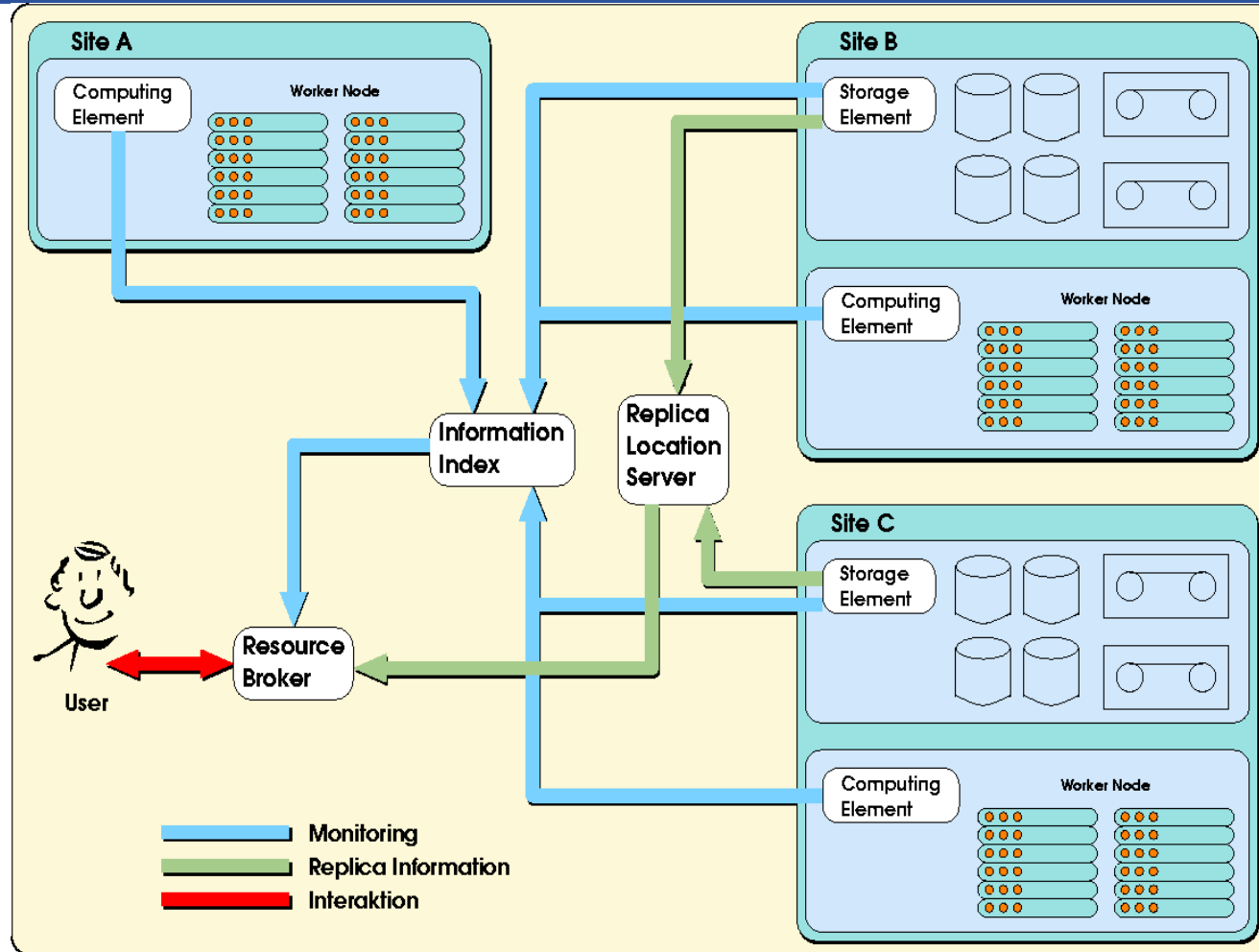
Grid elements

- **Computing Element (CE)**
- **Woker Node (WN)**
- **Storage Element (SE)**
- **User Interface (UI)**

site-wide

- **Resource Broker (RB)**
- **Berkeley Database Information Index (BDII)**
- **MyProxy Server (Proxy)**
- **Replica Location Service (RLS)**
- **Virtual Organisation Server (VO)**

**grid-wide**

Enabling Grids for E-sciencE

- **Computing Element (CE)**
  - gateway to local computing resources (worker nodes, WNs)
  - a Globus gatekeeper

- **Storage Element (SE)**
  - gateway to local storage (disk, tape)
  - a Globus gridftp server, an SRM interface

- **Layer of abstraction: local peculiarities irrelevant**

- **User Interface (UI)**
  - user's access point to the grid
 - client programs using some/all grid services
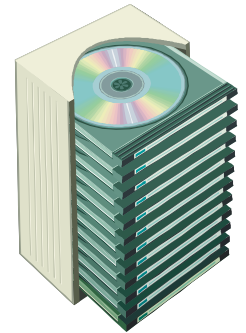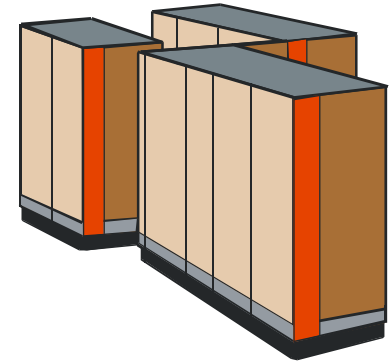
- **Actually consists of RB, LB (Logging and Bookkeeping), JSS (Job Submission Service)**

- **RB matches job requirements with CE offers (CPUs, files, pre-installed software)**

  - gets resource information from BDII and RLS

- **LB keeps track of job and its status**

- **JSS provides reliable submission system**

- **Primary job execution interface for users**

- **Layer of abstraction: knowledge of local sites irrelevant**

- **Only certain VOs are permitted to use a particular RB**

- **Aggregates service information from multiple grid sites**
  - CEs, SEs, RLSes, ...
  - accepted VOs
  - resource availability and usage (CPU, storage)
- **Currently in use: BDII**
  - basically an LDAP server
- **Used by RBs to collect information on sites**
  - defines RB's view of the Grid!
  - usually located "close" to an RB
- **Used by replica management tools to locate SEs, RLSes**

Enabling Grids for E-sciencE
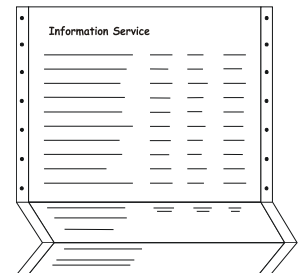
- **RLS maps logical file names (LFNs) to physical file names (PFNs) via globally unique identifiers (GUIDs)**
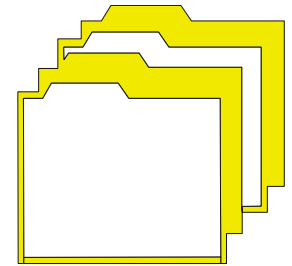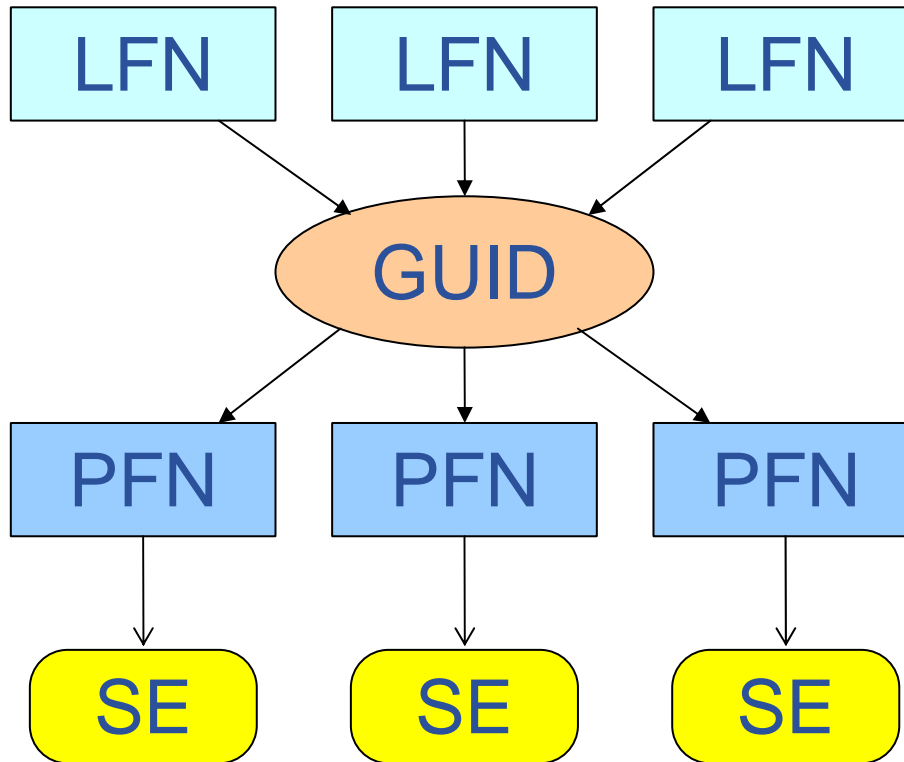
- **RLS remembers locations of files**
  - only deals with their locations
  - data transfer handled separately: PFNs point to actual storage location and access protocol
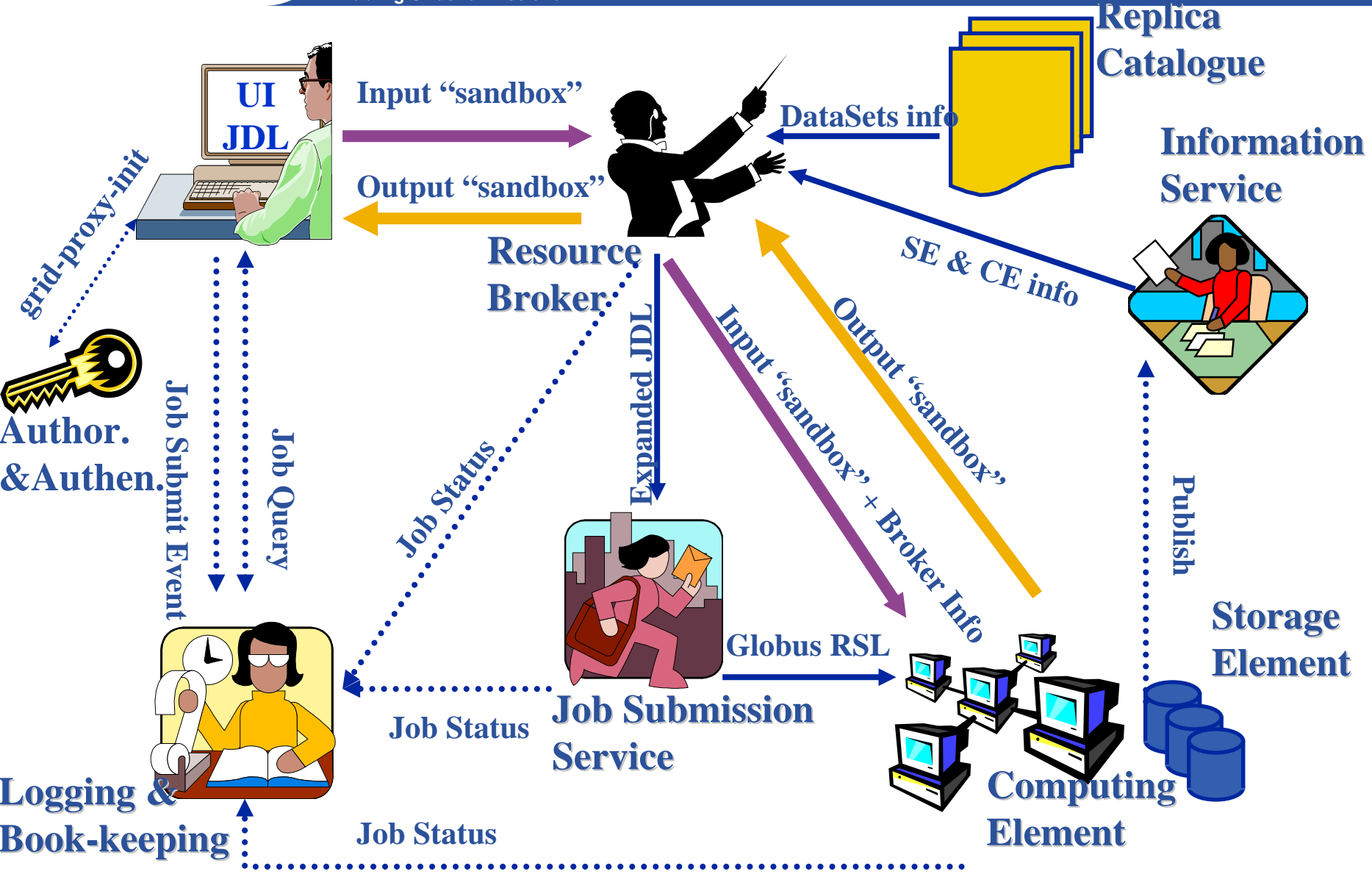- **Files can be replicated on multiple SEs**
- **Each file registered with the RLS has a unique ID**
  - same file gets different IDs when registered multiple times
- **LFNs are names that make sense to you**
- **Layer of abstraction: file location irrelevant**
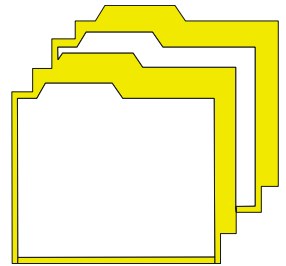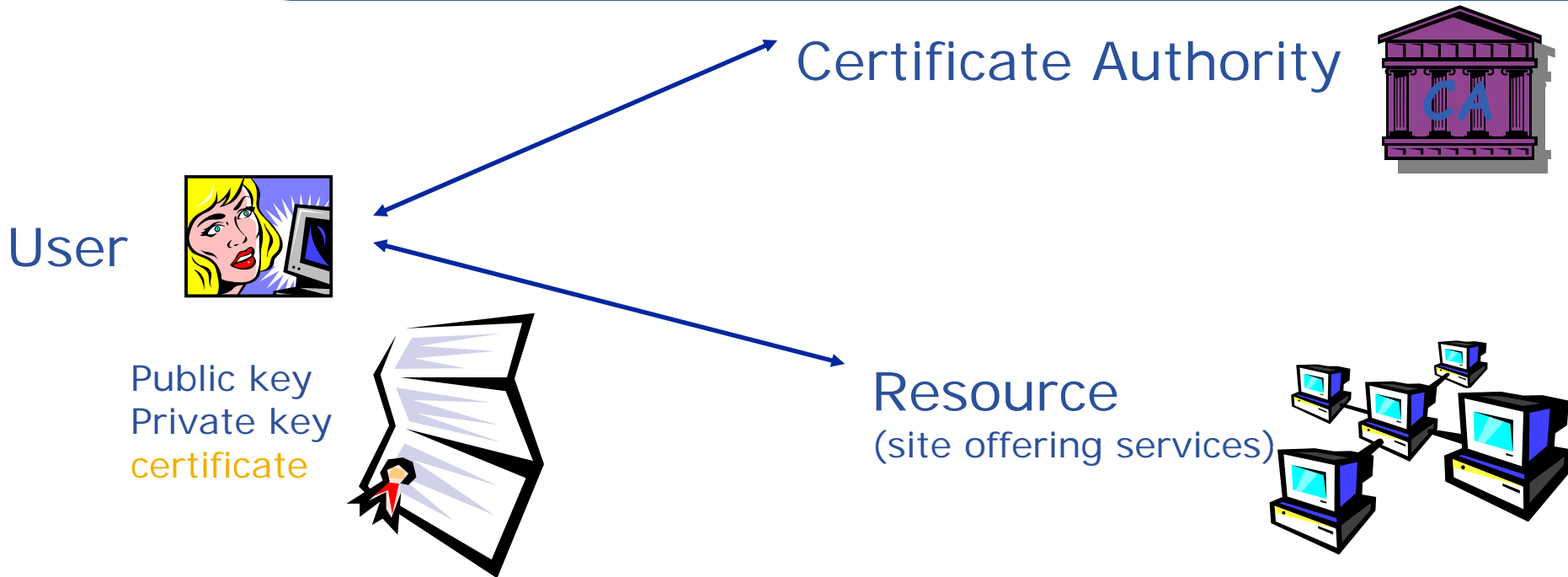
- **VO contains people working together on some activity**
- **Members listed in a VO server**
    - currently: LDAP server
    - Each member identified by their personal certificates, e.g. /O=GermanGrid/OU=GermanGrid/CN=Christopher Jung
    - VO manager adds/removes people "from VO"
    - server can be run at arbitrary location
    - server can be run by people not member of VO

Another view on the grid

UI JDL

Input "sandbox"

Output "sandbox"

Resource Broker

grid-proxy-init

Author. &Authen.

Replica Catalogue

DataSets info

Information Service

SE & CE info

Job Submit Event

Job Query

Job Status

Expanded JDL

Input "sandbox" + Broker Info

Output "sandbox"

Publish

Job Status

Job Submission Service

Globus RSL

Logging & Book-keeping

Job Status

Computing Element

Storage Element

Enabling Grids for E-sciencE

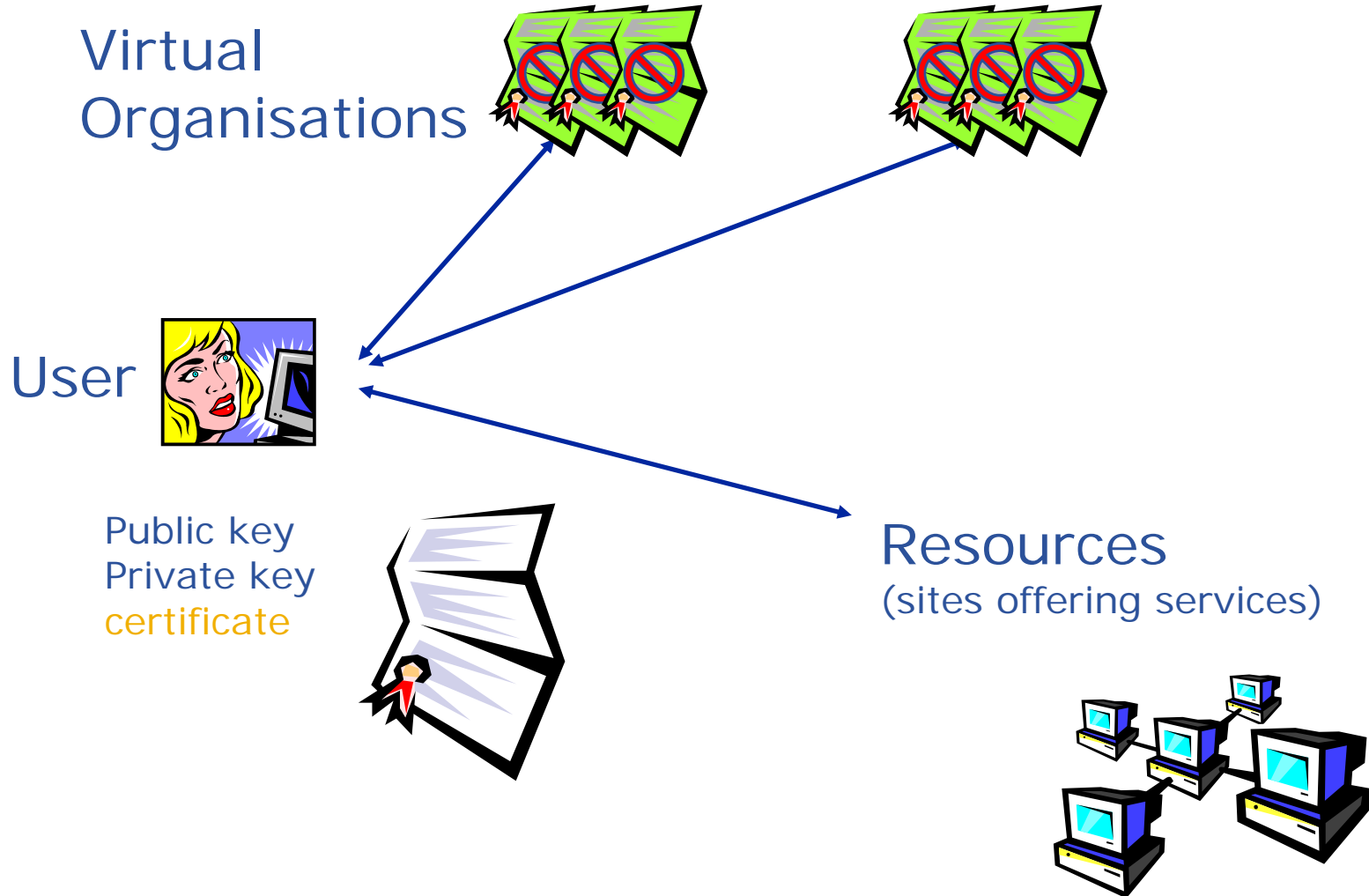- **Distribution of resources: secure access is a basic requirement**
  - secure communication
  - security across organisational boundaries
  - single "sign-on" for users of the Grid

- **Two basic concepts:**
  - Authentication: *Who am I?*
    - "Equivalent" to a passport, ID card etc.

  - Authorization: *What can I do?*
    - "Equivalent" to a visa or access list
    - Certain permissions, duties etc.

Enabling Grids for E-sciencE

Certificate Authority

User

Public key
Private key
certificate

Resource
(site offering services)

- Grid community mainly uses X.509 PKI (well established!)
- Each user has public and private keys; these keys are mathematically related
- So called asymmetric cryptography

Asymmetric cryptography

- **What is symmetric cryptography?**
  - Algorithms in which you can get the deciphering rules from knowledge of the ciphering rules in a "reasonable" amount of time
  - Examples: Caesarian code (shifting the text), stream cipher, …
  - Very fast

- **Asymmetric cryptography:**
  - The knowledge of the enciphering key does not help to calculate the deciphering key
  - Everybody publishes his/her public key
  - If you want to send a message to Mr A, you encode your message with A's public key. This message then can be encoded only with his private key
  - Rather slow
  - No problems when exchanging the keys

Virtual
Organisations

User

Public key
Private key
certificate

Resources
(sites offering services)

- **Getting a certificate:**
    1. Log on to a UI.
    2. Execute 'grid-cert-request' and follow the instructions. You will get a „cert request file". Send it to your CA: „GridKa-CA@iwr.fzk.de".
    3. Wait until you get a confirmation e-mail. Send a xerox copy of your passport to the CA (via ground mail); copy has to be charged by a person in charge (e.g. Andreas Gellrich).
    4. You will get a certificate per mail.
    5. Register with your VO (e.g. "http://lcg-registrar.cern.ch/").

    For this training, the certificates have been already
    pre-installed.

What does a certificate tell?

- **The certificate that you present to others contains:**
  - User identification
  - Your 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
  - Expiry date

```
Certificate:
   Data:
        Version: 3 (0x2)
        Serial Number: 820 (0x334)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=GermanGrid, CN=GridKa-CA
        Validity
           Not Before: Feb  9 14:45:00 2005 GMT
           Not After : Feb  9 14:45:00 2006 GMT
        Subject: O=GermanGrid, OU=EKP, CN=Christopher Jung
        Subject Public Key Info:
        ……
```

Questions?

Time to do something practical!

bmb+f - Förderschwerpunkt

Hadronen - und Kernphysik

Großgeräte der physikalischen Grundlagenforschung