Technical Requirements:

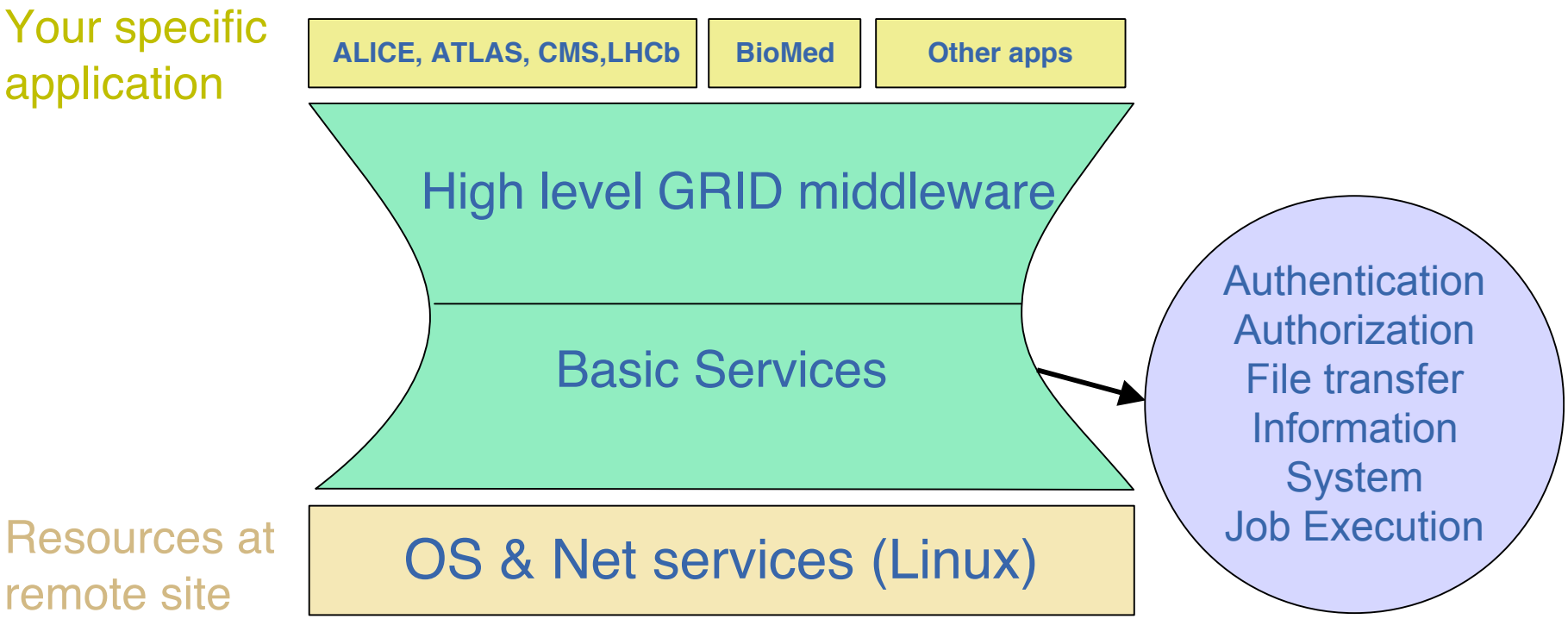
Components
Networks
Security

Yves Kemp, University of Karlsruhe

Karlsruhe Institute of Technology

The hourglass model

- **Middleware keeps the grid together**



Different versions of middleware:

- **Look at Agenda: e.g. Tuesday:**
  - GT4: Olaf Schneider
  - Unicore: Rebecca Breu
  - EGEE + the gLite Toolkit: Brendan Hamill

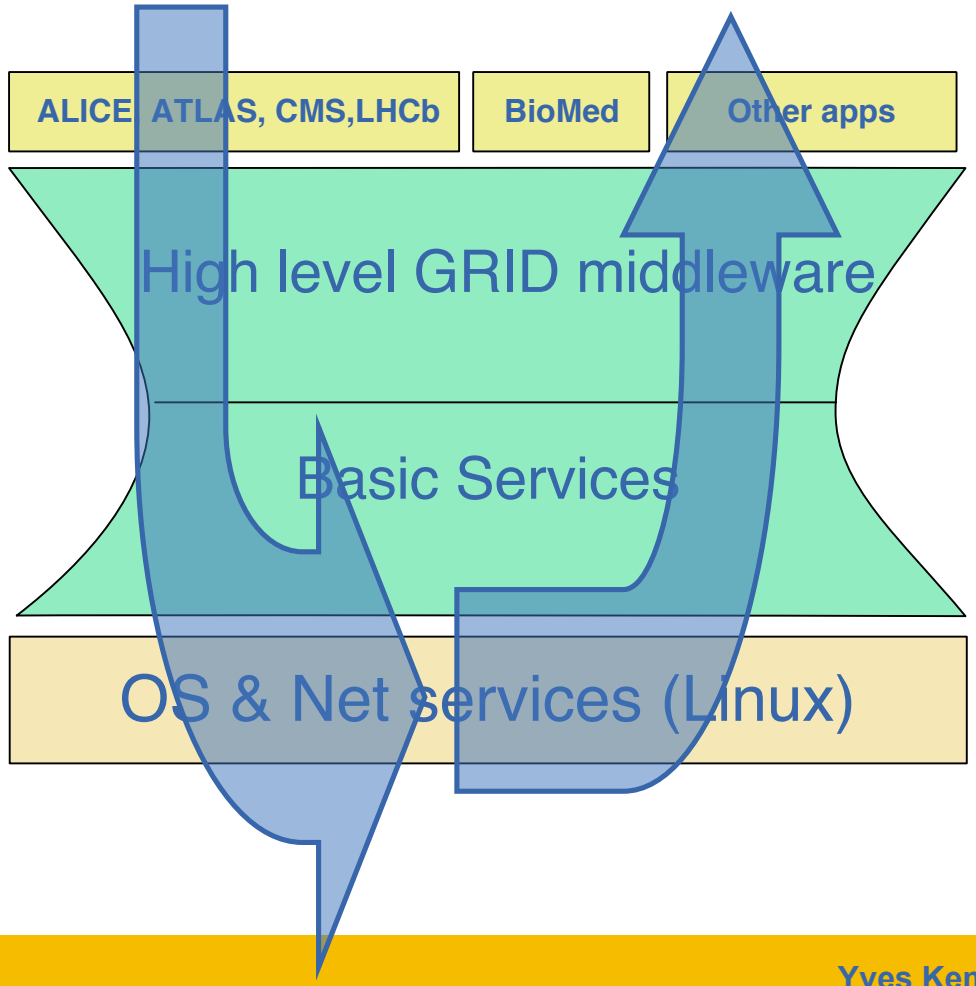
and many more …

This talk shows some concepts and components common to most middleware.

For more infos and questions on one specific middleware, please attend the respective talk or tutorial

This talk is about

- How your jobs get to the remote computer…
- … and how you get back the results



The very first step…

- **… introduce yourself to the Grid**
  - Authentication
  - Authorization
- **Authentication**
  - Who are You?
  - Which institution do You belong to?
  - Who certified You?

⇨**Certificate**

Comparable to a passport: Issued by a Certification Authority

- **Every country has a Certification Authority (CA)**
  - GridKa is the German Certification Authority
  - They do not provide Authorization!

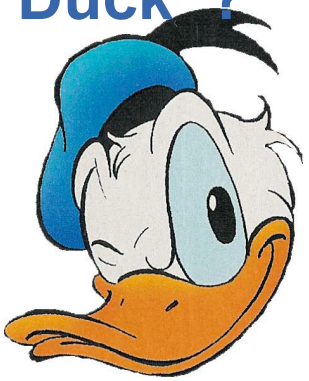
… and a second step

- **Authorization**
  - Which organisation(s) do You belong to?
  - What are You allowed to do?
  - Where are You allowed to do so?

  ➔Comparable to a visa: Issued by Virtual Organization(s)
- **Virtual Organization (VO):**
  - A group of people working together on same activity
- **Unlike Peer2Peer, you act as member of a VO**
  - You (personally) do not provide resources
  - Resources are not allocated to you (personally), but to your VO

Certificates

- **Based on asymmetric authentication**
  - The user generates a Private Key and a Public Key
  - The Private Key is private!
  - The Public Key is sent to the Certification Authority
- **The CA issues a X509 certificate using:**
  - The User Public Key
  - The User Identity (Name, Institute…)
  - Information about the Certification Authority
  - A Digital Signature
- **Why cannot You get a certificate for "Donald Duck"?**
  - The CA make sure that You do not fake your ID
  - Your supervisor (known to the CA) needs to sign a photocopy of your official passport which is sent to the CA



Certificates and proxies

- **Your Certificate is encrypted with a passport**
  - How to handle this when you submit a multitude of jobs that travel through the Grid?
- **You create a Proxy**
  - “Mini”-Certificate: Your certificate acts as CA for the proxy
  - Proxy has no password
  - Proxy propagates through the Grid
  - Only limited lifetime (24h e.g.)
- **Proxy allows for Single-Sign-On**
- **If your Certificate is stolen/hacked: Please alarm CA!**
- **If Proxy is stolen/hacked: Only limited damage, no action**

Now you can “log in to the Grid”

⇒You can send your job to the Grid

Let’s see which Grid components you will meet along your way

Simple Example

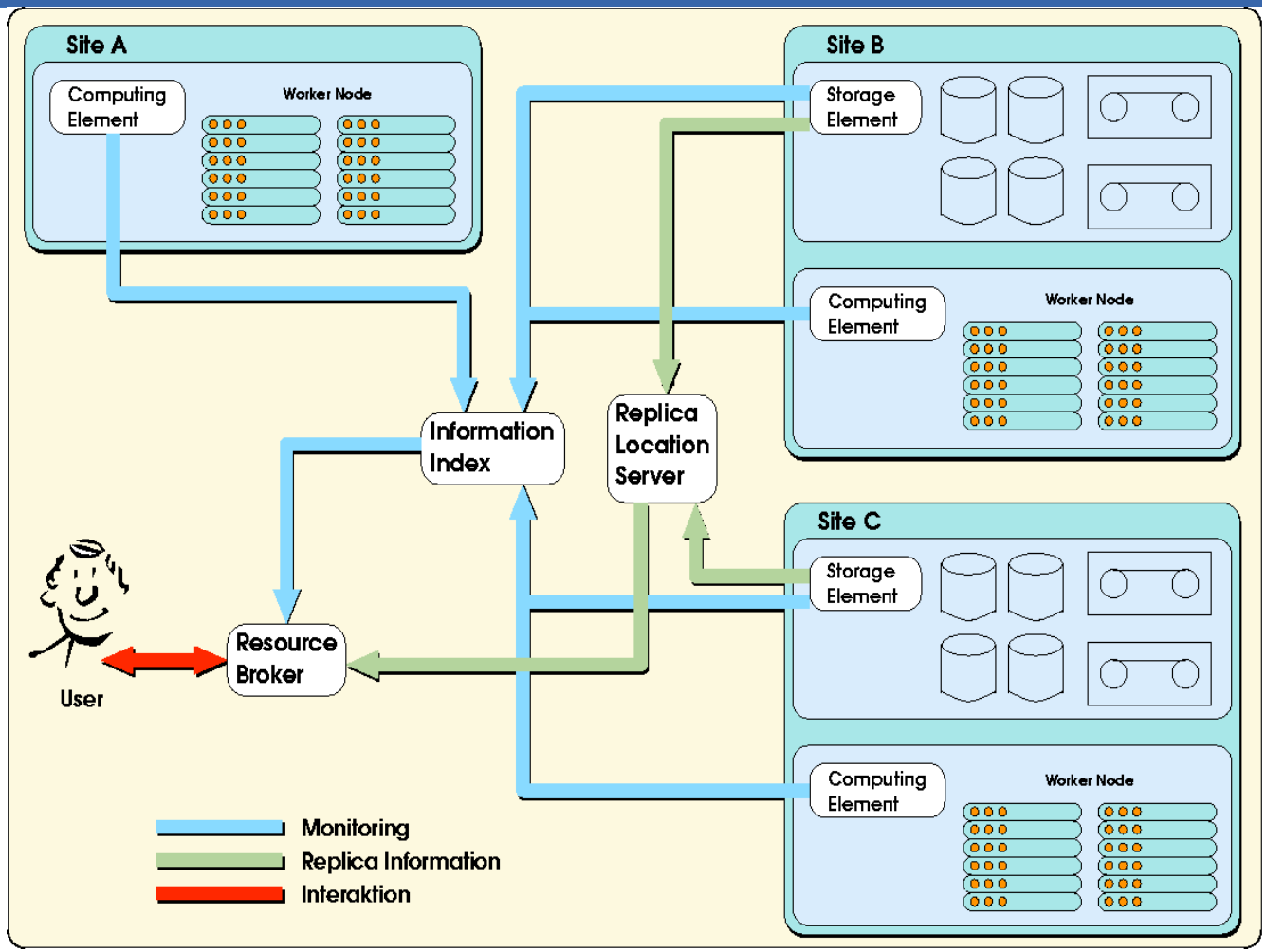
- **You pack all you need into an "input sandbox"**
  - Executable: `weather_forecast.bin`
  - Configuration files: `September12-September15.conf`
  - The program requires on the remote site:
    - 64-Bit Opteron System with > 4 GB RAM/CPU
    - SuSE 10.1 with software `Weather_Forecast` Version 2006.1.3 installed
    - German weather reports from Sept.1-Sept.10 available at local site
- **Large dataset (weather reports) are usually not contained in the sandbox, they are accessed via Grid mechanisms**
- **You send your job to the Grid**

? Where will it arrive ?

➔ The Resource Broker (RB) decides upon your VO, the requirements and the availability which connected site the job is sent to

How does the RB know?

- Different sites offer different services (computing, storage, software)
- The sites describe which resources they offer
- The status of the sites is continuously monitored



RB at the heart of the Grid!

The RB has decided upon the site:

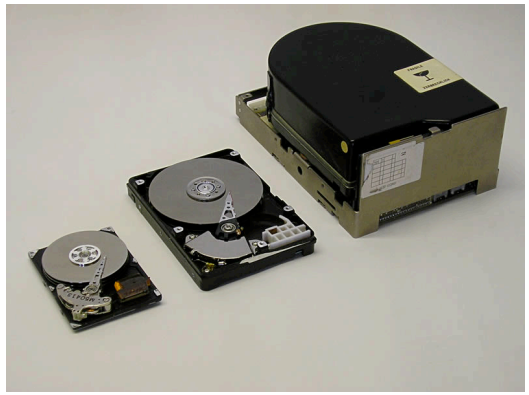
- **The RB sends your job to the destination site**
- **“Interface” of the Grid to the local site computing nodes is the Compute Element**
  - It does not compute jobs itself!

The CE will:

- **assign you a generic local user account on the destination cluster**
- **submit your job to the local batch queue**
  - The job itself is executed on a worker node
  - The priority is determined according to local rules (“50% to VO X, 30% to VO Y, 20% local users”)
- **Keep track of the job and get the (standard) output back**
- **Send the job output back to the RB, where it can be downloaded from**

What if you have large datasets?

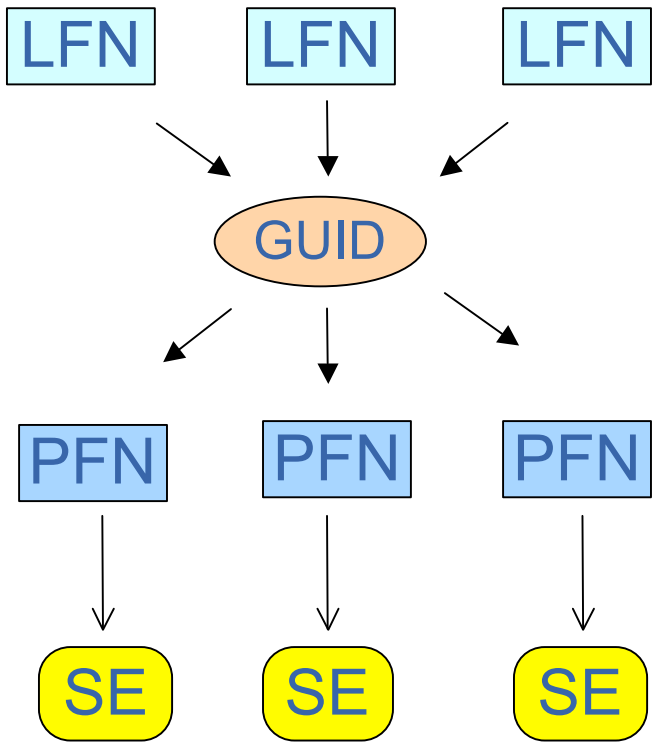
- **Either you need large data sets as import to your job**
  - Experiment data, Genome database, Client database, …
- **Or you produce large output files**
  - Monte Carlo simulations, stripped input files, ….



You need a Storage Element:

- **Does not necessarily store data itself**
- **Portal to local storage infrastructure:**
  - Fileserver, tape library, storage management systems…
  - Data security and space allocation: local policies
- **Can be accessed either from the worker node or via the Grid**
- **YOU have to specify which SE you want to use:**
  - The closest one to the site, your home site, a special site with large bandwidth / capacities …
  - Access through existing Grid commands or integrated into executables

More about storage:



- **"Filename" on the Grid:**
  - Global Unique Identifier (GUID)
  - guid:3a69a819-2023-4400-a2a1-f581ab942044
- **Easy access through Logical File Name (LFN)**
  - lfn:/grid/cms/yves/ExitingDataset.dat
  - lfn:/grid/cms/myboss/DataWithBadDetector.dat
- **Physical File Name (PFN)**
  - Actual location on SE disks
  - /storage/grid/experiments/cms/yves/ver04/run2342/results/data/file124.dat
  - Files can be replicated on different SE at different sites for better access
- **Managed by the File Cataloge**

Permissions:

- **VO contains people working together on some activity**
- **Not everyone should be able to do everything:**
  - Medicine: A student should not access the patient health records
  - Meteorology: Only data managers should handle common datasets
  - Particle physics: Only software managers should install VO specific software
- **Different roles and permissions within a VO can be granted to the same person**
  - I can select between my different possible roles when creating the proxy

Networks

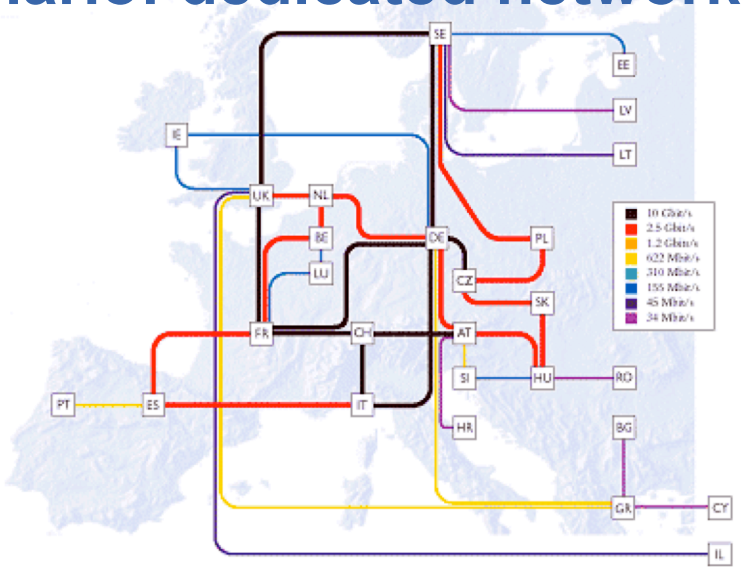
- The Grid idea is about distributed computing
- All Grid services use “normal” internet connections and standard internet protocols
- The Grid uses the same connections you use for email or WWW

But…

Networks, scenarios

- **Is the available bandwidth sufficient?**
  - Application: Compute all prime numbers with 150 digits ⇨ Only small data transfer
  - Analysis of large datasets in particle physics: Data transfer in the order of tens of TeraByte per day and site

- **Depending on the usage scenario: dedicated network:**
  - European research and education network GÉANT(2)
  - DFN and X-WIN in Germany
  - 10 Gbit or more between sites



General Security Considerations

- **What do I want to protect?**
  - The code written last week? The last five years?
  - Personal data (Credit card number, passwords…)?
  - The data from an expensive experiment/my patients?
- **Against what/whom do I want to protect?**
  - Accidental `rm -rf *` by me / my colleagues?
  - Sabotage by colleagues? Visit from Mr. H. Acker?
  - Hardware failure due to water / fire / nuclear war?
- **What price am I willing to pay to "be secure"?**
  - In terms of money / time?
  - In terms of change of behavior?

⇨**Answer these questions AND THEN take action!**

Security: File permissions

- **A file/directory is "world readable":**

```
drwxr-xr-x yves yves 102 Aug 1 19:32 Thesis
```

- **Assuming no hacks from the outside, this means:**
  - On my laptop, **only I** can see the content
  - On my institute desktop, **all institute members** can see the content
  - On a computer connected to the Grid, **potentially everyone** can see the content

"World readable" means the whole world can read it!

Security: Operating System

- **Meaning and importance of local exploits**
  - A local exploit offers a normal unprivileged user with a local account to gain root privileges
- **Who can use such an exploit?**
  - On your laptop: **Only Yourself** (but you probably do not have interest in doing so)
  - On your institute desktop: **All institute members** (they could be interested, but they have other possibilities getting root)
  - On the Grid: **Anybody** can use such an exploit

A local exploit is not local anymore on the Grid!

Security: Passwords

- **Some systems use Yellow Pages (a.k.a. NIS)**

```
ypcat passwd | grep kemp
kemp:SAR6EMgLgZcOY:11006:....
```

Encrypted password
A hacker will try to hack it!

- **People tend to have identical passwords on different systems**
  - Account of user X gets hacked on system Y:
  - All systems where X has access are endangered!
- **If you use SSH keys: Please set a password for them if you are crossing site boundaries!**
- **Have a good password for your Grid Certificate!**
  - Different from your usual one!
- **If you must write down passwords, please protect the paper!**
- **Forcing users to change passwords every three months is pseudo-security: users will not have strong passwords**

Security: Installation

- **Installation of middleware is intervention to system**
- **Some installations require >200 packages additional to base system**
  - Difficult to maintain (although automatic updates)
  - Difficult to configure in a secure way
- **Site open themselves to the outside: Firewalls?**
  - Either open them completely or at least large parts of them
  - Or encounter problems when firewall rules change / protocol changes
  - Some sites even have a “No Firewall”-policy

Security in the Grid, Conclusion

- **Security subject of rising importance in Grid**
- **Users:**
  - If YOUR account is hacked, not only you are affected, but also others!
  - YOU are affected if another account is hacked!
  - Please respect rules of common sense concerning passwords and physical security of machines!
- **Admins: Everything is global now, so administer you system as if the whole world would threaten it**
- **Developers:**
  - Transparent architecture of Middleware
  - Middleware installation minimum invasive to OS
  - Configuration transparent to admins
  - Good documentation important
  - “Security by Obscurity” will not work :-)

Instead of a conclusion:

Questions?

Outlook:

Many interesting talks and tutorials during the next days will feature more details than this overview talk