Security through Virtualization

inGRiD

DGI

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

MediGRID

Philipps Universität Marburg

Matthew Smith
Niels Fallenbeck
Matthias Schmidt

Distributed Systems Group
Philipps-University Marburg

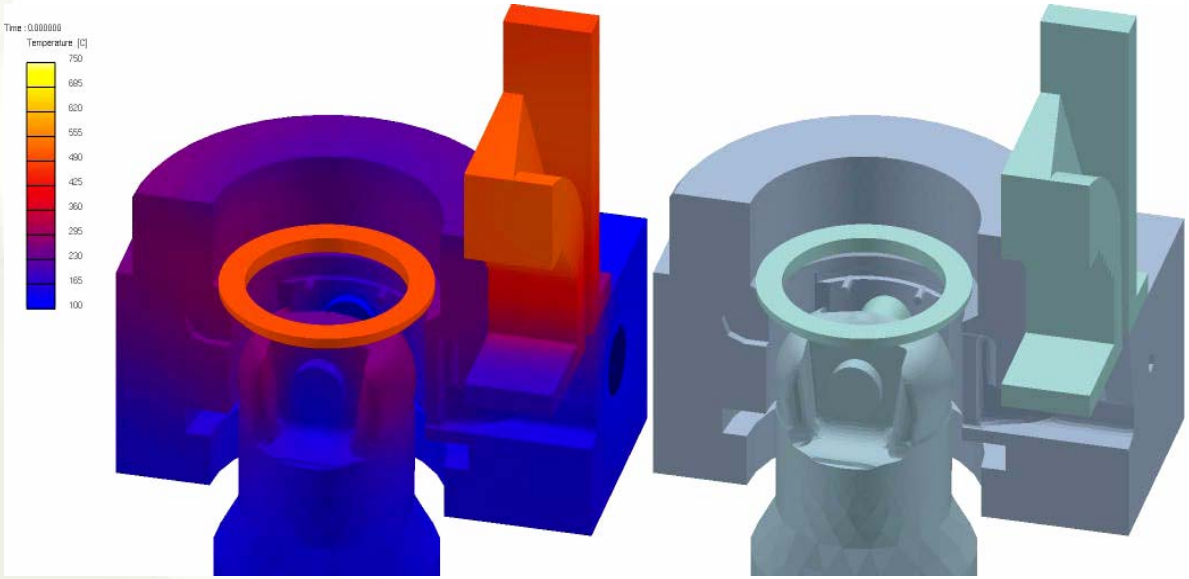
Outline

- Current Grid security issues
- Customized Image Creation
- Virtualization within the D-Grid
- Xen Grid Engine

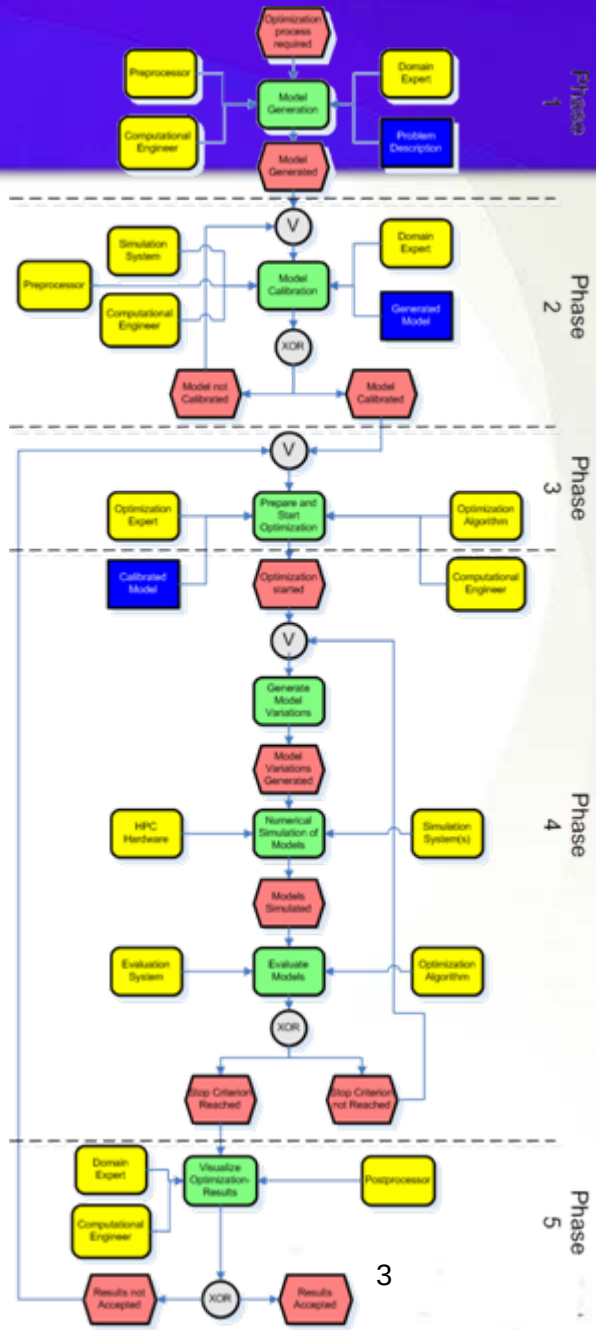
Sample Application (InGrid)

Metal Casting:

Numerical simulations are performed to substitute the expensive and time-consuming building processes for physical tools and prototypes

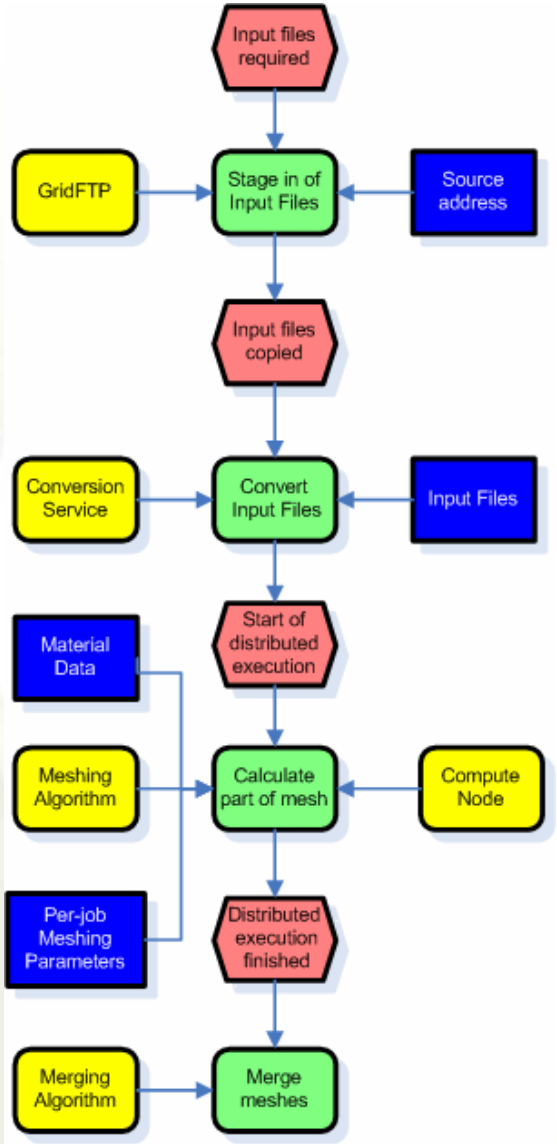


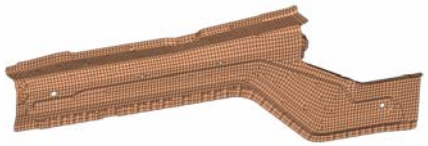
(Simulation of a motor piston)

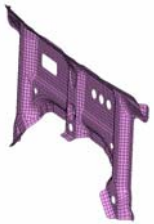


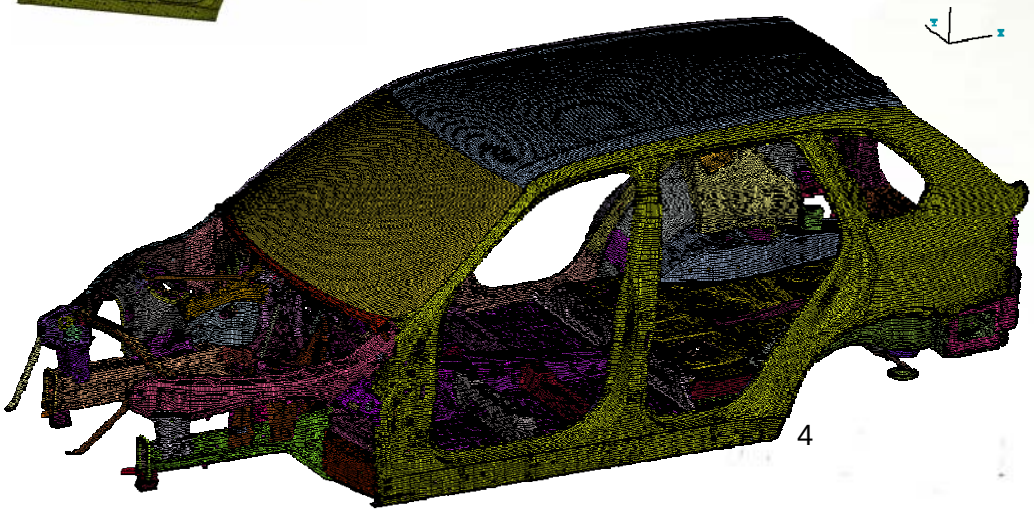
Sample Application (Biz2Grid)

Distributed Meshing in Computer Aided Engineering



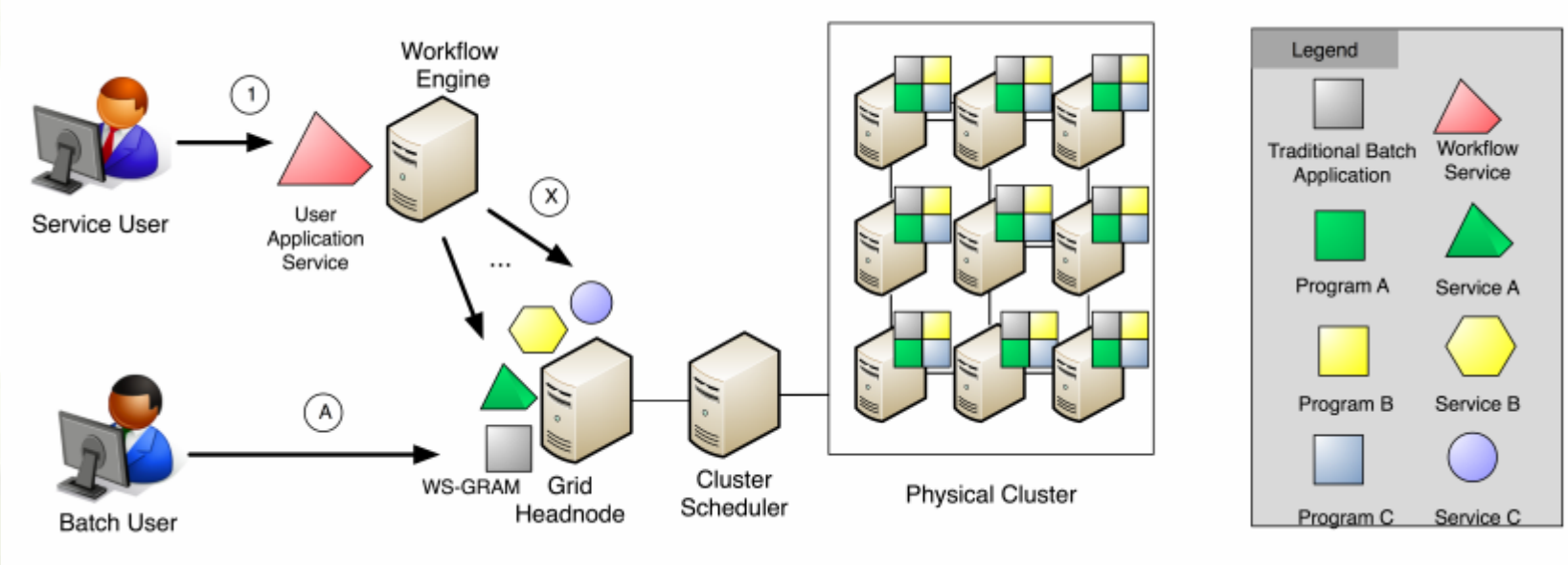






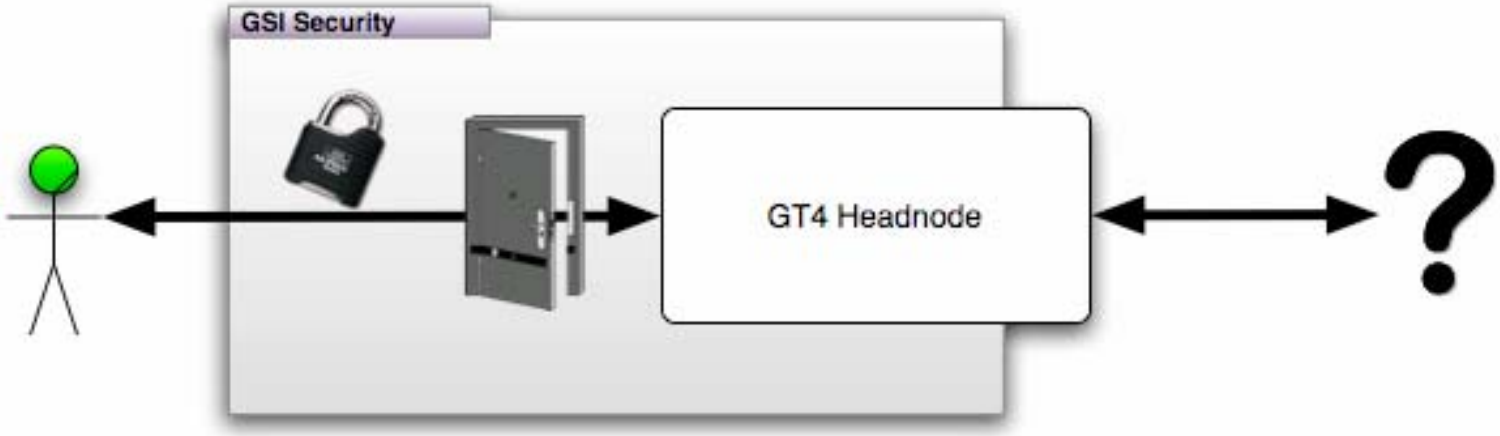
Services vs Jobs

- Install Globus on all Workernodes?



Security issues in Grid environments

- In a trusted environment, GSI covers nearly all security aspects to protect the Grid from outside threats.



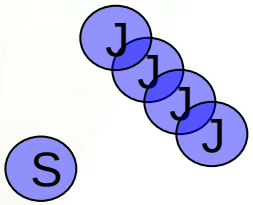
- This traditional view suffers from several security issues, especially if users may install software autonomously.

Security issues in Grid environments

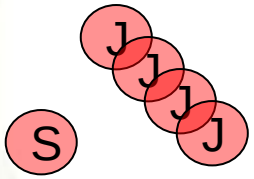
- Customers need to install their own software
  - Installation via the local admin is expensive and potentially opens the door for malicious users (rootkits, manipulated software packages, etc)
  - Manual installation way to complex for most users (GridFTP, GSIssh or GRAM remote Make)
- Different customers work on the same resources
  - Disclosure of sensitive data is possible
- Meta-Data information can be disclosed
  - Information about the used software can be gained
  - Workflow of other users can be traced
- These issues prevent commercial adoption of shared Grid technologies

Traditional Grid vs. virtualized Grid

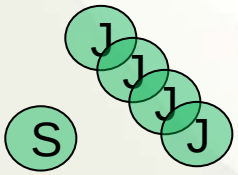
User A



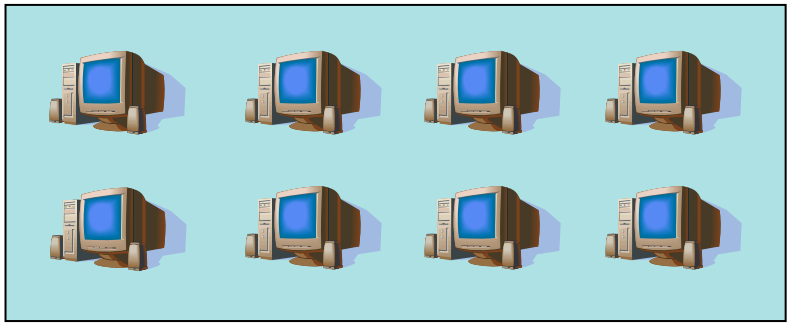
User M



User B



Traditional Grid Resources



Traditional Grid vs. virtualized Grid

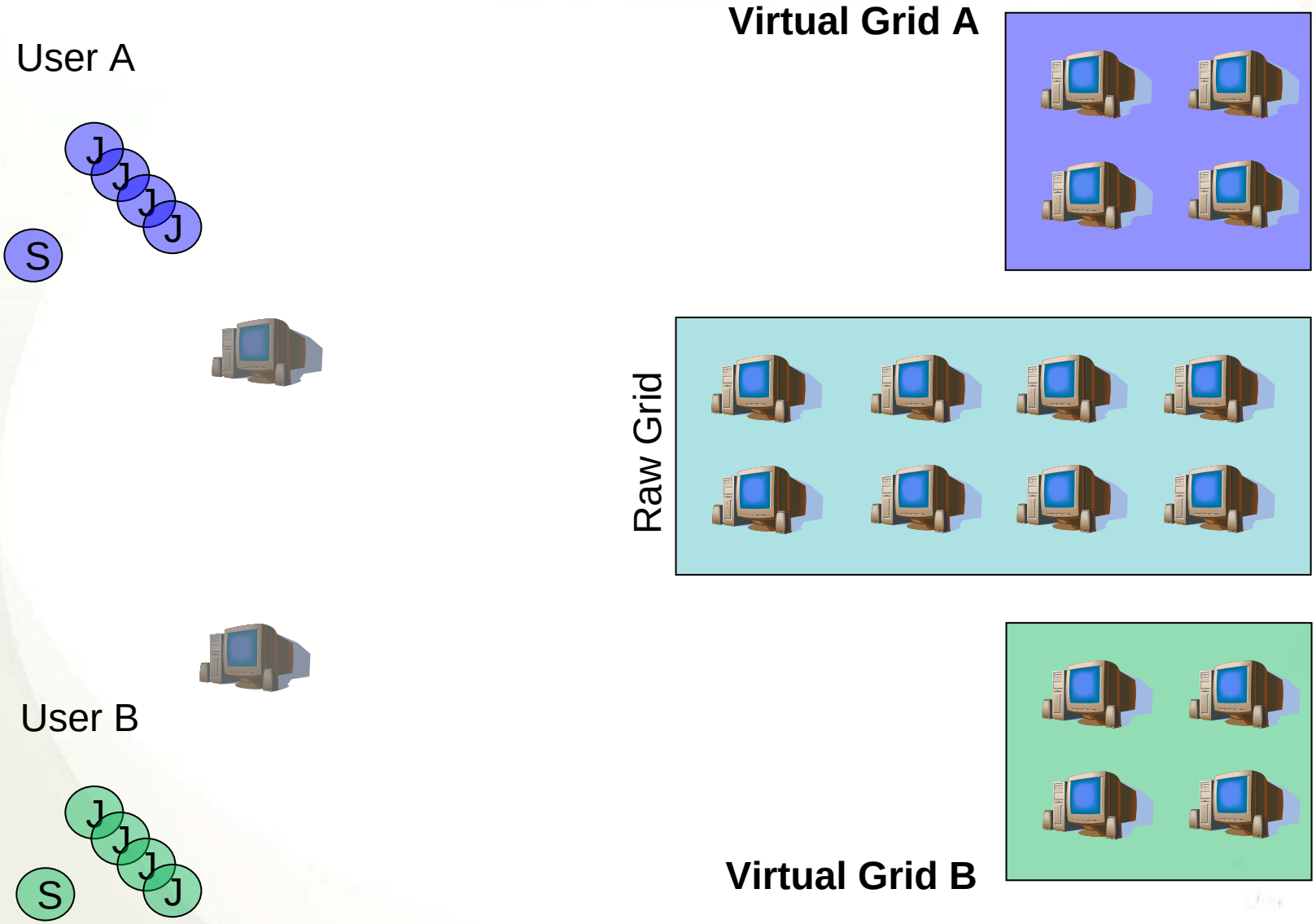
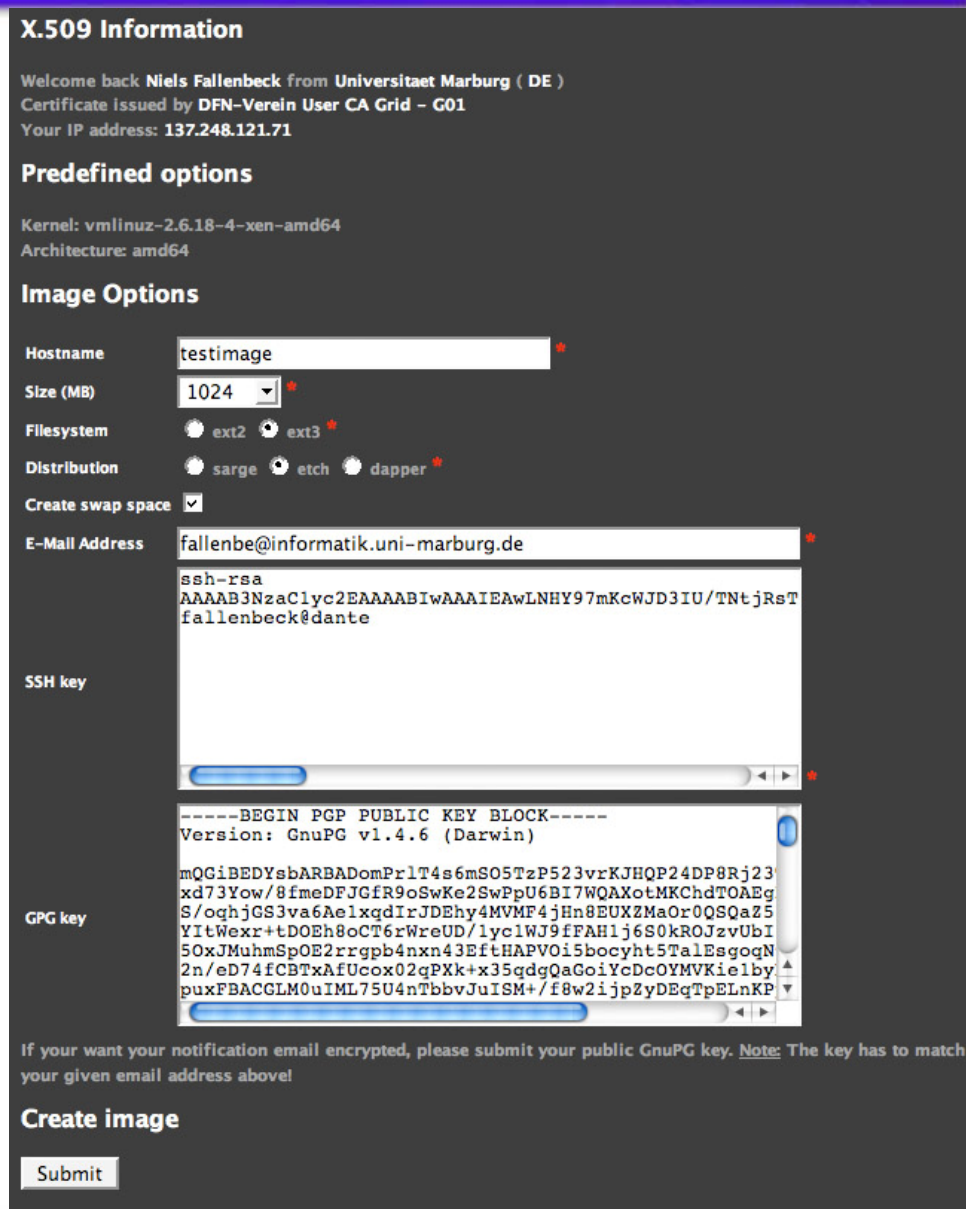


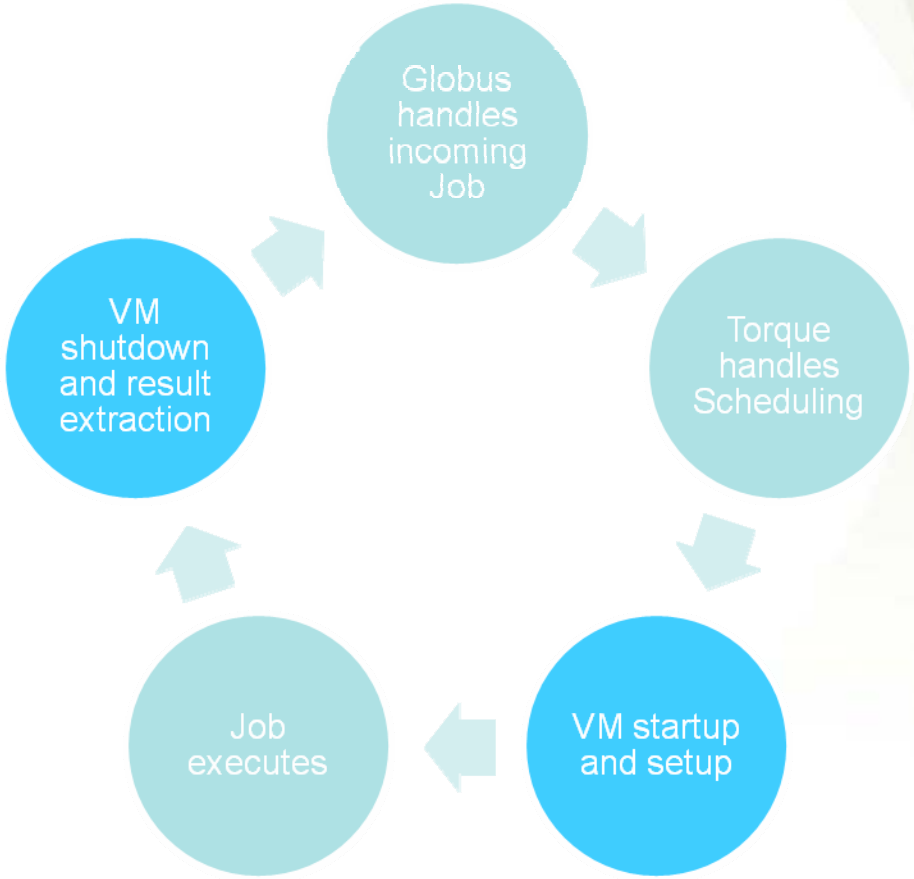
Image Creation Station (ICS)

- The ICS eases the installation of 3rd party software (root privileges no problem)
- A user can log in to the VM to install commercial software before the VM is used for job execution
- After one VM is installed, the remaining VM are cloned
- A malicious user cannot compromise the system



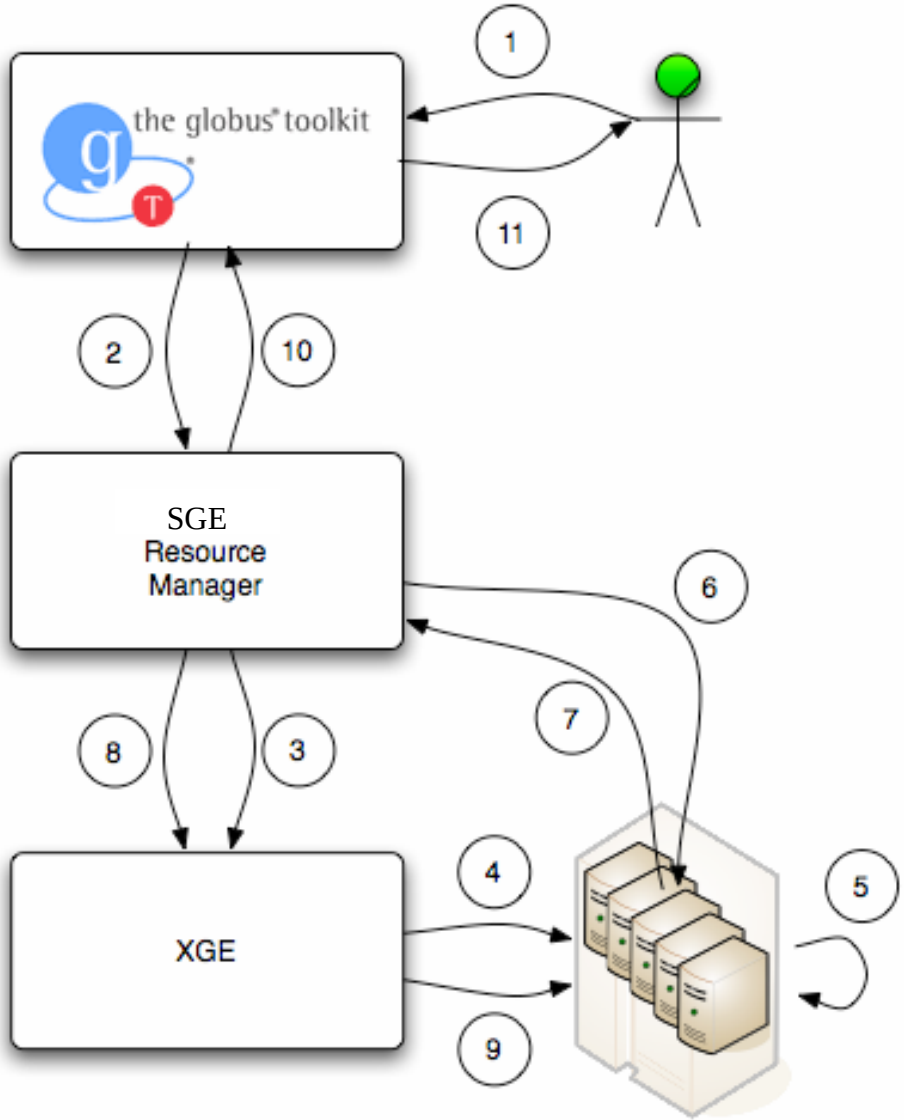
Virtualization within the D-Grid

- An incoming Job (e.g. via GRAM) is handled by Globus
- Globus passes the job to the cluster scheduler, (e.g.SGE).
- The corresponding number of user VMs boot up and are configured
- The Job is executed inside a VM
- Cluster scheduler collects all results and the VMs are shut down

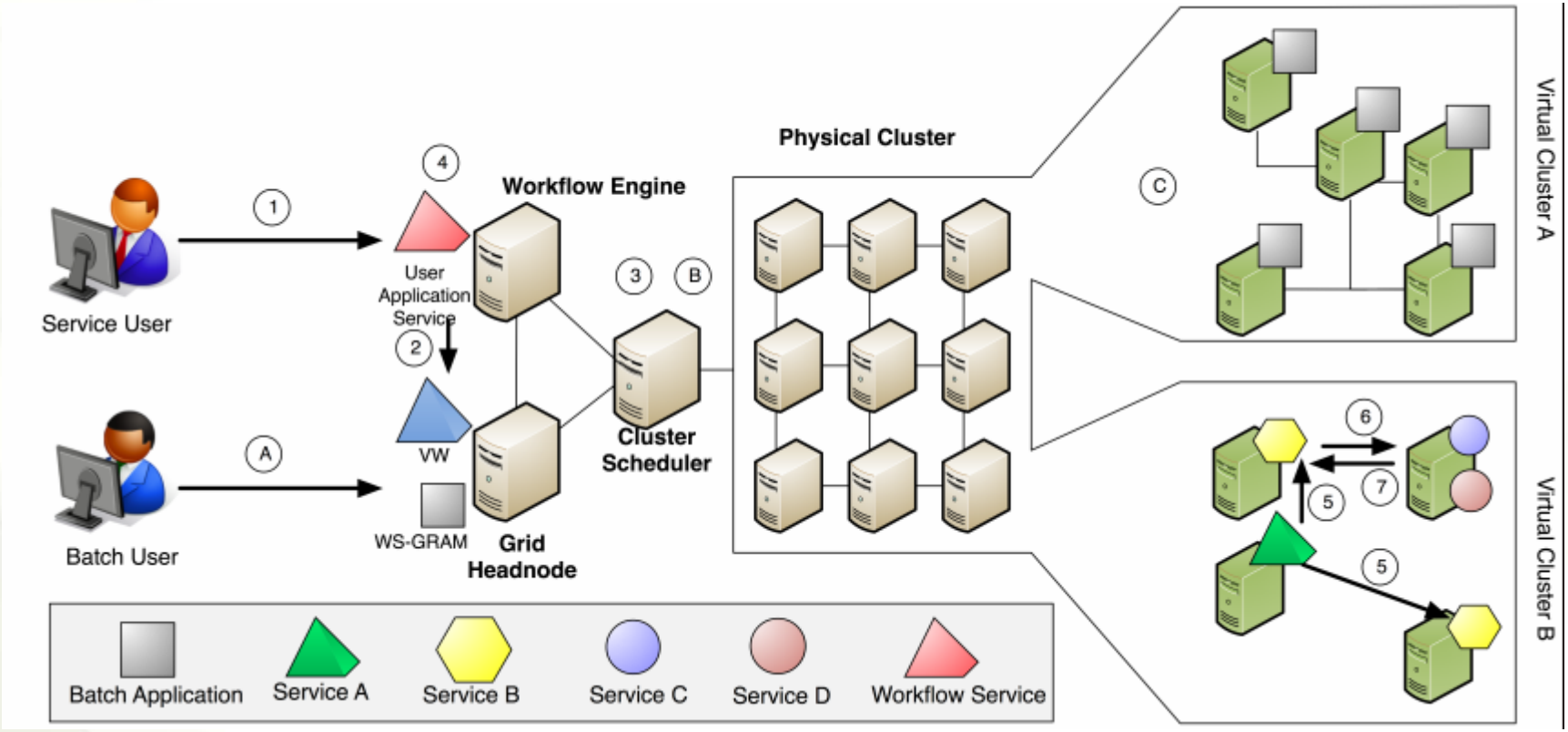


Xen Grid Engine (XGE)

- Virtualization Management Prototype Software developed at the University of Marburg
- Transparently coupled to the cluster scheduler (currently Sun Grid Engine)
- Minimally invasive approach is transparent for Grid middleware and users.
- Custer scheduler features are automatically utilized (e.g. Backfilling, advanced reservation, etc.)



Services & Jobs



Demo

- Video 1) Image Creation
- Video 2) Job Execution

Roadmap

Marburg Grid Site:

- ICS - available now
- XGE - 8 VMs available now
- Secure Workflow Engine - available now
- XGE - full installation coming shortly

Installation packages:

- Secure Workflow Engine - May 2008
- ICS & XGE - Summer 2008

Questions?

- Thank you for your attention
- Contact:
  - Matthew Smith, Niels Fallenbeck, Matthias Schmidt
  - {**matthew,fallenbe,schmidtm**}**@informatik.uni-marburg.de**

inGRID

Philipps Universität Marburg

DGI

MediGRID

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung