SISTEMI INFORMATIVI INFORMATION SYSTEMS

Introduction to Grid Computing

Dr. Giuliano Taffoni

INAF INFORMATION SYSTEMS UNIT

Plan of the presentation

- A view to the Grid
- Looking inside EGEE grid
- Overview of the Grid services
- Focus on Grid security

One definition

- *A computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities.*
    - Carl Kesselman,Ian Foster in ﾒThe Grid: Blueprint for a New Computing Infrastructureﾓ 1998

One definition

- *Grid computing is coordinated resource sharing and problem solving in dynamic, multi- institutional virtual organizations*
    - Carl Kesselman,Ian Foster in “the anatomy of the grid” 2000

Grid essentials

- “You can't be a real country unless you have a beer and an airline. It helps if you have some kind of a football team, or some nuclear weapons, but at the very least you need a beer”.
  - » Frank Zappa

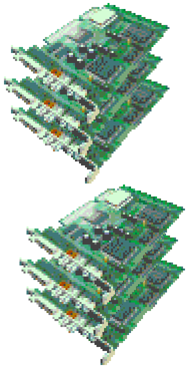
- You can't be a real Grid unless you have a **commodity** and a **discovery** mechanism. It helps if you have some kind of **middleware** or some supercomputers, but at the very least you need a commodity.

Grid synthesis

One user wants to access to intensive computational power

Grid synthesis

One user wants to access to intensive computational power

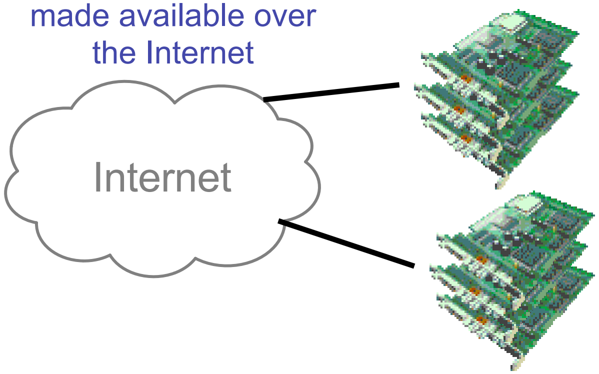


Some computing farms produce computing power to be shared

Grid synthesis

One user wants to access to intensive computational power

Computing power is made available over the Internet



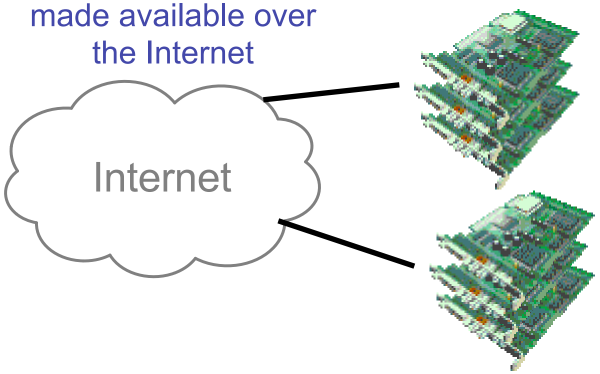
Some computing farms produce computing power to be shared

Grid synthesis

One user wants to access to intensive computational power

He/she comes to an agreement with some society that offers grid services

Computing power is made available over the Internet



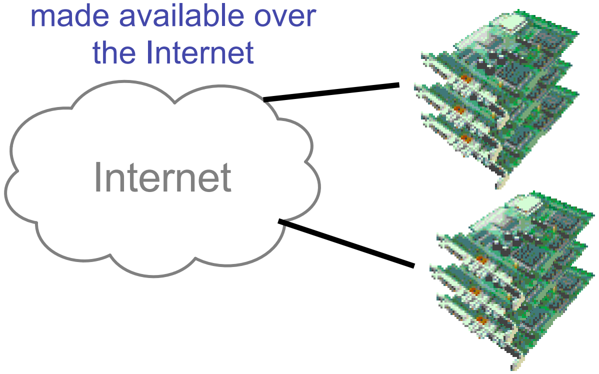
Some computing farms produce computing power to be shared

Grid synthesis

One user wants to access to intensive computational power

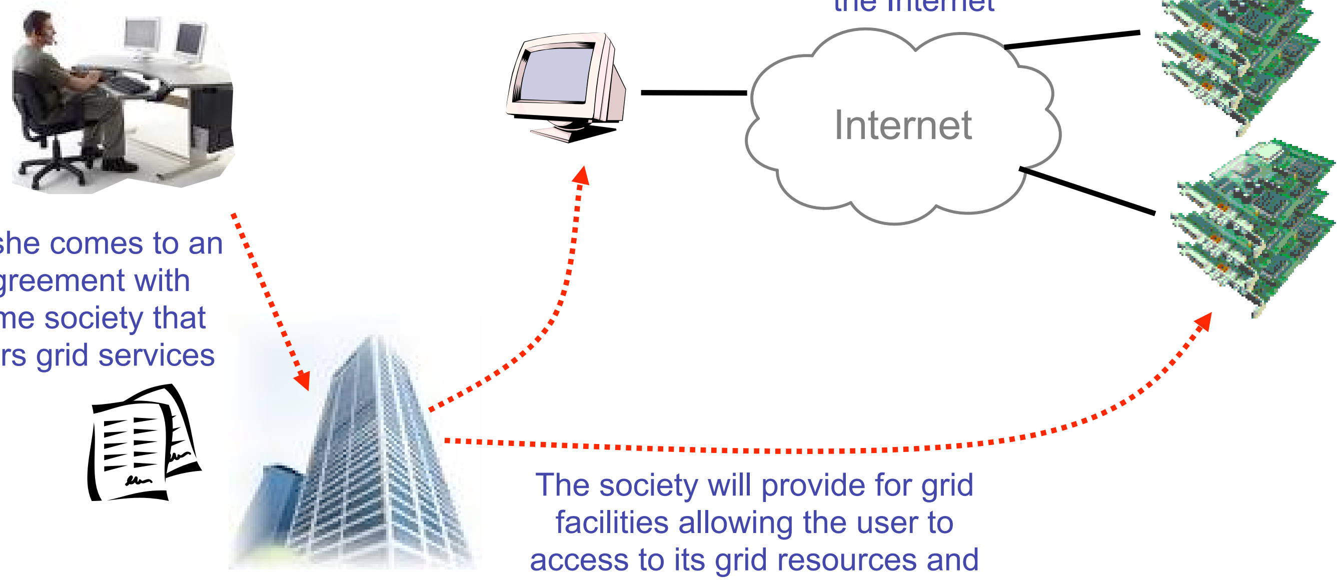
He/she comes to an agreement with some society that offers grid services

Computing power is made available over the Internet



Some computing farms produce computing power to be shared

Grid synthesis



One user wants to access to intensive computational power

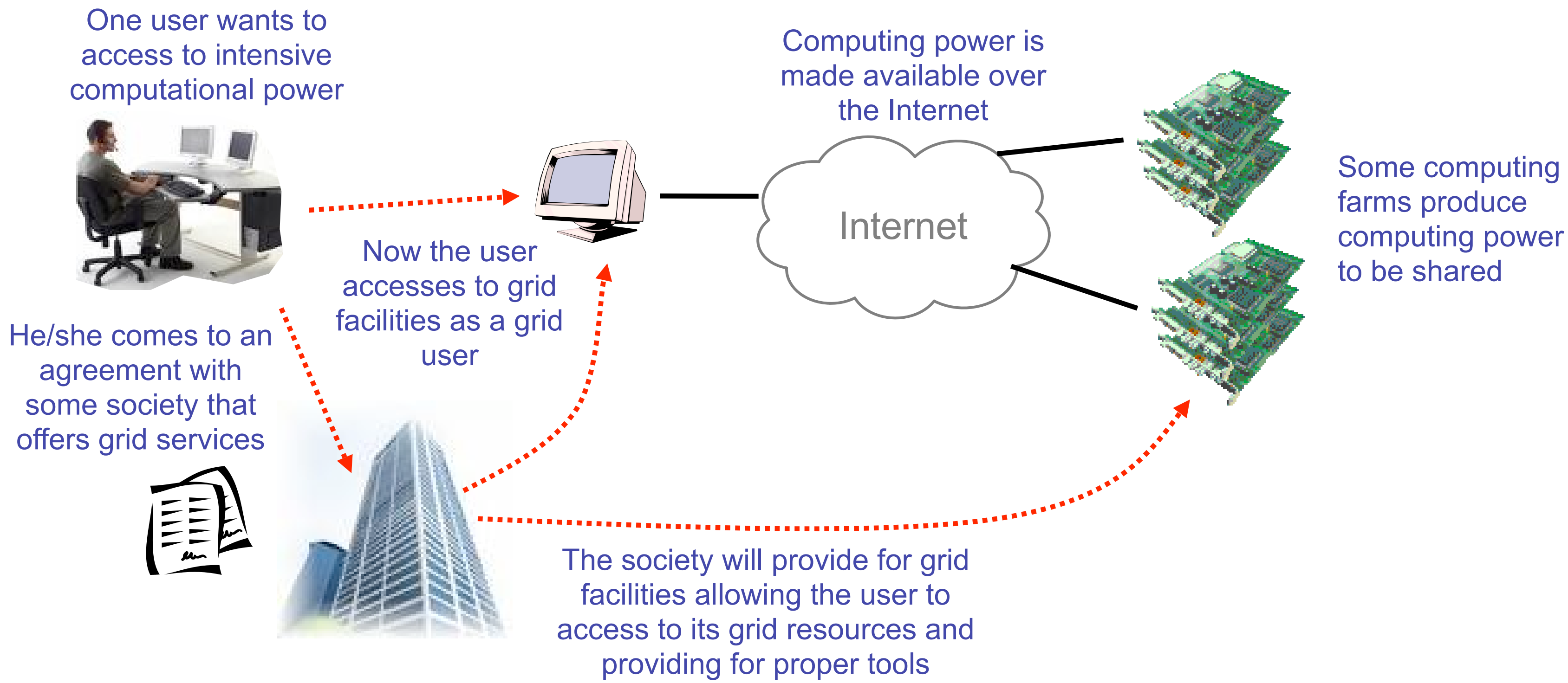
Computing power is made available over the Internet

Some computing farms produce computing power to be shared

He/she comes to an agreement with some society that offers grid services

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

Grid synthesis



One user wants to access to intensive computational power

Computing power is made available over the Internet

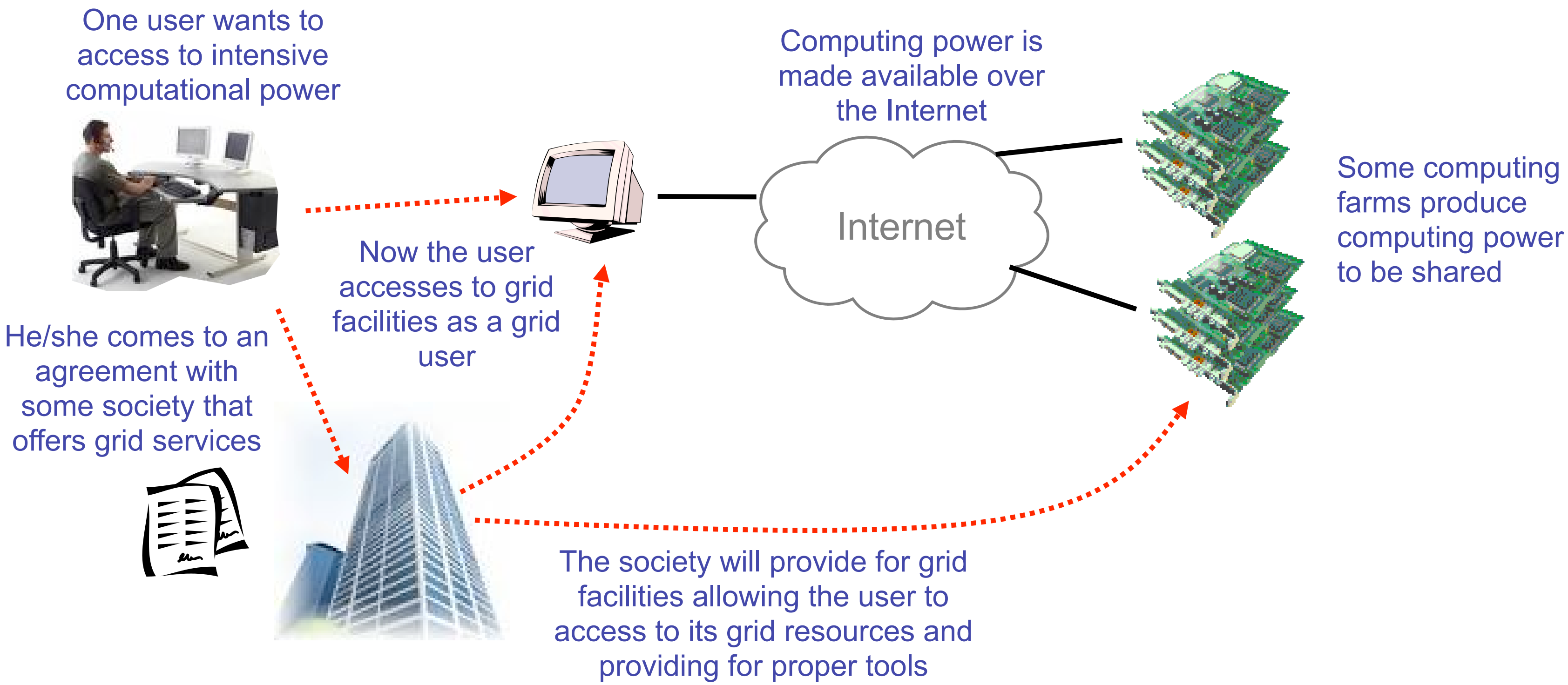
Some computing farms produce computing power to be shared

Now the user accesses to grid facilities as a grid user

He/she comes to an agreement with some society that offers grid services

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

Grid synthesis



One user wants to access to intensive computational power

Computing power is made available over the Internet

Some computing farms produce computing power to be shared

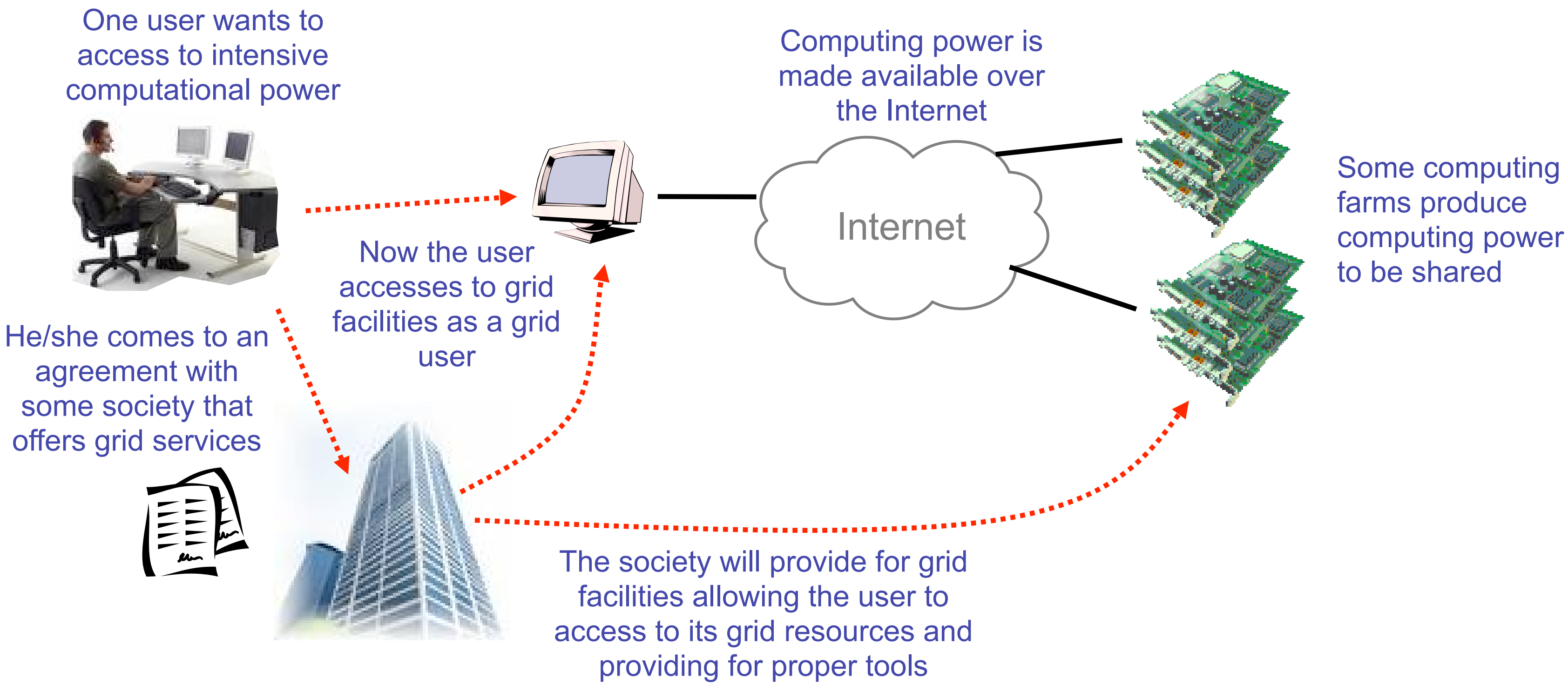
Now the user accesses to grid facilities as a grid user

He/she comes to an agreement with some society that offers grid services

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

– The user:

Grid synthesis



One user wants to access to intensive computational power

Now the user accesses to grid facilities as a grid user

He/she comes to an agreement with some society that offers grid services

Computing power is made available over the Internet

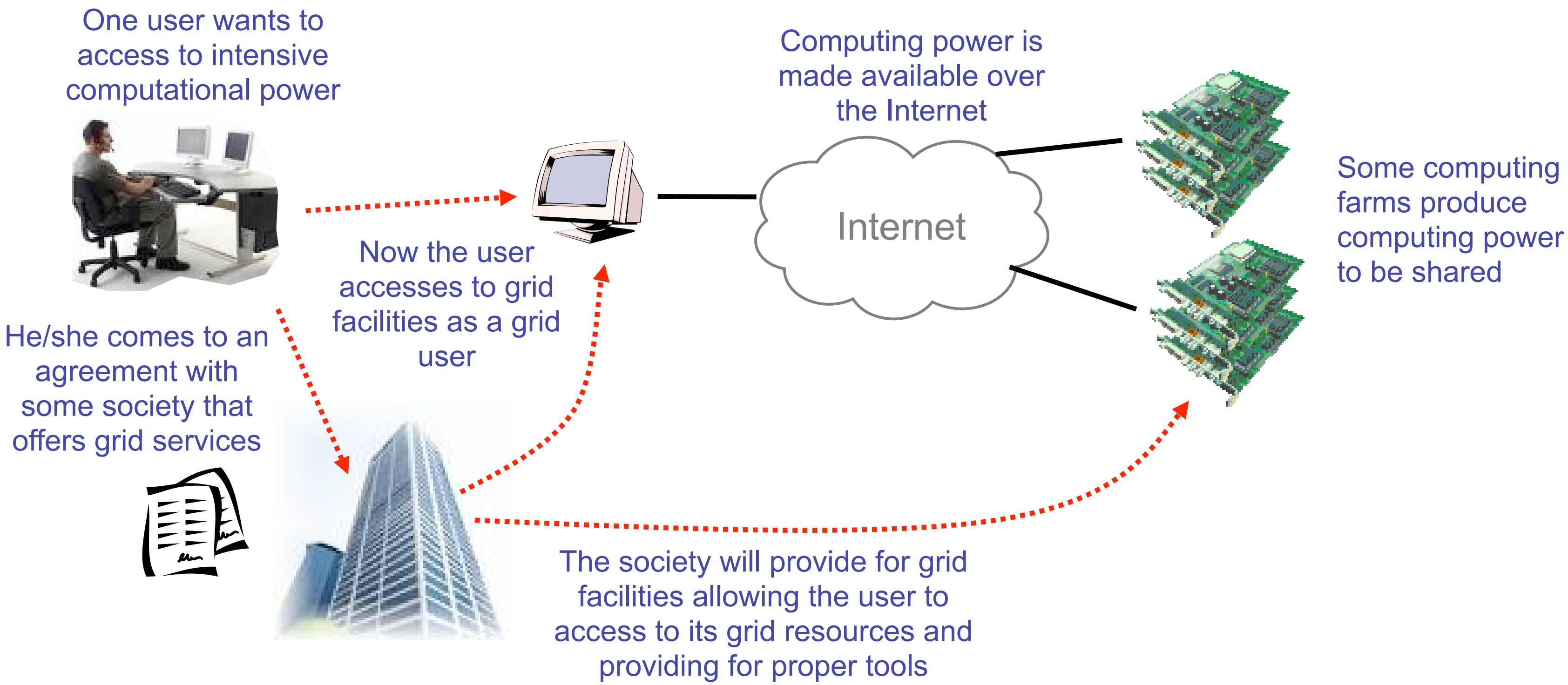
Internet

Some computing farms produce computing power to be shared

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

- The user:
  - Does not need to know what stays beyond the user interface

Grid synthesis



One user wants to access to intensive computational power

Computing power is made available over the Internet

Some computing farms produce computing power to be shared

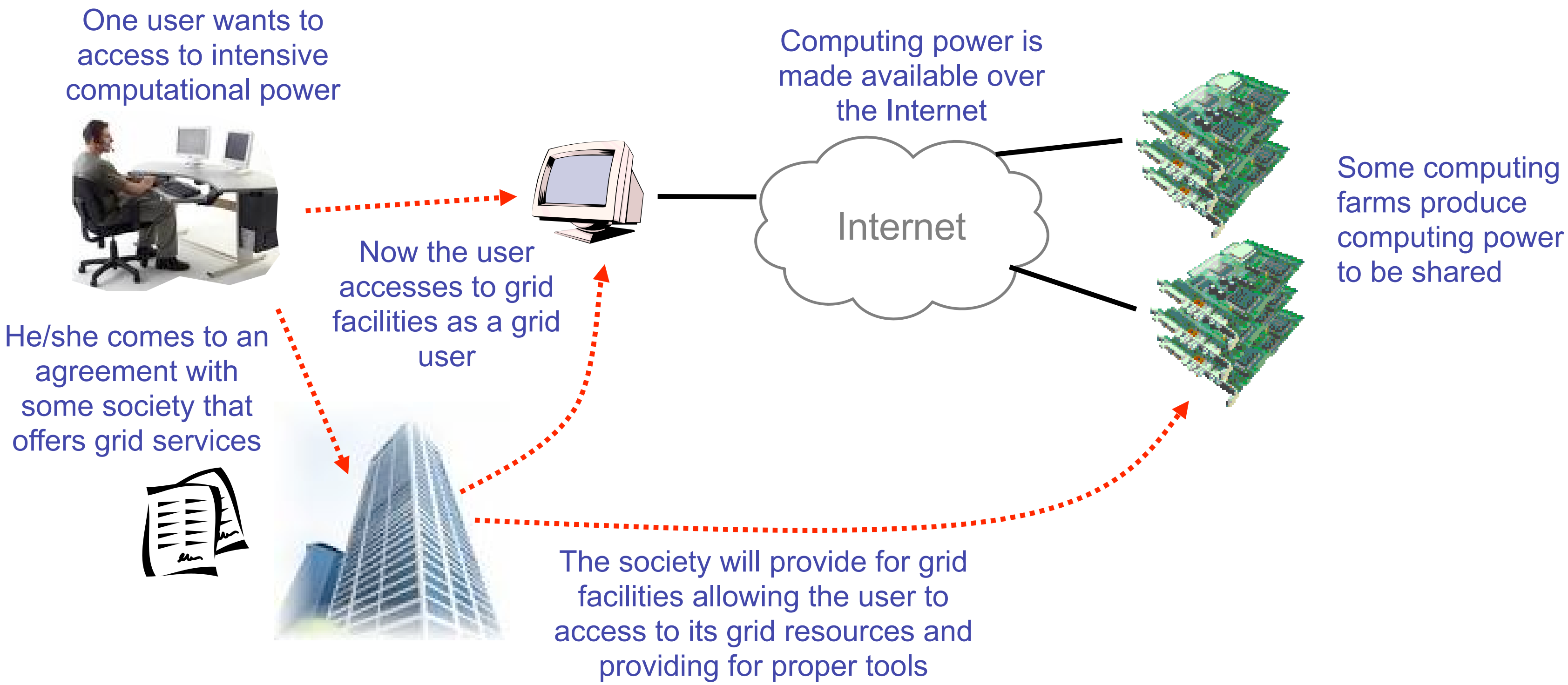
Now the user accesses to grid facilities as a grid user

He/she comes to an agreement with some society that offers grid services

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

- The user:
  - Does not need to know what stays beyond the user interface
  - Can access to a massive amounts of computational power through a simple terminal

Grid synthesis



One user wants to access to intensive computational power

He/she comes to an agreement with some society that offers grid services

Now the user accesses to grid facilities as a grid user

Computing power is made available over the Internet

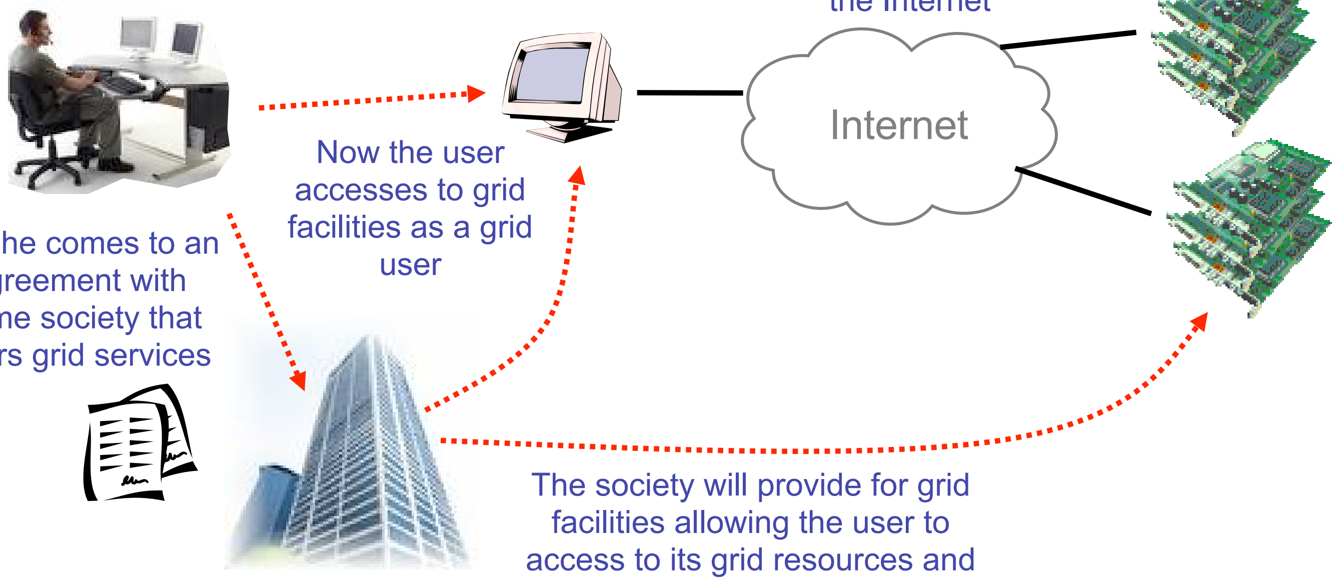
Internet

Some computing farms produce computing power to be shared

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

- The user:
  - Does not need to know what stays beyond the user interface
  - Can access to a massive amounts of computational power through a simple terminal
- The society:

Grid synthesis



One user wants to access to intensive computational power

Computing power is made available over the Internet

Some computing farms produce computing power to be shared

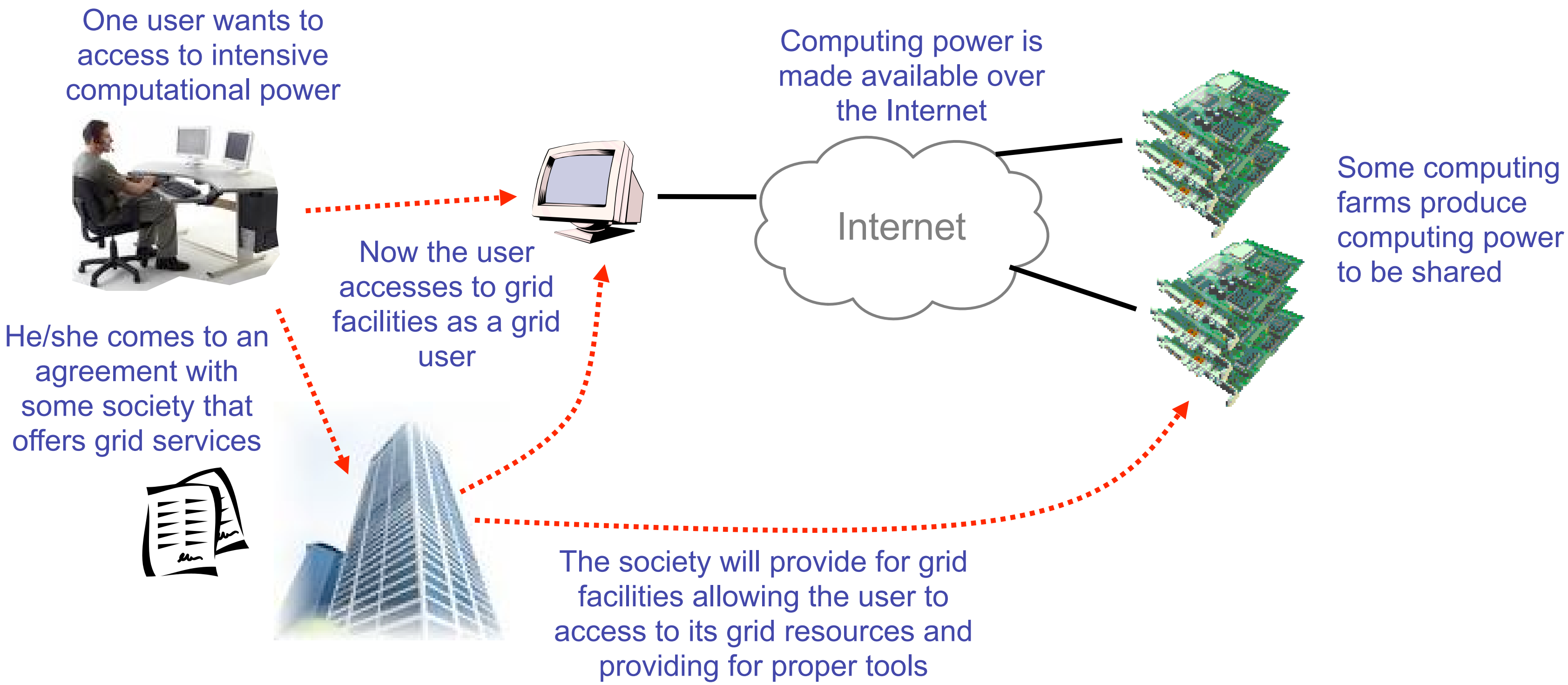
Now the user accesses to grid facilities as a grid user

He/she comes to an agreement with some society that offers grid services

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

- The user:
  - Does not need to know what stays beyond the user interface
  - Can access to a massive amounts of computational power through a simple terminal
- The society:
  - Can extend grid facilities at any moment

Grid synthesis



One user wants to access to intensive computational power

He/she comes to an agreement with some society that offers grid services

Now the user accesses to grid facilities as a grid user

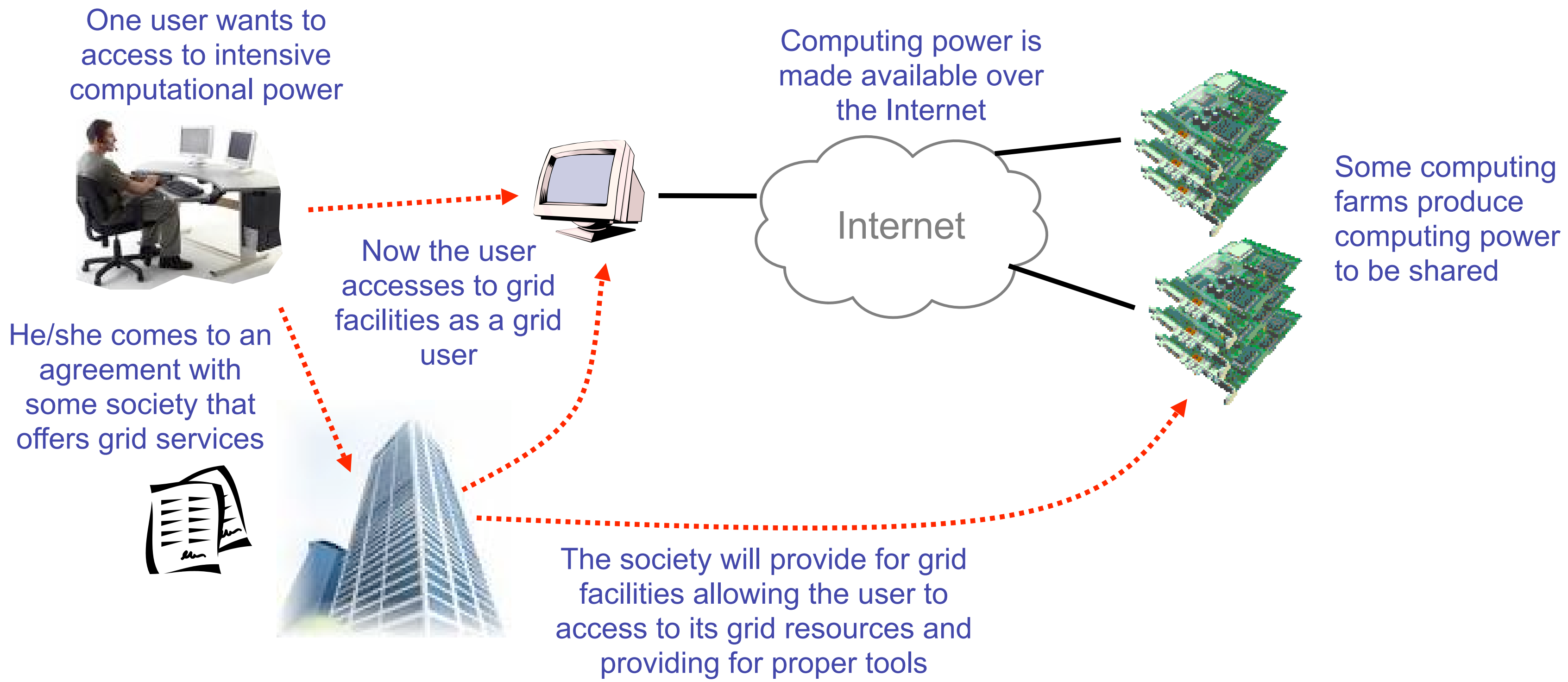
Computing power is made available over the Internet

Some computing farms produce computing power to be shared

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

- The user:
  - Does not need to know what stays beyond the user interface
  - Can access to a massive amounts of computational power through a simple terminal
- The society:
  - Can extend grid facilities at any moment
  - Manages the architecture of the grid

Grid synthesis


One user wants to access to intensive computational power

Computing power is made available over the Internet

Some computing farms produce computing power to be shared

Now the user accesses to grid facilities as a grid user

He/she comes to an agreement with some society that offers grid services

The society will provide for grid facilities allowing the user to access to its grid resources and providing for proper tools

- The user:
  - Does not need to know what stays beyond the user interface
  - Can access to a massive amounts of computational power through a simple terminal
- The society:
  - Can extend grid facilities at any moment
  - Manages the architecture of the grid
  - Defines policies and rules for accessing to grid resources

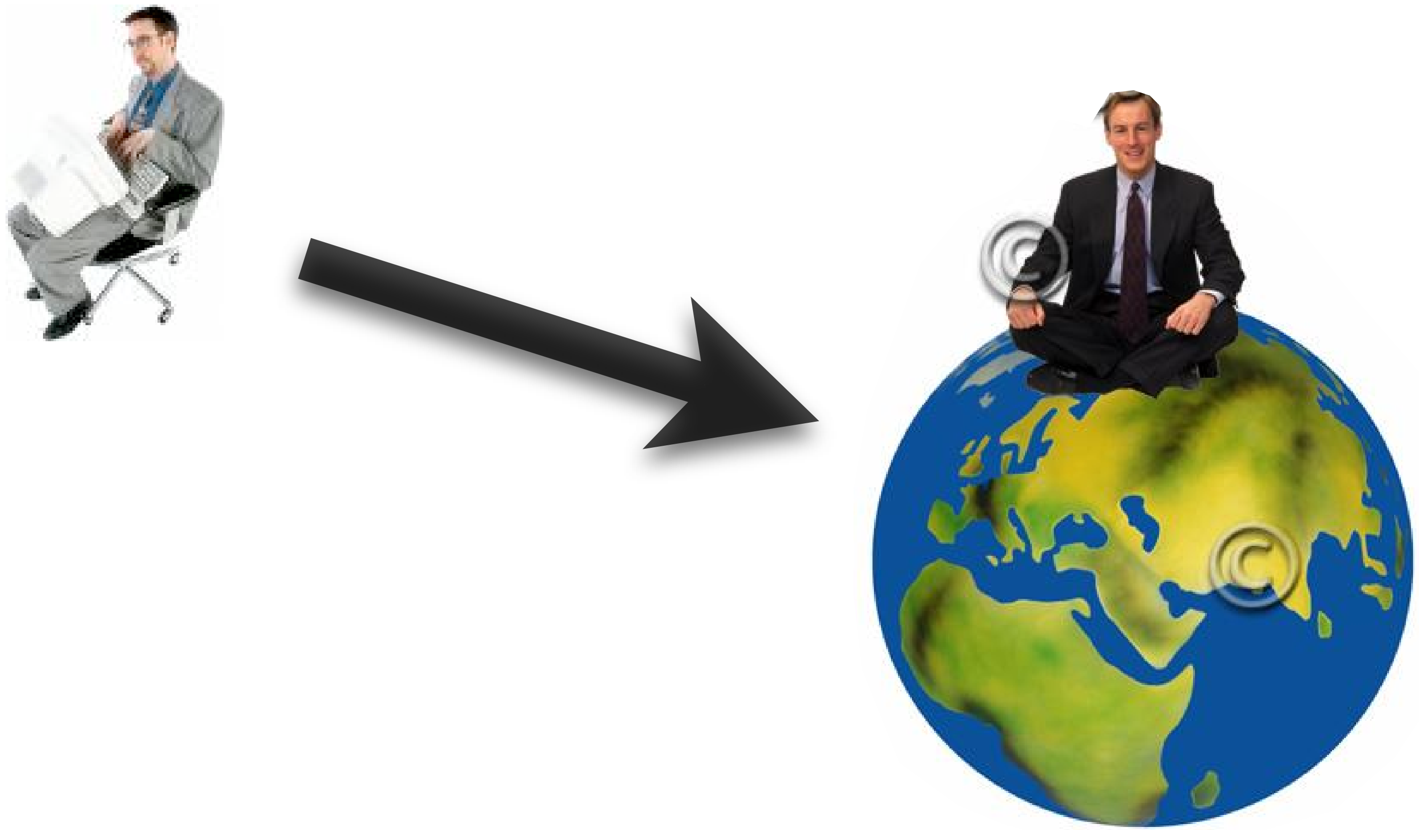
Applications for Grid

- Computation intensive
  - Interactive simulation (climate modeling)
  - Large-scale simulation and analysis (galaxy formation, atomistic simulations)
  - Engineering (parameter studies, optimization model)
- Data intensive
  - Experimental data analysis (e.g., H.E.P.)
  - Image & sensor analysis (astronomy, climate)
- Distributed collaboration
  - Online instrumentation (microscopes, x-ray) Remote visualization (climate studies, biology)
  - Engineering (large-scale structural testing)

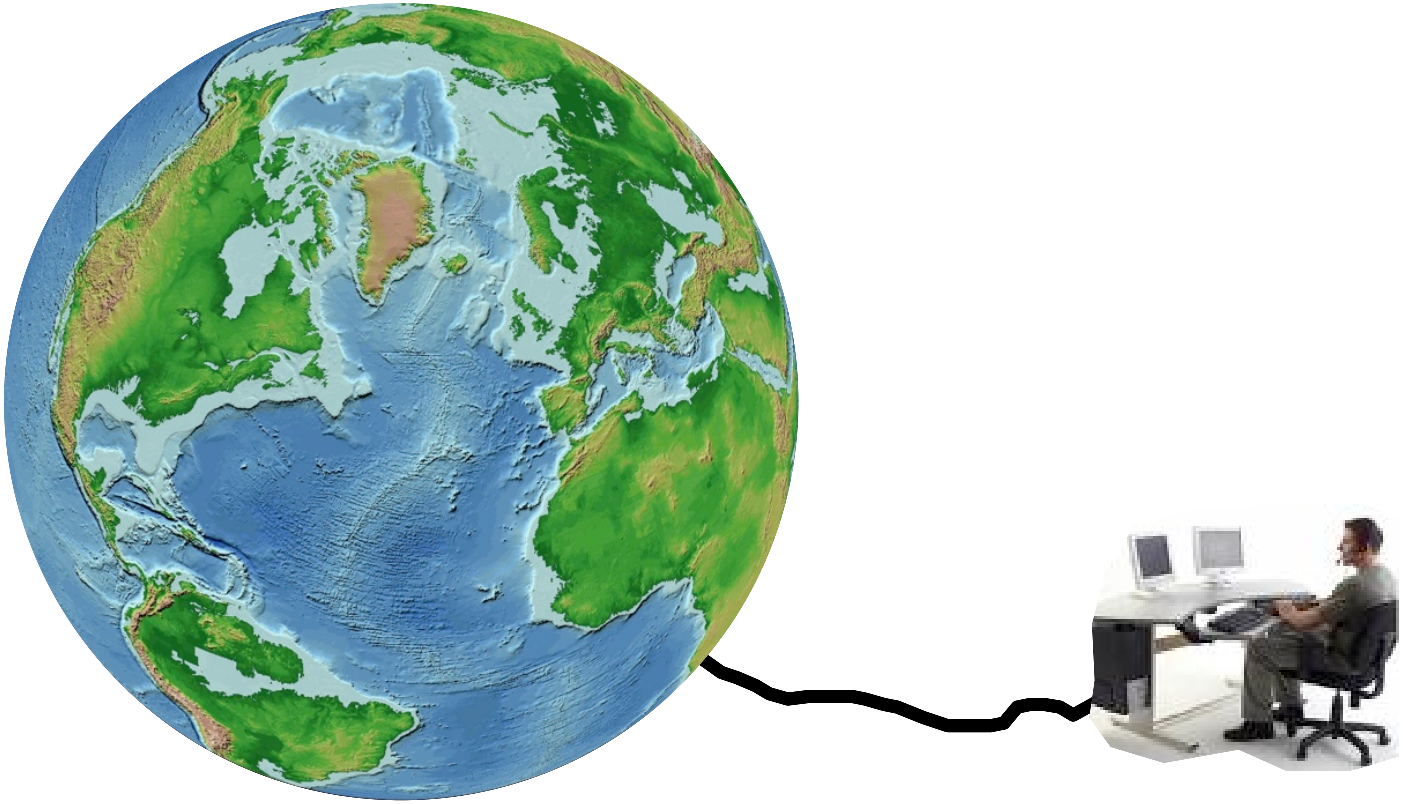
Virtual Organizations

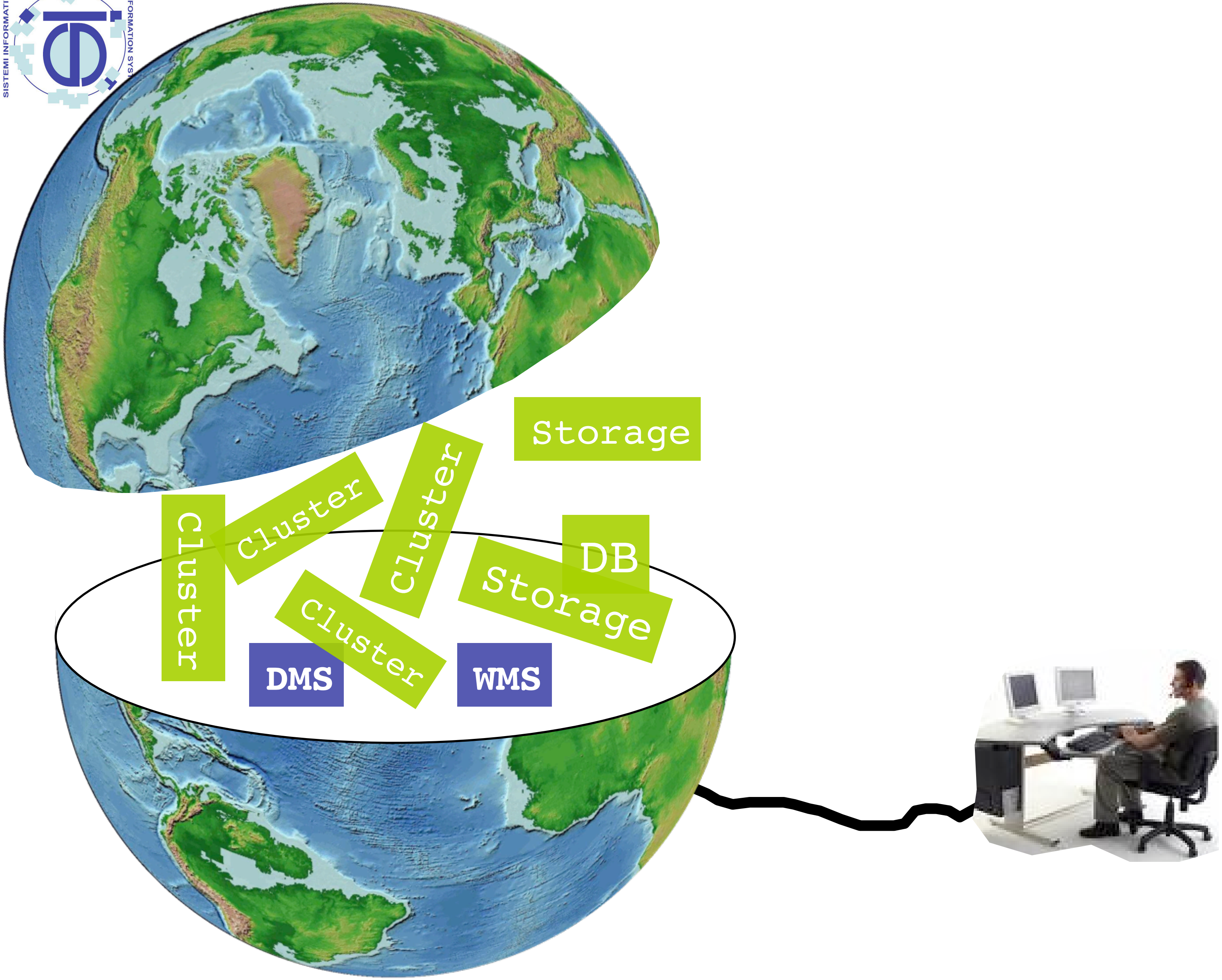
- Virtual Organization (VO)
  - Is a collection of people and resources working together to achieve the same goal
  - It is cross-domain (people and resources)
- One user
  - Identified by his/her personal X.509 certificate issued by trusted Certification Authorities (CA)
  - Can belong to more than one VO at the same time
  - Does not require detailed knowledge of grid technologies to access to the Grid

A change in the paradigm



What is the Grid?




Storage
Cluster
Cluster
Cluster
DB
Storage
Cluster
DMS
WMS

What is a Grid resource?

- Group of sites glued by the MIDDLEWARE;
- Sites are homogeneous as regards SW: Scientific Linux 30X Cern release;
- Sites are not homogeneous as regards HW: x86/x86_64 arch but of different kind and some supercomputer.
- Some collective services: WMS, DMS, VOMS etc…

What is a Grid site?

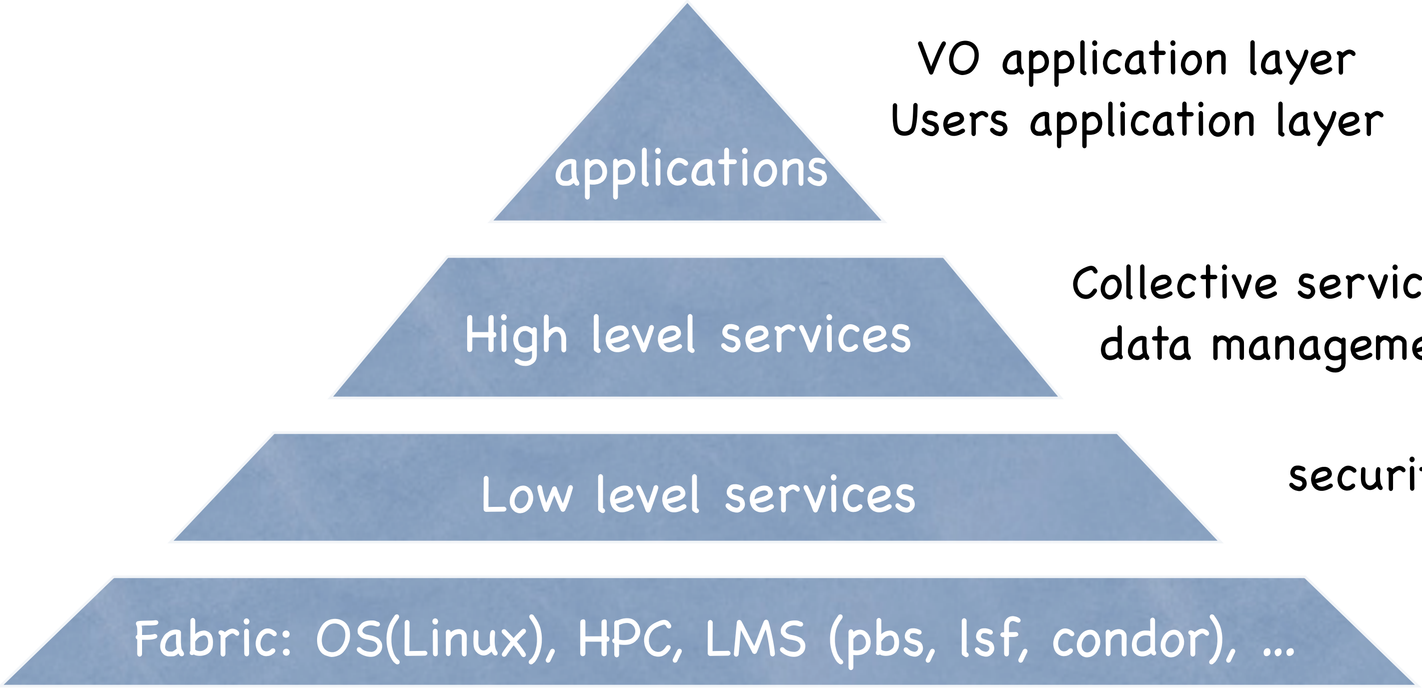
- Computing Element
- Storage Element
- Worker Nodes

- Master node
- Storage
- Cluster nodes

Scheduler+queue system
(PBS, LSF, Condor etc.)

INAF ISTITUTO NAZIONALE DI ASTROFISICA

The middleware layers



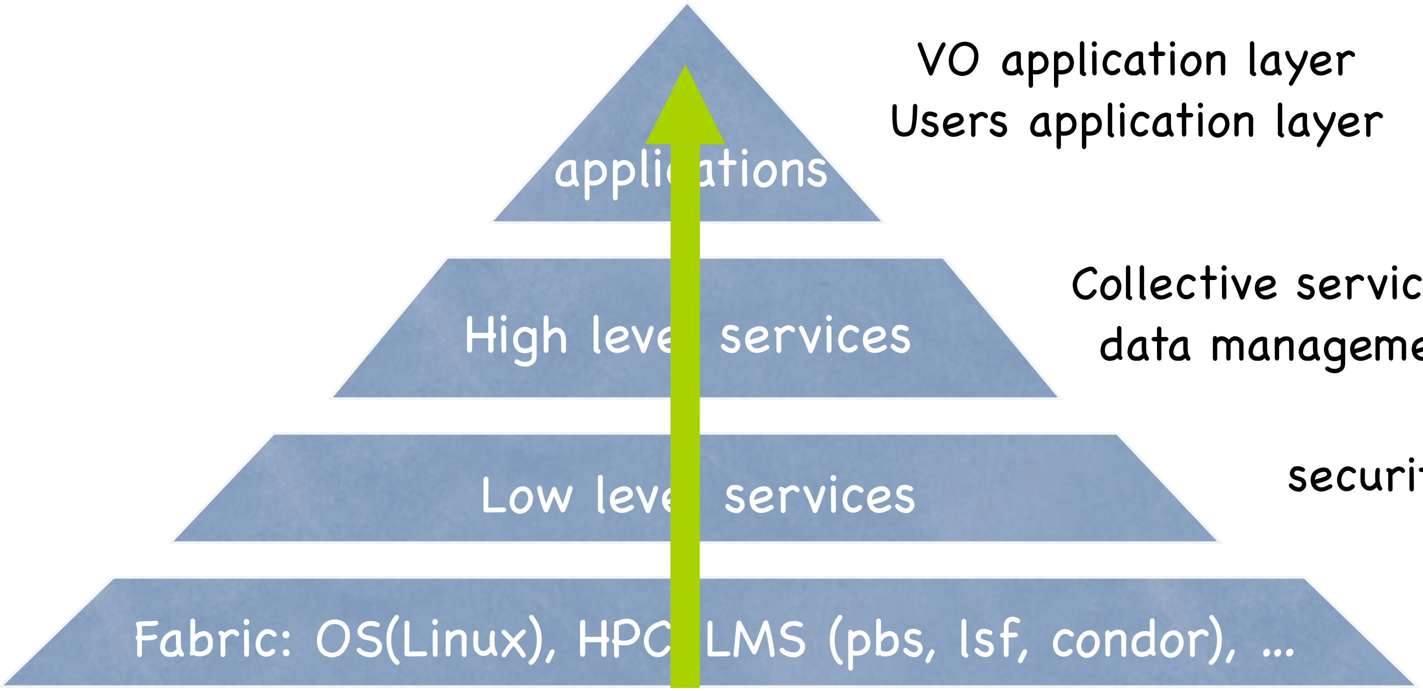
VO application layer
Users application layer

Collective services: scheduling, data management, info sys…

security, jobs, …

execution, files storing,…

The middleware layers



applications

High level services

Low level services

Fabric: OS(Linux), HPC, LMS (pbs, lsf, condor), …

VO application layer
Users application layer

Collective services: scheduling,
data management, info sys…

security, jobs, …

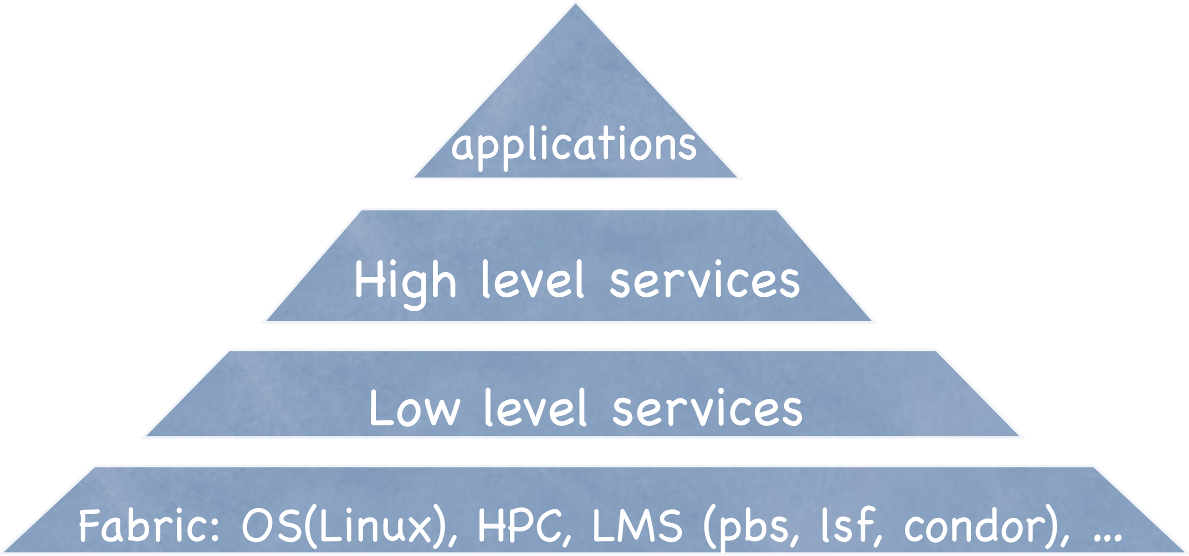
execution,
files storing,…

Middleware pillars

- Security:authentication and authorization
- Job management
- Monitoring and Discovery system
- Data management

Low level services

- Globus Alliance
- Globus Toolkit



applications

High level services

Low level services

Fabric: OS(Linux), HPC, LMS (pbs, lsf, condor), …

What is Globus Toolkit

- Collection of open source software
  - Provides low-level building blocks,
  - Medium-level services,
- You can use all GT or some part
- Usually people build their grids starting from GT

Which GT?

- Actual version is 4. (WS oriented)
- GT 2.4.3
  - It is the pre-webservices version, it is no more no more modified
  - It is included in any newer version of Globus.
  - It is in gLite and LCG middleware

The security problem

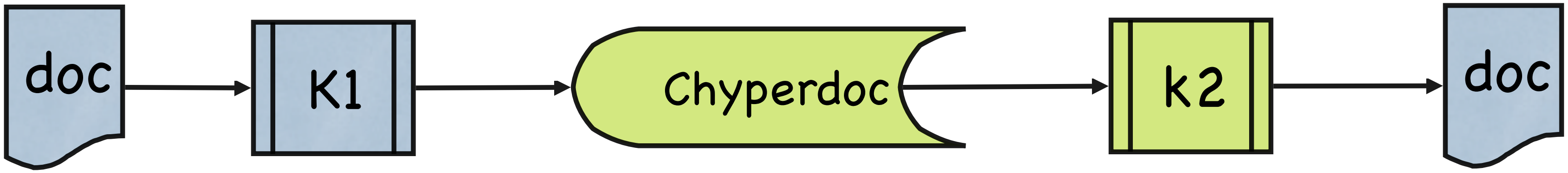
- **<u>Grid is a highly complex system</u>**
- Authentication: establishing identity
- Authorization: establishing rights
- Message protection

- Passwords are not scalable and secure

What we require to security

- Users point of view
  - – Easy to use, transparent, single-sign on, no password sharing
- Administrators point of view
  - – Define local access control
  - – Define local polices

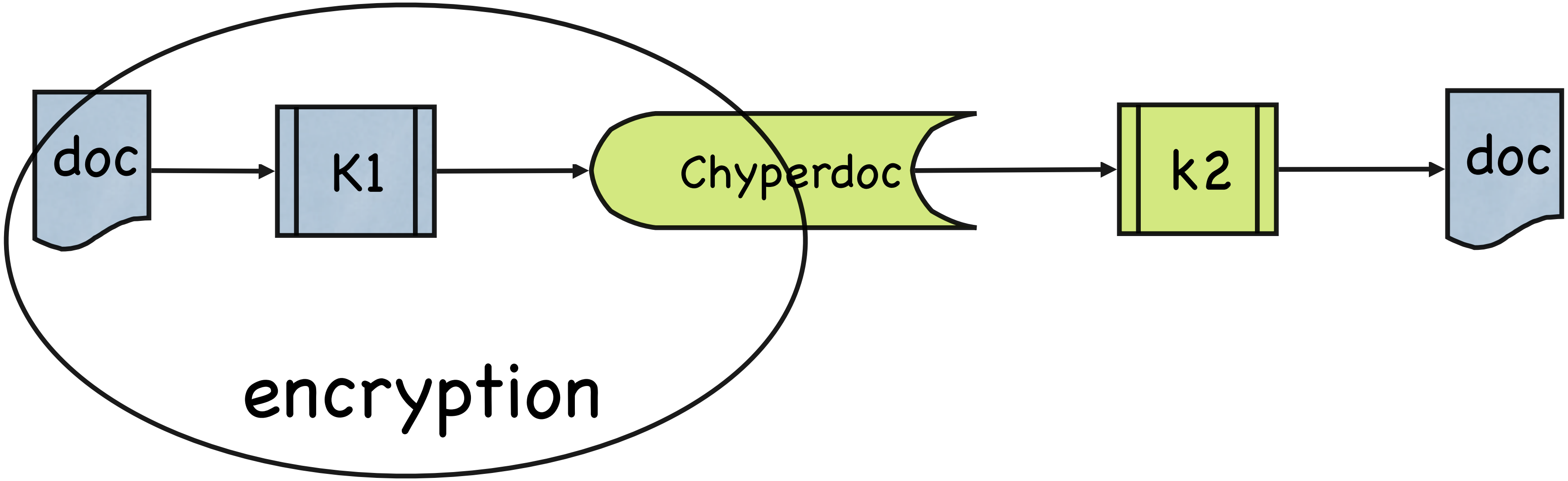
Cryptography primer



Symmetric algorithms: K1 == K2

Asymmetric algorithms: K1 != K2

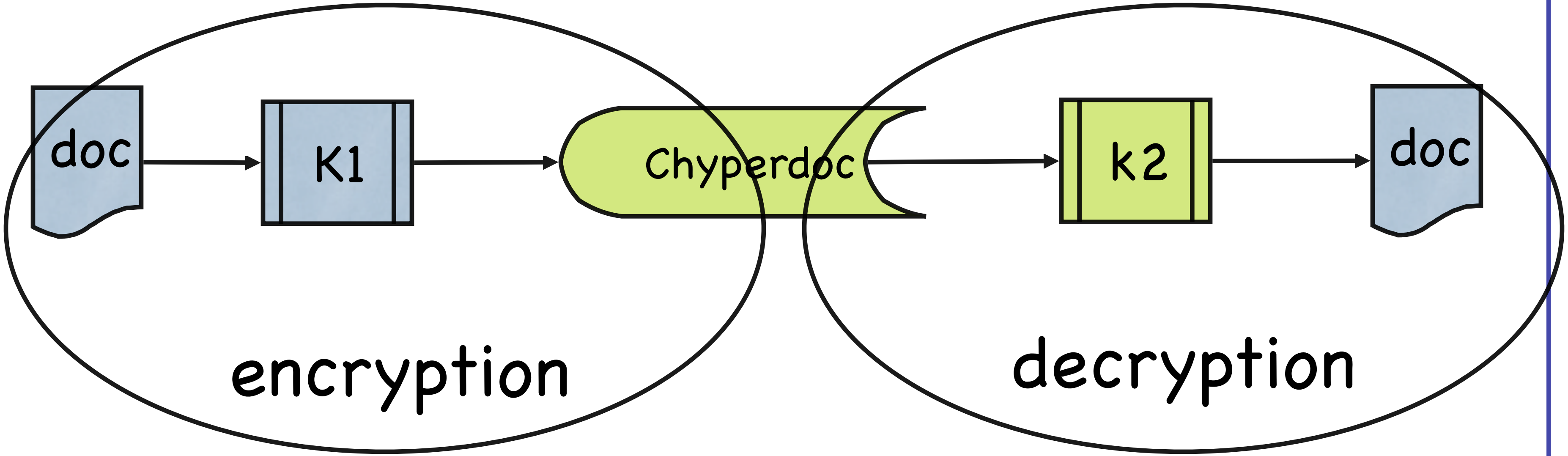
Cryptography primer



Symmetric algorithms: K1 == K2

Asymmetric algorithms: K1 != K2

Cryptography primer



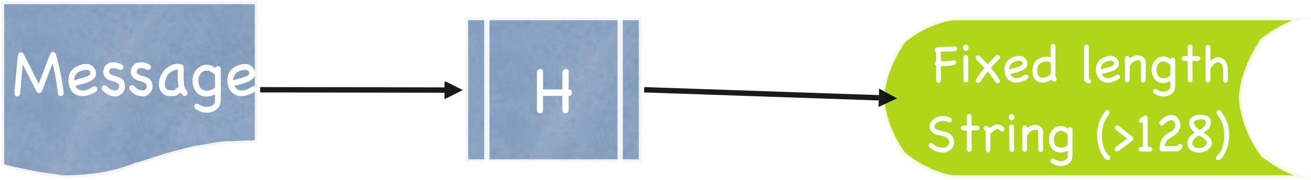
Symmetric algorithms: K1 == K2

Asymmetric algorithms: K1 != K2

PKI

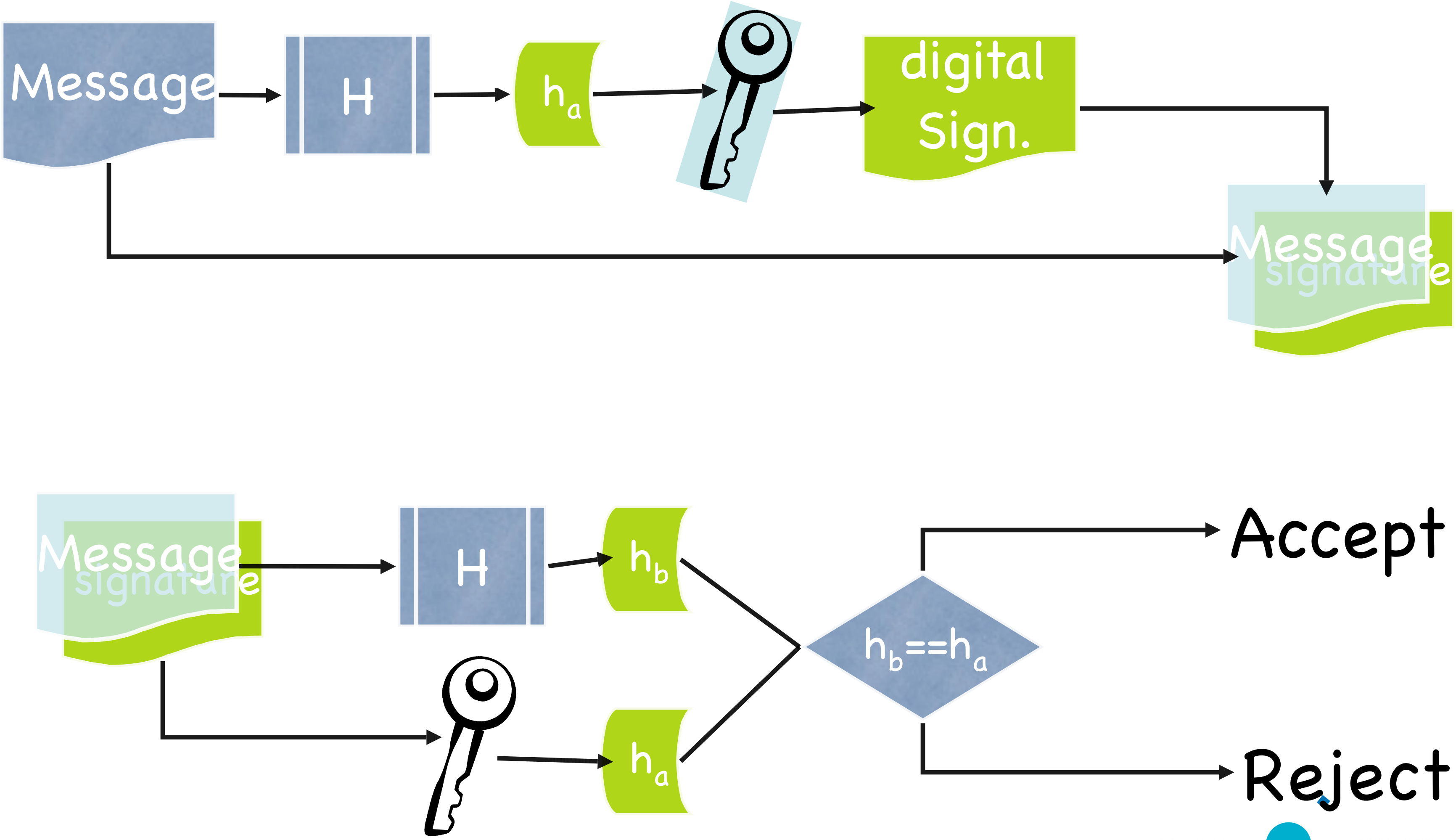
- Based on asymmetric algorithms
- Two keys: private key and public key
- It is “impossible” to derive private from public
- Data encrypted with one key can be only decrypted with the other

The hash function



- Easy to calculate
- Unique
- MD4, SHA etc.

The digital signature



Digital Certificate

- How can I be sure that user “A” is really “A”?
  - Someone else should guarantee the public key and the identity
  - Both “A” and “B” must trust this “third party”
- “web of trust” or Certification Authority

GRID Security Infrastructure

- Public key infrastructure (PKI)
- PKI: a key <=> a user
- PKI: asymmetric encryption
- X509 certificate

X.509 certificate

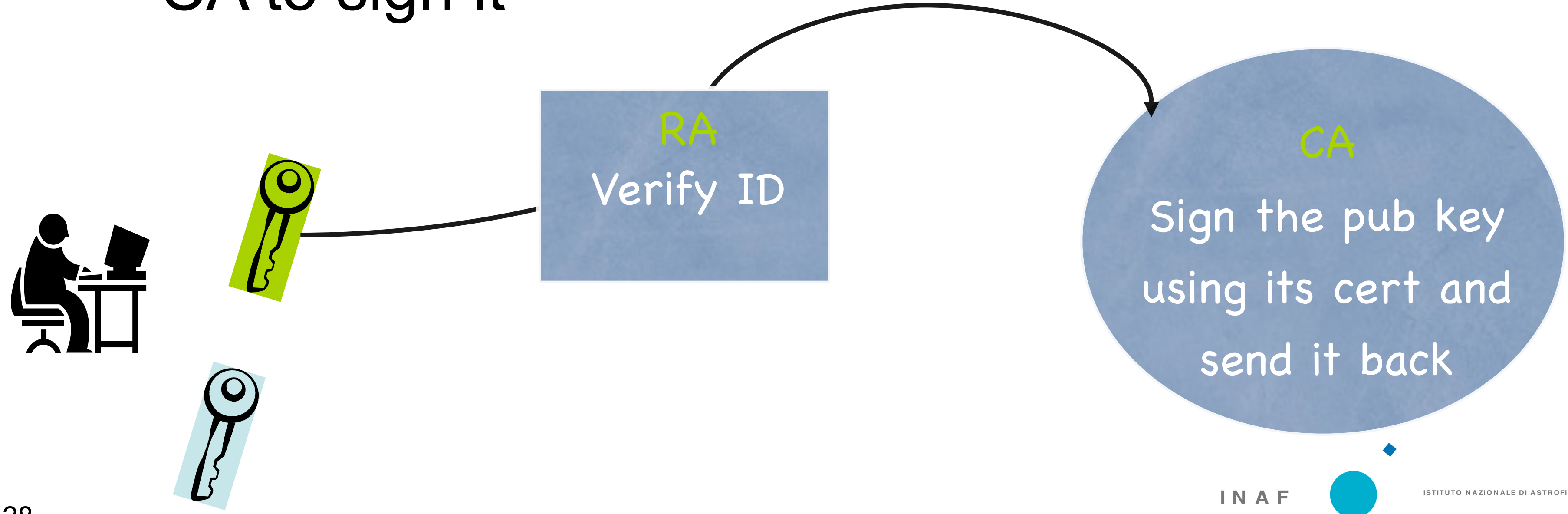
- ITU-T standard for PKI
- X.509 == IETF PKI cert + CRL of X.509v3 standard

- Certificate
- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
- Subject
- Subject Public Key Info
- Public Key Algorithm
- Subject Public Key
- Issuer Unique Identifier (Optional)
- Subject Unique Identifier (Optional)
- Extensions (Optional)
- ...
- Certificate Signature Algorithm
- Certificate Signature

United Kingdom of Great Britain and Northern
Passport Passeport
GBR
00 0000
BLOND
JAMIE
THE VILLAGE
0
M/F PORTMEIRION
29 JULY/JUIL 01
UNITED KI
PASSPORT
29 JULY/JUIL 11
P<GBTR<<JAMIE<BLOND<<<<<<<<<<<<<<<<<<<<<<
00 0000 000 0 00<<<<<<<<<<<<<<<<<<<<<<<<<

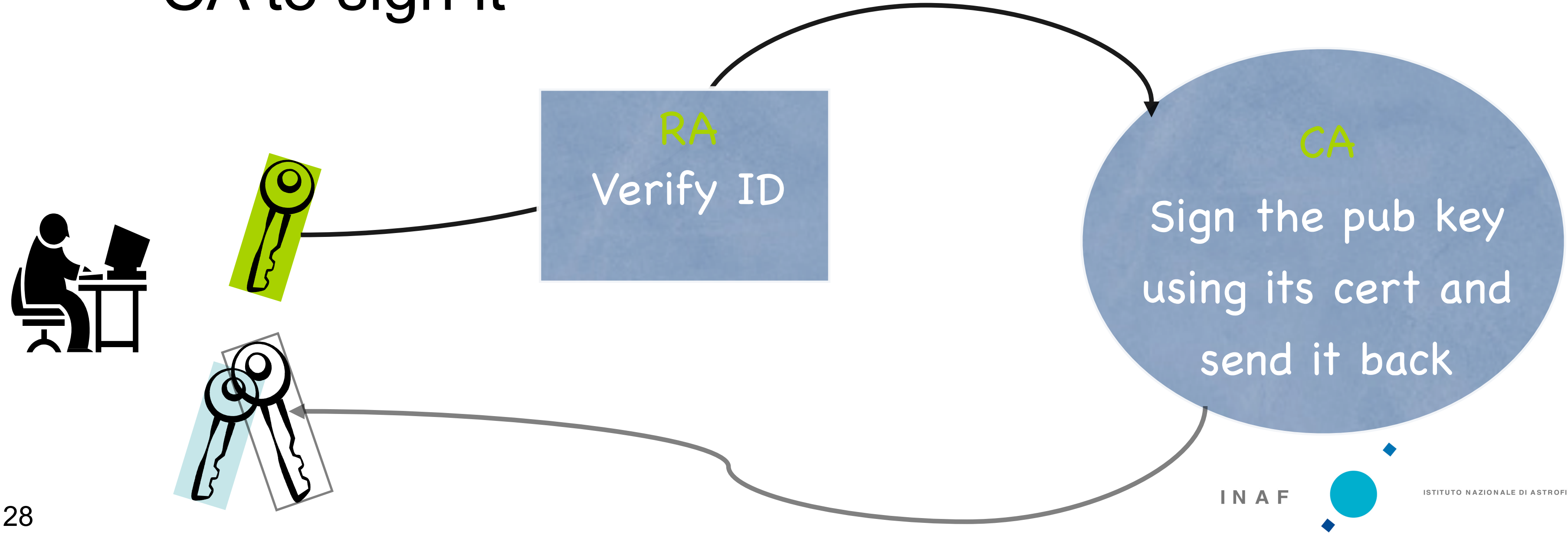
The role of CAs

- CA sign certificates
- CA PK can be used to verify a certificate
- To request a certificate a user must ask the CA to sign it



The role of CAs

- CA sign certificates
- CA PK can be used to verify a certificate
- To request a certificate a user must ask the CA to sign it



RA

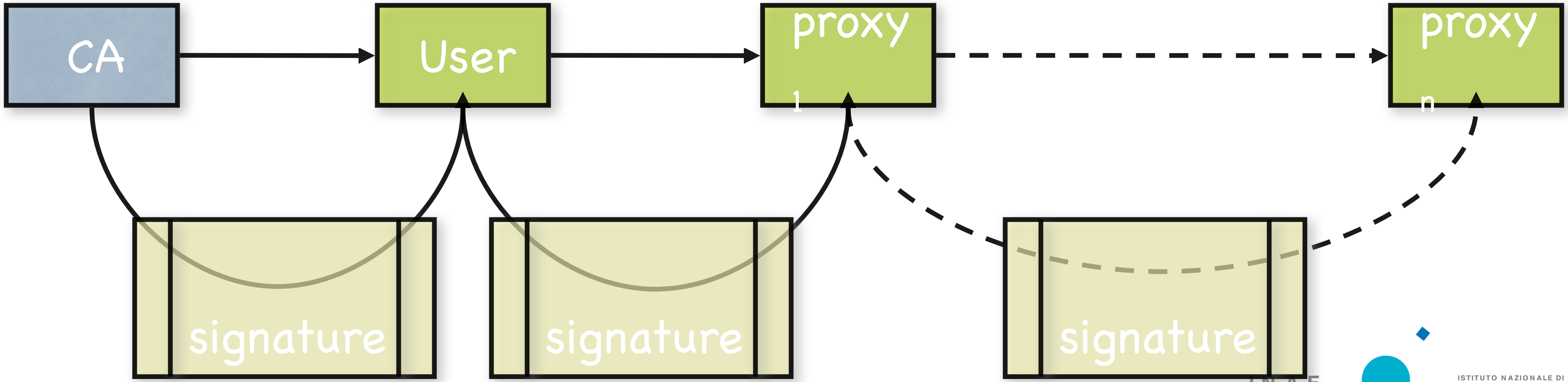
Verify ID

CA

Sign the pub key using its cert and send it back

GSI - proxies

- To support delegation: A delegates to B the right to act on behalf of A
- proxy certificates *extend X.509 certificates*
  - Short-lived certificates signed by the user’s certificate or a proxy
  - Reduces security risk, enables delegation



“Login” to the grid

- User cert lasts for a few months (~1 year)
- Proxy has a limited lifetime (minimized risk of “compromised credentials”)
- Proxy cert is created by the **grid-proxy-init** command

```
% grid-proxy-init
Your identity: /C=IT/O=INFN/OU=Personal/L=
Enter GRID pass phrase for this identity:
Creating proxy ........................................... Done
Your proxy is valid until: Thu Aug 31 21:56:18 2006
```

Passwd protected

Grid-proxy-init

- Private key is used to sign a proxy certificate with <u>its own</u>, new public/private key pair.
  - User’s private key not exposed after proxy has been signed
- Proxy is saved as /tmp/x509up_u503 readable only by the user.
- Proxy life is 12 hours user my change it

```
% grid-proxy-init -valid
<h:m>
```

Manage your proxy

- Check its validity
- Destroy it

```
%  grid-proxy-info
subject  : /C=IT/O=INFN/OU=Personal Certificate/L=INAF Trieste/CN=“userid”/CN=proxy
issuer   : /C=IT/O=INFN/OU=Personal Certificate/L=INAF Trieste/CN=“userid”
identity : /C=IT/O=INFN/OU=Personal Certificate/L=INAF Trieste/CN=“userid”
type     : full legacy globus proxy
strength : 512 bits
path     : /tmp/x509up_u503
timeleft : 11:46:39
% grid-proxy-destroy
%
```

MyProxy

- You may need:
  - To interact with a grid from many machines
  - To use a portal, and delegate to the portal the right to act on your behalf
  - To run jobs that might last longer than the lifetime of a short-lived proxy
- Solution: “MyProxy repository”

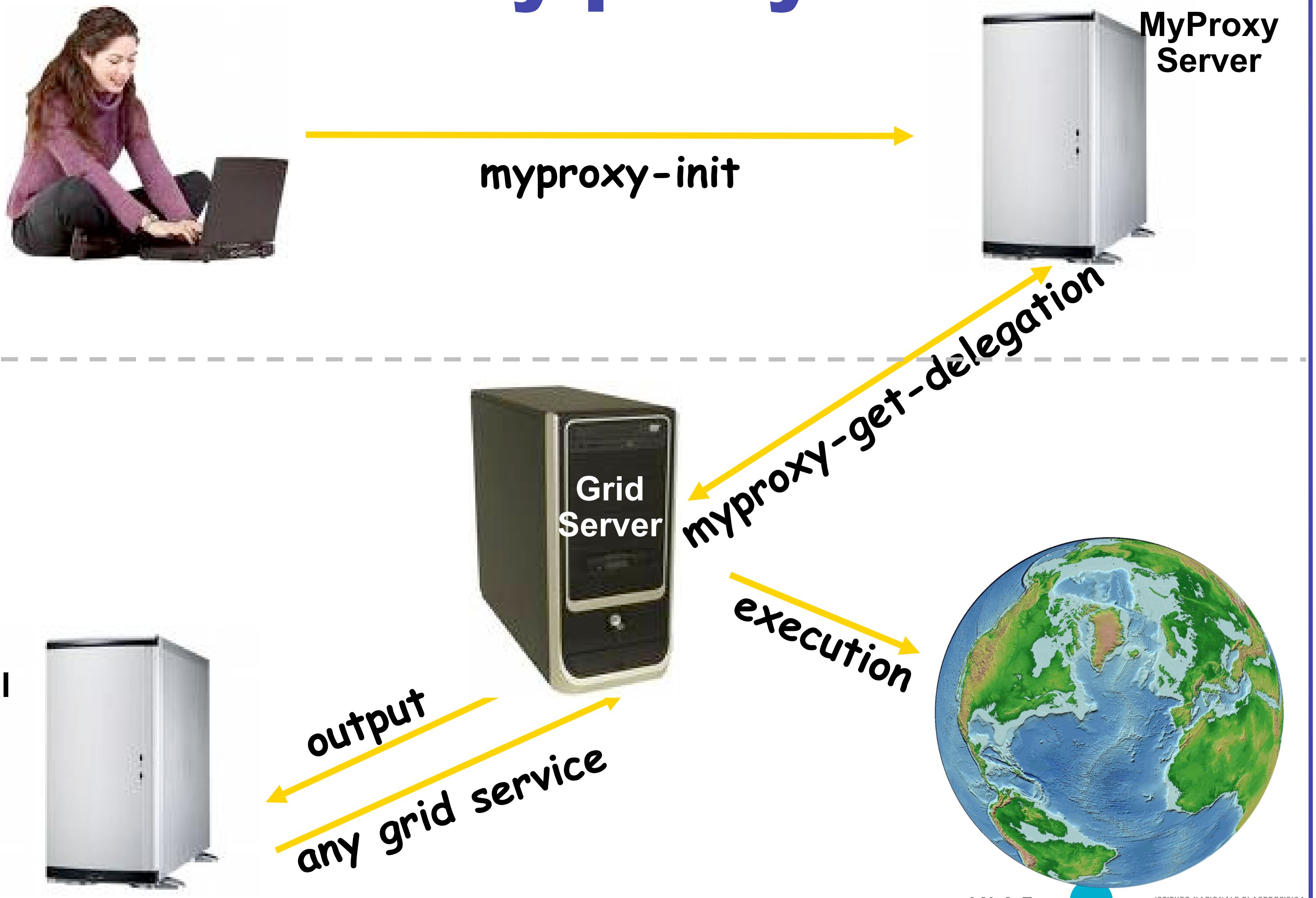
Long term jobs

- Proxy must have a limited lifetime
- When your proxy expires you lost your job.
- myproxy server:
  - Allows to create and store a long term proxy certificate:
- A dedicated service on the WMS can renew automatically the proxy

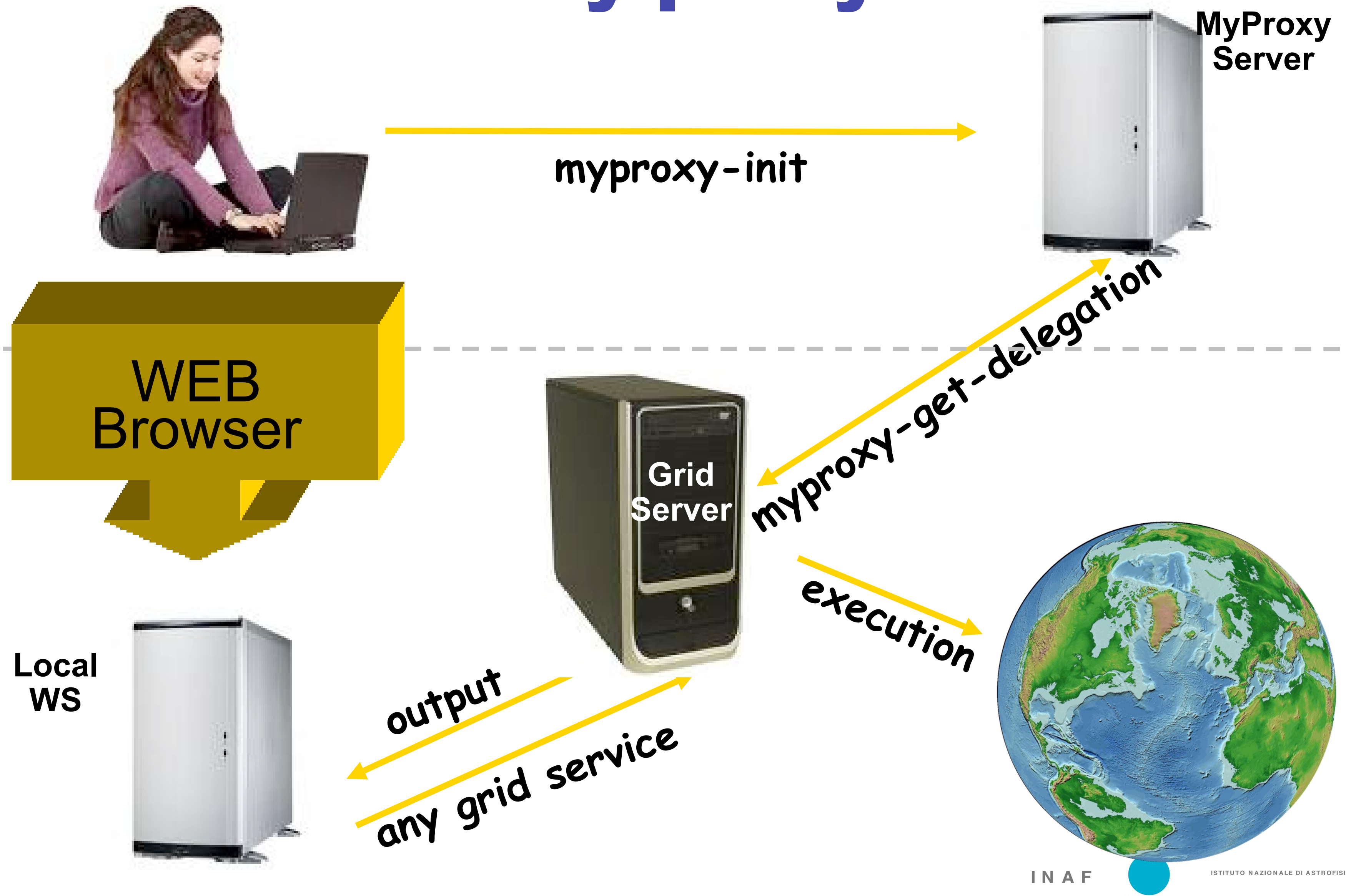
What is my-proxy?

- Online CA
  - Issues short-lived X.509 End Entity Cert
  - Avoid need for long-lived user keys
- Online Credential Repository
  - Issues short-lived X.509 proxy cert
  - Long-lived private keys never leave the server
- Supporting multiple authentication
  - passphrase, cert, PAM, etc.
- Open Source Software

My-proxy


MyProxy
Server
myproxy-init
myproxy-get-delegation
Grid
Server
execution
Local
WS
output
any grid service

My-proxy

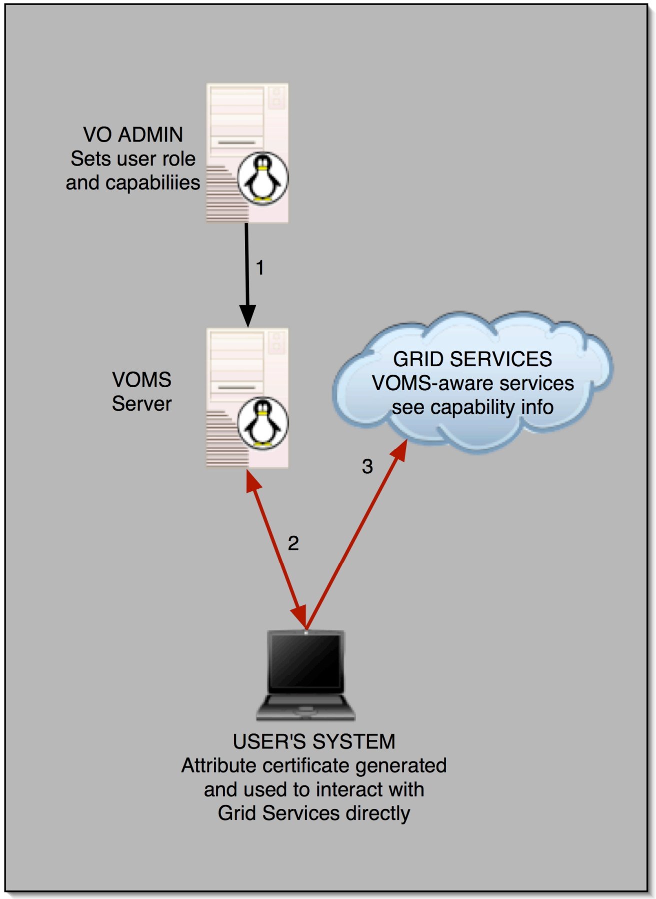

MyProxy Server
myproxy-init
WEB Browser
Grid Server
myproxy-get-delegation
execution
Local WS
output
any grid service

Authorization with GSI

- User is authorized as a member of a single VO
- All VO members have same rights
- Gridmapfiles are updated by VO management software: map the user’s DN to a local account
- grid-proxy-init

VOMS

- User can deal with multiple VOs
  - Aggregate rights
- VO can have groups
  - Different rights for each
  - Nested groups
- VO has roles
  - Assigned to specific purposes
- Proxy certificate carries the additional attributes



VOMS proxy init

- Fully compatible with Globus Toolkit
- Each VO has a database containing group membership, roles and capabilities information for each user
- User contacts VOMS server requesting his authorization info
- Server send authorization info to the client, which includes them in a proxy certificate

VOMS proxy init

- Fully compatible with Globus Toolkit
- Each VO has a database containing group membership, roles and capabilities information for each user
- User contacts VOMS server requesting his authorization info

```
% voms-proxy-init --voms gilda
Cannot find file or dir: /home/giorgio/.glite/vomses
Your identity: /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/
CN=Emidio Giorgio/Email=emidio.giorgio@ct.infn.it
Enter GRID pass phrase:
Your proxy is valid until Mon Jan 30 23:35:51 2006
Creating temporary
proxy.............................Done
Contacting  voms.ct.infn.it:15001 [/C=IT/O=GILDA/OU=Host/
L=INFN Catania/CN=voms.ct.infn.it/Email=] "gilda"
Creating proxy .................................... Done
Your proxy is valid until Mon Jan 30 23:35:51 2006
```

Get info from your proxy

- FQAN are included in an Attribute Certificate
- Attributes <=> identity

```
$ voms-proxy-init --voms gilda:/gilda/Role=<user>
$ voms-proxy-info -fqan
/gilda/Role=<user>/Capability=NULL
$ voms-proxy-info -all
subject   : /C=IT/O=INFN/OU=Personal Certificate/L=IN
issuer    : /C=IT/O=INFN/OU=Host/L=CNAF/CN=voms.cnaf.infn.it
attribute : /inaf/Role=<user>/Capability=NULL
timeleft  : 11:59:47
```

Job Management

- The challenge:
  - enabling access to heterogeneous resources and managing remote computation
- The solution:
  - Grid Resource Allocation Management protocol (GRAM)

Job Management Goal

- Provide a service to securely:
  - Create an environment for a job
  - Stage files to/from environment
  - Cause execution of job process(es)
  - Via various local resource managers
  - Monitor execution
  - Signal important state changes to client
  - Enable client access to output files
  - Streaming access during execution

What is GRAM?

- GRAM is a unifying remote interface to Resource Managers
  - yet preserves local site security/control.
- GRAM is for stateful job control
  - Reliable operation
  - Asynchronous monitoring and control
  - Remote credential management
  - File staging

Job Submission Model

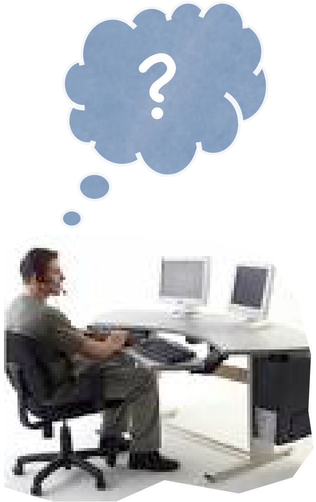
- Create and manage one job on a resource
- Submit and wait
- Not with an interactive TTY
  - File based stdin/out/err
  - Supported by all batch schedulers
- More complex than RPC
  - Optional steps before and after submission message
  - Job has complex lifecycle
    - Staging, execution, and cleanup states
  - Asynchronous monitoring

GRAM implementations

- GT2
  - pre-WebServices
  - proprietary protocol
  - EGEE/LCG
- GT4
  - Web Service Based
  - OGSA

Monitoring and discovery

- What is the status of a site?
- Which resource do I need to contact?
- GT2 MDS is a directory service that is based on the LDAP protocol.



Pre-WS MDS

- The MDS is a directory service that is based on the LDAP protocol.
- It is used to query both static and dynamic information on grid resources such: available CPUs, storage, etc.

MDS4

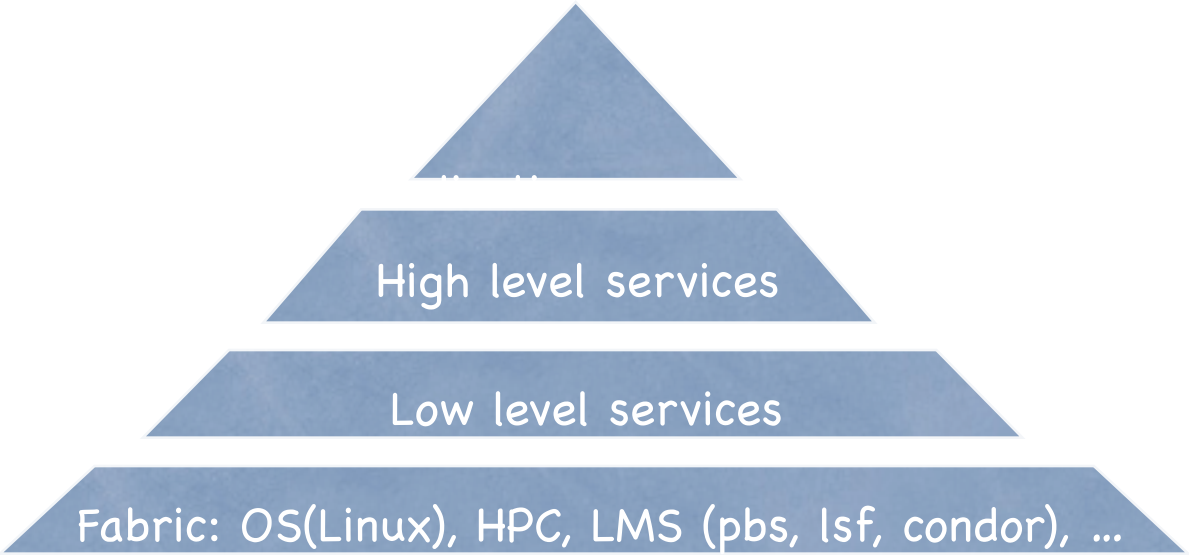
- WS based
- Index Service
  - collects data from various sources and provides a query/ subscription interface to that data
- Trigger Service
  - which collects data from various sources and can be configured to take action based on that data.
- Archive Service
  - access to historic data, is planned for a future release.
- Aggregator services
  - collect recent state information from registered information sources

Data Management

- Requirements
  - Fast: as fast as networks and protocols allow
  - Secure: server must only share files with strongly authenticated clients and no passwords in the clear or similar
  - Robust: Fault tolerant, time-tested protocol
- And the winner is…GRIDFTP

Grid environment

- Grid high level of complexity
- Direct the whole system
- High level services (on top of all)



Information & Monitoring

- Which resources are available?
- Where are them?
- Which is their status?
- How can I optimize their use?

We need a general information infrastructure:
Information System

Information system

- Uniform and Flexible access
- Scalable access to dynamic data
- Multiple information sources
- GIIS has its own scalability limits
  - GIIS kept at site level

IS solutions

- LCG BDII
  - LDAP with BD backend
  - Info caching, scalable, centralized.
  - Fast access (LDAP)

- gLite R-GMA
  - RDBMS implementation of GGF Grid Monitoring arch
  - Aggregate service info from multiple sites
  - Generic service discovery API
  - Used for monitoring

Data Management

- Where are data/files?
- Which data/file exist?
- How can I reach it?
- Are they accessible by others?

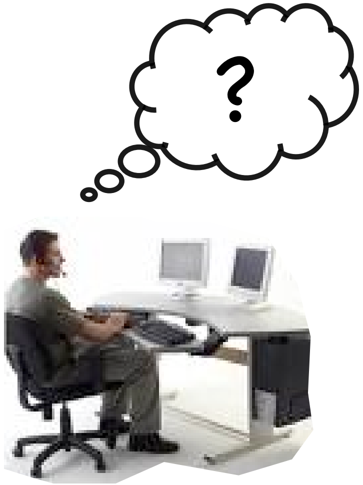
Data Management

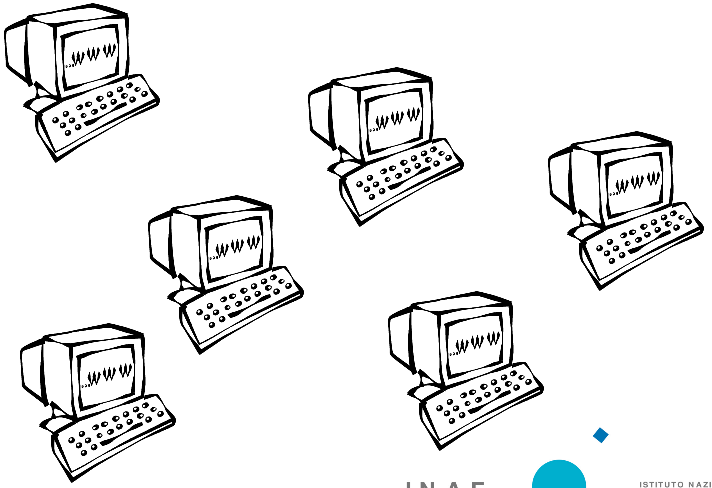
- Where are data/files?
- Which data/file exist?
- How can I reach it?
- Are they accessible by others?

Distributes storage space => filesystem

Job management

- Cooperation infrastructure for WAN distributed resources:
  - – Chaotic system to direct;
  - – Locate, book and use the “right” resource
- Scheduling service





Taxonomy of a scheduling system

- Centralized systems
- Distributed systems
- Hierarchical systems (hybrid type)

Centralized

- Single point of knowledge
- Optimum scheduling
- Single point of failure
- Example: Condor-G

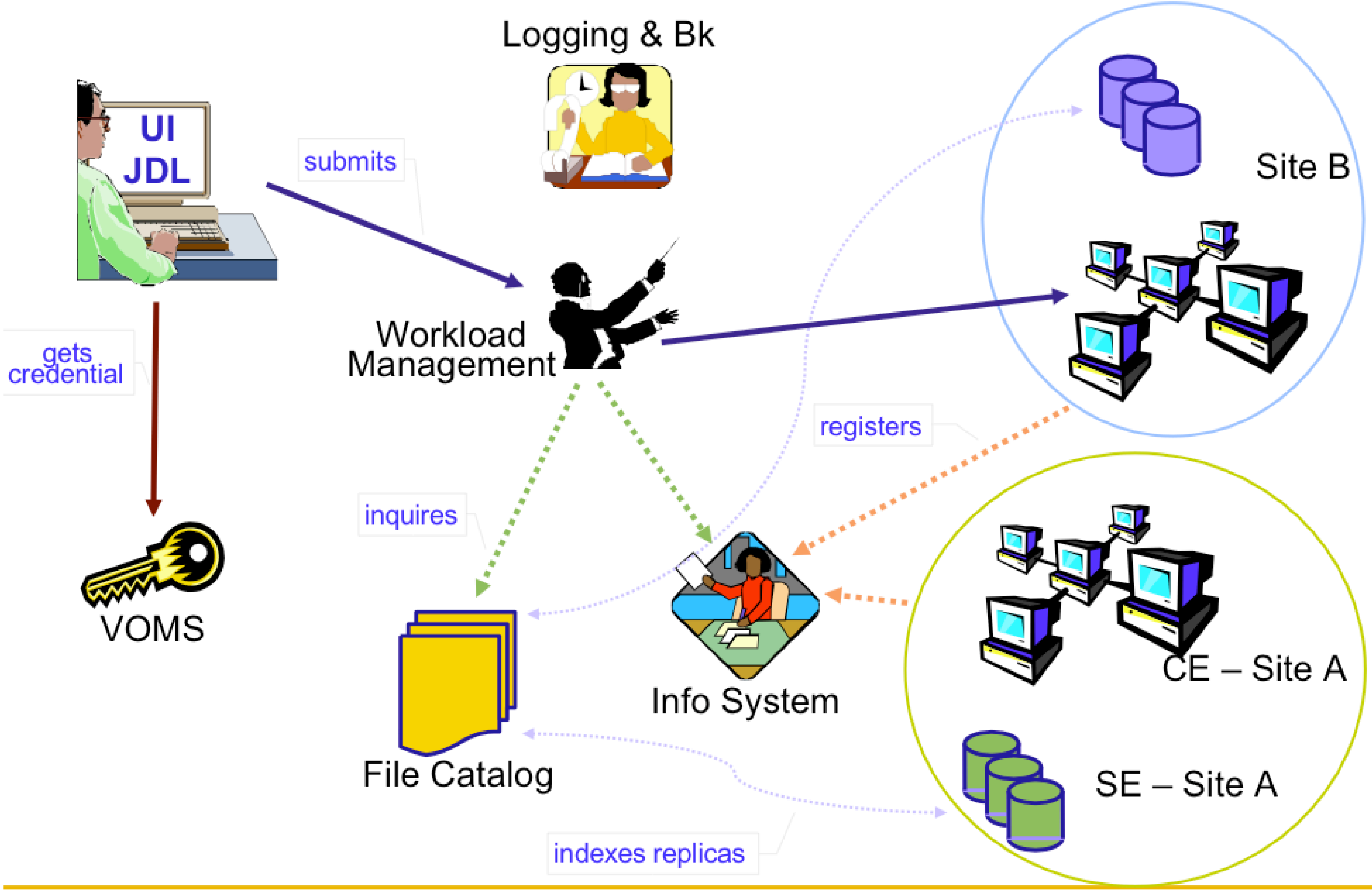
Distributed

- Application delegation method
- Optimum scaling & Fault tolerance
- Sub-optimal resource allocation
- Each Application has to develop a scheduler
- Example: NetSolve

Hybrid

- Distributed systems are scheduled by a centralized one
- Examples: Darwin and Nimrond-G, GridBUS

Glite WMS


Logging & Bk
UI
JDL
submits
gets credential
Workload Management
VOMS
inquires
File Catalog
Info System
registers
Site B
CE – Site A
SE – Site A
indexes replicas

The evolution of Grid architecture

- From Computational Resources to "Computational Resources"
- "Resource" tends to connote a tangible entity to be consumed: CPU, storage,
- New Resources for new needs:
  - Databases, java class
  - INSTRUMENTS and SENSORS

From Resources to Services: Managing Virtual Services

- But many interesting services may be decoupled from any particular resource
  - E.g. virtual data service, data analysis service
  - A service consumes resources, but how that happens is irrelevant to the client
- “Service” forms a better base abstraction
  - Can apply to physical or virtual

Open Grid Services Architecture

- Service-oriented architecture
  - – Key to virtualization, discovery, composition, local-remote transparency
- Leverage industry standards
  - – Internet, Web services
- Distributed service management
  - – A “component model for Web services” (or: a “service model for the Grid”)
- A framework for the definition of composable, interoperable services

Web Services

- A simple but powerful distributed system paradigm, that allows one to:
  - Describe a service (WSDL)
  - Invoke a service (SOAP)
  - Discover a service (various)
- Web services appears to offer a fighting chance at ubiquity (unlike CORBA)
  - Sophisticated tools emerging from industry
- But Web services does not go far enough to serve a common base for the Grid …

Web Services and Grid

- "Web services" address discovery & invocation of persistent services
  - Interface to persistent state of entire enterprise
- In Grids, must also support transient service instances, created/destroyed dynamically
  - Interfaces to the states of distributed activities
  - E.g. workflow, video conf., dist. data analysis
- Significant implications for how services are managed, named, discovered, and used
  - In fact, much of Grid is concerned with the management of service instances

Questions?